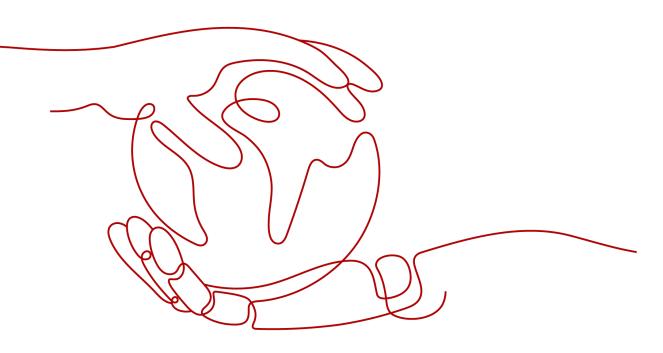
SecMaster

User Guide

 Issue
 10

 Date
 2024-03-28





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

NUAWEI 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 Authorizing SecMaster	1
2 Buying SecMaster	5
2.1 Buying the Standard Edition	5
2.2 Buying the Professional Edition	8
2.3 Upgrading the Service Edition	
2.4 Purchasing Value-Added Packages	16
2.5 Increasing the Quota	19
2.6 Unsubscribing from SecMaster	
3 Security Overview	23
3.1 Overview	23
3.2 Security Score	
4 Workspaces	
4.1 Workspace Overview	
4.2 Creating a Workspace	
4.3 Managing Workspaces	
4.3.1 Viewing Workspace Details	
4.3.2 Editing a Workspace	
4.3.3 Managing Workspace Tags	
4.3.4 Deleting a Workspace	
4.4 Workspace Agencies	39
4.4.1 Overview	39
4.4.2 Creating an Agency View	40
4.4.3 Creating an Agency	42
4.4.4 Authorizing an Agency	
4.4.5 Managing Agencies	45
5 Viewing Purchased Resources	51
6 Security Governance	52
6.1 Overview	
6.2 Security Compliance Pack Description	53
6.3 Procedure	57
6.4 Authorizing Service	58

6.5 Subscribing to Compliance Packs	
6.6 User Self-Assessment	
6.7 Security Compliance Overview	61
6.8 Evaluation Result	
6.9 Policy Check Result	65
6.10 Downloading a Compliance Report	
6.11 Unsubscribing from a Compliance Pack	69
7 Security Situation	70
7.1 Situation Overview	70
7.2 Large Screen	
7.2.1 Overall Situation Screen	
7.2.2 Monitoring Statistics Screen	
7.2.3 Asset Security Screen	
7.2.4 Threat Situation Screen	
7.2.5 Vulnerable Assets Screen	
7.3 Reports	110
7.3.1 Creating and Copying a Security Report	
7.3.2 Viewing a Security Report	
7.3.3 Downloading a Security Report	
7.3.4 Managing Security Reports	
7.4 Task Center	
7.4.1 Viewing To-Do Tasks	
7.4.2 Handling a To-Do Task	
7.4.3 Viewing Completed Tasks	128
8 Resource Manager	
8.1 Overview	130
8.2 Configuring Resource Subscription	131
8.3 Viewing Resource Information	132
8.4 Importing and Exporting Assets	
8.5 Editing and Deleting Resources	
9 Risk Prevention	138
9.1 Baseline Inspection	
9.1.1 Baseline Inspection Overview	
9.1.2 Creating a Custom Baseline Check Plan	
9.1.3 Starting an Immediate Baseline Check	
9.1.4 Handling Manual Check Items	
9.1.5 Viewing Baseline Inspection Results	144
9.1.6 Handling Baseline Inspection Results	
9.2 Vulnerability Management	
9.2.1 Overview	
9.2.2 Viewing Vulnerability Details	

9.2.3 Fixing Vulnerabilities	159
9.2.4 Importing and Exporting Vulnerabilities	
9.2.5 Ignoring and Unignoring a Vulnerability	
9.3 Viewing/Exporting Emergency Vulnerability Notices	
9.4 Policy Management	
9.4.1 Overview	
9.4.2 Viewing Defense Policies	
9.4.3 Configuring Defense Policies	
9.4.4 Adding or Editing an Emergency Policy	
9.4.5 Viewing Emergency Policies	176
9.4.6 Deleting an Emergency Policy	177
9.4.7 Blocking or Canceling Blocking of an IP Address or IP Address Range	178
10 Threat Operations	181
10.1 Incident Management	
10.1.1 Viewing Incidents	
10.1.2 Adding or Editing an Incident	183
10.1.3 Importing and Exporting Incidents	
10.1.4 Closing or Deleting Incidents	
10.2 Alert Management	190
10.2.1 Viewing Alerts	
10.2.2 Converting an Alert to an Incident or Associating an Alert with an Incident	
10.2.3 Adding or Editing an Alert	
10.2.4 Importing and Exporting Alerts	
10.2.5 Closing or Deleting an Alert	201
10.2.6 Handling Alerts based on Suggestions	202
10.2.7 One-click Blocking or Unblocking	
10.3 Indicator Management	210
10.3.1 Adding and Editing an Indicator	210
10.3.2 Disabling and Deleting an Indicator	
10.3.3 Importing and Exporting Intelligence Indicators	
10.3.4 Viewing Indicators	
10.4 Intelligent Modeling	218
10.4.1 Viewing Available Model Templates	219
10.4.2 Creating and Editing a Model	220
10.4.3 Viewing Available Models	
10.4.4 Managing Models	
10.5 Security Analysis	
10.5.1 Security Analysis Overview	230
10.5.2 How to Use Security Analysis	231
10.5.3 Log Fields	232
10.5.4 Configuring Indexes	276
10.5.5 Querying and Analyzing Data	278

10.5.6 Downloading Logs	
10.5.7 Query and Analysis Statements - SQL Syntax	
10.5.7.1 Basic Syntax	
10.5.7.2 Limitations and Constraints	
10.5.7.3 Query Statements	
10.5.7.4 Syntax of Analysis Statements	288
10.5.7.5 Analysis Statements - SELECT	
10.5.7.6 Analysis Statements - GROUP BY	
10.5.7.7 Analysis Statements - HAVING	292
10.5.7.8 Analysis Statements - ORDER BY	292
10.5.7.9 Analysis Statements - LIMIT	
10.5.7.10 Analysis Statements - Functions	293
10.5.7.11 Analysis Statements - Aggregate Functions	
10.5.8 Quick Query	299
10.5.9 Quickly Adding a Log Alarm Model	
10.5.10 Charts	304
10.5.10.1 Overview	
10.5.10.2 Tables	304
10.5.10.3 Line Charts	306
10.5.10.4 Bar Charts	
10.5.10.5 Pie Charts	
10.5.11 Managing Data Spaces	313
10.5.11.1 Creating a Data Space	313
10.5.11.2 Viewing Data Space Details	315
10.5.11.3 Editing a Data Space	316
10.5.11.4 Deleting a Data Space	317
10.5.12 Managing Pipelines	318
10.5.12.1 Creating a Pipeline	318
10.5.12.2 Viewing Pipeline Details	320
10.5.12.3 Editing a Pipeline	322
10.5.12.4 Deleting a Pipeline	324
10.6 Data Consumption	
10.7 Data Delivery	
10.7.1 Creating a Data Delivery	
10.7.2 Data Delivery Authorization	331
10.7.3 Checking the Data Delivery Status	
10.7.4 Managing Data Delivery	335
10.7.5 Delivering Logs to LTS	
10.8 Data Monitoring	
11 Security Orchestration	
11.1 Security Orchestration Overview	
11.2 Built-in Playbooks and Workflows	

11.3 Security Orchestration Process	
11.4 (Optional) Configuring and Enabling a Workflow	
11.5 (Optional) Configuring and Enabling a Playbook	
11.6 Operation Object Management	
11.6.1 Data Class	
11.6.1.1 Viewing Data Classes	
11.6.2 Type Management	
11.6.2.1 Managing Alert Types	
11.6.2.2 Managing Incident Types	
11.6.2.3 Viewing Threat Intelligence Types	
11.6.2.4 Managing Vulnerability Types	
11.6.2.5 Viewing Custom Types	
11.6.3 Classification & Mapping	
11.6.3.1 Viewing Categorical Mappings	
11.6.3.2 Creating, Copying, and Editing a Categorical Mapping	
11.6.3.3 Managing Categorical Mappings	
11.7 Playbook Orchestration Management	
11.7.1 Playbooks	
11.7.1.1 Submitting a Playbook Version	
11.7.1.2 Reviewing a Playbook Version	
11.7.1.3 Enabling a Playbook	
11.7.1.4 Managing Playbooks	
11.7.1.5 Managing Playbook Versions	
11.7.2 Workflows	404
11.7.2.1 Reviewing a Workflow Version	
11.7.2.2 Enabling a Workflow	405
11.7.2.3 Managing Workflows	407
11.7.2.4 Managing Workflow Versions	411
11.7.3 Asset Connections	419
11.7.3.1 Adding an Asset Connection	419
11.7.3.2 Managing Asset Connections	
11.7.4 Instance Management	
11.7.4.1 Viewing Monitored Playbook Instances	
11.8 Layout Management	
11.8.1 Viewing an Existing Layout Template	426
11.8.2 View Existing Layouts	
11.9 Plug-in Management	
11.9.1 Overview	
11.9.2 Viewing Plug-in Details	429
12 Settings	431
12.1 Data Collection	
12.1.1 Data Collection Overview	

12.1.2 Collecting Data	
12.1.3 Collection Management	
12.1.3.1 Managing Connections	
12.1.3.2 Managing Parsers	443
12.1.3.3 Managing Collection Channels	450
12.1.3.4 Managing Collection Nodes	457
12.1.4 Component Management	458
12.1.4.1 Managing Collection Nodes	458
12.1.4.2 Managing Components	
12.2 Data Integration	
12.2.1 Log Access Supported by SecMaster	464
12.2.2 Access Data	
12.3 Checks	467
12.4 Customizing Directories	469
13 How to Use Playbooks	472
13.1 Overview	
13.2 Automatic Renaming of Alert Names	472
13.2.1 Overview	
13.2.2 Configuring and Enabling the Playbook	
13.2.3 Verifying the Playbook	
13.3 Attack Link Analysis Alert Notification	
13.3.1 Overview	
13.3.2 Creating and Subscribing to a Topic	481
13.3.3 Configuring and Enabling the Playbook	
13.4 Automatic Notification of High-Risk Vulnerabilities	484
13.4.1 Overview	
13.4.2 Creating and Subscribing to a Topic	485
13.4.3 Configuring an Asset Connection	487
13.4.4 Configuring and Enabling the Playbook	
13.5 Automatic Notification of High-Risk Alerts	490
13.5.1 Overview	490
13.5.2 Creating and Subscribing to a Topic	491
13.5.3 Configuring and Enabling the Playbook	
13.6 Automatic Security Blocking of WAF Attacks	493
13.6.1 Overview	
13.6.2 Configuring an Asset Connection	495
13.6.3 Configuring and Enabling the Playbook	
13.7 HSS Isolation and Killing of Malware	498
13.7.1 Overview	
13.7.2 Configuring and Enabling the Playbook	500
13.8 Real-time Notification of Critical Organization and Management Operations	
13.8.1 Overview	501

13.8.2 Enabling an Alert Model13.8.3 Creating and Subscribing to a Topic12.8.4 Configurated Enabling the Plankash	504
13.8.4 Configuring and Enabling the Playbook 14 Permissions Management	
14.1 Creating a User and Granting Permissions	
14.2 SecMaster Custom Policies	
14.3 SecMaster Permissions and Supported Actions	511
15 Key Operations Recorded by CTS	
15.1 SecMaster Operations Recorded by CTS	
15.2 Querying Real-Time Traces	514
A Change History	518

Authorizing SecMaster

Scenario

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 when you use SecMaster for the first time. The following table lists the permissions you need to assign to SecMaster.

Permission	Description	Assign To	When to Use
ECS FullAccess	All permissions for ECS	SecMaste r_Agency	Used to work with security groups to block source IP address, execute playbooks that update security groups, and to query ECSs details.
WAF FullAccess	Web Application Firewall (WAF) administrator	SecMaste r_Agency	Used to work with WAF blacklists and address groups to block malicious source IP addresses and to check websites protected with WAF for baseline settings.
SecMaster FullAccess	SecMaster administrator	SecMaste r_Agency	Used to perform operations such as alert handling.
HSS FullAccess	All permissions for HSS	SecMaste r_Agency	Used to execute playbooks related to vulnerability management and host isolation, and to obtain the HSS status from baseline checks.
EPS ReadOnlyAcce ss	Read-only permissions for EPS.	SecMaste r_Agency	Used to execute WAF-related playbooks and workflows.

Table 1-1 Agency permissions

Permission	Description	Assign To	When to Use
ECS ReadOnlyAcce ss	Read-only permissions for ECSs.	SecMaste r_Agency	Used to query the number of ECSs during subscription and obtain ECS security settings for baseline checks.
Anti-DDoS ReadOnlyAcce ss	Read-only permissions for Anti-DDoS.	SecMaste r_Agency	Used to obtain Anti-DDoS asset details for baseline checks.
IAM ReadOnlyAcce ss	Read-only permissions for IAM.	SecMaste r_Agency	Used to obtain credential information during playbook and workflow execution.
WAF Administrator	WAF administrator, who has all permissions for WAF.	SecMaste r_Agency	Used to execute WAF-related playbooks and workflows.
SMN FullAccess	All permissions for SMN.	SecMaste r_Agency	Used to send playbook execution notifications.
RDS ReadOnlyAcce ss	Read-only permissions for RDS	SecMaste r_Agency	Used to execute playbooks related to asset connections.
EIP ReadOnlyAcce ss	Read-only permissions for EIP	SecMaste r_Agency	Used to execute asset connection playbooks and obtain EIP configurations for baseline checks.
Tenant Guest	Read-only permissions for all cloud services (except IAM)	SecMaste r_Agency	Used to execute the HTTP plug-in in playbooks.
NAT ReadOnlyAcce ss	Read-only permissions for NAT Gateway.	SecMaste r_Agency	Used to obtain NAT Gateway information for resource management.
VPC FullAccess	All permissions for VPC.	SecMaste r_Agency	Used to execute asset connection playbooks and isolation workflows, and obtain VPC details for baseline checks.

Permission	Description	Assign To	When to Use
OBS OperateAcces s	Allows a user to perform the basic operations, such as viewing the bucket list, obtaining bucket metadata, listing objects in a bucket, querying bucket location, uploading objects, obtaining objects, and obtaining an object ACL.	SecMaste r_Agency	Used to execute alert playbooks and obtain OBS asset details for baseline checks.
ELB ReadOnlyAcce ss	Read-only permissions for ELB.	SecMaste r_Agency	Used to obtain ELB asset details for baseline checks.
CFW FullAccess	All permissions for CFW.	SecMaste r_Agency	Used to execute preventive playbooks.
RMS ReadOnlyAcce ss	Read-only permissions for RMS.	SecMaste r_Agency	Used by the playbooks of notifying of critical O&M operations.

Prerequisites

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

Procedure

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

Figure 1-1 Workspace page

SecMaster	Management ③				🕞 Process
Security Overview Workspaces Management Agencies	Could Workspace $\label{eq:states} \overline{\nabla} \mbox{ Inter a same and layered for same.}$				C
Purchased Resources Security Governance(beta)	Connect accord 0 #Met22d \$648316 Region Projecting ************************************	Incidents 0	♥ Vulner 0 ⊜ Securit	• Alerts 1	C ি⊗ indicat 0 Playbo 9

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

is operation grants the following permissions to SecMaster so that you cMaster:	ı can use
ope of authority Tenant	
Select All	
CS ReadOnlyAccess Set lenant resource information in ECS ead-only permissions for Elastic Cloud Server	×
AM ReadOnlyAccess et Identity and Access Management Service info ead-only permissions for Identity and Access Management Service	×
BS OperateAccess Set Object Storage Service info perate-access permissions for Object Storage Service	×
ISS FullAccess Set Host Security Service info úll-access permissions for Host Security Service	×
enant Guest Set Cloud Service compliance info enant Guest (Exclude IAM)	×
IP Read/OnlyAccess Jet EIP Service info lead-only permissions for all EIP resources	Y
NDS ReadOnlyAccess tet Relational Database Service info ead-only permissions for Relational Database Service	×
VAF FullAccess Set WAF Service info Il permissions of WAF Service	×
IMN FullAccess ef Simple Message Notification Service info ull permissions for the Simple Message Notification Service	×
EW FullAccess bet CPW Service info ull permissions for the CFW Service	Y
/PC ReadOnlyAccess Set VPC Service Info The read-only permissions to all VPC resources, which can be used for statistics ar	nd survey

Figure 1-2 Authorizing for SecMaster

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

----End

2 Buying SecMaster

2.1 Buying the Standard Edition

Scenario

This section walks you through on how to buy SecMaster of the standard edition on a yearly/monthly basis.

D NOTE

During the purchase, if you are stuck due to insufficient permission, refer to **Assigning Permissions**.

Edition Description

SecMaster provides three editions: basic, standard, and professional. For details about function differences between the editions, see **Edition Differences**.

Edition	Billing Mode	Description
Basic	Yearly/Monthly (Free)	Allows you to know your security situation.
Standard	Yearly/Monthly	 Provides the security situation information and DJCP compliance. Provides plus features, such as Large Screen, Intelligent Analysis, and Security Orchestration.
Professional	 Pay-per-use billing Yearly/Monthly billing 	 Provides check on operation risks and regulation compliance. Provides plus features, such as Large Screen, Intelligent Analysis, and Security Orchestration.

Table 2-1 SecMaster editions

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** On the **Security Overview** page, click **Buy SecMaster** in the upper right corner.
- Step 4 (Optional) You need to perform access authorization before you purchase SecMaster for the first time. On the Access Authorization panel displayed, select Consent to Authorization and click Submit.
- **Step 5** On the **Buy SecMaster** page, configure SecMaster parameters.

Figure 2-1 Buying the standard edition

•					
	Specifications		Basic	Standard	Professional
Features		Understa	ind the security situation	Meet security posture and graded protection compliance operation requirements	Meet the daily safety operation and compliance inspection requirements of the enterprise
	Security Overview	×		×	×
Situation Awareness	Security Report				~
	Emergency vulnerabilit	×		✓	~
Baseline	y notices Baseline Complianc			 Supports basic baseline checks but does not provide details about check results 	 Supports baseline inspection and provides check result details
Complianc e	e Resource			~	~
	Manager Data			✓ Free ISAP (60M/day for each quota)	✓ Free ISAP (120Miday for each quota)
ISAP	Integration Search				·
	Statistics Alert Manageme			··· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
	nt Security			··· •	~
SOC	Threat				~
	Intelligence Loophole				· · · · · · · · · · · · · · · · · · ·
Security Operations	Arrangeme nt			Free SOC (500 operations/day for each quota)	✓ Free SOC (10,000 operations/day for each quota)
Security Operations Pull Up	Arrangeme nt + (Required W	ebsite Quota: 1)		 Free SOC (500 operations/day for each quota) 	✓ Free SOC (10,000 operations/day for each quota)
Operations Pull Up a You have 0 EC Value-added packag Screen	+ Required W	n monitor all of your E		Image: Project State State </td <td></td>	
Operations Pull Up a You have 0 EC Value-added packag Screen	nt + (Required W) S5s. To ensure SA ca)e (Meeting all course	n monitor all of your E discountly operation re security operation re security operation security		herdal data instance or attacks on uprotected ECSs. the EC	S quote should be 9 or more.
Coperations Pull Up a 1 1 You have 0 EC Value-added packag Screen Overall Overall	rt + Required VI + Required VI 55%. To ensure SAcaco 55%. To ensure SAcaco Situation Buy tow 0 + GED.	n monitor all of your E d secondly operation in the second second second Preview Notes and the second	squarements of enlargement)	herdal data leature er attacks en unpreheted ECSs, the EC	S goda should be 0 or more.
Coperations Pull Up a 1 1 You have 0 EC Value-added packag Screen Overall	rt + Required V 55s. To ensure SAc ac Performance SAc ac Struction Bay now 0 + GBD.	n monitor all of your E d security operation or Preview Monitor Preview Monitor Preview Monitor Monito	aparentesis of enlargeneral and an analysis of the second	herdal data leature er attacks en unpreheted ECSs, the EC	S quote should be 9 or more.
Coperations Pull Up a 1 1 You have 0 EC Value-added packag Screen Overall	et + Required V/ Sis. To ensure SA cat Sis. To ensure SA cat Situation Situation Buy tow 0 + GED be stored for at lease Buy work	n monitor all of your E d security operation or Preview Monitor Preview Monitor Preview Monitor Monito	squarements of enlargement)	herdal data leature er attacks en unpreheted ECSs, the EC	S goda should be 0 or more.
Particione Part Los a	et r et et et et	n montor al of your E f security operation m Presiev X 100 days according	aparentesis of enlargeneral and an analysis of the second	Arenda data loaturge er atlante en ungreiterdet (ECSs. the EC Arenda data loaturge er atlante en ungreiterdet (ECSs. the EC Arenda data analysis capacity for the logs personal the recommended data analysis capacity for the logs personal	S goda should be 0 or more.
Particione Part Los a	et + Required V/ Sis. To ensure SA cat Sis. To ensure SA cat Situation Situation Buy tow 0 + GED be stored for at lease Buy work	n montor al of your E f security operation m Presiev X 100 days according	eptements of entryments ontoring Statistics i	Arenda data loaturge er atlante en ungreiterdet (ECSs. the EC Arenda data loaturge er atlante en ungreiterdet (ECSs. the EC Arenda data analysis capacity for the logs personal the recommended data analysis capacity for the logs personal	S goda should be 0 or more.

Table 2-2 Parameters for	purchasing	the standard edition
--------------------------	------------	----------------------

Parameter	Description	
Billing Mode	Select Yearly/Monthly.	
Region	Select your region.	
Edition	Select the standard edition.	

Parameter	Description
ECS Quota	The ECS quota indicates the maximum number of ECSs that can be protected.
	The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.
	NOTE
	The maximum ECS quota cannot exceed 10,000.
	• If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. Increase the ECS quota timely when the number of host assets increases.
Value-added Package	Determine whether to enable or purchase the Large Screen, ISAP, or SOC function. If you want to purchase the value-added package, set the purchase quantity as required.
	You can purchase the value-added package together with the standard edition or solely purchase a value-added package later. For details, see Purchasing Value-Added Packages .
Tag	TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.
Required Duration	Set Required Duration . The required duration can be from one month to three years.
	NOTE The Auto-renew option enables the system to renew your service by the purchased period when the service is about to expire.

- **Step 6** Confirm the product details and click **Next**.
- **Step 7** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 8** On the payment page, select a payment method and complete the payment.

----End

Verification

After successful payment, you can view the purchased SecMaster version in the upper right corner of the **Purchased Resources** page on the management console.

Related Operations

- To change the asset quota, choose **Purchased Resources**, select the target region, and click **Increase Quota**. For details, see **Increasing the Quota**.
- If your yearly/monthly edition is about to expire or has expired, you can choose **Purchased Resources**, select the target region, and click **Renew** to make a renewal. For details, see **Renewing Your Subscriptions**.

 If you no longer use the SecMaster service, choose Security Overview, hover your cursor over the edition information in the upper right corner of the page, and click Unsubscribe or Cancel to unsubscribe from the service. For details, see Unsubscribing from SecMaster.

2.2 Buying the Professional Edition

Scenario

This section walks you through on how to buy SecMaster of the professional edition on a yearly/monthly or pay-per-use basis.

NOTE

During the purchase, if you are stuck due to insufficient permission, refer to Assigning Permissions.

Edition Description

SecMaster provides three editions: basic, standard, and professional. For details about function differences between the editions, see **Edition Differences**.

Edition	Billing Mode	Description
Basic	Yearly/Monthly (Free)	Allows you to know your security situation.
Standard	Yearly/Monthly	 Provides the security situation information and DJCP compliance.
		 Provides plus features, such as Large Screen, Intelligent Analysis, and Security Orchestration.
Professional	Pay-per-use billing	 Provides check on operation risks and regulation compliance.
	 Yearly/Monthly billing 	 Provides plus features, such as Large Screen, Intelligent Analysis, and Security Orchestration.

Table 2-3 SecMaster editions

Yearly/Monthly Billing

Step 1 Log in to the management console.

- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** On the **Security Overview** page, click **Buy SecMaster** in the upper right corner.

- **Step 4** (Optional) You need to perform access authorization before you purchase SecMaster for the first time. On the Access Authorization page that is displayed, select **Consent to Authorization** and click **Submit**.
- **Step 5** On the **Buy SecMaster** page, configure SecMaster parameters.

Figure 2-2 Purchasing SecMaster professional edition in yearly/monthly mode

	Specifications	Bask	Standard Meet security posture and graded protection compliance	Professional Next the daily contribution and compliance
Featur		Understand the security situation	operation requirements	Meet the daily safety operation and compliance inspection requirements of the enterprise
	Security Overview	×	×	×
Situation	ss Report			×
	Emergency vulnerabilit	*	~	~
Baseline	y notices Baseline Complianc		 Supports basic baseline checks but does not provide details about check results 	 Supports baseline inspection and provides check result details
Complia	Resource			
	Manager Data		✓ Free ISAP (60M/day for each quota)	✓ Free ISAP (120M/day for each quota)
ISAP	Integration			
	Statistics Alert			
	Manageme nt			· · · · · · · · · · · · · · · · · · ·
soc	Security Incident		·····	*
	Threat Intelligence			*
	Loophole			×
	Arrangeme nt + (Required W		Free SOC (500 operationskidsy for each got(a) definitial data leakage or attacks on unprotected ECSs, the ECS	Free SGC (18,000 operationality for each goods)
Coperatis Pul Up Outota – 1 You have 0 Vou have 0 Vou have 0 Xage Screen	Arrangeme nt + Required W ECSs. To ensure SA ca		exolo	dhora)
Coperatis Pul Up Outota – 1 You have 0 Vou have 0 Vou have 0 Xage Screen	Arrangeme nt + Required W ECSs. To ensure SA ca age [Meeting all-nound	nonitor al el your ECBs and defect ad prevent focaril y operation requirements al colorpores;	exolo	
Operatis Pull Up You have 0 Volue-added pack	Arrangeme nt + Required W ECCs. To ensure SA ca age Weeting at nour all Situation	n monitor al di yace ECDs and detect and prevent tescard; genration mysiemente (richtegranes)	exolo	
Operation Pult Up Value added pack Value added pack	Arrangeme at Arrangeme Arrange	n molec al el year ECS and delect ad prove (society operation ingenerent) el follogrand Frecher Provino Deur Deur Deur Deur Deur Deur Deur Deur	4 potential data least-oper or attacks on urgentected ECSs. The ECS	
Queratic Pult Up Juota Value added pack Value added pack Value added pack args Screen Over Cover	Arrangeme at Arrangeme Arrange	n molec al el year ECS and delect ad prove (society operation ingenerent) el follogrand Frecher Provino Deur Deur Deur Deur Deur Deur Deur Deur	4 potential data least-oper or attacks on urgentected ECSs. The ECS	could be 0 or more.

Table 2-4 Parameters for purchasing the professional edition in yearly/monthlymode

Parameter	Description	
Billing Mode	Select Yearly/Monthly.	
Region	Select your region.	
Edition	Select Professional.	
ECS Quota	The ECS quota indicates the maximum number of ECSs that can be protected.	
	The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.	
	NOTE	
	• The maximum ECS quota cannot exceed 10,000.	
	 If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result i security risks, such as data leakage. To prevent this, increase the quota upon an increase of the host asset quantity. 	

Parameter	Description
Value-added package	Determine whether to enable or purchase the Large Screen, ISAP, or SOC function. If you want to purchase the value-added package, set the purchase quantity as required.
	You can purchase the value-added package together with the standard edition or solely purchase a value-added package later. For details, see Purchasing Value-Added Packages .
Tag	TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.
Required Duration	Specify Required Duration . You can select a required duration in the range from one month to three years. NOTE The Auto-renew option enables the system to renew your service by the required duration when the service is about to expire.

- **Step 6** Confirm the product details and click **Next**.
- **Step 7** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 8** On the payment page, select a payment method and complete the payment.

----End

Pay-per-Use Billing

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- Step 3 On the Security Overview page, click Buy SecMaster in the upper right corner.
- Step 4 (Optional) You need to perform access authorization before you purchase SecMaster for the first time. On the Access Authorization page that is displayed, select Consent to Authorization and click Submit.
- **Step 5** On the **Buy SecMaster** page, configure SecMaster parameters.

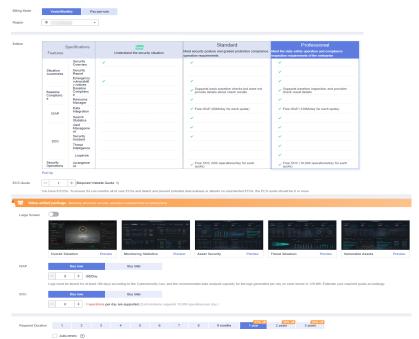


Figure 2-3 Purchasing SecMaster professional edition in yearly/monthly mode

Table 2-5 Parameters for purchasing the SecMaster professional edition in payper-use mode

Parameter	Description	
Billing Mode	Select Pay-per-use . From the time when the service is enabled to the time when the service ends, you are billed for the actual duration by the hour.	
Region	Select your region.	
Edition	Select Professional .	
ECS Quota	The ECS quota indicates the maximum number of ECSs that can be protected.	
	The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.	
	NOTE	
	The maximum ECS quota cannot exceed 10,000.	
	 If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. To prevent this, increase the ECS quota upon an increase of the host asset quantity. 	
Value-added package	Determine whether to enable or purchase the Large Screen , ISAP , or SOC function.	
	You can purchase the value-added package together with the standard edition or solely purchase a value-added package later. For details, see Purchasing Value-Added Packages .	

Parameter	Description
Labels	TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.

- **Step 6** Confirm the product details and click **Next**.
- **Step 7** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 8** On the payment page, select a payment method and complete the payment.

----End

Effective Conditions

After the payment is successful, you can view the purchased SecMaster version on the **Purchased Resources** page on the management console.

Related Operations

- To change the asset quota, choose **Purchased Resources**, select the target region, and click **Increase Quota**. For details, see **Increasing the Quota**.
- To enable the value-added package function, choose **Purchased Resources** and click **Buy Value-add Pack** in the upper right corner. For details, see **Purchasing Value-Added Packages**.
- If your yearly/monthly edition is about to expire or has expired, you can choose Purchased Resources, select the target region, and click Renew to make a renewal. For details, see Renewing Your Subscriptions.
- If you no longer need the asset quota or value-added package, choose Security Overview, hover your cursor over the edition information in the upper right corner of the page, and click Unsubscribe or Cancel to unsubscribe from the service. For details, see Unsubscribing from SecMaster.

2.3 Upgrading the Service Edition

The upgrade method includes version upgrade and quota increase. Select a method as needed.

Scenario	Description
Upgrade the edition	• Upgrading Basic to Standard or Professional : If you have enabled the basic edition, you can upgrade to the standard or professional edition.
	• Upgrading Standard to Professional: If you have purchased the standard edition, you can upgrade to the professional edition.

Table 2-6 Edition upgrade

Scenario	Description	
Increase the quota	You can increase the quota. For details, see Increasing the Quota .	
Upgrade the edition and increase the quota	Upgrading Standard to Professional : If you have purchased the standard edition, you can upgrade it to the professional edition and increase its quota at the same time.	
CAUTION An edition cannot be downgraded after the upgrade.		

NOTE

During the purchase, if you are stuck due to insufficient permission, refer to Assigning Permissions.

Edition Description

SecMaster provides three editions: basic, standard, and professional. For details about function differences between the editions, see **Edition Differences**.

Edition	Billing Mode	Description	
Basic	Yearly/Monthly (Free)	Allows you to know your security situation.	
Standard	Yearly/Monthly	 Provides the security situation information and DJCP compliance. 	
		 Provides plus features, such as Large Screen, Intelligent Analysis, and Security Orchestration. 	
Professional	 Pay-per-use billing 	 Provides check on operation risks and regulation compliance. 	
	 Yearly/Monthly billing 	 Provides plus features, such as Large Screen, Intelligent Analysis, and Security Orchestration. 	

Table 2-7 SecMaster editions

Upgrading Basic to Standard or Professional

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Purchased Resources**. Locate the target region and click **Upgrade**.

Figure 2-4 Upgrading the basic edition



- Step 4 On the Buy SecMaster page, configure SecMaster parameters.
 - 1. **Current Configuration**: configuration information of the purchased SecMaster version
 - 2. Upgrade Method: By default, Version Upgrade is selected.
 - 3. Edition: Select Standard or Professional.

Figure 2-5 Selecting an edition

Edition	S Features	pecifications	Basic Understand the security situation		Professional Meet the daily safety operation and compliance inspection requirements of the enterprise
		Security Overview	✓	*	✓
	Situation Awareness	Security Report			✓ Security Daily
		Industry Information	 Obtain information on hot security vulnerabilities in the industry 	✓	4
	Baseline Complianc	Baseline Complianc e		 It only supports checks of Classified Security 2.0 and cloud security checks 	✓
	e	Resource Manager		<	∢
	1015	Data Integration		✓ Free ISAP (60M/day for each quota)	✓ Free ISAP (120M/day for each quota)
	ISAP	Search Statistics		✓	✓
	SOC	Alert Manageme nt		×	✓
		Security Incident		<	∢
		Threat Intelligence			✓
		Loophole			✓
	Security Operations	Arrangeme nt		✓ Free SOC (500 operations/day for each quota)	 Free SOC (10,000 operations/day for each quota)
	Pull Up				
ECS Quota - 27 + Required Website Quota: 25)					
	You have 27 EC	Ss. To ensure SA c	an monitor all of your ECSs and detect and prevent pote	ential data leakage or attacks on unprotected ECSs, the ECS	quota should be 27 or more.
	(The maximum ECS quola you can buy: 270)				

- 4. **Tag**: TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.
- **Step 5** Confirm the product details and click **Next**.
- **Step 6** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 7** On the payment page, select a payment method and complete the payment.

----End

Upgrading Standard to Professional

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

- **Step 3** In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, locate the region where you want to upgrade and click **Upgrade**.
- **Step 4** On the **Buy SecMaster** page, configure SecMaster parameters.
 - 1. **Current Configuration**: version information of the current SecMaster before you increase the quota.
 - 2. Upgrade Method: Select Version Upgrade. You can also select Increase Quota.
 - 3. **Optional Version**: Select **Professional** to upgrade to the professional edition.

tion	S	pecifications	Basic	Standard	Professional
	Features		Understand the security situation	Meet security posture and graded protection compliance operation requirements	Meet the daily safety operation and compliance inspection requirements of the enterprise
		Security Overview	✓	×	×
	Situation Awareness	Security Report			✓ Security Daily
		Industry Information	 Obtain information on hot security vulnerabilities in the industry 	✓	*
	Baseline Complianc	Baseline Complianc e		 It only supports checks of Classified Security 2.0 and cloud security checks 	~
	e	Resource Manager		*	*
		Data Integration		✓ Only supports security service alerts	 Support cloud service security logs and alarms
	ISAP	Search Statistics		✓	✓
		Alert Manageme nt		×	×
	soc	Security Incident		*	*
	000	Threat Intelligence			✓
		Loophole			*
	Security Operations	Arrangeme nt			✓ SOAR
	Pull Up			·	
Quota	- 11	+ (Required W	ebsite Quota: 0)		
	You have 0 ECSs	. To ensure SA ca	n monitor all of your ECSs and detect and prevent p	otential data leakage or attacks on unprotected ECSs, the ECS	quota should be 0 or more.
	(The maximum E	CS quota you can	buy: 100)		

Figure 2-6 Selecting the professional edition

4. (Optional) **ECS Quota**: Configure the ECS quota.

Table 2-8 ECS quota description

Parameter	Description	
ECS Quota	The maximum number of ECSs that require protection from SecMaster.	
	The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.	
	NOTE	
	 The maximum ECS quota cannot exceed 10,000. 	
	 If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. To prevent this, increase the ECS quota upon an increase of the host asset quantity. 	

5. **Tag**: TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.

Step 5 Confirm the product details and click **Next**.

- **Step 6** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 7** On the payment page, select a payment method and complete the payment.

----End

Effective Conditions

After completing your payment, you can see your SecMaster edition in the upper right corner of the management console.

Related Operations

- To change the asset quota, choose **Purchased Resources**, select the target region, and click **Increase Quota**. For details, see **Increasing the Quota**.
- To enable the value-added package function, choose **Purchased Resources** and click **Buy Value-add Pack** in the upper right corner. For details, see **Purchasing Value-Added Packages**.
- If your yearly/monthly edition is about to expire or has expired, you can choose **Purchased Resources**, select the target region, and click **Renew** to make a renewal. For details, see **Renewing Your Subscriptions**.
- If you no longer need the asset quota or value-added package, choose
 Security Overview, hover your cursor over the edition information in the upper right corner of the page, and click Unsubscribe or Cancel to unsubscribe from the service. For details, see Unsubscribing from SecMaster.

2.4 Purchasing Value-Added Packages

Scenario

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

NOTE

During the purchase, if you are stuck due to insufficient permission, refer to Assigning Permissions.

Limitations and Constraints

- The value-added package is an additional payment item for the standard or professional edition. To use the value-added package, you need to purchase the standard or professional edition first.
- Value-added packages can be purchased in yearly/monthly or pay-per-use mode.

Prerequisites

You have purchased the SecMaster standard edition or professional edition.

Purchasing a Yearly/Monthly Value-added Package

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, click **Buy Value-added Pack** in the upper right corner.
- **Step 4** On the purchase page, configure required parameters.
 - 1. Select a billing mode, region, and project.
 - Billing Mode: Select Yearly/Monthly.
 - **Region**: Select a region.
 - 2. Configuration: configuration information of the purchased SecMaster version
 - 3. Select functions based on your requirements.

Figure 2-7 Purchasing a value-added package

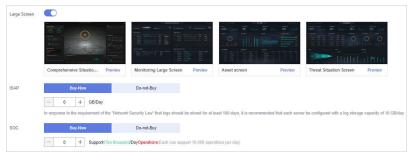


Table 2-9 Purchasing a value-added package

Feature	Buy Now	Do Not Buy
Large Screen	Toggle on the button next to Large Screen to buy the large screen function.	Retain the toggle-off status ().
ISAP	 Select Buy now. Set the amount of log volume you want to store daily. 	Select Buy later .
SOC	 Select Buy now. Set the number of daily operations allowed. 	Select Buy later .

- 4. **Tag**: TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.
- **Step 5** Set **Required Duration**. You can select the required duration from one month to three years.

The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

- **Step 6** Confirm the product details and click **Next**.
- **Step 7** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 8** On the payment page, select a payment method and complete the payment.

----End

Purchasing a Pay-per-Use Value-added Package

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, click **Buy Value-added Package** in the upper right corner.
- **Step 4** On the purchase page, configure required parameters.
 - 1. Select a billing mode, region, and project.
 - Billing mode: Select Pay-per-use.
 - **Region**: Select a region.
 - 2. Configuration: configuration information of the purchased SecMaster version
 - 3. Select functions based on your requirements.

Figure 2-8 Purchasing a value-added package

Large Screen				
	Comprehensive Situatio Preview	Monitoring Large Screen Preview	Asset screen Preview	Threat Situation Screen Preview
ISAP	Buy-Now	Do-not-Buy		
	In response to the requirement of the "Network	Security Law" that logs should be stored for at le	east 180 days, it is recommended that each serve	er be configured with a log storage capacity of 10 GB/
SOC	Buy-Now	Do-not-Buy 0.0002S /Operation	15	

Table 2-10 Pur	chasing a value-	added package
----------------	------------------	---------------

Feature	Buy Now	Buy Later
Large Screen	Toggle on the button next to Large Screen to buy the large screen function.	Retain the toggle-off status ().
ISAP	Select Buy now next to ISAP .	Select Buy later .
SOC	Select Buy now next to SOC .	Select Buy later .

- 4. **Tag**: TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.
- Step 5 Confirm the product details and click Next.
- **Step 6** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 7** On the payment page, select a payment method and complete the payment.

----End

Follow-up Operations

- If the large screen function is about to expire or has expired, click Renew to extend the validity period. For more details, see Renewing Your Subscriptions.
- If you no longer need the value-added package, go to the **Security Overview** page, hover the mouse over **Large Screen** in the upper right corner of the page, and click **Unsubscribe** or **Cancel** in the displayed pane. For details, see **Unsubscribing from SecMaster**.

2.5 Increasing the Quota

Scenario

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

NOTE

During the purchase, if you are stuck due to insufficient permission, refer to **Assigning Permissions**.

Limitations and Constraints

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

Procedure

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, locate the region where you want to add quotas and click **Increase Quota**.

Step 4 On the Buy SecMaster page, configure SecMaster parameters.

- 1. **Current Configuration**: version information of the current SecMaster before you increase the quota
- 2. Upgrade Method: Select Increase Quota.
- 3. ECS Quota: Set the ECS quota.

Figure 2-9 Increasing the quota

Upgrade Method	🗌 Version Upgrade 🛛 🗹 Increase Quota
ECS Quota	- 2 + (Required Website Cuota: 0)
	You have 2 ECSs. To ensure SA can monitor all of your ECSs and detect and prevent potential data leakage or attacks on unprotected ECSs, the ECS quota should be 2 or more.
	(The maximum ECS quota you can buy: 100)

Table 2-11 ECS quota description

Parameter	Description	
ECS Quota	The maximum number of ECSs that require protection from SecMaster.	
	The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.	
	NOTE	
	 The maximum ECS quota cannot exceed 10,000. 	
	 If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. To prevent this, increase the ECS quota upon an increase of the host asset quantity. 	

- 4. **Tag**: TMS's predefined tag function is recommended for adding the same tag to different cloud resources. You can also create tags when purchasing SecMaster.
- **Step 5** Confirm the product details and click **Next**.
- **Step 6** After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.
- **Step 7** On the payment page, select a payment method and complete the payment.

----End

2.6 Unsubscribing from SecMaster

Scenario

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

• Yearly/Monthly billing mode: a prepaid mode. You can unsubscribe from a purchased cloud service and apply for a full refund unconditionally within five

days of the purchase. Each account can request five-day unconditional full refund for 10 times in a year. Handling fees are required if you unsubscribe from a service over 5 days after it is purchased.

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

For more details about pricing and orders, go to the **Billing Center**.

NOTE

During the purchase, if you are stuck due to insufficient permission, refer to Assigning Permissions.

Limitations and Constraints

• In the standard and professional editions charged **Yearly/Monthly**, the asset quota and value-added packages need to be unsubscribed or canceled separately.

After all asset quotas (professional edition or standard edition) are unsubscribed from and the current edition is the basic edition, you can unsubscribe from value-added packages.

- In the pay-per-use professional edition, when you unsubscribe from or cancel the asset quota of the professional edition, the value-added package is also unsubscribed or canceled.
- The value-added packages cannot be used independently.

If you have subscribed to the value-added packages on your standard or professional edition, after you unsubscribe from the standard or professional edition, no data will be available for the value-added packages. So you need also cancel the value-added packages.

Unsubscribing from Yearly/Monthly Resources

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** Click **Standard** or **Professional** in the upper right corner. A window for you to manage SecMaster assets will be displayed.
- **Step 4** In the row of the ECS quota or value-added package billed on a yearly/monthly basis, click **Unsubscribe**.
- **Step 5** Locate the row that contains the target instance, and click **Unsubscribe** in the **Operation** column.
- **Step 6** Confirm the information about the resource to be unsubscribed, select the unsubscription reason, and select **I understand a handling fee will be charged for this unsubscription.**
- Step 7 Click Confirm.

Go to the edition management window and verify that the subscription to the ECS quota that is billed yearly/monthly is canceled.

----End

Canceling Pay-per-Use SecMaster Resources

- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** Click **Professional** in the upper right corner. The edition management window is displayed.
- **Step 4** In the row of the SecMaster edition purchased in pay-per-use billing mode, click **Cancel** to release the purchased SecMaster resources.

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

----End

Unsubscribing from a Plus Features

- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** Click **Standard** or **Professional** in the upper right corner. A window for you to manage SecMaster assets will be displayed.
- Step 4 Unsubscribe a Plus Feature
 - For a pay-per-use value-added package:

Click **Cancel** to release the pay-per-use asset quota. Go to the edition management window and verify that the subscription to resources billed on a pay-per-use basis is canceled.

- For yearly/monthly billed value-added packages:
 - a. Click **Unsubscribe**. The **Unsubscriptions** page is displayed.
 - b. Locate the row that contains the target instance, and click **Unsubscribe** in the **Operation** column.
 - c. Confirm the information about the resource to be unsubscribed, select the unsubscription reason, and select I understand a handling fee will be charged for this unsubscription.
 - d. Click **Confirm**.

After the unsubscription is successful, go to the version management page and verify that the yearly/monthly asset quota is canceled.

----End

3 Security Overview

3.1 Overview

SecMaster works with other cloud security services to centrally display cloud security posture on the **Security Overview** page. On this page, you will learn of asset security, including security evaluation results, security monitoring results, and security trends.

Procedure

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

SecMaster	Security Overview ⑦ +3 Back To Old Console	Professional : Buy Value-add Pack Buy SecMaster
Security Overview Workspaces Purchased Resources Security Governance(beta)	Security Score	Your Security Score over Time(Last 7 days) Petits 100 73 50 23 23 24 29/11 00/12 00/13 00/14 00/15 00/16
	Security Monitoring	FAQs View More
	Threat Alarms (Last 7 days) 0 Vulnerabilities 0 Abnormal Baseline Settings 21	What is SecMaster? What is SecMaster and Other Security Service?
	Critical 0 High 0 Others 0 High 0 Notium 0 Others 0 Critical 0 High 7 Others 14	What Are Data Sources of SecMaster? How Can I Update My Security Score in SecMaster?
	Top 5 Real-Time Unsafe Baseline Settings 🌑 Checking	How Can I Locate the Most Vulnerable Witry Is There Little or No Attack Data in
	Subject Level Affected Resource Number Triggered Security group inbound rules High 3 Aug 11, 2023 00:00:16 GMT+	Assets? SecMaster?
	Security group mounds rules engines a security group mounds rules engines a security group mounds rules engines and eng	Why is Attack Data in SecMaster Inconsistent Can I Use SecMaster Across Accounts? with That in WAF or HSS?

Figure 3-1 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 Secu	urity Ov	/erview
----------	---------	----------	---------

Paramete r	Statis tical Perio d	Update Frequency	Description
Security Score	Real- time	 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.
Vulnerabil ities	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 of your workloads on the cloud based on the SecMaster edition you are using. You can quickly understand the unprocessed risks and their threats to your assets. **Figure 3-2** shows an example.

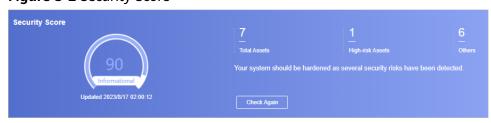


Figure 3-2 Security Score

- 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.

Figure 3-3 Security Monitoring

Security Monito	ring							
Threat Alarm	IS[Last 7 days]	1852	Vulnerabilit	ies	8	Abnormal Ba	seline Settings	6
Critical 0	High <mark>0</mark>	Others 1852	High 0	Medium 8	Others 0	Critical 0	High 1	Others 5

Parameter	Description		
Threat Alarms	This panel displays the uni- workspace of the current a quickly learn of the total n and the number of vulnera statistics are updated every	ccount for th umber of un bilities at ea	ne last 7 days . You can handled threat alerts
	Risk severity levels:		
			our workloads, and you dle the alert in a timely
			nts on your workloads, and handle the alert ir
		k, and inforn you should v	that are marked as national alerts detected view alert details and
	• To quickly view details of days, click the Threat A		
	 You can view details threat alert name, se time. 		
	 If no data is available generated for the last 	•	reat alerts are
	Figure 3-4 Viewing real	-time alerts	
	Top 5 Real-Time Threat Events 6 Checking		
	Subject Level [Key file directory change] [H8S] Medium	Asset Name ecs-	Triggered Aug 17, 2023 10:20:03 GMT+08:00
	[Key file directory change] [HSS] • Medium	ecs-	Aug 17, 2023 10:25:03 GMT+08:00
	[Key file directory change] [HSS] . Medium	ecs-	Aug 17, 2023 10:10:11 GMT+08:00
	[Key file directory change] [HSS]	ecs-	Aug 17, 2023 10:05:04 GMT+08:00
	[Key file directory change] [HSS] Medium	ecs-	

Table 3-2 Security Monitoring parameters

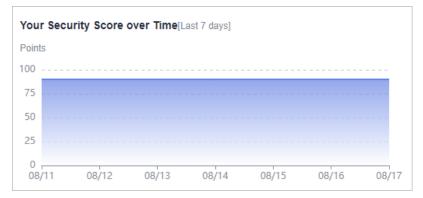
Parameter	Description				
Vulnerabilities	This panel displays the top five vulnerability types and the total number of unfixed vulnerabilities in your assets in all workspaces of your account for the last 7 days . You can quickly learn of the total number of unfixed vulnerabilities an the number of vulnerabilities at each severity level. The statistics are updated every 5 minutes.				
	Risk severity levels:				
	 High: There are vulnerabilities on your workloads, and you should view vulnerability details and handle them in a timely manner. 				
	 Medium: There are abnormal incidents on your workloads, and you should view vulnerability details and handle the vulnerability in a timely manner. 				
	 Others: There are risky incidents that are marked as low-risk or informational in your systems, and you should view vulnerability details and take necessary actions. 				
	• When you click the Top 5 Vulnerability Types tab, the system displays top 5 vulnerability types.				
	 Vulnerability rankings are based on the number of host 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. 				
	Figure 3-5 Top 5 Vulnerability Types				
	Top 5 Vulnerability Types Top 5 Real-Time Vulnerabilities (Checking				
	Vulnerability ID Vulnerable Servers				
	CVE-2020-27066 1				
	CVE-2020-36557 1				
	CVE-2020-36538 1				
	CVE-2024/8/12 1				
	CVE-2021-1920 1				
	 Click Top 5 Real-Time Vulnerabilities tab. The system displays the top 5 vulnerability incidents for the last 7 day You can quickly view vulnerability details. 				
	 You can view details such as the vulnerability name, severity, asset name, and discovery time. 				

Damanakan	Description					
Parameter	Description					
	 If no data is available here, no vulnerabilities are detected on the current day. Figure 3-6 Viewing real-time vulnerabilities 					
	Top 5 Vulnerability Types Top 5 Real-Time Vulnerabilities 🌒 Checking					
	Subject Level Asset Name Triggered EulerOS-SA-2022-2273 Moderate karnel. • Medium ecs Aug 08, 2022 20 54 52 GMT-08 00					
	EutriOS-SA-2022-2213 Moderale kernel • Medium ecs- Aug 06, 2022-2014-32 ONI 1100.00 EutriOS-SA-2022-2712 Moderale kernel • Medium ecs- Aug 06, 2022-2014-32 ONI 1100.00					
	EulerOS-SA-2023-1507 Moderate: kernel Medium ecs-4 Aug 08, 2023-20:54:52 GMT-08:00					
	EularOS-SA-2022-1328 Important: kernel • Medium ecs Aug 08, 2022 20:54:52 GMT-08:00					
	EulerOS-SA-2022-1523 Low: kernel secur • Medium ecs- Aug 08, 2023 20:54:52 GMT-08:00					
Settings	 learn of total number of violations and the number of violations at each severity level. The statistics are updated every 5 minutes. Risk severity levels: 					
	 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 incidents on your workloads. 					
	 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, click the Abnormal Baseline Settings panel.					
	 You can view details of the top compliance risks discovered in the latest check, such as check item name, severity, asset name, and discovery time. 					
	 If no data is available, no violations are detected for the last 30 days. 					
	Figure 3-7 Viewing compliance risks					
	Top 5 Real-Time Unsafe Baseline Settings 👔 Checking					
	Subject Level Affected Resource Number Triggered Security group inbound rules e High 3 Aug 11, 2023 00:00:16 GMT-00:00					
	Open high-risk and remote management p • High 3 Aug 10, 2022 00 00 25 GMT+68 00					
	IAM user passmord strength High 1 Aug 10, 2022 00 00 27 GMT-96 00					
	IAM user password configuration High 1 Aug 10, 2023 00:00 19 GMT-08:00					
	IAM user operation Protection • High 1 Aug 10, 2023 00:00:17 GMT-68:00					

Your Security Score over Time

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

Figure 3-8 Your Security Score over Time



3.2 Security Score

Scenario

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

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.

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

Unscored Check Items

 Table 3-4 lists the security check items and corresponding points.

Category	Unscored Item	Points	Suggestion	Maximum Unscored Point
Enabling of security services	Security-related services not enabled	-	Enable security- related services.	30
Compliance Check	Critical non- compliance items not fixed	10	Fix compliance violations by referring	20
	High-risk non- compliance items not fixed	5	recommended fixes and start a scan again. The security score will	
	Medium-risk non- compliance items not fixed	2	be updated.	

Table 3-4 Unscored check items

Category	Unscored Item	Points	Suggestion	Maximum Unscored Point	
	Low-risk non- compliance items not fixed	0.1			
Vulnerabilit ies	Critical vulnerabilities not fixed	10	Fix vulnerabilities by referring corresponding	20	
	High-risk vulnerabilities not fixed	5	suggestions and start a scan again. The security score will be updated.		
	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	30	
	High-risk alerts not fixed	5	suggestions. The security score will be updated		
	Medium-risk alerts not fixed	2	accordingly.		
	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 and regions to support workspace operation modes in different scenarios.

- Workspace agencies:
 - Workspace data hosting: All workspaces of a single account can be aggregated to a workspace for cross-account centralized security operations.
 - Workspace hosting: You can create agencies to let a user centrally view the asset risks, alerts, and incidents of multiple workspaces.

What Is a Data Space?

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

What Is a Data Pipeline?

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

General Rules for Workspaces

- Paid SecMaster: A maximum of five workspaces can be created for a single account in a single region.
- Free SecMaster: Only one workspace can be created for a single account in a single region.
- Permanent deletion of workspaces: Workspaces are deleted immediately and cannot be restored.

- Workspace agencies:
 - A maximum of one workspace agency view can be created for an account in a region.
 - A maximum of 100 workspaces can be managed in a workspace agency view in a region for a single account or across several accounts.
 - A maximum of 10 workspaces can be managed in a workspace agency view under a single account in a region.
 - A maximum of 10 agencies can be created under a single account.
- Currently, performing operations in different workspaces in multiple windows of the same browser is not supported.

4.2 Creating a Workspace

Scenario

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

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

This section describes how to create a workspace.

Limitations and Constraints

- Paid SecMaster: A maximum of five workspaces can be created for a single account in a single region.
- Free SecMaster: Only one workspace can be created for a single account in a single region.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces > Management**.

Figure 4-1 Workspace page

SecMaster	Management (3)	Process
Security Overview Workspaces	Oracle WithSupport To form a name and keyword for search.	C
Purchased Resources Security Governance(beta)	Owner stoop 0 ekel22d 944821% Regin Prendrum mitgefeeldt More II incidents 0 0 Valent 0 0 Aleris 1 12 indicat 0 Not hoted - Assets 1 III Securit 0 III Indicat 1 III Prendrum	

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

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

Parameter	Description
Region	Select the region where the workspace to be added is located.
Project Type	Select the type of project that the workspace you want to create belongs to.
	If you select Enterprise Project , you need to 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.
	To learn more, see Enabling the Enterprise Center . You can use enterprise projects to more efficiently manage cloud resources and project members.
	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	Create a name for your workspace. The name must meet the following requirements:
	 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.

NOTE

SecMaster allows you to view the information about all region workspaces on the workspace management page. If the workspace information cannot be viewed and a message is displayed indicating that you have not purchased SecMaster, enable any SecMaster edition.

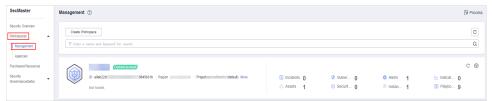
For example, if you have purchased SecMaster and created workspaces in the **CN-Hong Kong** region, when you switch to the **AP-Bangkok** region, you can still view the workspaces in the **CN-Hong Kong** region on the space management page. If the system displays a message indicating that you have not purchased SecMaster and cannot view the workspace information, enable any SecMaster edition.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces > Management**.

Figure 4-2 Workspace page



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

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

Figure 4-3 Workspace details



Table 4-2 Workspace parameters

Parameter	Description
Workspace Name	Name of the workspace
Workspace Type	Type of the workspace. The options are Self-owned , Managed View , and Managed .
ID	ID of the workspace
Region	Region to which the workspace belongs
Project	Project to which the workspace belongs
More	Workspace details

Parameter	Description
Hosting Status	Whether the workspace is hosted
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 ⁽²⁾ 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

After a workspace is added, 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces > Management**.

Figure 4-4 Workspace page

SecMaster	Management ①				Process
Security Overview Workspaces	Create Workspace To fater a name and knywood for sameh.				C
Purchased Resources Security Governance(beta)	Owned scores 0 #86226 9645319 Region Poped: ************************************	Incidents 0 Assets 1	♥ Vulner 0	O Alerts 1 i Instan 1	C ⊗ iv Indicat 0 S Playbo 9

Step 4 Click ⁽²⁾ on the right of the workspace. The workspace details page is displayed.

Figure 4-5 Workspace details page



- **Step 5** On the **Basic Information** tab page displayed, click **Edit**.
- **Step 6** Edit the workspace name, tag, or description and click **Save**.

----End

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 10 tags can be added for a workspace.

Procedure

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

Figure 4-6 Workspace page

SecMaster	Management (?)				Process
Security Overview Workspaces	Create Withingtons $\label{eq:state} \overline{\ensuremath{\mathbb{T}}} \ensuremath{\mbox{ for states}},$				C
Purchased Resources Security Governance(beta)	0 #9422d \$645019 Report Paget, """(default) More Not Insteid	 Incidents 0 Assets 1 	♥ Vulner 0	O Alerts 1 ⊗ Instan 1	C ® ⊵ Indicat 0 B Playbo 9

Step 4 Click ⁽²⁾ on the right of the target workspace to go to the details page.

Figure 4-7 Workspace details page

Current	eccount.								с®
ID fe7de	52 Region on-south-1 Projecton-south-1(default) More	Incidents	7	Vulner	36	 Alerts 	63458	🗠 Indicat 1	
Not currently hosting.		Assets	0	Securi	1	🖹 Instan	94223	Playb 10	1

Step 5 On the workspace details page, choose **Tag Management**.

Figure 4-8 Tag Management

<		
Basic Information Tag Management		
Add Tag You can add 9 more tags. A tag is a pair of key and v blank.	value. For hierarchical management, use both keys and values. For cr	ommon management, you can use keys only and leave values C
Кеу	Value	Operation
Key_0001	Value_0001	Edit Delete

Step 6 On the **Tag Management** page, manage tags.

Table 4-3 Managing tags

Operation	Description
Adding a tag	 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	 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	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 .

----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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces > Management**.

Figure 4-9 Workspace page

SecMaster	Management ③				Process
Security Overview Workspaces Management	Create Workspace If form a name and layered for seach.				C Q
Agencies Purchased Resources Security Governance(beta)	Collect activation 0 ebet224 9445016 Repon Project ************************************	 Incidents 0 Assets 1 	♥ Vulner 0 ⊜ Securit 0	 Alerts 1 Instan 1 	C ⑧ ⊻ Indicat 0 S Pløybo 9

Step 4 Click ¹ next to the workspace you want to delete.

Figure 4-10 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**.

A 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

4.4 Workspace Agencies

4.4.1 Overview

A workspace agency allows you to perform cross-account secure operations. You can centrally view asset risks, alerts, and incidents in workspaces of other users.

Step		Description
1	Creating an Agency View	You need to create an agency view to manage the delegation that other users give you for workspace hosting.
2	Creating an Agency	SecMaster allows you to create agencies to authorize other users in the project to manage your workspaces. This way, other users can view asset risks, alerts, and incidents in your workspace and perform security operations for you in a unified manner.
3	Authorizing an Agency	You need to grant permission to other users to manage your workspaces and they need to accept your delegation to attach your workspaces to their workspaces.
		 After you create an agency, authorize the user you specified in the agency to manage your workspaces.
		 Choose Workspaces > Agencies > Managing and receive workspaces that need to be managed by you centrally.
		Your workspaces will be attached to a workspace of the agency user for unified management.

Table 4-4 Process

Limitations and Constraints

- A maximum of one workspace agency view can be created for an account in a region.
- A maximum of 100 workspaces can be managed in a workspace agency view under a single account in a region.
- A maximum of 10 workspaces can be managed in a workspace agency view under a single account in a region.
- A maximum of 50 agencies can be created under a single account.

4.4.2 Creating an Agency View

Scenario

To manage other users' workspaces, you need to create an agency view to bind the workspaces to your workspace.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-11 Agencies

Master	Agencies 🕥			(Scenario Create Agenc
inty Overview	You have not created any agencies	yet. Create one now.		Poper 1 Proj	Өни
Aanagement ligencies hased Resources rity emance(Bata)	Create Agency Host a workspace in a project to another tenant.	2 Accept Agency Wall for the other account to accept the agency or withdraw the agency and manage the workspace with the current account.	3 Manage North Sector S		
	Agency Views Workspaces Managed by Me	My Workspaces Managed by Others			
		ing manapaces manages by Onicia			
	Create Agency Vew Batch Delete				
	Create Agency View Batch Delote Q, Select a property or entire a koyword.				C
		0 Werkspace NameID 0	Managad 0 Created 0	Description 0	C C Operation

- **Step 4** On the **View** tab, click **Create Agency View**. The **Create Agency View** slide-out panel is displayed.
- **Step 5** Set parameters required for creating the agency view.

Parameter	Description
Agency View Name	Name of the view
Bind Space Name	The workspace you want to bind to other users' workspaces
Description	Description of the view

Table 4-5 Parameters for creating an agency view

Step 6 Click OK.

The created agency view is displayed in the **Agency Views** tab.

----End

Related Operations

- Editing an agency view
 - a. Locate the row that contains the agency view, and click **Edit** in the **Operation** column.
 - b. In the **Edit Agency View** pane that is displayed, modify the agency view parameters and click **OK**.
- Deleting an agency view
 - a. Locate the row that contains the agency view, and click **Delete** in the **Operation** column.
 - b. In the displayed dialog box, click **Confirm**.

4.4.3 Creating an Agency

Scenario

SecMaster allows you to create agencies to authorize other users in the project to manage your workspaces. This way, other users can view asset risks, alerts, and incidents and perform security operations for you in a unified manner.

Limitations and Constraints

If you select **Organization** for **Initiated By**, there are some limitations you need to know:

- If you select all accounts under all organizations for the agency, the agency works for workspaces of new accounts of an organization.
- If you select all accounts of a specific organization for the agency, it takes a while for workspaces of new accounts of the organization to be synchronized in the agency.

Prerequisites

- An agency view has been created by the agency user. For details about how to create an agency view, see **Creating an Agency View**.
- You have authorized the workspaces to access the cloud service data.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure	4-12	Agencies
--------	------	----------

cMaster	4	gencies 💿			C Scenario	Create Agenc
curty Overview		You have not created any agencies yet. Create one	now.		Pepel 1 Workpace heating is an account	GHI
Management Agencies chased Resources curlly vertrance(Beta)		Create Agency Host a workpace in a project to worker levent Host a workpace in a project to worker levent	y	Manage No need to over the part of the need to over the part of the need to over the part of the need to over the need to ove		uni 💄
		Agency Views Workspaces Managed by Me My Workspaces Man	aged by Others			
		Agency Views Workspaces Managed by Me My Workspaces Man Create Agency View Batch Delete	aged by Others			
			aged by Others			C
	4	Create Agency Wew Batch Delete		Managed 0 Created 0	Description 0	C I Operation
	•	Create Agency Vew Batch Delete Q. Select a property or entire a leyword. A defect y Vew Name © Region © Wickspace Nu		Managnd 0 Created 0 0 Dec 13, 2023 09 37 52 OMT-00 00	Description : -	

Step 4 Click **Create Agency** in the upper right corner of the page.

Step 5 On the **Create Agency** slide-out is displayed, configure agency parameters.

Parameter		Description
Initiated By	,	Agency creator. If you use an administrator account of an organization or an agency account to log in to SecMaster, you can select a workspace under the organization for workspace hosting. The Organizations service is an account management service that enables you to consolidate multiple accounts into an organization so that you can centrally manage these accounts. For details, see Overview of Organizations.
Agency Created By	Workspac e	A workspace to be managed by this agency
Agency Accepted By	Account	 Account name of the user who delegate the management permission to this agency. Take the following steps to obtain the account name: 1. Log in to the management console, hover the mouse over the username in the upper right corner, and select My Credentials from the drop-down list. The API Credentials page is displayed by default. 2. On the API Credentials page, obtain the Account Name. Figure 4-13 Account Name
	Agency View	An existing agency view.
Agency Informati	Agency Name	Name of the agency
on	Agency Duration	How long the agency works

Parameter		Description
	Agency Status	 Agency permission policy. You can query the meaning of a policy in IAM. To view the meaning, perform the following steps: 1. Log in to the management console, hover the mouse over the username in the upper right corner, and select Identity and Access Management from the drop-down list. The IAM users page is displayed. 2. In the navigation pane on the left, choose Permissions > Policies. On the Policies page, enter the policy name in the search box. View the meaning and scope of the policy.
	Descriptio n	Description of the agency

Step 6 Click Confirm.

----End

Follow-up Operations

You need to wait for agency user's acceptance of your delegation. As an agency user, you need to accept the delegation from other users. For details, see **Authorizing an Agency**.

4.4.4 Authorizing an Agency

Scenario

As an agency user, you need to accept the authorization to access the workspaces. The accepted workspaces will be attached to your workspaces.

Prerequisites

An agency has been created. For details, see **Creating an Agency**.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-14 Agencies

SecMaster		Agencies 💿			Scenario	Create Agency
Security Overview Workspaces		You have not created any agencies yet. Create one now.			GHide	
Management Agencies Purchased Resources Security Governance(Beta)	Ŧ	Create Agency Host a workspace in a project to another tenant.	Accept Agency Well for the other account to accept the agency or withdraw he agency and manage the workspace with the current account.	Manage Workspaces Centrally Workspaces will be centrally managed by the account who accepts the corresponding agency.		Access 2
		Agency Views Workspaces Managed by Me My Wo	vikspaces Managed by Others			
		Q. Select a property or enter a keyword.				C 😔
	1	Agency View Name 0 Region 0	Workspace NamelD 0	Managed 0 Created 0	Description 0	Operation
			05520693-92e6-4b12-ac08-f1872219d8cb	0 Dec 13, 2023 09:37:52 GMT+08:00		Edit Delete
		10 v Total Records: 1 < 1 >				

- **Step 4** On the **Agencies** page, click the **Workspaces Managed by Me** tab. In the row containing the workspace you want to manage, click **Accept** in the **Operation** column.
- **Step 5** In the displayed dialog box, click **Confirm**.

----End

Follow-up Operations

Choose **Workspaces** > **Management**, click the name of the created agency view. You can view details about workspaces managed in the agency view.

4.4.5 Managing Agencies

Scenario

On the **Agencies** page, you can manage agency views, workspaces you are managing for others, and agencies managing your workspaces.

- **Agency Views**: On this tab, you can view all agency views you create and their details.
- Workspaces Managed by Me: On this tab, you can view workspaces managed in the agency view you create.
- **My Workspaces Managed by Others**: On this tab, you can view which agency views are managing workspaces you create.

Agency Views

Step 1 Log in to the management console.

- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-15 Agencies

Master	A	Agencies 🕥 🖉 🖓 🖓 Gaterator				
nty Overview spaces		You have not created any agencies yet. Create one now.			Poper1 Poper1	
tanagement gencies hased Resources rity emance(Beta)		Create Agency Host a workspace in a project to another tenant.	2 Accept Agency Wall for the other account to accept the agency or withdraw the agency and manage the vertispace with the current account.	Manage Workspoes event who accepts the conseption gency.		urr
	Agency Yessis Wootspaces Managed by Me My Wootspaces Managed by Otters					
		Create Agency View Batch Delete				
		Q Select a property or enter a keyword.				C
	1	Agency View Name © Region ©	Workspace NameID 0	Managed 0 Created 0	Description ¢	Operation
			0552b593-92e6-4b12-ec08-f187221958cb	0 Dec 13, 2023 09:37:52 GMT+08:00		Edit Delete

Step 4 On the **Agencies** page, click the **Agency Views** tab.

Step 5 On the **Agency Views** tab, manage your agency views.

• Viewing agency views

Table 4-7 Agency view information

Parameter	Description
Agency View Name	Name of an agency view
Region	Region where the agency view is located.
Workspace Name/ID	Name and ID of a workspace bound to an agency view
	You can click the name of a bound workspace to access the workspace.
Managed Workspaces	Number of workspaces in an agency view
Created	Time when an agency view is created
Description	Description of an agency view
Operation	You can edit or delete an agency view.

- Editing an agency view
 - a. Locate the row that contains the agency view, and click **Edit** in the **Operation** column.
 - b. On the **Edit Agency View** slide-out panel, modify the parameters and click **OK**.
- Deleting an agency view
 - a. Locate the row that contains the agency view, and click **Delete** in the **Operation** column.

To delete multiple agency views, select them in the agency view list and click **Batch Delete** above the list.

b. In the displayed dialog box, click **Confirm**.

----End

Workspaces Managed by Me

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-16 Agencies

SecMaster	Agencies 🕥			Create Agency	
Security Overview Varispaces	You have not created any agencies yet. Create one now.		Project 1 Project 2 Project 2	GHide	
Management Agencies Purchased Resources	Cruste Agency Host a vortigate in a project to another femant that a vortigate in a project to another femant that a vortigate in a project to another femant that avoid a vortigate in a project to another femant	Workspaces identifies		Acces &	
Security Governance(Beta)	for some only and here				
	Agency Views Workspaces Managed by Me Mr Workspaces Managed by Others				
	Create Agesty View Baltit Delne				
	Q. Select a property or enter a keyword.			C 🔘	
	Agency View Name 🔅 Region 🔅 Workspace NameID 🔅	Managed Created Created	Description ¢	Operation	
	05520693-9216-4012-ec06-f187221948co	0 Dec 13, 2023 09:37:52 GMT+08:00	-	Edit Delate	
	10 • Total Records: 1 < 1 >				

Step 4 On the **Agencies** page, click the **Workspaces Managed by Me** tab.

- **Step 5** View and manage workspaces managed by you.
 - Viewing workspaces managed by you

Table 4-8 Workspace parameters

Parameter	Description	
Agency Name	Name of an agency view.	
Name/ID	Name and ID of the workspace managed in your agency view.	
Initiation Mode	Creator of the agency	
Agency Status	Delegation status	
Selected Status	Whether the delegation is selected	
Agency Duration	How long an agency works	
Agency Started	Time the agency starts working.	
Agency Policy	Permissions granted to an agency.	
Operation	You can accept or delete agency tasks managed by yourself.	

• Managing workspaces managed by you

Operation	Description
Accepting a workspace agency	 Locate the row that contains the workspace agency, and click Accept in the Operation column. To accept multiple workspace agencies, select them in the list and click Accept above the list. In the displayed dialog box, click Confirm.
Rejecting a workspace agency	 Locate the row that contains the workspace agency, and click Reject in the Operation column. To reject multiple workspace agencies, select them in the list and click Reject above the list. In the displayed dialog box, click Confirm.
Releasing a workspace agency	 Locate the row that contains the workspace agency, click More in the Operation column, and select Release. To release multiple workspace agencies, select them in the list and click Release above the list. In the displayed dialog box, click Confirm.
Deleting a workspace agency	 Locate the row that contains the workspace agency, click More in the Operation column, and select Delete. To delete multiple workspace agencies, select them in the list and click Delete above the list. In the displayed dialog box, click Confirm.

Table 4-9 Managing workspaces managed by you

----End

My Workspaces Managed by Others

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

Figure 4-17 Agencies

cMaster	A	Agencies 🕥 🦪 🔂 🖓 🖓			Create Agen	
urty Overview kspaces		You have not created any agencies yet. Create one now.			GH	
anagement gencies ased Resources Ry mance(Beta)		Create Agency Host a workspace in a project to another breast.	2 Accept Agency Wall for the other account to accept the agency or withdraw the agency and manage the workspace with the current account.	Manage Workspose Work		Acces Log
	Agency Veers Workspaces Managed by Me My Workspaces Managed by Others					
		Agency Views Workspaces Managed by Me My	Workspaces Managed by Others			
		Agency Views Workspaces Managed by Me My Create Agency View Batch Dekte	Workspaces Managed by Others			
			Workspaces Managed by Others			C
	•	Create Agency Wew Batch Delete	Workspace Name/D ©	Managed 0 Created 0	Officialities of	C Queration
	•	Create Agency View Batch Delete Q. Select a property or enter a keyword.		Managed 0 Created 0 0 Dec 13, 2023 09 37 52 GMT-08 50	Description +	

- Step 4 On the Agencies page, click the My Workspaces Managed by Others tab.
- **Step 5** On the **My Workspaces Managed by Others** tab, view and manage the workspaces that are managed by others.
 - Viewing your workspaces managed by others

Table 4-10 Viewing your workspaces managed by others

Parameter	Description	
Agency Name	Name of an agency view	
Name/ID	Name and ID of your workspace	
Agency Account	Account username who accepts the workspace agency	
Initiation Mode	Creator of the agency	
Agency View Name	Name of the agency view	
Agency Duration	How long an agency works	
Agency Status	Delegation status	
Agency Started	Time the agency starts working.	
Agency Policy	Permissions granted to a workspace agency	
Operation	Through this column, you can modify or delete a workspace agency.	

• Managing your workspaces managed by others

Table 4-11	Viewing your	[·] workspaces	managed by others
------------	--------------	-------------------------	-------------------

Operation	Description
Modifying an accepted workspace agency	 Locate the row that contains the workspace agency, and click Modify in the Operation column.
	 In the displayed dialog box, modify the agency information.
	3. Click Confirm .

Operation	Description	
Withdrawing an accepted workspace agency	 Locate the row that contains the workspace agency, and click Withdraw in the Operation column. To recall multiple workspace agencies, select them in the list and click Recall above the list. 	
	2. In the displayed dialog box, click Confirm .	
Reapplying for a workspace agency	If your workspace agency is rejected by others, you can send the workspace agency request again and ask others to accept it.	
	 Locate the row that contains the workspace agency, click More in the Operation column, and select Reapply. 	
	2. In the displayed dialog box, click Confirm .	
Releasing a workspace agency	 Locate the row that contains the workspace agency, click More in the Operation column, and select Release. To release multiple workspace agencies, select them in the list and click Release above the list. 	
	2. In the displayed dialog box, click Confirm .	
Deleting a workspace agency	 Locate the row that contains the workspace agency, click More in the Operation column, and select Delete. To delete multiple workspace agencies, select them in the list and click Delete above the list. 	
	2. In the displayed dialog box, click Confirm .	

----End

5 Viewing Purchased Resources

Scenario

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

Procedure

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

Figure 5-1 Purchased Resources

SecMaster	Purchased Resources			Ruy Value-add Pack Duy SecMaster
Security Overview Workspaces Purchased Resources Security	Total/Subscribed Regions 2/2	Upgradeable O	Versions About to Expire ①	Total Caola 73
Governance(bata)				Region + please enter Q. C
	CN-Hong Kong Dimg Mono Pay-per-use Professional Create Time 2023/06/10.855.01	Custa 20	Expire Time Lasting	Increase Dueta Vitil Expere / Venu-add 0/1
	AP-Singapore	Cuota 53	Suptre Time 663Day	Upgrade Renew Increase Queta Vitil Eugen / Vature add 1/2

Step 4 View details on the purchased resource page.

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

----End

6 Security Governance

6.1 Overview

What Is Security Governance?

Security Governance is an automatic security assessment and compliance governance platform. It provides the unified cloud service cybersecurity & compliance standard (3CS). It offers security governance templates to help you comply with PCI DSS, ISO 27701, ISO 27001, and more. It automatically checks your services against preset compliance policies, intuitively presents your service compliance status, and allows you to quickly download compliance reports.

NOTE

Security Governance is available to limited users. To use this function, contact Huawei Cloud technical support.

Features

Security Governance provides you with security governance templates and checks your services based on regulation terms in the compliance packs.

Compliance Pack

Huawei's security governance templates include detailed terms, scan policies, compliance evaluation items, and improvement suggestions from Huawei experts, covering PCI DSS, ISO27701, ISO27001, privacy protection, and other standards. You can subscribe to and unsubscribe from compliance packs and view results.

• Policy Check

The compliance status of cloud assets is checked periodically through codebased scanning. You can view compliance risks on the dashboard, and obtain corresponding improvement suggestions from our experts.

• Compliance Evaluation

Security Governance integrates regulatory clauses and standard requirements into compliance pack check items. You complete evaluation of your services using the compliance pack, and view evaluation results. You can also view historical results, upload and download evidence, and take actions based on suggestions from our experts.

Result Display

Security Governance displays the evaluation results and compliance status on the dashboard, including the compliance rates of the compliance packs you subscribed to, and the compliance rate of each term the regulations and standards, each security, as well as the policy check results.

Advantages

• Compliance as a Service

Security Governance provides the unified Cloud Service Cybersecurity & Compliance Standard (3CS). It integrates regulatory clauses and standard requirements into your business and information technologies by providing various 3CS-based security governance templates.

Improved Efficiency

Security Governance opens security governance templates for you to be compliant with PCI DSS, ISO 27701, and ISO 27001, providing compliance policies and evaluation items. With your authorization, Security Governance automatically scans your cloud assets against compliance policies, and the service evaluation items help you quickly manage the compliance status. You can download compliance reports in few clicks.

• Intuitive Display

Security Governance presents both the overall compliance information and requirement-specific compliance status on the dashboard. You can easily identify potential problems and take actions based on expert suggestions.

6.2 Security Compliance Pack Description

Security Governance provides security compliance packs. You can select the required security compliance pack by following the guide provided therein.

• Security Standard

Security Standard

Security Governance provides the following compliance packs listed in **Table 6-1** for you to comply with various privacy protection laws. You can refer to the guidelines and subscribe to compliance packs as you need.

Pack	Description	App lica ble Regi on	Cat ego ry	Dom ain	Guidelines
PCI DSS	This compliance pack provides check items and guidelines to help you evaluate your data security management. It also suggests improvements based on the internationally recognized Payment Card Industry Data Security Standard (PCI DSS) Version 3.2.1 May 2018 to help you comply with the terms.	Glob al	Indu stry stan dard s	Data secu rity	 Applicable to entities that handle payment cards. These entities include merchants, processing organizations, receipt organizations, card issuing organizations, and service providers. Applicable to entities that store, process, or transmit cardholder data, such as main account information (PAN, usually a bank card number), cardholder name, card validity period, and business code, or sensitive verification data, such as full track data, credit card security code, and PIN. Applicable to entities that need to detect data security risks and obtain risk control measures. Subscribe to this pack if your entity meets any of the preceding descriptions.

 Table 6-1 Security standards compliance packs

Pack	Description	App lica ble Regi on	Cat ego ry	Dom ain	Guidelines
ISO/IEC 27001:2013	This compliance pack provides check items and guidelines to help you evaluate your data security management. It also suggests improvements based on ISO 27001:2013 – Information Security Management Systems to help you comply with the terms.	Glob al	Inte rnat iona l stan dard s	Infor mati on secu rity	ISO 27001 is a globally recognized standard for information security. It adopts a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving your information security management system. Subscribe to this pack to identify and manage the security risks of information you hold.

Pack	Description	App lica ble Regi on	Cat ego ry	Dom ain	Guidelines
ISO/IEC 27701:2019	This compliance pack provides check items and guidelines to help you evaluate your data security management. It also suggests improvements based on ISO 27701:2019 – Privacy Information Management Systems to help you comply with the terms.	Glob	Inte rnat iona l stan dard s	Priva cy prot ectio n	 Applicable to entities that are responsible for Personally Identifiable Information (PII) as it poses privacy requirements on how to collect, use, transmit, store, and delete data. PII (also referred to as "personal data" in this pack) includes name, phone number, email address, and ID card information. Applicable to entities that work as PII controllers (also referred to as "data controllers" in this pack) and/or PII processors (also referred to as "data processors"). PII controllers are privacy stakeholders who determine the purposes and methods of PII processing, while PII process the data based on these purposes and methods. Applicable to entities that need to detect privacy protection risks and obtain risk control measures Subscribe to this pack if your entity meets any of the preceding descriptions.

6.3 Procedure

Table 6-2 shows the process of using SecMaster security governance.

Figure 6-1 Procedure

Process Flow			
	-2	-3	
Authorize Service	Subscribe to Compliance Packs	Policy Check	View Result
Authorize Compass to access your cloud services.	Compliance packs contain security regulations and standards.	Compass checks your service compliance. View Result Evaluation Use our checklist to evaluate your service compliance. Evaluate	Compass will evaluate your service compliance based on the policy check and evaluation results.

Table 6-2 Procedure

Step	Description	
Authorizing access to cloud resources	Before using the security governance, you need to grant the permission to access your cloud service resources. After the permission is granted, you can use policy scanning to quickly identify the security compliance of cloud assets.	
Subscribing to compliance packs	SecMaster provides different security compliance packs. You can select the required security compliance pack.	
Self-evaluation	After subscribing to a security compliance pack, you use evaluate your compliance by referring to the terms in the compliance pack.	
Viewing the result	 After policy scanning or self-assessment, you can view the security governance status. Security Compliance Overview: View the compliance overview of laws and regulations, standards, compliance statuses under each security compliance pack, and policy scanning overview. Viewing the Governance Result: View the overall and detailed compliance status with each security compliance pack. Viewing the Policy Scanning Result: View the policy scanning result and its details. 	

6.4 Authorizing Service

Scenario

Before using the security governance, you need to grant the permission to access your cloud service resources. After the permission is granted, you can use policy scanning to quickly identify the security compliance of cloud assets.

Authorizing SecMaster to access your cloud assets.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-2 Subscriptions page

SecMaster	Dashboard @ What Is Compass? @ Process Flow			
Security Overview Workspaces Purchased Resources Security Overview(obda) Subscriptions(bela) Policies(bela)	Process Flow Authorize Service Authorize Compass to access your cloud access: Authorize	O Subscribe to Compliance Packs Compliance pack content recordly regulations and fabouries Budgerbe	Organization of the service completese. Very fragment Very fragment	Aver Result Compare and execution provides on the participation of the participation of the participation of the Result Vere Result
	4			

- **Step 4** On the **Subscriptions** page, click **Authorize** in the **Authorize Service** process. The service authorization dialog box is displayed.
- Step 5 In the displayed dialog box, click Agree to authorize.
 - ----End

6.5 Subscribing to Compliance Packs

Scenario

A compliance pack is an open security governance template. It includes original standards and regulation terms, check policies, compliance evaluation items, and improvement suggestions from our experts, covering PCI DSS, ISO 27701, ISO 27001, privacy laws, and other regulations and standards.

This topic describes how to subscribe to a security compliance pack.

Prerequisites

Service authorization has been completed. If the service is not authorized, authorize it first. For details, see **Authorizing Service**.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-3 Subscriptions page

SecMaster	Subscriptions					
Security Overview Workspaces	Subscribe to Compliance Pack					Enter a pack name. Q C
Purchased Resources	Compliance Pack	Status	Compliance		Updated	Operation
Security Governance(beta)	V PCI DSS	Subscribed		Fully compliant 0 terms Partially compliant 249 terms	Feb 16, 2023 19:09:50 GM	View Result Unsubscribe Download Repo
Compliance Overview(beta)	V ISO/IEC 27701:2019	Subscribed		Fully compliant 0 terms Partially compliant 161 terms	Jun 12, 2023 15:00:15 GM	View Result Unsubscribe Download Repo
Subscriptions(beta) Policies(beta)	V ISO/IEC 27001:2013	 Subscribed 		Fully compliant 0 terms Partially compliant 114 terms	Mar 16, 2023 10:34:06 GM	View Result Unsubscribe Download Repo

Step 4 Click Subscribe to Compliance Pack in the subscription list page.

If you subscribe for the first time, click **Subscribe** in the **Subscribe to Compliance Pack** page.

Step 5 On the **Subscribe to Compliance Packs** page, select a security compliance pack and click **Subscribe** in the lower right corner to confirm the subscription.

For details about the security compliance pack, see **Security Compliance Pack Description**.

Step 6 In the dialog box that is displayed, click **OK** to return to the subscription list page and view details about the compliance pack.

To evaluate immediately, click **Evaluate** in the displayed dialog box. For details, see **User Self-Assessment**.

----End

6.6 User Self-Assessment

Scenario

After subscribing to the security compliance pack, you can assess security based on international standards.

Prerequisites

You have subscribed to the security compliance pack. For details, see **Subscribing to Compliance Packs**.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure	6-4 Subscription	s page
--------	------------------	--------

SecMaster		Sul	bscriptions					
Security Overview Workspaces	.		Subscribe to Compliance Pack					Enter a pack name. Q C
Purchased Resources			Compliance Pack	Status	Compliance		Updated	Operation
Security Governance(beta)	•		V PCI DSS	 Subscribed 		Fully compliant 0 terms Partially compliant 249 terms	Feb 16, 2023 19:09:50 GM	View Result Unsubscribe Download Repo
Compliance Overview(beta)			V ISO/IEC 27701:2019	Subscribed		Fully compliant 0 terms Partially compliant 161 terms	Jun 12, 2023 15:00:15 GM	View Result Unsubscribe Download Repo
Policies(beta)			V ISO/IEC 27001:2013	Subscribed		Fully compliant 0 terms Partially compliant 114 terms	Mar 16, 2023 10:34:06 GM	View Result Unsubscribe Download Repo

Step 4 Click ✓ on the left of the compliance pack to be self-assessed to expand the compliance pack information. In the Tenant Self-Assessment area, click **Evaluate** in the **Operation** column. The evaluation page is displayed.

Figure 6-5 Self-evaluation

Compase	Bubacriptions			
Contesare	Notecola to morphance Para			Annual a part carra
Decerty Oscensoro -	TOTAL CONTRACTOR MARK	Abatura		
Publicities	A STREET AND A STREET AND A STREET	 Outrouriteest 		Party complexed 101 barries 247 barries 249 barries 24
	Thatk Type	Mates	Partially Compliant or Failed Borns	Machaban Transration
	Evaluation	in program		Jun DR. 2022 To be DRT-10.000 Evaluate
	Party Lines.	1		PAGE AND AND AN ADDRESS AND ADDRES
	PGI 000	 Outpourteed 		Party constants of the second
	· · · · · · · · · · · · · · · · · · ·	Subscribes		Furth consistences and appendix the second s
	· · · · · · · · · · · · · · · · · · ·	· MARKAN MARK		Pully compliant. O lawse that RN, 2001 14 all 10 INMY IN IN
	 Grana Datar avaires 2.0 L3 	 Outrouriteent 		Forty company in National Just 10, 2022 12:04:33 GMT+08:00 View Result Unsubscriber Devention Report

Step 5 On the **Evaluation** page, perform self-assessment on each check item.

Figure 6-6 Evaluation page

International standard	
1. The cyber security and privacy protection management policies and processes must be officially released and communicated to stateholders in a timely manner so that the stateholders understand their own roles and responsibilities.	rence
Fully compliant Partially compliant Non-compliant NA	
Enter remarks.	
2. Resources must be well prepared so that a budget for personnel, technologies, network environments, facilities, information, and finance can be developed to help achieve the cyber security and privacy protection objectives.	rence
Fully compliant Partially compliant Non-compliant N/A	
Enter remarks. Vew Atlactment	
 The cyber security and privacy protection management policies, processes, standards, and documents must be reviewed and updated at least once a year, based on the information obtained from continuously monitored data and regular assessment. Partornel wino develop, distitute, and update the documents must be designated. 	rence
Fully compliant Partially compliant Non-compliant N/A	
Enter remarks.	

- To upload an attachment, click **View Attachment** > **Upload Attachment** and upload related credential information.
- During the evaluation, click **Reference** on the right of the evaluation item to view basic information, related terms, and historical records of the check item.
- **Step 6** After the evaluation is complete, click **Submit** in the lower right corner.

----End

6.7 Security Compliance Overview

Scenario

After subscribing to a security compliance pack, you can view the compliance overview, standard term compliance overview, and policy scanning overview of the subscribed security compliance pack on the **Dashboard** page.

Prerequisites

You have subscribed to the security compliance pack. For details, see **Subscribing to Compliance Packs**.

View the compliance with laws and regulations and standard clauses.

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Compliance Overview**. The **Compliance Overview** page is displayed.

Figure 6-7 Compliance overview page

SecMaster	Dashboard		
Security Overview Workspaces 👻	Compliance with Terms	Updated: Nov 22, 2023 19/01-45 GMT-00.00 Compliance Packs 19/0162 27001 2013	Updated: Nov 22, 2023 19 01:45 GMT+08.00
Purchased Resources			1% Fully compliant 2 terms Partially comp 112 terms
Governance(beta)		PCLDSS	0% Fully compliant 0 terms Partially comp 249 terms
Overview(beta) Subscriptions(beta)		 Fully compliant 4 terms (0.45%) Pantially compliant 0 terms (0.00%) 	
Policies(beta)		 Non-compliant 0 Sterms (0.00%) N/A 0 terms (0.00%) 	
		 Not checked 883 terms (99.55%) 	
	4		

Step 4 On the **Compliance Overview** page, view the **Compliance with Terms**.

Figure 6-8 Compliance with terms

SecMaster	Dashboard							
Security Overview	O Compass will be discontinued on Dec 5, 2023. Learn more. To use the similar functions, go to Seculator.							
Verdragende Verdragende Purchased Risources Boorn Governant/citets) Comprises/beta Duborg/bros/beta Policies/beta	Compliance with the discontinued on Deck 3, 2021. Learn	mont To use the somethar functions, got 10 toofstander Updatest Feb 20, 2023 22 20 th OMF -01 00 Compliance Packs Biology 22 2013 22 20 10 Biology 22 2013 22 2013 22 2013 Biology 22 2013 22 2013 Biology 22 2013 22 2013 22 2013 22 2013 Biology 22 2013 22 2013 22 2013 Biology 22 2013 22 2013 22 2013 22 2013 Biology 22 2013 22 2013 22 2013 Biology 22 2013 22 2013 22 2013 Biology 22 2013 22 2013 22 2013 Biology 22 2013 22 2013 Biology 22 2013 22 2013 22 2013	Updaniel Feb 28, 2023 22 20 66 GMT-98 50 ¹⁵ Full company Palloty comp 12 terms					
End								

Viewing Policy Check Results

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-9 Subscriptions page

SecMaster	Dashboard @ What is Compass? @ Process Flow			
Security Overview	Process Flow			
Workspaces •		-2	-3	-4
Security Governance(bata)	Authorize Service Authorize Compass to access your cloud services.	Subscribe to Compliance Packs Compliance packs contain security regulations and standards.	Policy Check Compass checks your service compliance. View Result	View Result Compass will evaluate your service compliance based on the policy check and evaluation results.
Compliance Overview(beta) Subscriptions(beta)	Authorize	Subscribe	Evaluation Use our checklist to evaluate your service compilance. Evaluate	View Result
Policies(beta)			Evenate	

Step 4 On the Compliance Overview page, view the Policy Check.

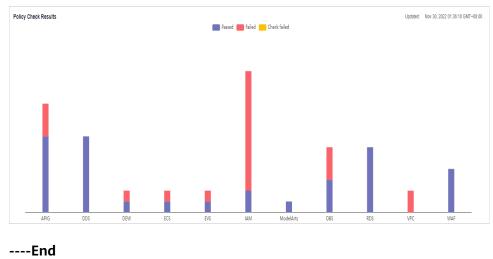


Figure 6-10 Policy check results

6.8 Evaluation Result

Scenario

After you subscribe to the security compliance pack, SecMaster automatically scans your system based on the security compliance pack. After the scanning, you can view the overall compliance status and improvement suggestions.

Prerequisites

You have subscribed to the security compliance packs. For details, see **Subscribing to Compliance Packs**.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-11 Subscriptions page

SecMaster	Subscriptions						
Security Overview Workspaces 💌		Subscribe to Compliance Pack					Enter a pack name. Q C
Purchased Resources		Compliance Pack	Status	Compliance		Updated	Operation
Security Governance(beta)		V PCIDSS	Subscribed		Fully compliant 0 terms Partially compliant 249 terms	Feb 16, 2023 19:09:50 GM	View Result Unsubscribe Download Repo
Compliance Overview(beta)		V ISO/IEC 27701:2019	 Subscribed 		Fully compliant 0 terms Partially compliant 161 terms	Jun 12, 2023 15:00:15 GM	View Result Unsubscribe Download Repo
Subscriptions(beta) Policies(beta)		V ISO/IEC 27001:2013	 Subscribed 		Fully compliant 0 terms Partially compliant 114 terms	Mar 16, 2023 10:34:06 GM	View Result Unsubscribe Download Repo

Step 4 Click **View Result** in the **Operation** column. The **Evaluation Result** page is displayed.

Figure 6-12 View result

	Compliance Pack	Status	Compliance		Updated	Operation
~	China DJCP (MLPS) 2.0 L4	Subscribed		Fully compliant 101 terms Partially compliant 162 terms	Jun 06, 2022 16:52:38 GMT+08:00	View Result Unsubscribe Download Report
~	PCIDSS	Subscribed		Fully compliant 0 terms Partially compliant 249 terms	Dec 03, 2021 14:48:04 GMT+08:00	View Result Unsubscribe Download Report
~	ISO/IEC 27701:2019	Subscribed		Fully compliant 2 terms Partially compliant 159 terms	May 26, 2022 20:23:32 GMT+08:	View Result Unsubscribe Download Report

Step 5 View the evaluation results.

Figure 6-13 Evaluation result page

Subscriptions / View Result: China DJCP (MLPS) 2.0 L4				
Overview 🕲	 Fully compliant 101 terms (88-0%) Partially compliant 1 terms (63-8%) Non-compliant 0 terms (60-0%) NAA 0 terms (60-0%) Rot checked 161 terms (61-25%) 	Compliance Pack Applicable Region Category Domain Description	China DUCP (MLPS) 2.0.1.4 China National standard Nation's security This consideration of the standard standards with a security with a security management. It also supports propresented issued the level 4 requerements of China's national standards protection of cybersocrity.	Hide
Updated Jun 05, 2022 16:52:38 GMT+08:00				
China DJCP (MLPS) 2 0 L4	Terms 263	1	161	
Compliance	Fully compliant	101 🛑 Partially co	mpliant 1 🛑 Non-compliant 0 🔜 N/A 0 💼 Not checked 161	

- View the overall compliance of the currently subscribed security compliance pack.
- To view the details of a term, select the clause in the navigation tree on the left. The details of the term are displayed on the right, including the term content, compliance status, and improvement suggestions.

To view the basic information and historical records of the term, click the term name. The detailed information about the term is displayed on the right.

- To perform a self-evaluation on a specified term, perform the following steps:
 - a. In the navigation pane on the left, select the terms to be self-evaluated.

Figure 6-14 Selecting terms

27701			
1% Compliance	Tems 161 2 Fully compliant	159 2 🛑 Partially compliant. 0 📂 Non-compl	art 0 🔜 N/A 0 🔜 Notcheoled 159
All results	Q Term: ⑦ The control, implementation guidance and other	ar information stated in ISO/IEC 27002.2013, 13.1.1 a	opties.
6.4 Human resource security 6.5 Asset management 6.6 Access control	Evaluation ⑦ Requirement	Result	Suggestion
6.8 Physical and environmental security 6.9 Operations security 6.9 Operations security	Network control and isolation measures must be		Take appropriate network control and isolation measures, i.
6.10 Communications security 6.10.1 Network security management	Policy Check ③		
6.10.1.1 Network controls 6.10.1.2 Security in network services 6.10.1.3 Segregation in networks	Policy IAM ACL should specify the IP address ranges for	Result or console Failed	Suggestion Configure IP address ranges for console access on the IA.

b. Click the name of a check item. On the displayed page, click **Edit** and enter the compliance status and evaluation remarks.

If related credentials are available, click Upload Files.

Figure 6-15 Self-evaluation

Evaluation		×
Basic Information	History	
	Submit	
Category	International standard	
Requirement	Network control and isolation measures must be taken to secure data and applications in the system.	
Check Items	Check whether network control and isolation measures are taken. - Network control: Manage and control the networks, for example, by restricting the devices that can be connected, restricting functions of each port, and mutually authenticating device identities. - Network isolation: Isolate services, users, and information systems on the network.	
Evaluation Result	Fully compliant Non-compliant N/A Partially compliant	
Remarks	Enter remarks.	
Attachments	Upload Files	
	 Only jpg, jpgg, csy, doc, docx, xis, xlsx, ppt, pptx, zip, and msg files are supported. You can upload a maximum of 5 MB files at a time. 	
Suggestion	Take appropriate network control and isolation measures, including but not limited to the following: - Network control: Manage and control the networks, for example, by restricting the devices that can be connected, restricting functions of each port, and mutually authenticating device identities. - Network isolation: isolate services, users, and information systems on the network.	

c. After the evaluation is complete, click **Submit** in the upper right corner to complete the evaluation of a single check item.

----End

6.9 Policy Check Result

Scenario

On the **Policy Check** page, you can view the overall check result of subscribed security compliance packs and the check result of each cloud service.

NOTE

The policy check is automatically performed at 01:30 every day and the check result is generated.

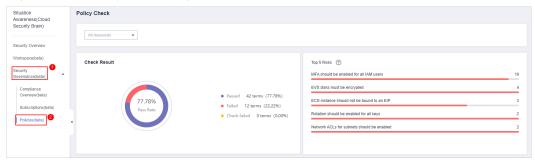
Prerequisites

You have subscribed to the security compliance packs. For details, see **Subscribing to Compliance Packs**.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Policies**. The **Policy Check** page is displayed.

Figure 6-16 Policy check page



Step 4 View policy check result.

Check Result			Top 5 Risks (?)		
			MFA should be enabled for all IAM us	ers	19
			EVS disks must be encrypted		4
77.78%		terms (77.78%)	ECS instance should not be bound to	an EIP	:
Pass Rate	Check failed		Rotation should be enabled for all ke	rs	1
			Network ACLs for subnets should be	enabled	1
		All	packs	▼ Enter a policy name.	QC
Policy	Result	Suggestion		Updated	Operation
Shared API Gateway should be accessed via HTTPS	 Passed 	Exercise caution when	performing this operation. After you enable	Nov 30, 2022 01:35:09 GMT+08:00	Details
Dedicated API Gateway should be accessed via HTTPS	Passed	Exercise caution when	performing this operation. After you enable	Nov 30, 2022 01:34:13 GMT+08:00	Details

Figure 6-17 Policy check

- By default, the check status of all resource policies displayed.
 - Check result: overall pass rate, passed policies, failed policies, and check failures.
 - Top 5 risks: Top 5 policies with the most failures.
- To view the check result of all policies of a resource, select the resource from the filter box in the upper part.

Figure 6-18 Selecting a resource

Policy Check			
All resources 👻			
Check Result		Top 5 Risks ⑦	19
		WPA should be enabled for an IAW users	4
77.78%	 Passed 42 terms (77.78%) Failed 12 terms (22.22%) 	ECS instance should not be bound to an EIP	3
Pass Rate	Check failed 0 terms (0.00%)	Rotation should be enabled for all keys	2
		Network ACLs for subnets should be enabled	2

• To view the scanning status of all resources in a policy, select the corresponding compliance pack in the upper part of the table. You can also filter the results by result type or policy name.

		All packs All results	Enter a policy name.	Q
Policy	Result	Suggestion	Updated	Operation
Shared API Gateway should be accessed via HTTPS	Passed	Exercise caution when performing this operation. After you enable \ldots	Nov 30, 2022 01:35:09 GMT+08:00	Details
Dedicated API Gateway should be accessed via HTTPS	Passed	Exercise caution when performing this operation. After you enable \ldots	Nov 30, 2022 01:34:13 GMT+08:00	Details
APIs in shared API Gateway should be bound to signature keys	Passed	Perform the following operations to bind a signature key to an API a	Nov 30, 2022 01:34:41 GMT+08:00	Details
APIs in dedicated API Gateway should be bound to signature keys	Passed	Perform the following operations to bind a signature key to an API a	Nov 30, 2022 01:34:41 GMT+08:00	Details
API gateways should be deployed in regions in the Chinese mainland	Passed	Migrate the API gateway that failed the check to a region in the Chi	Nov 30, 2022 01:35:57 GMT+08:00	Details
ACL rules of shared API gateways should not allow access from 0.0	Passed	Configure a new ACL rule based on your API demand, and then del	Nov 30, 2022 01:30:48 GMT+08:00	Details
ACL rules of dedicated API gateways should not allow access from	Passed	Configure a new ACL rule for the API gateway that failed the check \ldots	Nov 30, 2022 01:30:47 GMT+08:00	Details
The logging function should be enabled for the exclusive API gateway	Passed	Enable the logging function for a dedicated gateway. The operation	Nov 30, 2022 01:30:50 GMT+08:00	Details
An ACL should be bound to APIs of shared API Gateway	Passed	If the required APIs need to be bound to an ACL for minimum acces	Nov 30, 2022 01:30:47 GMT+08:00	Details
An ACL should be bound to APIs of exclusive API Gateway	Passed	If the required APIs need to be bound to an ACL for minimum acces	Nov 30, 2022 01:30:02 GMT+08:00	Details
10 • Total Records: 54 < 1 2 3 4 5 6 >				

Figure 6-19 Selecting a compliance pack

• To view the check result of a policy over a resource, select the corresponding resource from the filter box in the upper part, and then select the corresponding compliance pack in the upper part of the table.

Figure 6-20 Viewing th	e result o	of a po	licy over a res	ource	
Policy Check					
All resources					
Check Result			Top 5 Risks 🕜		
			MFA should be enabled for all IAM users		1
			EVS disks must be encrypted		
77.78%	 Passed 42 terms (2) Failed 12 terms (2) 		ECS instance should not be bound to an El	P	:
Pass Rate	Check failed 0 term		Rotation should be enabled for all keys		:
			Network ACLs for subnets should be enable	d	:
		2 All pa	cks	 Enter a policy name. 	QC
Policy	Result Sug	gestion		Updated	Operation
Shared API Gateway should be accessed via HTTPS	Passed Exe	rcise caution when pe	rforming this operation. After you enable	Nov 30, 2022 01:35:09 GMT+08:00	Details

Exercise caution when performing this operation. After you enable \ldots

Nov 30, 2022 01:34:13 GMT+08:00

Step 5 In the policy table, click Details in the Operation column of a policy to go to the policy check result page and view improvement suggestions, as shown in Figure 6-21.

Passed

Dedicated API Gateway should be accessed via HTTPS

Figure 6-21 Details of a check

Policy	Shared	Shared API Gateway should be accessed via HTTPS								
Result	Faile	1								
Description	HTTPS	can enhance data tra	ansfer se	ecurity. This policy cl	necks w	whether API Gateway	y is ac	cessed via HTTPS. If it is, your service pass	es the check.	
Suggestion										
Total	1	Passed	0	Failed	1	Check failed	0			
Resource Nar	ne/ID							source Type	Result	Updated
HttpEchoDem	lemo							G:shared_api	 Failed 	Nov 30, 2022 01:36:11 GMT+08:00

NOTE

SecMaster automatically scans the resources at 01:30 a.m. every day and generates the scanning results.

----End

6.10 Downloading a Compliance Report

Scenario

Security Governance provides security compliance reports. You can download the reports to learn of how well your services comply with mainstream security standards.

Prerequisites

You have subscribed to the security compliance packs. For details, see **Subscribing to Compliance Packs**.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-22 Subscriptions page

SecMaster	Dashboard			
Security Overview	Process Flow			
Workspaces 👻	-1	-2	-3	-4
Purchased Resources Security	Authorize Service	Subscribe to Compliance Packs	Policy Check Compass checks your service compliance.	View Result Compass will evaluate your service compliance
Governance(beta)	Authorize Compass to access your cloud services.	Compliance packs contain security regulations and standards.	View Result	based on the policy check and evaluation results.
Compliance Overview(beta)	Authorize	Subscribe	Evaluation Use our checklist to evaluate your service	View Result
Subscriptions(beta)			compliance. Evaluate	
Policies(beta)				
	•			

Step 4 On the Subscriptions page, click Download Report in the Operation column.

The system will download the specified compliance report to a local path.

----End

6.11 Unsubscribing from a Compliance Pack

Scenario

If you need to cancel the subscription to a compliance pack, you can unsubscribe from it on the **Subscriptions** page.

Prerequisites

You have subscribed to the security compliance packs. For details, see **Subscribing to Compliance Packs**.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-23 Subscriptions page



- **Step 4** On the **Subscriptions** page, locate the row that contains the security compliance pack to be unsubscribed from, click **Unsubscribe** in the **Operation** column.
- **Step 5** In the displayed dialog box, click **OK**.

D NOTE

Your service compliance data related to this pack will be deleted and cannot be restored. Exercise caution when performing this operation.

----End

7 Security Situation

7.1 Situation Overview

The **Situation Overview** page displays the overall security assessment of resources in the current workspace in real time. You will learn of asset security, including the asset security assessment results, security monitoring results, and security trend.

Procedure

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

Figure 7-1 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspaces	Crede Workspace $\label{eq:constraint} \overline{\nabla} \ \text{Inter a more and layouth for search}.$				C
Purchased Resources Security Governance(beta)	Commit bound D add077 bdda12 Region Project- More Not housed	Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 instan 0	Selected Spaces C 🛞 // Indicat 0 Playbo 0

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

<								E Get Star
Security Situation Large Screen Reports Task Center Resource Manager Threet Operations Threet Operations	Security Score		O Total Assets Our system should be harden Handle Now Oteck Age		0 convers currly risks have been detected.		Your Security Score over Time)st 7 days Posts 100 75 25 0 11/15 11/16 11/17 11/18	
Security Orchestration 👻 Settings 👻	Security Monitoring			_			FAQs View More	
	Threat Alarms[Last 7 days] Critical 0 High 0	0 Vulnera Others 0 High 0	bilities Medium 0	O Others 0	Abnormal Baseline Settings	21 Others 13	What is SecMaster?	What Are Differences Between SecMaster and Other Security Service?
	Top 5 Real-Time Unsafe Baseline Set					View More	What Are Data Sources of SecMaster?	How Can I Update My Security Score in SecMaster?
	Subject	• High	Affected Reso	surce Number	Tripgered Nov 20, 2023 00:00:07 GM	T+08:00	Why is There Little or No Atlack Data	Why Is Attack Data in SecMaster
	Security group inbound rules	• High	3		Nov 21, 2023 00:03:33 GM	T+08:00	in SecMaster?	Inconsistent with That in WAF or HSS?
	Open high-risk and remote management p	• High	3		Nov 20, 2023 00:00:22 GM Nov 20, 2023 00:00:16 GM		Can I Use SecMaster Across Accounts?	What is a Brute-Force Attack Event?

Figure 7-2 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.

Paramete r	Refer ence Perio d	Update Frequency	Description
Security Score	Real- time	 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.
Vulnerabil ities	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.

Table 7-1 Situation Overview

Paramete r	Refer ence Perio d	Update Frequency	Description
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 based on the SecMaster edition you are using. You can quickly understand the unprocessed risks and their threats to your assets. **Figure 7-3** shows an example.

Figure 7-3 Security Score

Security Score		0	0	0
80		Total Assets	High-risk Assets	
Updated 2023/11/2*			hardened as several security risks	nave been delected.
	1 02.00.03	Handle Now C	heck Again	

- 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.

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 cloud assets in real time and scores your assets.

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.

Severit y	Security Score	Description
Secure	100	Congratulations. Your assets are secure.
Informa tional	80 ≤ Security Score < 100	Your system should be hardened as several security risks have been detected.
Low	60 ≤ Security Score < 80	Your system should be hardened in a timely manner as too many security risks have been detected.

 Table 7-2 Security score table

Severit y	Security Score	Description
Medium	40 ≤ Security Score < 60	Your system should be hardened, or your assets will be vulnerable to attacks.
High	20 ≤ Security Score < 40	Detected risks should be handled immediately, or your assets will be vulnerable to attacks.
Critical	0≤ Security Score <20	Detected risks should be handled immediately, or your assets may be attacked.

• Unscored Check Items

 Table 7-3 lists the security check items and corresponding points.

Table	7-3	Unscored	check items	
		enscorea	chiech iteriis	

Category	Unscored Item	Points	Suggestion	Maximu m Unscored Point
Enabling of security services	Security-related services not enabled	-	Enable security- related services.	30
Complianc e 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		
Vulnerabili ties	Critical vulnerabilities not fixed	10	Fix vulnerabilities by referring corresponding	20
	High-risk vulnerabilities not fixed	5	suggestions and start a scan again. The security score will be updated.	

Category	Unscored Item	Points	Suggestion	Maximu m Unscored Point
	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	30
	High-risk alerts not fixed	5	suggestions. The security score will be updated accordingly.	
	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.

- gaile - Coocarrey more may	Figure	7-4	Security	Monitoring
------------------------------	--------	-----	----------	------------

Security Monitoring					
Threat Alarms[Last 7 days]	10K+	Vulnerabilities[Last 7 days]	141	Abnormal Baseline Settings	256
Critical 2 High 3	Others 13711	High 20 Medium 115	Others 6	Critical 0 High 108	Others 148

Parameter	Description		
Threat Alarms	for the last 7 days. of unhandled threa	You can quickly lear t alerts and the nun	at alerts in a workspace of the total number of rof vulnerabilities odated every 5 minutes
	Risk severity lev	els:	
			our workloads, and yo dle the alert in a time
		ıld view alert details	nts on your workloads, and handle the alert
	medium-risk,	ms, and you should	that are marked as national alerts detecte view alert details and
		details of top 5 threa hreat Alarms panel	at alerts for the last 7
		details of those thre ame, severity, asset	eats, including the name, and discovery
		available here, no th r the last 7 days.	reat alerts are
	view more al query alert ir	erts. You can also cu	o the Alerts page and stomize filter criteria t ils about how to view
	Figure 7-5 View	ing real-time alerts	
	Top 5 Real-Time Threat Events 🛛 🛞 Ch	ecking	View More
	Subject Lev		Triggered
		edium ecs t	2022-01-12T09:58:25.857+08:
		edium ecs	2022-01-11T22:19:44.295+08:
	Local File Inclusion M	edium ecs- t	2022-01-11T20:45:53.757+08:

Table 7-4 Security Monitoring parameters

Parameter	Description	
Vulnerabilities	This panel displays the top five total number of unfixed vulner workspace for the last 7 days. total number of unfixed vulner vulnerabilities at each severity every 5 minutes.	rabilities in your assets in a You can quickly learn of the rabilities and the number of
	Risk severity levels:	
		bilities on your workloads, and bility details and handle them
	 Medium: There are abno workloads, and you shou handle the vulnerability 	ıld view vulnerability details ar
	low-risk or informationa	ncidents that are marked as l in your systems, and you v details and take necessary
	• When you click the Top 5 V system displays top 5 vulne	
		e based on the number of host ne vulnerability ranked the first
	when the hosts have Ho version 2.0 installed. If n	Top 5 Vulnerability Types onl st Security Service (HSS) Agen o data is displayed or you wan ty types, upgrade Agent from
	Figure 7-6 Top 5 Vulnerabi	lity Types
	Top 5 Vulnerability Types Top 5 Real-Time Vu	lnerabilities 🕥 Checking
	Vulnerability ID	Vulnerable Servers
	CVE-2C	1
	CVE-20	1
	CVE-20	1
	CVE-2	1
	CVE-20%	1
	 Click Top 5 Real-Time Vuln displays the top 5 vulnerabi You can quickly view vulner 	nerabilities tab. The system ility incidents for the last 7 day rability details.
	severity, asset name, and	h as the vulnerability name, I discovery time.

Parameter	Description		
	 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. For details, see Viewing Vulnerability Details. 		
	Details. Figure 7-7 Viewing real-time vulnerabilities		
	Details. Figure 7-7 Viewing real-time vulnerabilities Top 5 Vulnerability Types Top 5 Real-Time Vulnerabilities Checking		
	Details. Figure 7-7 Viewing real-time vulnerabilities Top 5 Vulnerability Types Top 5 Real-Time Vulnerabilities Checking Subject Level Asset Name Triggered		
	Details. Figure 7-7 Viewing real-time vulnerabilities Top 5 Vulnerability Types Top 5 Real-Time Vulnerabilities Checking Subject Level Asset Name Triggered EulerOS-SA- (expat securit © Critical concort 2 2022-07-05T0522:10.057+08.00		
	Details. Figure 7-7 Viewing real-time vulnerabilities Top 5 Vulnerability Types Top 5 Real-Time Vulnerabilitie Checking Subject Level Asset Name Triggered EulerOS-SA- expansion - Critical concort 2 2022-07-03170525:10.057+0800 EulerOS-SA- (heroid securi Critical concort 2 2022-07-03170523:10.057+0800		

Parameter	Description			
Abnormal Baseline Settings	This panel displays the total number of compliance violatio 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.			
	Risk severity levels:			
	 Critical: There are intrusions to your workloads, and you should view details about compliance risks and handle them in a timely manner. 			
	 High: There are abnormal incidents on your workloads, and you should view details about compliance risks and handle them in a timely manner. 			
	 Others: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view details about compliance risks and take necessary actions. 			
	• To quickly view details of top 5 abnormal compliance risks discovered for the last 30 days, click the Abnormal Baseline Settings panel.			
	 You can view details of the top compliance risks discovered in the latest check, such as check item name, severity, asset name, and discovery time. 			
	 If no data is available, no compliance violations are detected for the last 30 days. 			
	 You can click View More to go to the Baseline Inspection page and view more compliance risks. You can also customize filter criteria to make an advanced search. For details, see Viewing Baseline Inspection Results. 			
	Figure 7-8 Viewing compliance risks			
	Top 5 Real-Time Unsafe Baseline Settings Checking View More			
	Subject Level Asset Name Triggered OBS bucket server-side encry • Medium obs 2022-01-11700.0046.903+08			
	Log metric filtering and alarm Medium su 2022-01-11700.00:46.903+08			
	Log metric filtering and alarm Medium sul 2022-01-11T00:00-46.903+08			
	Log metric filtering and alarm Medium vpc 2022-01-11T00.00:46.903+08			
	Log metric filtering and alarm Medium vpc- 2022-01-11T00:00:46:903+08:			

Your Security Score over Time

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

Figure 7-9 Your Security Score over Time



7.2 Large Screen

7.2.1 Overall Situation Screen

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

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

Prerequisites

You have enabled Large Screen. For details, see Purchasing Value-Added Packages.

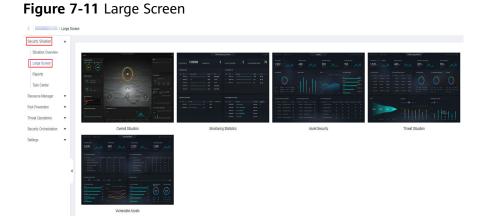
Procedure

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

Figure 7-10 Workspace	management page
-----------------------	-----------------

SecMaster	Management ③				D Process
Security Overview Workspaces	Could V001spec $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Constant Report Constant Report Constant Report Constant Report Project- Mare Not house.	 Incidents 0 Assets 0 	♥ Vulner 0	O Alerts 0 instan 0	Selected Spaces C ⊗ indicat 0 S Playbo 0

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



Step 5 Click the **Overall Situation** screen. The large screen for overall situation awareness is displayed. Figure 7-12 shows an example.

This screen includes many graphs.

Figure 7-12 Overall Situation screen



----End

Security Score

The security score of the current assets is displayed, as shown in Figure 7-13.

Paramete r	Refer ence Perio d	Update Frequency	Description
Security Score	Real- time	 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. 	 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. 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.

Figure 7-13 Security Score



Alert Statistics

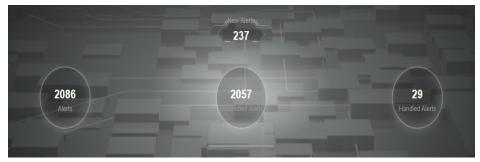
The alert statistics of interconnected services are displayed, as shown in **Figure 7-14**.

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

Parameter	Referenc e Period	Update Frequenc Y	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.
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.

Table 7-6 Alert statistics

Figure 7-14 Alert Statistics

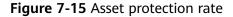


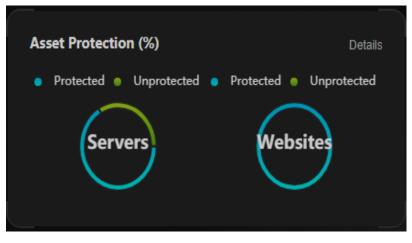
Asset Protection

The protection status of servers and websites is displayed, including the proportion of protected and unprotected assets, as shown in **Figure 7-15**. You can hover the cursor over a module to view the number of protected/unprotected assets.

Parameter	Referenc e Period	Update Frequenc Y	Description		
Asset Protection (%)	Last 7 days	5 minutes	The protection status of servers and websites is displayed, including the proportion of protected and unprotected assets.		
			 Servers: numbers of ECSs protected and not protected by HSS 		
			 Websites: Numbers of websites protected and not protected by WAF 		

Table 7-7 Asset protection rate





Baseline Inspection

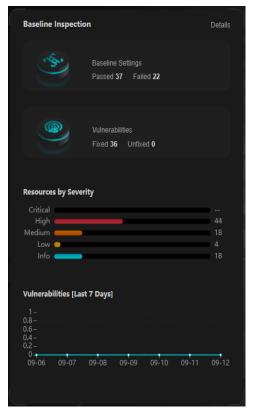
The fixing status of the baseline configuration and vulnerabilities of your assets, distribution of risky resources, and vulnerability fixing trend within seven days are displayed, as shown in **Figure 7-16**.

- 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 7-8 Baseline inspection

Parameter	Referenc e Period	Update Frequenc Y	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.

Figure 7-16 Baseline Inspection



Recent Threats

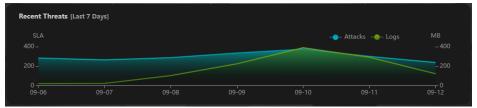
The numbers of threatened assets and security logs reported every day in the last seven days are displayed, as shown in **Figure 7-17**.

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.

Parameter	Referenc e Period	Update Frequenc Y	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 Operation >
			Alerts in the current workspace.
Logs	Last 7 days	5 minutes	Number of security logs reported every day in the last seven days.

 Table 7-9
 Recent threats

Figure 7-17 Recent threats



To-Dos

The to-do items in the current workspace are displayed, as shown in Figure 7-18.

Table 7-10 To-dos

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

Figure 7-18 To-Dos



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, as shown in **Figure 7-19**.

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

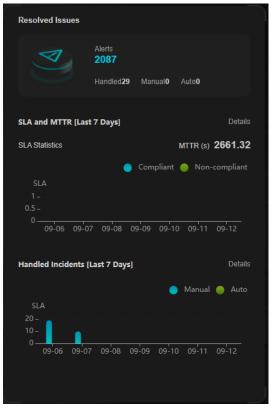
Parameter		Refer ence Perio d	Upda te Frequ ency	Description
Alerts	Alerts	Last 7 days	5 minut	Number of new alerts generated in the last seven days.
	Handled		es	Number of alerts that have been cleared in the last seven days.
	Manual			Number of alerts that were handled within the SLA time in the last seven days.
				Alerts handled as planned and earlier than planned are counted.

Table 7-11 Resolved issues

Parameter		Refer ence Perio d	Upda te Frequ ency	Description
	Auto			Number of alerts that were automatically handled by SecMaster playbooks. 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.
SLA and MTTR [Last 7 Days]	SLA Statistics	Last 7 days	5 minut es	 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 ≤ SLA, it indicates the alert was handled in a timely manner. Otherwise, the alert fails to meet SLA requirements. Compliant: The alert closure time is the same as or earlier than planned. Non-compliant: The alert closure time is later than planned.
	MTTR			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.

Parameter	Refer ence Perio d	Upda te Frequ ency	Description
Handled Incidents [Last 7 Days]	Last 7 days	5 minut es	 Total number of alerts handled in the last seven days. Manual: Number of alerts manually closed on the Alerts page. Auto: Number of alerts automatically closed by SecMaster playbooks. 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.

Figure 7-19 Resolved issues



7.2.2 Monitoring Statistics Screen

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of SecMaster on big

screens to achieve better demonstration effect. It is not ideal to just zoom in the console. Now, SecMaster **Large Screen** is a good choice for you to display the service console on bigger screens for a better visual effect.

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

Prerequisites

You have enabled Large Screen. For details, see Purchasing Value-Added Packages.

Procedure

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

Figure 7-20 Workspace management page

SecMaster	Management (3)				🕞 Process
Security Overview Workspaces	Credit Workspeen T later a name and layword for search.				C
Purchased Resources Security Governance(beta)	General access General	 Incidents 0 Assets 0 	♥ Vulner 0 i Securl 0	O Alerts 0 instan0	Selected Spaces C ⑧ iv Indicat 0 B Playbo 0

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

 Stands Unique Control
 Image: Stands Unique Control
 <t

Figure 7-21 Large Screen

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

This screen includes many graphs.

						Moi	nitoring	Statistics					
Unhanc	fled Alerts		1508	nhandled Incid	lents		3	Unhand	led Vulnerabilities	5	Unhandled Ba	seline Settings	1
Unhand	died Alerts							Unhand	led Incidents				
	Sep 12, 2023 1			e Medium					2022/12/01 23:41			undefined	
	Sep 12, 2023 1	r.13		• Medium					2023/01/05 16:53			• Warning	
	Sep 12, 2023 1	2.08		• Medium					2023/01/05 16:59			• Warning	
	Sep 12, 2023 1	r.03		- Medium									
	Sep 12, 2023 1	153		e Medium									
Unhanc	fled Vulnerabilitic							Unhand	led Baseline Setting				
	2022/12/01 11:44			windows	- Low				2023/02/07 20:51			Automatic check	
	2022/12/01 11:44			App	- Low				2023/02/07 00:00			Automatic check	
	2022/12/01 11:44			App	- Low				2023/02/07 00:00			Automatic check	
	2022/12/01 11:44			web cms	- Low				2023/02/07 00:00			Automatic check	
	2022/12/01 11:44			linux	- Low				2023/02/07 00:00			Automatic check	

Figure 7-22 Monitoring Statistics Large Screen

----End

Monitoring Statistics Overview

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

Table 7-12 Monitoring	Statistics Overview
-----------------------	---------------------

Parameter	Statistica l Period	Update Frequenc Y	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.

Figure 7-23 Monitoring Statistics Overview

Unhandled Alarms 1508	Unhandled Events	3	Unhandled Vulnerabilities	5	Unhandled Baseline Settings	21
-----------------------	------------------	---	---------------------------	---	-----------------------------	----

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	7-13	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.

Figure 7-24 Unhandled Alerts

Unhandl	led Alerts				
No.	Discovered	Description	Severity	Туре	
1	Sep 12, 2023 17:18		Medium		
2	Sep 12, 2023 17:13		Medium		
3	Sep 12, 2023 17:08		Medium		
4	Sep 12, 2023 17:03		🖕 Medium		
5	Sep 12, 2023 16:53		e Medium		

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.

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.

Table 7-14 Unhandled Incidents

Figure 7-25 Unhandled Incidents

Unhand	led Incidents			
No.	Discovered	Description	Severity	Туре
	2022/12/01 23:41	[CFW] [2022-11-10 11:32:01]	undefined	
2	2023/01/05 16:53		• Warning	-
3	2023/01/05 16:59		• Warning	

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.

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.

 Table 7-15 Unhandled Vulnerabilities

Figure 7-26 Unhandled Vulnerabilities

Unhand	dled Vulnerabilitie	s					
	Discovered	Description			Туре	Severity	Affected Assets
	2022/12/01 11:44		date		windows	o Low	
2	2022/12/01 11:44				Арр	o Low	4
3	2022/12/01 11:44				Арр	- Low	4
4	2022/12/01 11:44		update		web-cms	- Low	
5	2022/12/01 11:44			security up	linux	Low	

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.

Parameter	Statistics Cycle	Update Frequenc Y	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.

Table 7-16 Unh	andled Baseline Settings
----------------	--------------------------

Figure 7-27 Unhandled Baseline Settings

in the second second				
Unhand	led Baseline Setting	s		
No.	Discovered	Description	Check Method	Vulnerable Resources
	2023/02/07 20:51	IAM user login protection	Automatic check	29
2	2023/02/07 00:00	Enabling of EVS disk encryption	Automatic check	6
3	2023/02/07 00:00	CBR disk backup availability	Automatic check	5
4	2023/02/07 00:00	Log metric filtering and alarm events (subnet changes)	Automatic check	4
5	2023/02/07 00:00	Log metric filtering and alarm events (security group changes)	Automatic check	3

7.2.3 Asset Security Screen

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

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

Prerequisites

You have enabled **Large Screen**. For details, see **Purchasing Value-Added Packages**.

Procedure

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

Figure 7-28 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Centre Wantappea If later a name and layound for sounds.				C
Agenues Purchased Resources Security Governance(beta) ▼	Orman second O additr7 dolar2 Region Project- Nov Not factor.	Incidents 0	♥ Vuiner 0 ⊜ Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C i Indicat 0 Playbo 0

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

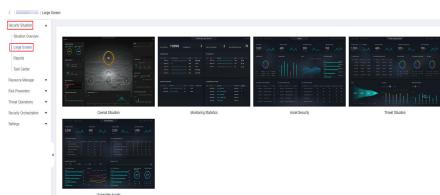


Figure 7-29 Large Screen

Step 5 Click the **Asset Security** image to go to the large screen for assets.

This screen includes many graphs.

Figure 7-30 Asset Security Screen

User Name s Workspace-SecMaster	Asset	Security	O Local Time Sep 12, 2023 19 24 🔰 🛞 Statistics Cycle: 7 Days
Assets 73 Last Week + 3	Attacked Assets 2 Last Week + 6	Unprotected Assets 40 Last Week + 2	Vulnerable Assets 47 Last Week = 36
Austicity Type	Protection by Asset Type (%)		barg yang naka (00 barg) 14
Top 5 Assets with the Most Vulnerabilities		Top 5 Departments with the Highest Protection Rate	
No. Asset IP Address D			et protection rate WAF protection rate Host protection rate Vulnerability Fix Rate
		1 Test 100 2 Security 102	

----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	7-17	Asset	Security	Screen
-------	------	-------	----------	--------

Parameter	Statistica l Period	Update Frequenc Y	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.

Parameter	Statistica l Period	Update Frequenc Y	Description
Unprotected Assets	Real-time	Hourly	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.
			Unprotected assets include the assets managed on the Resource Manager page and with no corresponding security controls enabled.
Assets with Vulnerabilities or Unsafe Settings	Real-time	Hourly	These assets include assets affected by vulnerabilities and assets have unsafe settings discovered during baseline inspection. The duplicated assets are counted only once.
			The vulnerability data comes from Risk Prevention > Vulnerabilities , and the baseline inspection data comes from Risk Prevention > Baseline Inspection > Resources to Check .

Figure 7-31 Asset Security Screen



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 7-18 Asset Distribution

Parameter	Statistica l Period	Update Frequenc Y	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.

Parameter	Statistica l Period	Update Frequenc Y	Description
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	Last 7 days	Hourly	Top 5 attacked assets in the last seven days and the number of attacks.
Assets			The data comes from Threat Operations > Alerts . You can view details on this page.

Figure 7-32 Asset Distribution

Assets by Type	Protection by Asset Type (%)	Asset Changes	Top 5 Attacked Assets			
	5. 100 75		hei Linus ander 1996 in CS27) 			
Hest 40 (54,79%) EP 22 (30,14%) Webute 4 (54,89%) V7C 6 (8,22%) P 0 (0,00%) Device 0 (0,00%)	59		abor 1995; 0527)			
 Database 1 (1.37%) 	0 - Hoot Website Database BP VPC					

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 7-19 Top 5 Assets with the Most Vulnerabilities and Top 5 Departments with	
the Highest Protection Rate	

Parameter	Statistica l Period	Update Frequenc Y	Description
Top 5 Assets with the Most Vulnerabilities	Real-time	Hourly	Top 5 assets with the most vulnerabilities in different departments. 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.

Parameter	Statistica l Period	Update Frequenc Y	Description
Top 5 Departments with the Highest Protection Rate	Real-time	Hourly	This graphs list the 5 departments that have the highest protection rate, in descending order.
			Note that the assets on Resource Manager must have department details provided, or the assets cannot be counted toward this rate.

Figure 7-33 Top 5 Assets with the Most Vulnerabilities and Top 5 Departments with the Highest Protection Rate

TOP 37ASSES WITH UK	Top 5 Assets with the Most Vulnerabilities			Top 5 Departments with the Highest Protection Rate						
No.										
					Test	100%	100%	100%	100%	
					Security	100%	100%	100%	0%	

7.2.4 Threat Situation Screen

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

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

Prerequisites

You have enabled **Large Screen**. For details, see **Purchasing Value-Added Packages**.

Procedure

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

Figure 7-34 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspaces	Credit Workspace $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Constant Constant Const Constant Const Constant Con	Incidents 0 Assets 0	♥ Vulner () ⊜ Securi ()	Alerts 0	Selected Spaces C 🛞 V Indicat 0 Playbo 0

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

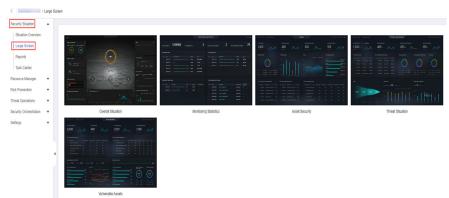


Figure 7-35 Large Screen

Step 5 Click the **Threat Situation** image to go to the information page.

This screen includes many graphs.

User Name	Threat Situation	O Local Time Sep 12, 2023 19.48 ☉ Statistics Cycle: 7 Days
Network Attacks O Last Week, • 0	Application Attacks 4 Latt Views + 4	Server Attacks 422721 Last Vitres + 3448
Top 51 Minland Allack Sources No. Source IP Attack Source Region Attachs	Rg S I Network Altack Types 1 2 4 2 13 1 1 2 4 2 13 1 1 10 1 1 10 1 1 10 1 1 10 1 1 10 1 1 10 1 1 10 1 1 10 1 1 10 1 1 10 1 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10 1 10	Iop 5 Application Attack Types Iop 5 Server Attacks Types • SOLEA 1 (600%) • SOLEA 2 (600%)
Aret Statistics 96077 42725 21 Leg parameter Thesais Alefs	LogAnagos Loganas 165 by a + 165 andreadide scarred + 165 date + 000 anosta 165 by a + 165 andreadide scarred + 165 date + 000 anosta 100 andread + 100 anosta 100 anosta	Threads by Model Hotom, 77 9 12 23 24 25 26 26 20 10 10 10 10 10 10 10 10 10 1

Figure 7-36 Threat Situation screen

----End

Threat Situation screen

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

Parameter		Statis tical Perio d	Upda te Frequ ency	Description
Network Attacks	Occurrenc es	Last 7 days	Hourl y	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.
Applicatio n Attacks	Occurrenc es	Last 7 days	Hourl y	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	Occurrenc es	Last 7 days	Hourl y	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.

 Table 7-20 Threat Situation screen

Figure 7-37 Threat Situation screen

Network Attacks	Application Attacks	Server Attacks
64 Last Week * 22	O Last Week 🗸 0	51874

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.

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.

Parameter	Statistica l Period	Update Frequenc Y	Description
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.

Figure 7-38 Attack source distribution

Top 5 Network	Attack Sources		Top 5 Ne	Top 5 Network Attack Types			
No. Sou	rce IP Attack Source R	egion Attacks		Source IP	Attack Source Region	Attacks	
				242		4	
			2	1.36	_		

Attacks by Type

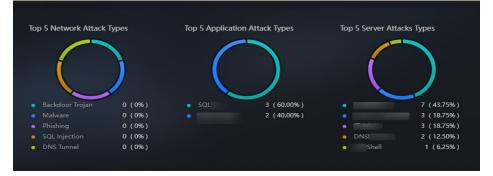
This graph shows top 5 network attack types, top 5 application attack types, and server attack types.

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.

Table 7-22 Attacks by Type

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

Figure 7-39 Attack type distribution



Threat Situation Statistics

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

Parameter		Statis tical Perio d	Upda te Frequ ency	Description
Alert Statistics	Logs	Last 7 days	Hourl y	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.

Table 7-23 Threat Situation Statistics

Parameter		Statis tical Perio d	Upda te Frequ ency	Description
	Incidents			This number reflects incidents collected in Threat Operations > Incidents for the last seven days.
Log Analysis	Log volume	Last 7 days	Hourl y	Total volume network, application, and server access logs for the last seven days, in MB.
	РоР			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	Hourl y	The number includes the models in Threat Operations > Intelligent Modeling.
	Statistical table	Last 7 days	Hourl y	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.

Figure 7-40 Threat situation statistics



7.2.5 Vulnerable Assets Screen

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of SecMaster on big screens to achieve better demonstration effect. It is not ideal to just zoom in the

console. Now, SecMaster **Large Screen** is a good choice for you to display the service console on bigger screens for a better visual effect.

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

Prerequisites

You have enabled Large Screen. For details, see Purchasing Value-Added Packages.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-41 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspeces Management Agencies	Could Workspace $\overline{V} \mbox{ Inter a more and layoutd for search}.$				C Q
Purchased Resources Security Governance(beta)	December 2000 Decembe	 ∋ incidents 0 ○ Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C i Indicat 0 B Playbo 0

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

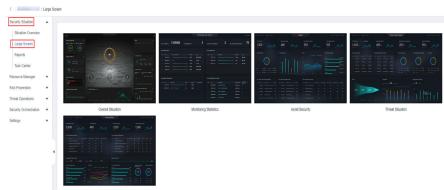


Figure 7-42 Large Screen

Step 5 Click the **Vulnerable Assets** image to go to the information page. This screen includes many graphs.



Figure 7-43 Vulnerable Assets Screen

----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.

Parameter	Statistica l Period	Update Frequenc Y	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 is not enabled.

Table 7-24 Vulnerable Assets Overview

Figure 7-44 Vulnerable Assets Screen



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.

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.

Table 7-25 Vulnerable departments

Figure 7-45 Top 5 Vulnerable Departments

	Department	Vulnerability Risk	Vulnerabilities	Unprotected
	Test	2	0	0
2	Security		39	0

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.

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.

 Table 7-26 Department with the most unprotected assets

Figure 7-46 Top 5 Department with the Most Unprotected Assets

	Department	Policies Not Covered	DBSS	WAF	DDos		CFW
Т	Test	0	0	0	0	0	0
s	Security	0	0	0	0	0	0

Vulnerability Fix Rate

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

Parameter	Statistica l Period	Update Frequenc Y	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.

Figure 7-47 Vulnerability fixing rate

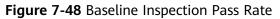
Vulnerability Types Vulnerability Changes • High Risk • Medium Risk • Low Risk • Linux 68 Windows 34	Vulnerability Fix Rate High 36.11%	 Medium 16.07% 	• Low 20.00% • Tip 100.00%	
			High Risk Medium Risk Low Risk	
Windows 34			68	
	Windows		34	
Application 5 0 09-06 09-07 09-08 09-09 09-11 05	Application		U	9-12

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.

Parameter	Statistica l Period	Update Frequenc Y	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.

Table 7-28 Baseline Inspection Pass Rate





7.3 Reports

7.3.1 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.

Limitations and Constraints

A maximum of 10 security reports (including daily, weekly, and monthly reports) can be created in a single workspace of a single account.

Prerequisites

You have purchased the SecMaster professional edition and the edition is within the validity period.

Creating a Report

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

Figure 7-49 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspaces	Crede Workspace $\label{eq:constraint} \overline{\nabla} \mbox{ Inter a more and layouth for search.}$				C
Purchased Resources Security Governance(beta)	eterne accest • add977 bide12 Region Project- Nov Net hold.	S Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

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

Figure 7-50 Reports

<	/ Repo	rts		
Security Situation Situation Overview	•	Type: All 🔹 Enable Status: All 🔹 🏹 Add filter		×Q
Large Screen Reports Task Center		+		
Resource Manager Risk Prevention	• •		Edit Copy Delete	
Threat Operations	•			
Security Orchestration	*			
Settings	*			

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

Step 6 Configure basic information of the report.

Parameter	Description
Report Name	Name of the report you want to create.
Schedule	Select a report type.
	• Daily : SecMaster collects security information from 0:00 to 24:00 of the previous day by default.
	• Weekly: SecMaster collects statistics on security information from 00:00 on Monday to 24:00 on Sunday of the previous week.
	• Monthly : SecMaster collects statistics on security information from 00:00 on the first day to 24:00 on the last day of the previous month.
	• Custom : Customize a time range.
Data Scope	This field displays the data scope based on Schedule you specified.
	If you select Daily , Weekly , or Monthly for Schedule , the system displays the report data scope accordingly.
Schedule	If you select Daily , Weekly , or Monthly for Schedule , you still need to set when you want SecMaster to set reports.
	• Daily : By default, SecMaster sends a report that includes security information generated from 00:00:00 to 23:59:59 on the previous day every day at the time you specify.
	• Weekly: Set the time when the weekly report is sent. By default, the system sends a report for the data from 00:00 last Monday to 24:00 last Sunday.
	• Monthly : By default, the system sends a report that includes the security information for the previous month on a monthly basis at the time you specify.
Send Interval	If you select Custom for Schedule , you need to set a report send interval.
Send Rule	If you select Custom for Schedule , you need to set when to send the report and the data scope.
	You can set up to five rules for sending reports.
Email Subject	Set the subject of the email for sending the report.
Recipient Email	Add the email address of each recipient.
	• You can add up to 100 email addresses.
	 Separate multiple email addresses with commas (,). Example: test01@example.com,test02@example.com

Parameter	Description
(Optional) Copy To	Add the email address of each recipient you want to copy the report to.
	You can add up to 100 email addresses.
	• Separate multiple email addresses with commas (,). Example: test03@example.com,test04@example.com
(Optional) Remarks	Remarks for the security report.

- **Step 7** Click **Next: Report Choose** in the upper right corner. The **Report Selection** page is displayed.
- **Step 8** In the existing report layout area on the left, select a report layout. After selecting, you can preview the report layout in the right pane.

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

- Downloading a report
 - a. Click \blacksquare in the upper left corner of the preview page on the right.
 - b. In the displayed dialog box, select a report format, and click **OK**. The system automatically downloads the report to the local PC.
- Viewing a report in full screen: Click 🖳 in the upper left corner of the preview page on the right.
- **Step 9** Click **Complete** in the lower right corner. On the displayed **Reports** page, view the created report.

----End

Copying a Report

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

Figure 7-51	Workspace	management page
-------------	-----------	-----------------

SecMaster	Management ③				D Process
Security Overview Workspaces	Could V001spec $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Constant Report Constant Report Constant Report Constant Report Report Report Report Report Report	 Incidents 0 Assets 0 	♥ Vulner 0	O Alerts 0 instan 0	Selected Spaces C ⊗ indicat 0 S Playbo 0

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

Figure 7-52 Reports

<	/ Rep	orts			
Security Situation Situation Overview	*	Type: All 💿 Enable Status: All 💿 🕅 Add filter		× Q	С
Large Screen					
Reports			Enable		
Task Center		+			
Resource Manager	*		Edit Copy Delete		
Risk Prevention	*				
Threat Operations	*				
Security Orchestration	*				
Settings	*				

- **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.
 - Downloading a report
 - a. Click $\stackrel{\checkmark}{\bigsqcup}$ in the upper left corner of the preview page on the right.
 - b. In the displayed dialog box, select a report format, and click **OK**. The system automatically downloads the report to the local PC.
 - Viewing a report in full screen: Click 🖃 in the upper left corner of the preview page on the right.
- **Step 8** Click **Complete** in the lower right corner. On the displayed **Reports** page, view the newly created report.

----End

7.3.2 Viewing a Security Report

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

Figure 7-53 Workspace management page

SecMaster	Management ①				📝 Process
Security Overview Workspaces	Create Wintegace $\overline{\nabla} \ \mbox{Interse and largered for search}.$				C Q
Purchased Resources Security Governance(beta)	D add9777 Sala (2 Report Preport- More More Marked	Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 S Instan 0	Selected Spaces C i Indicat 0 E Playto 0

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

Figure 7-54 Reports < / / Reports Security Situation x Q C Large Screen Enable 🔵 Reports Task Center + Resource Manager Edil isk Prevention Threat Operations Recurity Orchestration *

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

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

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

----End

Content in the Daily Report Template

Table 7-30 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.
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.

Darameter	Description
Parameter	Description
Baseline Inspection	Displays the statistics of the latest baseline check, including the following information:
	The number of baseline check items
	Number of compliance check items in the latest baseline check
	Non-compliant check items in the latest baseline check
Security Vulnerabilities	Displays the vulnerability statistics of the accessed cloud services on the previous day , including the following information:
	Number of vulnerabilities
	Number of unfixed vulnerabilities
Policy Coverage	Displays the coverage of current security products, including the following information:
	• Number of instances protected by security products (= Number of protected ECSs + Number of 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 current asset security status, including the following information:
	Total number of current assets
	Number of vulnerable assets
Security Analysis	Displays the security analysis statistics of the previous day , including the following information:
	Total traffic of security logs on the previous day
	Number of security log models
Security Response (Overview)	Displays the security response statistics for the previous day , including the following information:
	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	 Displays the asset security status for the previous day, including the following information: 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	Displays the threat posture of assets on the previous day , including the following information: 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 network attack sources distribution HSS inspection findings
Log analysis	 Displays the log analysis results for the previous day, including the following information: 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)	Displays the security response information for the previous day , including the following information:
	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	Displays information about external security hotspots for the previous day .

Content in the Weekly Report Template

Table 7-31 Con	ntent in the	Weekly	Report	Template
----------------	--------------	--------	--------	----------

Parameter	Description		
Data Scope	SecMaster collects security information from 00:00 on Monday to 24:00 on Sunday of the previous week.		
Security Score	Score 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.		
Baseline Inspection	Displays the statistics of the latest baseline check in the previous week, including the following information:		
	The number of baseline check items		
	 Number of compliance check items in the latest baseline check 		
	 Non-compliant check items in the latest baseline check 		
Security vulnerabilities	Displays the vulnerability statistics of the accessed cloud services for the last week , including the following information:		
Number of vulnerabilities.			
	Number of unfixed vulnerabilities		

Parameter	Description
Policy Coverage	Displays the latest asset security information on the last day of the previous week, including the following information:
	 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 in the last week, including the following information:
	Total number of assets
	Number of vulnerable assets
Security analysis	Displays the security analysis statistics, including the following information:
	Total security log traffic of last week
	 Number of security log models on the last day of the last week
Security Response (Overview)	Displays the security response information for the previous week, including the following information:
	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	Displays the latest asset security information on the last day of the previous week, including the following information:
	• 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	 Displays the latest threat posture n on the last day of the previous week, including the following information: 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 HSS inspection findings
Log analysis	 Displays the log analysis results for the previous week, including the following information: 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)	 Displays the security response information for the previous week, including the following information: 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	This part includes information about external security hotspots.

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:		
	The number of baseline check itemsNumber of compliance check items in the latest		
	 baseline check Non-compliant 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:		
	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:		
	 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:		
	Total number of assets		
	Number of vulnerable assets		

Table 7-32 Content in the monthly report template

Parameter	Description
Security analysis	Displays the security analysis statistics, including the following information:
	• 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:
	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:
	 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	Displays the latest threat posture n on the last day of the previous month, including the following information:			
	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	Displays the log analysis results for the previous month, including the following information:			
	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)	 Displays the security response information for the previous month, including the following information: 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.			

7.3.3 Downloading a Security Report

Scenario

You can use custom layouts to generate security reports. Such reports are downloadable.

This topic describes how to download a report.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-55 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspaces	$\begin{tabular}{c} \hline \end{tabular} \hline \end{tabular} $				C
Purchased Resources Security Governance(beta)	Conservation Order 2 Report Pept- Mare Not Instructed	 Incidents 0 Assets 0 	♥ Vulner 0 Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

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

Figure 7-56 Reports

	/ Repo	orts		
Security Situation Situation Overview	*	Type: All 💿 Enable Status: All 💿 🛛 Add filter		× Q C
Large Screen				
Reports			Enable	
Task Center		+		
Resource Manager	*		Edit Copy Delete	
Risk Prevention	•			
Threat Operations	*			
Security Orchestration	•			
Settings	•			

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

7.3.4 Managing Security Reports

Scenario

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

Procedure

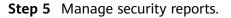
- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-57 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspeces	Credit Writigest T litter a same and keyword for stateh.				C
Agencies Purchased Resources Security Governance(beta)	Contract Contract Contrat Contract Contract Contract	 Incidents 0 Assets 0 	Vulner 0	 Alerts 0 instan 0 	Selected Spaces C ⊗ iv Indicat 0 E Playbo 0

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

Figure 7	-58 Re	ports		
	Reports			
Security Situation	Type: All	Enable Status: All I Add filter	и	× Q C
Large Screen				
Reports			Enable	
Task Center		+	•	
Resource Manager	•		Edit Copy Delete	
Risk Prevention	•			
Threat Operations	*			
Security Orchestration	•			
Settings	•			



Operation	Step
Enabling/disabling a security report	On the Reports page, locate the desired report and toggle the slider on or off.
	 If the slider is toggled on, the security report is enabled.
	 If the slider is toggled off, the security report is disabled.
Editing a Security Report	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	 On the Reports page, locate the desired report and click Delete.
	2. In the Warning dialog box displayed, click OK .

 Table 7-33 Managing security reports

----End

7.4 Task Center

7.4.1 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-59 Workspace management page

SecMaster	Management 💮	🕞 Process
Security Overview Workspaces Management Agencies	Oracle Windspace If Inter a name and layout for search.	C
Purchased Resources Security Governance(beta)	D addent? Select 2 Region i Project Move E Incidents () @ Vulner () @ Alerts () ½ Incidents	ited Spaces C 🛞 licat () lybo ()

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

Figure 7-60 To-Dos

<	/ Task Cer	nter									
Security Situation											
Situation Overview		To-Dos Co	ompleted								
Large Screen		L						Created By	▼ Enter a F	ceyword. Q	С
Task Center		Task Name	Service Type 🏼 🏹	Associated Ob	Created By	Reviewed By	Remarks	Created	Updated	Operation	
Resource Manager	•		Playbook - Nod	Automatic notifi	system			2023/06/28 17:03:55	2023/06/28 17:03:55	Review	
Risk Prevention	•			Automatic notifi	system	-	-	2023/06/28 17:02:34	2023/06/28 17:02:34	Review	
Threat Operations	*			Automatic notifi	system	-	-	2023/06/14 17:00:09	2023/06/14 17:00:09	Review	
Security Orchestration	Ţ	-	Playbook - Nod	Automatic notifi	system		-	2023/06/10 15:13:57	2023/06/10 15:13:57	Review	
			Playbook - Nod	Automatic notifi	system		-	2023/06/10 10:18:14	2023/06/10 10:18:14	Review	

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

When there are a large number of to-do tasks, you can select **Created By** or **Task Name**, enter a keyword, and click \bigcirc to quickly locate a specific task.

Parameter	Description
Task Name	Name of a task.
Service Type	Type of a task. • Workflow release • Playbook release • Playbook - Node Review
Associated Object	Name of the corresponding playbook or process.
Created By	Indicates the user who creates a task.
Reviewed By	Reviewer of the playbook/process
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.

Table 7-34 To-do task parameters

7.4.2 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-61 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	Credit Watspace $\overline{ \ensuremath{\mathbb{T}}} \ensuremath{\mathbb{T}} \ensurem$				C
Purchased Resources Security Governance(beta)	O edd9777 Weller 2 Region Project - More Not finated. Finated. Finated. Finated.	inclidents 0 Assets 0	 ♥ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ № Indicat 0 Playbo 0

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

Figure 7-62 To-Dos

<	/ Task Cent	ter									
Security Situation											
Situation Overview		To-Dos C	ompleted								
Large Screen								Created By	▼ Enter a	keyword. C	a C
Task Center		Task Name	Service Type 🏼 🍟	Associated Ob	Created By	Reviewed By	Remarks	Created	Updated	Operation	
Resource Manager	-		Playbook - Nod	Automatic notifi	system			2023/06/28 17:03:55	2023/06/28 17:03:55	Review	
Risk Prevention	*		Playbook - Nod	Automatic notifi	system	-	-	2023/06/28 17:02:34	2023/06/28 17:02:34	Review	
Threat Operations	*		Playbook - Nod	Automatic notifi	system	-	-	2023/06/14 17:00:09	2023/06/14 17:00:09	Review	
Security Orchestration			Playbook - Nod	Automatic notifi	system		-	2023/06/10 15:13:57	2023/06/10 15:13:57	Review	
			Playbook - Nod	Automatic notifi	system		-	2023/06/10 10:18:14	2023/06/10 10:18:14	Review	

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

The approval mode varies according to the service type.

- Playbook release: The **Playbook Release** page is displayed on the right. Enter review comments and approve the playbook as prompted.
- Process release: The **Process Release** page is displayed on the right. Enter the **Comment** and approve the application as prompted.

• Playbook-Node Review: The **Playbook-Node Review** page is displayed on the right. You can select **Continue** or **Terminate**.

----End

7.4.3 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-63 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Childs WithSpace If later a name and layouth for woods.				C
Agencies Purchased Resources Security Governance(beta)	Constitution D add077 dedx12 Region Project- Mere Not hoted	incidents 0	♥ Vulner 0 i Securl 0	 Alerts Instan 0 	Selected Spaces C ⑧ ↓ Indicat 0 Playbo 0

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

Figure 7-64 Completed

< / Та	sk Cert	er											
Security Situation	*												
Situation Overview			To-Dos Com	pleted									
Large Screen			Q. Select a proper	ty or enter a keyword.									c ©
Reports			Task 0	Work 0	Object 0	Created By 0	Remarks 0	Reviewed By 0	Comment ©	Description 0	Created 0	Updated ©	
Task Center				Process Publish	ouplet t	1	-		Agree		Dec 01, 2023 1	Dec 01, 2023 1	
Resource Manager Risk Prevention	Ţ												
Threat Operations	Ţ.		10 • Total R	ecords: 1 < 1	>								
Security Orchestration	÷.												
Settings	÷												

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

When there are a large number of to-do tasks, you can select an attribute, enter a keyword in the search box, and click Q to quickly search for a specific to-do task.

Table 7-35 Completed task parameters

Parameter	Description
Task	Name of a task.

Parameter	Description
Work	Type of a task.
	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.
Expired	Time the task expires.

----End

8 Resource Manager

8.1 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.

Asset Source and Corresponding Security Products

, <u>5</u> ,							
Parameter	Source	Security Product					
Servers	Elastic Cloud Server (ECS)	Host Security Service (HSS)					
Website	Web Application Firewall (WAF)	Web Application Firewall (WAF)					
Database	Relational Database Service (RDS)	Database Security Service (DBSS)					
VPC	Virtual Private Cloud (VPC)	Cloud Firewall (CFW)					
EIP	Elastic IP (EIP)	CNAD Basic (Anti-DDoS)					
Device	On-premises devices						

Table 8-1 Asset source and corresponding security products

Note:

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

8.2 Configuring Resource Subscription

Scenario

SecMaster can synchronize asset information only in the workspace where asset subscription is enabled. After the subscription, the resource information will be displayed synchronously within one minute.

This section describes how to make a subscription to resources.

NOTE

Only cloud resources can be subscribed to and synchronized. 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-1 Workspace management page

SecMaster	Management 🕥	Process
Security Overview Workspaces Management Agencies	Counter Windowski Windowski \widehat{V} factor as marked and happened for meach.	C
Purchased Resources Security Governance(beta)	0 additify Region Project - Nove III Incidents: 0 © Valmer 0 Arefs: 0 Not boold. O Arefs: 0 III Incidents: 0 © Valmer 0 Arefs: 0	Selected Spaces C ⑧ Imdicat 0 Playbo 0

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

Figure 8-2 Resource Manager

< / Resource	ce Manager										@Asset Subscription
Recurity Inhanton	-										
Resource Menager		All Resource Servers	Webshe Databa	ise VPC EIP	Device IP						
Resource Manager											
	~			latch Edd							C O
Thread Operations	-	C). Enter a teryword. By delauit, in									۲
	*	Resource Name	Resource Type	iP Address	Department	Erreironment Supplier T	Protected Status	Alam	Invident	Valuerabilities	Operation
teetoops	~		standowywe	k(Privale(P)		Claud service	Unproducted	0	0	D	Dolete
			standservers	k(PrivaletP)		Cloud service	Protected	0	0	0	Datata
		NDPLeos-	cloudservers	7(PrivalaiP), 1		Cleard service	Unprotected	0	0	0	Delete
			cloudsarvars	1((PrivatelP)		Clevel service	Unprotected	0	0	0	Delete
		. w	cioudservers	5 (PrivatelP)		Cleud service	Unprotected	0	0	0	Dolete
		— — — — — — — — — — — — — — — — — — —	cioudservers	14(PrivatelP)		Cloud service	Unprotected	0	0	0	Dolete
			cioudservers	 Privatei P1, 1 		Cloud service	Protected	0	0	0	Dolete
		NDR-ecs-	cioudservers	1 i(Private/P)		Cloud service	Unprotected	0	0	0	Dolete
		ecs-090-6	cioudservers	1. SPrivate/P1		Cloud service	Unprotected		0	0	Dorete
			cioudservers	1 NPTivateIP)		Cloud service	Protected		0	0	Dorete
		10 • Total Records: 48	< 1 2 3 4 8 3	> m							

- **Step 5** On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.
- **Step 6** 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.
- Step 7 Click OK.

After the subscription, the resource information will be displayed within one minute.

----End

8.3 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 purchased the SecMaster standard or professional edition.

Procedure

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

Figure 8-3 Workspace management page

SecMaster	Management ③		🗇 Process
Security Overview Workspeces	Cealst Wanspace If form a name and keyword for search.		C
Purchased Resources Security Governance(beta)		ncidents 0 🕹 Vulner Assets 0 🗟 Securi	 Selected Spaces C ⑧ i⊻ Indicat 0 S Playbo 0

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

Figure 8-4 Resource Manager

< / / Resource Manager										@Asset Subscription
Recurty Readon ·										
Resource Menager	Al Resource Servers	Website Databa	ase VPC EIP	Device IP						
Resource Manager	Ball/I Deteta	Inchronize Assets	NACE FOR							C 0
Risk Prevention V										
Thread Operations	Q. Enter a heyward. By default, In									œ
Security Orchestration -	Resource Name	Resource Type	IP Address	Department	Environment Supplier T	Protected Matua	Atam	Incident	Valoerabilities	Operation
Gettings ·		cloudservers	1(Pr7va56(P)		Cloud service	Unprotected	0	0	0	Dateto
	- eci-	cloudservers	S(PyyvaterP)		Croud service	Protected	0	0	0	Donese
	NDR-ect-	cioudservers	7(Pitvaba/P),1		Cloud service	Unprotected	0	0	0	Durate
	- ece- 18	cioudservers	10 (PTNIMIP)		Croud service	Unprotected	0	0	0	Durete
	. w	cioudservers	1		Cloud service	Unprotected	0	0	0	Durate
•		cioudservers	1 HOPTWINEP)		Cloud service	Unprotected	0	0	0	Durete
	- +c+	cioudservers	1 (PrivaterP).1		Cloud service	Protected	0	0	0	Durete
	NDR-ect-	cioudservers	1 (PrivatorP),		Cloud service	Unprotected	0	0	0	Durate
	eci-090-6	cioudservers	1 (PrivatorP),		Cloud service	Unprotected	0	0	0	Durete
		cioudservers	1 IOPTIVAMIP)		Cloud service	Protected	0	0	0	Dateta
	10 • Total Records: 48	< 11 2 3 4 8	> 00							

Step 5 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 a large number of resources on this page, you can select **Resource Type** and click Q to search for a specific resource.

- 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 a resource, click its name to go to the details page. On the details page, you can:
 - View the basic information, environment information, and managed resources.
 - 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.

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

Table 8-2 Asset source and corresponding security products

Note:

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

----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**.

8.4 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.

Prerequisites

You have purchased the SecMaster standard or professional edition.

Limitations and Constraints

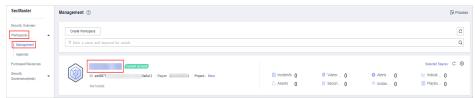
- Only .xlsx files no larger than 5 MB can be imported.
- A maximum of 9,999 resource records can be exported.

Importing Assets

Step 1 Log in to the management console.

- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-5 Workspace management page



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

Figure 8-6 Resource Manager

< / / Reso	urce Manaper										@Asset Subscription
Recurity Illustion	×										
Resource Menager		All Resource Servers	Website Datab	ase VPC EIP	Device IP						
Resource Manager											C C D
Risk Prevention	*	Hadar Develo Bydere Byddroniae Assess Budar Balt									
Threat Operations	~										
Security Grohestration	-	Resource Name	Resource Type	IP Address	Department	Environment Supplier T	Protected Mature	Atam	Incident	Valoorabilities	Operation
Gettings	*		cloudservers	K(ProvadorP)		Croud service	Unprotected	0	0	0	Doloto
		441-	cloudservers	IOPYIVation P1		Cloud service	Protected	0	0	0	Dorete
		NDR-ect-	cloudservers	7(PrivateP),1		Cloud service	Unprotected	0	0	0	Defete
		- +cr- 18	cloudservers	1(OPTWM4P)		Cloud service	Unprotected	0	0	0	Defete
		w q	cloudservers	1		Cloud service	Unprotected	0	0	0	Defete
	· ·	· · · · · · · · · · · · · · · · · · ·	cloudservers	1 (40PTN/848P)		Cloud service	Unprotected	0	0	0	Defete
		440	cloudservers	1 (Private P), 1		Cloud service	Protected	0	0	0	Defete
		NDR-ect-	cloudservers	1 i(Privato(P)		Cloud service	Unprotected	0	0	0	Defete
		eci-090-4	cloudservers	1 *(Private(P)		Cloud service	Unprotected	0	0	0	Defete
		- +	cloudservers	1 10PTN/848P)		Cloud service	Protected	0	0	0	Defete
		10 + Total Records: 48	< 1 2 3 4 8	> 00							

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 filled, 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-7 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspeces	$$\ensuremath{\mathbb{T}}$$ Could Workspace $$\ensuremath{\mathbb{T}}$$ Enter a name and keyword for search.				C
Purchased Resources Security Governance(beta)	0 409977 54412 Regon Proc- More Not hoted.	 Incidents 0 Assets 0 	Vulner 0	Alerts 0	Selected Spaces C ⑧ ↓ Indicat 0 ⑤ Playbo 0

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

Figure 8-8 Resource Manager

/ Resource	e Manaper										@Assel Subscription
tecurity Situation	-										
besource Menager		All Plesource Dervers	Website Databa	ise VPC EIP	Device IP						
Resource Manager											C 0 0
aix Prevention	-	Radith Database Byrachererizes Associas Burdath Data									
isreal Operations	-		Q. Enter a layourd. By default, the search is performed by name or a combination of search criteria.								
ecurity Orchestration		Resource Name	Resource Type	iP Address	Department	Erreironmeni Supplier T	Protected Status	Alarm	Involdent	Valnevabilities	Operation
ethoge .	-		standaervers	1(Private(P)		Claud service	Unprotected	0	0	0	Dolata
			standservers	k(Private(P)		Claud service	Protected	0	0	0	Datata
		NDR-ees-	cloudsarvers	7(PrivalaiP), 1		Cleard service	Unprelacted	0	0	0	Dolete
		- ecs	cicudaarvara	1((PrivatelP)		Clevel service	Unprelacted	0	0	0	Delete
			cioudsarvers	5 (PrivatelP)		Clevel service	Unprefacted	0	0	0	Dolete
			cioudservers	14(PrivatelP)		Cloud service	Unprotected	0	0	0	Dolete
			cioudservers	 Privatei P1, 1 		Cloud service	Protected	0	0	0	Defete
		NDR-ect-	cioudservers	1 i(Private/P),		Cloud service	Unprotected	0	0	0	Defete
		ecs-090-1	cioudservers	1. (Private/P)		Cloud service	Unprotected		0	0	Defete
		· ·	cioudservers	1 (OPTicateIP)		Cloud service	Protected	0	0	0	Defete
		10 - Total Records: 48	< 🚺 2 3 4 8	> 00							

- **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 \square in the upper right corner of the list.
- **Step 7** In the **Export** dialog box, set asset parameters.

Table 8-3 Exporting assets

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

Step 8 Click OK.

The system automatically downloads the Excel to your local PC.

----End

8.5 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.

Prerequisites

You have purchased the SecMaster standard or professional edition.

Limitations and Constraints

Only assets imported outside the cloud can be deleted.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-9 Workspace management page

SecMaster	Management ⑦				Process
Security Overview Workspaces	$\begin{tabular}{c} \hline \end{tabular} \hline $$ Total a name and layout for seach. \end{tabular}$				C
Purchased Resources Security Governance(beta)	D 405077 64412 Report Pages- Kee	Incidents 0 ○ Assets 0	♥ Vulner 0 ⊜ Securi 0	Alerts O Instan	Selected Spaces C

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

Figure 8-10 Resource Manager

< / Reso	irce Manager										@Asset Subscription
Recurity Situation	w										
Resource Menager	÷ .	Al Resource Bervers	Website Databa	ise VPC EIP	Device IP						
Resource Manager											
Paix Prevention	¥	Bably Dolets Byslam Bys	nohronies Assels	laters that							C ©
Threat Operations	Q. Enter a largeward. By default, the search is performed by name or a combination of search criteria.										۲
Security Orchestration	*	Resource Name	Resource Type	iP Address	Department	Erreironment Supplier T	Protected Kialus	Alarm	Involdent	Valnevabilities	Operation
memoga	~		standaervers	1(Privale(P)		Cloud service	Unprotected	0	0	0	Dolete
			sinudanvers	k(Privatel P)		Claud service	Protected	0	0	0	Datata
		NDR-ecs-	cloudservers	7(PrivateP),1		Clevel service	Unprotected	0	0	0	Doleta
			cloudservers	11 (PrivateIP)		Clevel service	Unprotected	0	0	0	Dalata
		- w	cieudaarvara	1. SOPrivateiP)		Cleud service	Unprotected	0	0	0	Delete
		— — — — — — — — — — — — — — — — — — —	cioudservers	(i4(PrivateIP)		Cloud service	Unprotected	0	0	0	Delete
			cioudservers	5 (Privatei P), 1		Cloud service	Protected	0	0	0	Defete
		NOR-ect-	cioudservers	s i(Private/P)		Cloud service	Unprotected	0	0	0	Defete
		ece-090-4	cioudservers	1 (Private P)		Cloud service	Unprotected	0	0	0	Defete
		• •	cioudservers	1 IOPTivate(P)		Cloud service	Protected	0	0	0	Defete
		10 • Total Records: 48	< 🚺 2 3 4 8 3	> 0x							

Step 5 Edit or delete the resource.

Table 8-4 Parameters for	r resource edit or deletion
--------------------------	-----------------------------

Operation	Procedure
Batch Edit	 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.
	S. CIICK OR .
Batch Delete	 On the Resource Manager page, click the corresponding resource type tab. For example, if you want to delete servers, click the Servers tab.
	 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

9 Risk Prevention

9.1 Baseline Inspection

9.1.1 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.

For your cloud services, you can learn of unsafe settings that are discovered by SecMaster based on security standards **Cloud Security Compliance Check 1.0** and **Network Security**.

Limitations and Constraints

The SecMaster basic edition does not support baseline inspection. The basic edition does not support viewing of cloud service baseline details. To learn about your cloud service configuration status and ensure your cloud service configurations are appropriate, you are advised to use the professional edition. For details, see **Buying the Professional Edition**.

Baseline Check Methods

• Automated baseline checks

Every three days SecMaster checks your assets under your account in the current region from 00:00 to 06:00.

You can specify a schedule and start time to let SecMaster perform baseline inspection. For details, see **Creating a Custom Baseline 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.

For details about manual checks, see Handling Manual Check Items.

Process

No.	Operation	Description			
1	(Optional) Creating a Custom Baseline Check Plan	 SecMaster uses the default check plan to check all assets. Default plan: SecMaster checks your assets under your account in the current region every three days from 00:00 to 06:00. Custom planc: SacMaster performs baceling. 			
		 Custom plans: SecMaster performs baseline inspections based on the standards and time you specify in the custom check plans. 			
2	(Optional) Starting an	The baseline inspection supports periodic and immediate checks.			
	Immediate Baseline Check	• 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, affected assets, and details about the baseline inspection items.			
4	Handling Baseline Inspection Results	You can handle risky items based on the rectification suggestions.			

Table 9-1 Process

9.1.2 Creating a Custom Baseline Check Plan

Scenario

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. You can also specify custom check periods and time.

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

Limitations and Constraints

- A security standard can be added to only one check plan.
- Only the standard and professional editions support this function.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-1 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Checks**. On the displayed page, click **Create Plan**. The **Create Check Plan** page is displayed on the right.

Figure	9-2	Creating	a c	check	plan
--------	-----	----------	-----	-------	------

<	/ Checks			
Security Situation	*			
Resource Manager	*	Create Plan		
Risk Prevention	*			
Threat Operations	•	default(Default) Check Now	Check Now	Edit Delete
Security Orchestration	•	0 Schedule: every 3 days at 0:00-6:00	🛱 Schedule: every 1 days at 0:00-6:00 💽	
Settings 1	*	Security Standards	Security Standards	
Collection Management		Cloud Security Compliance Check 1.0	Network Security	
Components				
Data Integration				
Checks 2				
Directory Customization				

Step 5 Configure the check plan.

1. Enter the basic information by referring to **Table 9-2**.

Table 9-2 Basic information about a check plan

Parameter	Description
Name	Plan name
Schedule	Select how often and when the check plan is executed.
	 Schedule: every day, every 3 days, every 7 days, every 15 days, or every 30 days
	 Check start time: 00:00-06:00, 06:00-12:00, 12:00-18:00, or 18:00-24:00

2. Select a security standard for the plan.

Select the baseline check items to be checked.

Step 6 Click OK.

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

----End

Related Operations

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

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

Only user-defined check plans can be modified.

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

Only user-defined check plans can be deleted.

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

9.1.3 Starting an Immediate Baseline Check

Scenario

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 check plan.

Limitations and Constraints

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

Starting a Check Based on Selected Standards

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-3 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Creds Workspace $\label{eq:states} \overline{V} \mbox{ Itsr a none and layoutd for search}.$				C
Purchased Resources Security Governance(beta)	Omeration 0: dol077 dol072 Report Projed- Mare Not head. Not head. Not head. Not head.	Incidents 0 Assets 0	 Vuiner 0 ⊜ Securi 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. In the upper right corner of the page, click **Check Now**.

Figure 9-4 Check Now

< Security Situation	.							
Resource Manager	•	Workspace	Latest checked: Mar 27, 2	2023 00:00:56 GMT+08:00	Security Standards 3/3	Check	llem	Check Now Configure Check Plan
	•	Pass Rate (10%	 Passed Failed Ignored 	Resources by Threat Ser Critical High Medium	Failed Check	0	
,	*		0%	Errors Pending	Low Informational	2	15 3	

Step 5 In the displayed dialog box, 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

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

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

Figure 9-5 Workspace management page

SecMaster	Management ①				🗇 Process
Security Overview Workspaces	Credit Workspace $eq:static_s$				C
Purchased Resources Security Governance(beta)	Or add/077 deda12 Report Not hoted	Incidents 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C i Indicat 0 Playbo 0

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

Figure 9-6 Checks page

< / / Checks		
Security Situation		
Resource Manager 🔹	Region v	
Risk Prevention 🔻	Create Plan	
Threat Operations -		
Security Orchestration 🔻	default(Default) Check Now	Check Now Edit Delete
Settings	Schedule: every 3 days at 0:00-6:00	Schedule: every 1 days at 0:00-6:00
Collectors	Security Standards	Security Standards
Components	Cloud Security Compliance Check 1.0	DJCP 2.0 Level 3 Requirements
Data Integration		
Checks		
Directory Customization		

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

SecMaster immediately executes the selected baseline check plan.

----End

9.1.4 Handling Manual Check Items

Scenario

For all check items in **DJCP 2.0 Level 3 Requirements** and some check items in **Cloud Security Compliance Check 1.0** and **Network Security**, you need to manually check them and fill in the results on the SecMaster console. They will be used to assess the overall compliance of your services.

This topic describes how to start manual checks in baseline inspection.

Prerequisites

• You have completed the check offline.

Constraints and Limitations

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

Procedure

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

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

Figure 9-7 Workspace management page

SecMaster	Management 💿				🕞 Process
Security Overview Workspaces Management Agencies	Could Hopkageat $\label{eq:generalized_state} T \mbox{ for a name and layered for search}.$				C
Purchased Resources Security Governance(beta)	Ormer Jococci 0 #555777 646412 Report Priped More Not Includ. F F F F	incidents 0 Assets 0	 ♥ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 iv Indicat 0 Playbo 0

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

Figure 9-8 Accessing the baseline inspection page

< / Baselin	specian Findings								
Security Situation Resource Manager	Baseline Inspection Check Result	Sandier respective Check Result							
Risk Prevention	Worksace Latert checket: Feb 36, 2024 15:30:42 OMT-00:00	Security Standards Direct times 3a -	Check Naw Configure Check Plan						
Vulnerability Notices Policy management	Pass Rate (2)	Resources by Threat Sevenity							
Threat Operations Security Orchestration	Passed Failed	Falled Check Items Vulnerable Resources Onlical 0 0							
Setings 💌	the space of	High 2 75 Madam 8 8 - Law 0 6 - Informational 8 14 -							

- **Step 5** On the **Security Standards** tab page, locate the row that contains the check item whose result you need to report to SecMaster manually, click **Manual Check** in the **Operation** column.
- Step 6 In the displayed dialog box, select a result and click OK.

NOTE

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

----End

9.1.5 Viewing Baseline Inspection Results

Scenario

You can view all check results on the **Baseline Inspection** page. You can view the check results of automatic check items of associated assets on the **Result** tab.

- Viewing Check Results on the Baseline Inspection Tab
- Viewing Check Results on the Result Tab

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

Prerequisites

- You have purchased the SecMaster professional edition and the edition is within the validity period.
- Cloud service baseline scanning has been performed.

Viewing Check Results on the Baseline Inspection Tab

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

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

Figure 9-9 Workspace management page



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

Figure	9-10 Accessing the baseline inspection page
< / Basel	Ine Inspection Findings
Security Situation	Baseline Inspection Check Result
Resource Manager	Laseine inspection Unex Kesur
Risk Prevention	

Security Situation 🔹	Baseline Inspection Check Result			
Resource Manager 🔹 💌	Baseline Inspection			
Risk Prevention				
Baseline Inspection	Workspace	Security Standards	Check liens	Check Naw
Vulnerabilities	Latest checked: Feb 26, 2024 15:30:42 GMT+08:00	3.0		Configure Check Plan
Emergency				
Vulnerability Notices		Resources by Threat Severity		
Policy management	Pass Rate ⑦	Resources by Triest Seventy		
Threat Operations 🔹	• Passed	Failed Check I	tems Vulnerable Resources	
Security Orchestration 🔹	• Failed	Critical	0	
Settings 👻	1 1 0/ Ignored	High 7	75	
	11% 0% Errors	Medium 8	8 💼	
	Pending	Low 5	6 💻	
		Informational 3	14	

Step 5 On the **Baseline Inspection** tab, view the baseline check result. For details about the parameters, see Table 9-3.

Figure 9-11 Viewing Baseline Inspection Results

Pass Rate		Risk Severity			Security Standard Compliance St	atus	Security Policy	Check Results	
69%	 Passed Failed Errors 	Critical High Medium Low Info	Faled Check Items C C C C C C C C C C C C	Quantity 0 4 11 10 15	Network Security	23%	60 ⁰⁶¹	WP ²³ On Bold - Second-	Crock Se-
Security Standards	Import Export Q. Select a property or enter a	keyword.							С
-	Check Item 💠	Result \$	Resour ¢ Reso	urce Name 💠	Severity ≑	Suggestion \Leftrightarrow		Last Scanned 💠	Operation
DJCP 2.0 Level 3 Requir	Check Item \$		Resour Resour Resour Resource Resource	urce Name 💠	Severity \$	Suggestion \Leftrightarrow		Last Scanned Jan 16, 2024 15:57:33 GMT+	Operation View Details
Cloud Security Complian DJCP 2.0 Level 3 Requir Network Security		larm		urce Name 💠			for RDS is enabled	Jan 16, 2024 15:57:33 GMT+	

Parameter	Description					
Workspace	Name of the current workspace.					
	Under the workspace name, the latest baseline check time is displayed.					
Security Standards	Number of security standards used for the latest check/ Total security standards.					
Check Item	Total number of check items in the latest baseline check.					
Pass Rate	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, Ignored , Errors , or Pending .					
Resources by Threat Severity	Numbers of unsafe resources at different severities in the last baseline inspection.					
	Severity: Critical, High, Medium, Low, and Informational.					
Security Standards	This tab displays check results by security standard.					
	• The Security Standards tab displays all baseline check standards and other details, including the check item, status, category, vulnerable resources, description, and latest check time.					
	• To view details about a baseline check item, click View Details in the Operation column. On the Baseline inspection issues page, view the detailed description, check result, and suggestions of the check item.					
	NOTE SecMaster basic edition does not support viewing of cloud service baseline inspection details. After Buying the Professional Edition , you can view details about unsafe resources and suggestions.					

 Table 9-3 Baseline inspection results

Parameter	Description
Resources to Check	This tab displays check results by checked resources.
	• The Resources to Check tab displays all checked resources and their details, including the resource name, resource type, check items, and vulnerable items.
	 To view the check details of a resource, locate the row that contains the target resource and click View Details in the Operation column. On the resource details page, view the check items, check status, check method, and last check time of the resource. NOTE SecMaster basic and standard editions do not support viewing of cloud service baseline inspection details. After Buying the Professional Edition, you can view details about unsafe resources and suggestions.
Result	This tab displays check results by check item.
	The Result tab lists all check results and their details, including the check items, check results, resource types, resource names, and latest check time.
	NOTE SecMaster basic and standard editions do not support viewing of check results. To learn about your cloud service configuration status and ensure your cloud service configurations are appropriate, the professional edition is recommended. For details, see Buying the Professional Edition .

----End

Viewing Check Results on the Result Tab

SecMaster allows you to view the check results of automatic check items by checked resource.

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

Figure 9-12 Workspace management page

SecMaster	Management 💿				D Process
Security Overview Workspaces Management Agencies	Creals Wonspace $\label{eq:product} \overline{\nabla} \mbox{ Inter a same and layourd for search}.$				C
Purchased Resources Security Governance(beta)	Constanting Constanti	incidents 0 Assets 0	 ◊ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 indicat 0 Playbo 0

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

Figure 9-13 Compliance baseline log

<										
Security Situation	٣	010	ud Service Access							
Resource Manager	Ŧ	-	ou de vice riccess							
Risk Prevention	•									
Threat Operations	٣									
Security Orchestration	٣		Access Service Logs							
Settings 1	*		Cloud Services	Logs	Region Level	Workspace	Storage Location (?)	Lifecycle	Lifecycle Scope	Automatically convert
Management			Web Application Firewall (?)	💽 WAF attack log 🕥	Region		/sec_waf_attack	7 Days	7~10 Days	
Data Integration			ner Apricator Henari (j	WVF access log	Region	-	/sec_waf_access	7 Days	7~10 Days	-
Checks Directory			Cloud Service Compliance Check	Compliance Baseline Log	Region		i/sec_secmaster_baseline	7 Days	7~10 Days	
Customization			Object Storage Service	Object Storage Service acces	: Region	_	/ sec_obs_access	7 Days	7~10 Days	-

After the setting is complete, you can perform an immediate check on the **Baseline Inspection** page. You can view check results on the **Check Result** page 10 minutes later. For details about operations related to immediate check, see **Starting an Immediate Baseline Check**.

If no immediate checks are performed, the system performs the check at the specified time according to the preset check plan. 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. On the displayed page, click the Result tab.

Figure 9-14 Check result tab

< / / Baseline Inspec	tion									
Security Situation • Resource Manaper •	Baseline Inspection Check R	rout 🔒								
Risk Prevention	Pass Rate		Risk Severity			Security Standard Compliance Status		Security Policy Check R	asults	
Vulnerabilities Eimergancy Vulnerability Notices Policy management Threat Operations	69%	 Passed Failed Errors 	Critical High Medium Low	Failed Check Items	Quantity 0 4 11 10	Network Security	23%			
Security Orchestration + Settings +			Low		10			Agency	Obs Buchets	Cloud Servers

Step 6 On the **Result** tab, view the check results of automatic check items for associated assets. **Table 9-4** describes the parameters.

Figure 9-15 Viewing check results

Pass Rate		Risk Severity			Security Standard Compliance State	us	Security Policy	Check Results	
			Failed Check Items	Quantity	Network Security	23%	1		
	Passed	Critical	0	0	Network Security	2376			
69%	Failed	High	2	4					
09%	Errors	Medium	4		Cloud Security Compliance Check 1	.0 29%		1.1.1	
		Low	5	10					
		Info	4	15			AGENCI	WPC OUS BUCK SECURIN-	Cloud Se-
a	Import Export Q. Select a property or enter a keyv	rord.							C
ecurity Standards d Cloud Security Complan DUCP 2.0 Level 3 Requir		rord. Result \$	Resour ¢	Resource Name 0	Severity 0	Supposition ©		Last Scenned 0	C
I DJCP 2.0 Level 3 Requir	Q Select a property or enter a keyv	Result 0	Resour ¢ vpcs	Resource Name 🗘	Seventy © Midum	Suggestion \$		Last Scanned © Jan 16, 2024 15:57:33 GMT+	Operation
a	Q. Select a property or enter a keyv C. Check Item \$	Result 0		Resource Name 0			y for RDS is enabled		C Operation View Details View Details

Parameter	Description				
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 .				
Risk 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 Informational.				
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.				
Security Policy Check Results	This graph shows how many failed and passed check items your cloud services have in the last baseline check.				
Security Standards and the check result list	 All security standards and check results are displayed. To view the check results of a security standard, click the security standard on the left. The check result details will be displayed on the right. 				
	 To view details about a baseline check item, click View Details in the Operation column. On the Baseline inspection issues page, view the detailed description, check result, and suggestions of the check item. NOTE 				
	SecMaster basic edition does not support viewing of cloud service baseline inspection details. After Buying the Professional Edition , you can view details about unsafe resources and hardening suggestions.				

 Table 9-4 Check result parameters

----End

9.1.6 Handling Baseline Inspection Results

Scenario

To handle the check result, perform the following operations:

• Handling Unsafe Settings: Rectify the risk check items based on the check result.

- **Reporting Manual Check Results to SecMaster**: For manual check items, after you finish each check, report the check result to SecMaster. The pass rate is calculated based on results from both manual and automatic checks.
- Ignoring a Check Item: If you have custom requirements for a check item, ignore the check item. For example, SecMaster checks whether the session timeout duration is set to 15 minutes, while you need to set it to 20 minutes. In this situation, ignore this check item so that SecMaster no longer executes this check.
- Importing and Exporting Check Results: You can import or export check results.

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

- Your professional edition SecMaster is available.
- The cloud service baseline has been scanned.

Handling Unsafe Settings

The following describes how to fix unsafe settings discovered by check item **IAM** user login protection.

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

Figure 9-16 Workspace management page

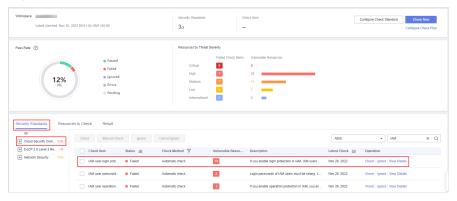
SecMaster	anagement 🕥								
Security Overview Workspaces Management Agencies	Credit Workspace $\overline{V} \ \ \text{for search}.$	(C) (Q)							
Purchased Resources Security Governance(beta)	Commit account Commit account D add077 Sele12 Repor Prace- Nov Asset 0 Asset 0	· · · ·							

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

Figure 9-17 Accessing the baseline inspection page

Step 5 On the **Security Standards** tab, choose **Cloud Security Compliance Check 1.0** to view the status of each check item.

Figure 9-18 Check item status



- If the icon of a check item status is green, the configuration is correct and no unsafe settings found.
- If the icon of a check item status is red, there may be inappropriate configurations and the assets may have potential risks.
- **Step 6** In the **IAM user login protection** row, click **View Details** in the **Operation** column to go to the details page.
- **Step 7** View the risk details and fix the unsafe settings by referring to details in the **Result** and **Recommendation** columns.

Parameter	Description				
Status	Displays the check status of the current check item.If the result is Passed, the configuration corresponding to the check item is appropriate.				
	 If the result is Failed, the configuration corresponding to the check item is inappropriate. The check results will be listed. 				
Latest Check	Last time when the current check item was performed.				
Check Method	Method used by the current check item.				

Table 9-5 Check items

Parameter	Description
Severity	Severity of the unsafe settings discovered against the current check item.
Impact	Security impact caused by unsafe settings discovered against the current check item.
Standard and Category	Security standard and category of the current check item.
Description	Check content of the current check items.
Check Process	Check process of the current check item.
Reference	Links of documentation related to the check item. Click the reference link to go to the detailed page.
Resource	Resource to which the current check item belongs.
	 The check result can be Passed or Failed. If the result is Passed, the configuration corresponding to the check item is appropriate. If unsafe settings are found, the detailed information is listed. You can click the button in the Operation
	column to go to page and fix the configuration.

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

----End

Reporting Manual Check Results to SecMaster

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

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

Figure 9-19	Workspace	management page
-------------	-----------	-----------------

SecMaster	Management ①				🕞 Process
Security Overview Workspaces	$\label{eq:rescaled} \fbox{\begin{tabular}{c} \hline \mbox{Crude Workspect} \\ \hline \hline & \end{tabular} \end{tabular} \mbox{ for search.} \\ \hline \end{tabular}$				C
Purchased Resources Security Governance(beta)	Comme accest 6 additi77 bedat2 Region Project- Non Not house.	 Incidents 0 Assets 0 	♥ Vutner 0 i Securl 0	O Alerts 0 instan 0	Selected Spaces C 🛞

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

Figure 9-20 Accessing the baseline inspection page

<	C results inspection Findings										
s	ecurity Situation	٣	Baseline Inspec	tion Check Resul							
R	esource Manager	۳	Cost internation	Check Result	an.						
R	isk Prevention	•									
	Baseline Inspection		Workspace				Security Standards		Check Items		Check Now
	Vulnerabilities			Latest checked: Feb 26, 21	1024 15:30:42 GM	T+08.00	3/3				Configure Check Plan
	Emergency Vulnerability Notices										
	Policy management		Pass Rate (0			Resources by Threat S	eventy			
т	hreat Operations	*				Passed		Failed Ch	eck Items Vuln	erable Resources	
s	ecurity Orchestration	÷				• Failed	Critical	0	0		
s	ettings	÷		11%		e Ignored	High	7	75		
				0%		e Errors	Medium	8	8	-	
						Pending	Low	5		-	
			1				Informational	3	14		

- **Step 5** On the **Security Standards** tab page, locate the row that contains the check item whose result you need to report to SecMaster manually, click **Manual Check** in the **Operation** column.
- **Step 6** In the displayed dialog box, select a result and click **OK**.

D NOTE

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

----End

Ignoring a Check Item

If you have custom requirements for a check item, ignore the check item. For example, SecMaster checks whether the session timeout duration is set to 15 minutes, while you need to set it to 20 minutes. In this situation, ignore this check item so that SecMaster no longer executes this check.

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

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

Figure 9-21 Workspace management page

SecMaster	Management ③				📝 Process
Security Overview Workspeces Management Agencies	Could Withington $\label{eq:prod} \overline{\mathbb{V}} \mbox{ Intro a name and largeout for search}.$				Q
Purchased Resources Security Governance(beta)	O additifity O	Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	● Alerts 0 linstan 0	Selected Spaces C 🛞 iv Indicat 0 Playbo 0

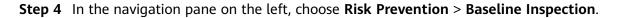


Figure 9-22 Accessing the baseline inspection page

C / Baarline Inspector Printings									
Security Situation 🔹	Baseline Inspection Check Result								
Resource Manager 🔹 🔻	Check Result								
Risk Prevention									
Baseline inspection	Workspace		Security Standards	Check Items	Check Now				
Vulnerabilities	Latest checked: Feb 26, 2024 15:30	2 GMT+08.00	3/3	-	Configure Check Plan				
Emergency Vulnerability Notices									
Policy management	Pass Rate (2)		Resources by Threat Severity						
Threat Operations		Passed	Faller	Check Items Vulnerable Resources					
Security Orchestration 💌		• Failed	Critical	0					
Setings 💌	11%	Ignored	High 7	75					
	0%	Errors	Medium 8	8 					
		Pending	Low 5 Informational 3	6 14 					

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

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

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

- 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 **Unignore** in the **Operation** column. Then, in the displayed dialog box, click **OK**.

----End

Importing and Exporting Check Results

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

Figure 9-23 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Crash Wangara $\overline{\nabla} \mbox{ for same and layers for search}.$				C
Purchased Resources Security Governance(beta)	constants constants	S Incidents 0 Assets 0	♥ Vuiner 0	O Alerts 0 instan 0	Selected Spaces C

Step 4 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Result** tab.

Figure 9-24 Check result tab

< / / Bayeline importion											
Security Situation											
Resource Manager 🔹 💌	Baseline Inspection	Baseline Inspection Check Result									
Rick Prevention											
Baseline Inspection	Pass Rate		Risk Severity			Security Standard Compliance Status		Security Policy	Check Results		
Vulnerabilities				Falled Check Items	Quantity						
Emergency		Passed	Critical	•	0	Network Security	23%				
Vulnerability Notices	i	 Failed 	High	2	4						
Policy management	69%	Errors	Medium	4		Cloud Security Compliance Check 1.0	29%				
Threat Operations 🔹 👻			Low	5	10		2375		1	1.1	
Security Orchestration 🛛 👻			Info	4	15			Agency	Obs Suchets		Cloud Servers
Settings 👻											

Step 5 Import or export the check result.

• Import:

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.
- a. In the upper left corner above the check result list, click Import.
- b. In the dialog box displayed, click **Download Template** and complete the template.
- c. In the displayed dialog box, click **Add File** and upload the completed template file.
- d. Click OK.
- Export:
 - a. Select target check items from the result list and click **Export** in the upper left corner above the check result list.
 - b. In the displayed dialog box, select the format and data columns you want.
 - c. Click OK.

----End

9.2 Vulnerability Management

9.2.1 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.

For details about how HSS scans for vulnerabilities and which types of vulnerability it scans for, see **HSS Vulnerability Management Overview**.

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:

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.

9.2.2 Viewing Vulnerability Details

Scenario

This topic describes where to view details about Linux, Windows, Web-CMS, and application vulnerabilities.

Prerequisites

- You have purchased the SecMaster professional edition and the edition is within the validity period.
- HSS logs have been connected to SecMaster and the function of automatically converting logs into alerts has been enabled. For details, see Data Integration.

Procedure

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

Figure 9-25 Workspace management page

SecMaster	Management () (P Process
Security Overview Workspaces	Oracle Windspace C T later a name and layout for search. Q
Purchased Resources Security Governance(beta)	C @ 0 #0877 bit/2 Regin Paged- Mars © Valer. 0 0 Alers 0 bit/2 Indicet. 0 Not Instant Not Instant - Aserts 0 Becost. 0 Instant. 0 IP Report. 0 IP Report. 0 Image: Note: 0 Image: 0 Image: Note: 0 Image: 0

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

Ry Stauties V								
eca Managar 🛛 🔻	ValoerabilityStatistics							
Prevention	Vulnerability Type Dist	bibution		Top 5 Valoerabilities	Vulnerability ID	Vulnerability Type	Top 5 Volnerable Resources	
aseline Inspection				Name10 o	Affected		e High e Medium e Low	
inerabilities			Linux Vulnerability	CVE-2021-41617	3		eu-	
nergincy Jinerability Notices			 Windows Walnerabilities 	CVE-2022-24903	а			
licy management		309	Web-CMS Vulnerability	CVE-2023-48795	3		ect-	
t Operations •			Application Vulnerabilities	CVE-2018-25032	2		ecs-	
				CVE-2019-12749	2			
	4 Linux Vulnerabilities	Windows Wilners	billies Web CMS Vulnerabilit					
		Windows Wilners	billies Web CMS Vulnerabili					((())
	Batch Repeir	import	bilities Vieb CMS Valnerability	tes Application Vulnerabilities				
	Batch Repeir	Import By default, the search is		tes Application Vulnerabilities	ABected Assets	Watemphility (D	Last Scanned	
	Batto Repeir	Import By default, the search is Name	performed by name or a combination of s-	tes Application Vulnerabilities		Vulsensbillty ID CVI-2019-1426	Last Scanned 28240128 14.45 20.832 GMT-08 89	G
	Bath Repair	Import By default, the search is Name 29 Important Cont0	performed by name or a combination of s graded	tes Application Vulnerabilities earch ortenia. D	Affected Assets			Handled

Figure 9-26 Accessing the vulnerability management page

Step 5 View vulnerability information on the **Vulnerabilities** page.

Table 9-7 Viewing vulnerability information

Parameter	Description			
Vulnerability Type Distribution	This graph displays the total number of vulnerabilities and the distribution of vulnerabilities by type.			
Top 5 Vulnerabilities	• 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.			

Parameter	Description
Top 5 Vulnerable Resources	This graph displays the five resources with the most vulnerabilities.
Vulnerability List	 The vulnerable list area includes Linux Vulnerabilities, Windows Vulnerabilities, Web- CMS Vulnerabilities, and Application Vulnerabilities tabs. Table 9-8 lists parameters for these vulnerability tabs.
	• To quickly search for a specific vulnerability, use filters in your search. Specifically, you can specify the vulnerability name, vulnerability ID, severity, and handling status, enter a keyword in the search box, and click Q.
	• 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	9-8	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

9.2.3 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.

The fixing method varies depending on the vulnerability type. Select a method based on the vulnerability type. The recommended fixing methods are as follows.

Vulnerability Type	Recommended Fixing Method	
Linux vulnerabilities	Use either of the following methods:	
Windows vulnerabilities	 Use the repair function on the SecMaster console to fix the vulnerability. 	
	 Manually fix the vulnerability based on the suggestions provided on the console. 	
	Then, you can use the verification function to quickly check whether the vulnerability has been fixed.	
Web-CMS vulnerabilities	Manually fix the vulnerability based on the suggestions provided on the console.	
Application vulnerabilities		

Table 9-9 Recommended fixing methods

- 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. For details, see **Purchasing a Server Backup Vault**. 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. If the server cannot access the Internet or the services provided by the external image source are unstable, you can use the image source provided by Huawei Cloud to fix vulnerabilities. To ensure that the vulnerability is successfully fixed, ensure that the image source . For details, see Configuring the Image Source.

Constraints

• For details about how to fix vulnerabilities detected by HSS, see **Types of Vulnerabilities That Can Be Scanned and Fixed**.

- CentOS 6 and CentOS 8 are officially End of Life (EOL) and no longer maintained. HSS scans them for vulnerabilities based on Red Hat patch notices but cannot fix them. You are advised to change to other OSs.
- Ubuntu 18.04 and earlier versions do not support free patch updates. You need to purchase and configure Ubuntu Pro to install upgrade packages, or vulnerability fix will fail.
- The kernel vulnerabilities on CCE, MRS, and BMS servers cannot be fixed. Fixing them may make some functions unavailable.
- Kernel vulnerabilities of CCE hosts cannot be automatically fixed. HSS automatically filters out such vulnerabilities when fixing vulnerability in batches.
- 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**.

Fixing Vulnerabilities on the Console

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

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

Figure 9-27 W	Vorkspace managen	nent page
---------------	-------------------	-----------

SecMaster	Management 💮				Process
Security Overview Workspaces Management Agencies	$\label{eq:rescaled} \fbox{\begin{tabular}{c} \hline \begin{tabular}{c} \hline \begin$				C Q
Purchased Resources Security Governance(beta)		 ∋ Incidents 0 ○ Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C i Indicat 0 Playbo 0

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

Figure 9-28 Accessing the vulnerability management page

	erabilities							
nty Stuation •	VulnerabilityStatistics							
Prevention	Vulnerability Type Distribution	Top 5 Valnerabilities	Waterability ID	Valnerability Type	Top 5 Vulnerable Resources			
aseline Inspection			Name10 o	Affected		High Medium Low		
diverabilities mergoncy		 Linux Vulnerability 	CVE-2021-41617	3		ecc-		
inerability Notices	309	Windows Witterabilities	CVE-2022-24903	3		ect-		
ilicy management	309	Web-CMS Vulnerability	CVE-2023-40785	3				
ity Orchestration 👻		Application Vulnerabilities	CVE-2018-25032	2		ect-		
р т			CVE-2019-12749	2				
	Linux Vulnerabilities Windows Vulnera Bain Report	billies Web-CMS Vulnerabilie	s Application Vulnerabilities					C 0
								()
	Batch Report			Affected Assets	Weeksbilly (D	Last Scanned	Handled	
	Balan Repair Impot	performed by name or a combination of sea graded	ech otheria.	Affected Assets	Webenability (D) CVIE-2019-14336	Last Scanned 2024/91/29 14 49 20 832 GMT-98 99	Handled Handled	
	Baith Repair Impat Q. Enter a keyvort. By default, the search is Voleesability Name	performed by name or a combination of sea graded Medium	nch orbenia. 10	Affected Assets 1			Handled	

- 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 9-10**.

D NOTE

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

Table 9-10 Vulnerability fix c	ommands	

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

• Vulnerability Fixing Methods

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

- Method 1: Create a VM to fix the vulnerability.

i. Create an image for the ECS host whose vulnerability needs to be fixed. For details, see **Creating a Full-ECS Image from an ECS**.

- ii. Use the image to create an ECS. For details, see **Creating an ECS** from an Image.
- 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. For details, see **Creating a CSBS Backup**.
 - 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. For details, see **Using Backups to Restore Servers**.

D NOTE

- Use method 1 if you are fixing a vulnerability for the first time and cannot estimate the impact on services. You are advised use pay-per-use billing for newly created ECSs. After the service switchover, you can change the billing mode to yearly/monthly. In this way, you can release the ECSs at any time to save costs if the vulnerability fails to be fixed.
- 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.

Method	Operation
Manual verification	 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: CentOS, Fedora, EulerOS, Red Hat, and Oracle: rpm -qa grep Software name Debian and Ubuntu: dpkg -l grep Software name Gentoo: emergesearch Software name Perform a manual scan on the HSS console to check the vulnerability fixing result.
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.

Table 9-11 Verification

Related Operations

If you evaluate that some vulnerabilities do not affect your services and do not want to view the vulnerabilities in the vulnerability list, you can whitelist the vulnerabilities. After they are whitelisted, the vulnerabilities will be ignored in the vulnerability list and no alarms will be reported. The vulnerabilities will not be scanned and the vulnerability information will not be displayed when the next vulnerability scan task is executed. For details, see **Handling Vulnerabilities**.

9.2.4 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-29 Workspace management page



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

Figure 9-30 Accessing the vulnerability management page

< / / Volnesabilit	100 C									
Security Situation	AutoerabilityStatistics									
Resource Manager Rick Prevention	Vulnerability Type Distribution		Top 5 Valverabilities	Wexceller D	Vulnerability Type	op 5 Vulnerable Resources				
Baseline Inspection	309		Namo1D o	Affected		High • Medium • Low				
Vulnerabilities		Linux Vulnerability	CVE-2021-41617	3		N9-				
Vulnerability Notices		 Windows Winerabilities 	CVE-2022-24903	а		101-				
Policy management Threat Operations		Web-CMS Vulnerability	CVE-2023-48795	3						
Security Orchestration 👻		Application Valnerabilities	CVE-2018-25032	2		105-				
Settings 👻			CVE-2019-12749	2						
	Linux Valenzebilities Windows Winersbillites Web-CVIS Valenzabilities Application Valenzabilities									
	Bath Repair (Import)							C C		
	C). Enter a keyword. By default, the search is p								۲	
	Vulnerability Name	graded	D	Affected Assets	Vulnerability ID	Last Scanned	Handled			
	CESA-2019/2829 Important CentO	e Medium	CESA-2019.2829	1	CVE-2019-14835	2024/01/29 14:49:20:832 GMT+08:00	Handled			
	CESA-2019 2864 Important CantO	le Medium	CE5A-2018/2954	1	CVE-2018-20959,CVE-2019-13638	2024/01/29 14:49:30.775 GMT=00.90	Handled			
	CESA-2019 3055 important CentO	😑 High	CESA-2018.3055	1	CVE-2010-20856.CVE-2019-10126	2024/01/29 14:49:20.890 GMT+08:00	Handled		_	

- Step 5 On the displayed page, click Linux Vulnerabilities, Windows Vulnerabilities, Web-CMS Vulnerabilities, or Application Vulnerabilities.
- **Step 6** Click **Import** above the vulnerability list. The **Import** dialog box is displayed.
- **Step 7** In the **Import** dialog box, click **Download Template** to download a template, and fill in the downloaded template according to the requirements.
- **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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-31 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	$\label{eq:rescaled} \fbox{\begin{tabular}{lllllllllllllllllllllllllllllllllll$				C
Purchased Resources Security Governance(beta)	Current account 0 4699777 Vedia12 Region Paged- Mare Not hoted.	 Incidents 0 △ Assets 0 	 ◊ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 Mindicat 0 Playto 0

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

Figure 9-32 Accessing the vulnerability management page

tanaper 👻	ValuerabilityStatistics							
ntion 🔺	Vulnerability Type Distribution		Top 5 Valnerabilities	Waterability ID	Valnerability Type	Top 5 Valnerable Resources		
e Inspection			Name1D o	Affected		High Medium Low		
billes ncv		 Linux Vulnerability 	CVE-2021-41617	3		ecs-		
billy Notices		Windows Walnerabilities	CVE-2022-24903	3				
ranagement	309	Web-CMS Vulnerability	CVE-2023-40785	3		622		
stors •		Application Vulnerabilities	CVE-2018-25032	2		601-		
			CVE-2019-12749	2				
	1		C40201912749	2				
	Linux Vulnerabilities Windows Vulne	abilities Web-CMS Vulnerabilitie		2				
	Linux Vulnerabilities Windows Vulne Basa Rapor Preset	abilities Web-CMS Vuinerabilitie		2				C C
			s Application Vulnerabilities	2				C C
	Beich Report		s Application Vulnerabilities	2 Allocited Assets	Weeksbilly D	Lost Scanned	Handled	C C

- Step 5 On the displayed page, click Linux Vulnerabilities, Windows Vulnerabilities, Web-CMS Vulnerabilities, or Application Vulnerabilities.
- **Step 6** Click ^C in the upper right corner above the vulnerability list. The **Export** dialog box is displayed.

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

Table 9-12	Exporting	vulnerabilities
------------	-----------	-----------------

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

Step 8 Click OK.

The system automatically downloads the Excel to your local PC.

----End

9.2.5 Ignoring and Unignoring a Vulnerability

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

Figure 9-33 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspeces	Credit Workspace $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Or addroll for the constant Or addroll for the constant for the c	incidents Assets	♥ Vulner 0 ⊜ Securl 0	Alerts Alerts Alerts Alerts Alerts	Selected Spaces C ⑧ ↓ Indicat 0 B Playbo 0

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

/ Vulnerability								
	unerabilityStatistics							
tion 🔺	Vulnerability Type Distribution		Top 5 Valnerabilities	Welnerability ID	Vulnerability Type	op 5 Velhereble Resources		
Inspection			Name10 o	Affected		e High 😐 Medium 😐 Low		
billes NY		Linux Valmerability	CVE-2021-41617	3		ecc-		
Ry Ilby Notices		 Windows Walnerabilities 	CVE-2022-24903	3				
anagement	309	Web-CMS Vulnerability	CVE-2023-60785	3		ecs		
atom •		Application Vulnerabilities	CVE-2018-25032	2		ecs-		
			CVE-2019-12749	2				
1	Unux Vulnerabilities Windows Winerab	illies Web-CMS Vulnerabilitie	s Application Vulnerabilities					C C 6
	Q. Enter a keyword. By default, the search is p	informed by name or a combination of sac	anti mbala					0
	Vulnerability Name	graded	D	Affected Assets	Waterability ID	Last Scanned	Handled	~
			CE8A-2019.2829	1	CVE-2019-14835	2024/01/29 14:49:20.832 GMT+08:00	Handled	
	CESA-2012 2954 Important CantO	e Medum	CE5A-2012-2954	4	CVE-2018-20959,CVE-2019-13538	2024/01/29 14:49:30.775 GMT+00.00	Handled	

Figure 9-34 Accessing the vulnerability management page

- Step 5 On the displayed page, click Linux Vulnerabilities, Windows Vulnerabilities, Web-CMS Vulnerabilities, or Application Vulnerabilities.
- **Step 6** In the vulnerability list, click the name of the target vulnerability. The vulnerability details page is displayed.
- **Step 7** Ignore or unignore the target vulnerability.
 - Ignore

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

- Unignore
 - a. On the **Vulnerability Details** page, click **Affected Resources**. In the resource list, locate the row that contains the target resource and click **More** and then **Cancel Ignore** in the **Operation** column.
 - b. In the confirmation dialog box, confirm the information and click **OK**.

----End

9.3 Viewing/Exporting Emergency Vulnerability Notices

Background

SecMaster obtains data from Huawei Cloud security notices and dynamically displays security vulnerabilities disclosed in the industry, making it easier for you to obtain security vulnerability details, impact scope, and handling suggestions.

With the emergency vulnerability notices, you can easily:

- Backtrack disclosed vulnerabilities dated from April 2014.
- View latest vulnerability notices which are updated every 5 minutes.
- View emergency vulnerability notices by disclosure time.
- Search for emergency vulnerability notices by keyword.
- Export the list of emergency vulnerability notices.

Scenario

This topic describes how to view and export emergency vulnerability notices.

Limitations and Constraints

- Only disclosed vulnerability notices dated from April 2014 can be backtracked.
- Only vulnerability notice list can be exported. To learn details, click the link of the notice name you want.

Viewing Emergency Vulnerability Notices

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-35 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	Credit Vibrispen $\label{eq:Vibrispendix} \overline{V} \mbox{ Inter a none and layoutd for search}.$				C Q
Purchased Resources Security Governance(beta)	Ormet accord 0: 469977 defa12 Report Project- More Nid hoted. Video Video Video	 Incidents 0 Assets 0 	♥ Vuiner 0	O Alerts 0 instan 0	Selected Spaces C 🛞 indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Risk Prevention** > **Emergency Vulnerability Notices**.

Figure 9-36 Accessing the emergency vulnerability notices page

Security Situation	-	
Resource Manager	*	Al(200) • Umread Read Alt time • Enter a keyword. Q Updeted: Aug 17, 2023 16:15:06 GMT+08:00 ① Mark all as read []
Risk Prevention	*	Disclosed
Baseline Inspection Vulnerabilities		Aug 10, 2023 09:21:07 GMT+00:00 Microsoft Releases August 2023 Security Updates
Emergency		Jul 27, 2023 16:15:43 GMT+08:00 Apache Shiro Authentication Bypass Vulnerability (CVE-2023-34478)
Vulnerability Notices		Jul 17, 2023 17:32:23 GMT+08:00 Apache RocketMQ Remote Code Execution Vulnerability (CVE-2023-37582)
Policy management Threat Operations	-	Jul 14, 2023 11:12:26 GMT+08:00 Microsoft Releases July 2023 Security Updates
Security Orchestration	-	Jun 15, 2023 17:01:29 GMT+08:00 Microsoft Releases June 2023 Security Updates
Settings	-	Jun 12, 2023 15:39:55 GMT+08:00 Nacos Jraft Hessian Deserialization Remote Code Execution Vulnerability
		May 11, 2023 15:44-18 GMT+08:00 Microsoft Releases May 2023 Security Updates
	1	Arr 20 2023 16:46/12 (24XTa00:00 Ansarba Sumereal Membra Jurihanitudion Durvers Mulawarbillity (CVE2/023.2787.4)

Step 5 View the update time of emergency vulnerability notices.

View the update time next to **Updated** in the upper right corner above the list of notices.

Step 6 View details of an emergency vulnerability notice.

Click the name of the emergency vulnerability you wish to learn about to switch to the vulnerability notice page. You can view the vulnerability disclosure process, severity, affected products, and handling method.

Step 7 View emergency vulnerability notices by time range.

Select **All time**, **Last 7 days**, **Last 3 days**, or **Last 24 hours** to view the emergency vulnerability notices reported during the selected period.

Step 8 Search for historical emergency vulnerability notices.

Enter a keyword in the search box to search for emergency vulnerability notices that meet the filter criteria.

----End

Exporting Emergency Vulnerability Notices

On the **Emergency Vulnerability Notices** tab, click the export icon in the upper right corner to download listed notices as an Excel file. You can then view emergency vulnerability notices offline.

The exported Excel file contains the notice names, disclosure time, and links.

9.4 Policy Management

9.4.1 Overview

You can use SecMaster to manage and maintain tasks across accounts with ease, making it simple to implement protection of different services, including WAF, CFW, VPC security groups and IAM.

In the policy management module, 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 blacklist policies of CFW/WAF/VPC security groups/IAM.
- 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. A maximum of 50 IP addresses or IAM users can be selected as blocked objects for an emergency policy.
- If an IP address or IP address range or an IAM user is added to the blacklist, CFW/WAF/VPC/IAM will block requests from that IP address without checking whether the requests are malicious.

9.4.2 Viewing Defense Policies

Scenario

This section describes how to view defense policies.

There are seven defense lines, physical, identity, server, maintenance, data, application, and network defense lines.

Procedure

Step 1 Log in to the management console.

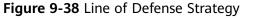
Step 2 Click — in the upper left corner of the page and choose Security & Compliance > SecMaster.

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

Figure 9-37 Workspace management page

SecMaster	Management (?)				Process
Security Overview Workspeces Management Agencies	Credit WithSpace If later a name and layound for search.				C
Purchased Resources Security Governance(beta)	Control Second 0 469977 Veder2 Region I Project- None Not Include.	incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 instan 0	Selected Spaces C ⓒ indicat 0 Playbo 0

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



< / / Polcy management						
Security Situation 🔹	Line of Defense Strategy Em	nergency strategy				
Resource Manager 🔹 💌	0					
Risk Prevention						
Baseline Inspection						
Vulnerability	30			3		
Emergency Valnerability Notices	50			Security Cloud Brain		
Policy management	Health Score					
Threat Operations 💌	139 Total Assets					Layer 7 Defense Line
Security Orchest 👻	3 Guantity of High-Risk		(a) (a)			
Settings 💌	Assets	Ph	sical Defense Line Identity Defense Line Network Defense	ine Application Defense Line Host Defense Line Def	a Defense Line O&M Defense Line	
	136 Number of assets at other risk levels					
	116 Threat Alarm					Resource
	167 Winerability Risk	2221			2 2 2	
	62 Baseline Risk	a a a		9 9 9 9	RDS 2	
			0000		NDS 2	
		ECS 11	Website 11	IP 60	-	

Step 5 View defense policy statistics.

• Health Score: indicates the current health status of resources.

The score ranges from 0 to 100. The higher the security score, the more secure your resources. For details, see **Security Score**.

- **Total Assets**: displays how many assets, high-risk assets, and assets at other risk levels you have.
- Threat alarm, vulnerability, and baseline check statistics: display unhandled threat alarms, unfixed vulnerabilities, and risky baseline settings.
 - **Threat Alarm**: Displays threat alarms that have not been handled in **the last seven days**.
 - Vulnerability Risk: Displays the top 5 types of vulnerabilities in assets and the total number of vulnerabilities that have not been fixed in the last seven days.
 - Baseline Risk: displays resources by risk severity, including critical, high, medium, low, and informational levels, based on the latest baseline inspection results.
- SecMaster Protection Overview: displays the protection status and resource information in the seven defense lines.
 - In the seven defense line area, you can click the icon of a defense line to view the protection products and protection statistics of the defense line.
 - You can view the resource statistics in the resource area.

----End

9.4.3 Configuring Defense Policies

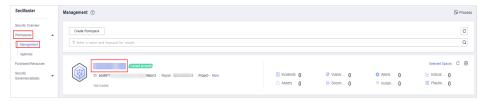
Scenario

This section describes how to configure protection policies.

Procedure

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

Figure 9-39 Workspace management page



Step 4 In the navigation pane on the left, choose Risk Prevention > Policy Management.

-			55			
< / Po	licy management.					
Security Situation 💌	Line of Defense Strategy	Emergency strategy				
Resource Manager 🔹 👻	0					
Risk Prevention						
Baseline Inspection						
Vulnerability	30 Beref Chad Rep					
Emergency Vulnerability Notices				Security Cloud Brain		
Policy management	Health Score					
Threat Operations 👻	139 Total Assets					Layer 7 Defense Line
Security Orchest 🔹	3 Quantity of High-Risk					
Settings •	Assets 136 Number of assets at		Physical Defense Line Identity Defense Line Network Defense	Line Application Defense Line Host Defense Line Data De	rlense Line O&M Defense Line	
	other risk levels					
	116 Threat Alarm					Resource
	167 Vulnerability Risk					
	62 Baseline Risk				RDS 2	
					3	
		ECS 11	Website 11	IP 60		

Figure 9-40 Line of Defense Strategy

- **Step 5** Click the name of the defense line to which the security service belongs. The cloud service information corresponding to the defense line slides out from the right.
- **Step 6** On the tab page of the corresponding cloud service, click **Protection Policy** to go to the configuration page.

If you have not purchased the corresponding cloud service, click the service name under service overview in the tab to go to the service console and purchase the service.

- **Step 7** On the policy configuration page, configure policies of the corresponding cloud service.
 - Anti-DDoS policy configuration:
 - Configuring a Protection Policy

- Configuring a Proteciton Policy
- CFW protection policies: Configuring Intrusion Prevention and Basic Defense Rule Management
- WAF protection policies: Creating a Protection Policy
- HSS protection policies: Enabling HSS, Creating a Policy Group, and Installation and Configuration

----End

9.4.4 Adding or Editing an Emergency Policy

Scenario

SecMaster can create blacklist policies for CFW/WAF/VPC security groups/IAM.

An emergency policy is used to quickly block attacks. You can select a block type based on the alert source to block attackers. **Table 9-13** lists recommended settings. You can also block a single attack source based on the comprehensive investigation of multiple alerts.

Alert Type	Defense Layer	Recommended Policy		
HSS alerts	Server protection	VPC policies are recommended to block traffic.		
WAF alerts	Application protection	WAF policies are recommended to block traffic.		
CFW alerts	Network protection	CFW policies are recommended to block traffic.		
IAM alerts	Identity authentication	IAM policies are recommended to block traffic.		
OBS and DBSS alerts	Data protection	You can use VPC or CFW policies based on actual attack scenarios and investigation results to disconnect attack sources from protected resources.		

Table 9-13 Recommended blocking policies

This topic describes how to add or 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. A maximum of 50 IP addresses or IAM users can be selected as blocked objects for an emergency policy.

- If an IP address or IP address range or an IAM user is added to the blacklist, CFW/WAF/VPC/IAM 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, IP address ranges, or IAM user names, cannot be modified.

Prerequisites

If the blocked object is an IAM user, you need to create a SecMaster agency before adding an emergency policy. For details, see **Creating a SecMaster Agency**.

Adding an Emergency Policy

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

Figure 9-41 Workspace management page

SecMaster	Management ()		🕞 Process
Security Overview Workspaces Management Agencies	Orable Windspee V Enter a more and legende for search.		C
Purchased Resources Security Governance(beta)	Control Contro Control Control Control Control Control Control Control Control Co	 Alerts Instan 0 	Selected Spaces C 🗟

Step 4 In the navigation pane on the left, choose Risk Prevention > Policy management. Then, click the Emergency strategy tab to go to the emergency policy page.

Figure 9-42 Emergency strategy page

	lcy management										
vity Situation 🔻 🔻	Line of Defense Strategy Em	ergency strategy									
ource Manager 🛛 🔻											
Prevention 0		-									
Baseline Inspection	Number of delivered policie	ez (j)	8	Top 3 Operation	Connections ⑦			Top 5 Blocking Areas 💿	Statistics by week		
Alinerabilities	WAF		3	rank	Operation Connect	ion	Number of				
Emergency	CFW		1	1			4			10	
Admerability Notices				2			3				
Policy management							4				
et Operations 🛛 🔻				3			1	_	2		
urity Orchestration 💌											
ngs 🔍 👻											
	Add Batch Delete										
	Q. By default, data is searched b	y keyword.									C
	Block Object 0	Label 0		Number of d 0	Block Type 0	Creator 0	Reason Descri	Creation Time 0	Operation		
	1 151	label		1	Source Ip	op_svc_ssa_cc	安全云涧荫动化	Mar 04, 2024 11:39:43 GMT+06:00	Edit Batch Block	Cancel Blocking in Batches	Delete
	i	label		1	Source Ip	ep_6vc_558_cc	安全云照目动化	Mar 02, 2024 11:21:06 GMT+06:00	Edit Batch Block	Cancel Blocking in Batches	Delete

Step 5 On the **Emergency strategy** 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.

Parameter	Description
Blocked Object Type	Type of the object to be blocked. You can select IP or IAM .
Block Object	 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 (,). Example: Single IP address: 192.168.0.0 IP address range: 192.168.0.0/12 If you select IAM for Blocked Object Type, enter IAM user names.
	 A maximum of 50 IP addresses, IP address ranges, or IAM users can be blocked by an emergency policy once.
Label	Label of a custom emergency policy.
Operation Connection	Select the operation connection for the policy.
Block Aging	Check whether the policy needs to be stopped.
	• 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.
Reason Description	Description of the custom policy.

Table 9-14 Emergency policy parameters

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, IP address ranges, or IAM user names, cannot be modified.

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

Figure 9-43 Workspace management page

SecMaster	Management (🕼 Process
Security Overview Workspeces Management Agencies	Create Wanspece				C Q
Purchased Resources Security Governance(beta)	General econom D add0077 dede12 Region Project- Nove Not hoted:	incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C i Indicat 0 ⊫ Playbo 0

Step 4 In the navigation pane on the left, choose Risk Prevention > Policy management. Then, click the Emergency strategy tab to go to the emergency policy page.

Figure 9-44 Emergency strategy page

< //	Polic)	r management										
Security Situation		Line of Defense Strategy Emergency strateg										
Resource Manager 🔹 👻												
Risk Prevention 0 Baseline Inspection		Number of delivered policies ③			Top 3 Operation	Connections ⑦			Top 5 Blocking Areas 💮	Statistics by week		
Vulnerabilities		VPC WAF	8		rank	Operation Connection	4	Number of				
Emergency Vulnerability Notices		CFW	1		1			8	_			10
Policy management					2			3				
Threat Operations					3			1		2		
Security Orchestration 🛛 👻												
Settings 👻												
	4	Add Batch Delete										
		Q. By default, data is searched by keyword.										C 💿
		Block Object 0	Label 0	N	umber of d 0	Block Type 0	Creator 0	Reason Descri	Creation Time 0	Operation		
		1 151	label	1		Source Ip	op_svc_ssa_cc	安全云旗自动化	Mar 04, 2024 11:39:43 GMT+08:00	Edit Batch Block	Cancel Blocking in B	Satches Delete
		114	label	1		Source Ip	00_5VC_558_CC	安全云朝目动化	Mar 02, 2024 11:21:06 GMT+00:00	Edit Batch Block	Cancel Blocking in I	Satches Delete
		10 v Total Records: 2 < 1 >										

- **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 9-15 Emergency policy parameters

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.
Block Aging	 Check whether the policy needs to be stopped. 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.

Parameter	Description
Reason Description	Description of the custom policy.

Step 7 Click OK.

----End

Creating a SecMaster Agency

If the blocked object is an IAM user, you need to create a SecMaster agency before adding an emergency policy. Perform the following steps:

- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Management & Governance > Identity and Access Management.
- **Step 3** Add a custom policy.
 - 1. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.
 - 2. Configure a policy.
 - **Policy Name**: Enter a policy name.
 - **Policy View**: Select **JSON**.
 - **Policy Content**: Copy the following content and paste it in the text box.

```
"Version": "1.1",
"Statement": [
{
"Effect": "Allow",
"Action": [
"iam:users:updateUser"
]
}
]
```

a. Click OK.

}

Step 4 Create an agency.

- 1. In the navigation pane on the left, choose **Agencies**. On the page displayed, click **SecMaster_Agency**. The **Basic Information** page of **SecMaster_Agency** is displayed by default.
- 2. On the **Permissions** tab page, click **Authorize**.
- 3. On the **Select Policy/Role** page, search for and select the policy added in **Step 3** and click **Next**.
- 4. Set the authorization scope. Select **All resources** for **Scope**. After the setting is complete, click **OK**.

----End

9.4.5 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-45 Workspace management page



Step 4 In the navigation pane on the left, choose Risk Prevention > Policy management. Then, click the Emergency strategy tab to go to the emergency policy page.

Figure 9-46 Emergency strategy page

< / P	biloy mar	ragement									
Security Situation 🗸 🔻	Line	of Defense Strategy Emergency stra	ategy 8								
Resource Manager 🔹											
Risk Prevention		Number of delivered policies ③			Top 3 Operation	Connections (?)			Top 5 Blocking Areas 💮	Statistics by week	
Baseline Inspection		VPC		8	rank	Operation Connection	15	Number of			
Emergency		WAF CPW		3	1			4		10	
Vulnerability Notices					2			3			
Policy management					3			1		2	
Security Orchestration											
Settings •											
	•	Add Batch Delete									
		Q. By default, data is searched by keyword.									C (
		Block Object 0	Label 0		Number of d 0	Block Type 0	Creator 0	Reason Descri	Creation Time 0	Operation	
		1 151	label		1	Source Ip	op_svc_ssa_cc	安全云旗自动化	Mar 04, 2024 11:39:43 GMT+08:00	Edit Batch Block Cancel Blocking in Batches	Delete
		inclusion114	label		1	Source Ip	0p_6VC_558_CC	安全云照目动化	Mar 02, 2024 11:21:06 GMT+06:00	Edit Batch Block Cancel Blocking in Batches	Delote
		10 💌 Total Records: 2 🛛 < 🚺 >									

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.

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

 Table 9-16 Emergency policy parameters

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

9.4.6 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-47 Workspace management page

SecMaster	Management ③				D Process
Security Overview Workspaces	Credit Workspace $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Contract Control Contro Control Control Control Contr	 Incidents 0 Assets 0 	♥ Vulner 0 i Securl 0	O Alerts 0 instan0	Selected Spaces C 🗟 Mindicat 0 S Playbo 0

Step 4 In the navigation pane on the left, choose Risk Prevention > Policy management. Then, click the Emergency strategy tab to go to the emergency policy page.

urity Situation •	Line of Defense Strategy	rgency strategy									
Prevention Baseline Inspection	Number of delivered policie:	• ①		Top 3 Operation	Connections ⑦			Top 5 Blocking Areas 🕥	Statistics by week		
Vuinerabilities	VPC		8	rank	Operation Connect	ion	Number of				
Emergency	CFW		3	1			8				10
Vulnerability Notices				2			3				
Policy management				3			1		,		
at Operations 💌							1		2		
rity Orchestration 🔻											
igs w											
	Add Batch Delete										
	Q. By default, data is searched by	keyword.									С
	Block Object 0	Label 0		Number of d 0	Block Type 0	Creator 0	Reason Descri Cre	ation Time 0	Operation		
	151	label		1	Source Ip	00_5VC_558_CC	安全云脑草动化 Ma	04, 2024 11:39:43 GMT+08:00	Edit Batch Block	Cancel Blocking	n Batches Delete

Figure 9-48 Emergency strategy 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

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

Scenario

If an IP address, IAM user, 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, IAM user, 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 or IP address range or an IAM user is added to the blacklist, CFW/WAF/VPC/IAM 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 left corner of the page and choose Security & Compliance > SecMaster.

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

Figure 9-49 Workspace management page

SecMaster	Management ③				🗇 Process
Security Overview Workspaces	Credit Workspace $\overline{\nabla} \ \ \ \ \ \ \ \ \ \ \ \ \ $				Q
Purchased Resources Security Governance(beta)	Constant Cons	S Incidents 0 Assets 0	Ø Vulner 0 ⊜ Securi 0	O Alerts O instan O	Selected Spaces C

Step 4 In the navigation pane on the left, choose Risk Prevention > Policy management. Then, click the Emergency strategy tab to go to the emergency policy page.

Figure 9-50 Emergency strategy page

< / Pi	olicy ma	nagement									
Security Situation 🔹	Line	e of Defense Strategy Emergency strategy									
Resource Manager 🛛 👻											
Resc Prevention •		Number of delivered policies ③	8 3 1	Top 3 Operation nank 1 2 3	n Connections ⑦ Operation Connection	28	Number of 8 3	Top 5 Blocking Areas 💮	Italistics by week	10	
Security Orchestration 💌											
Settings 👻											
	4	Add Babb Delete Q. By delauf, data is searched by keyword. Block Object 0 Block Object 0 Block Object 10 Block Object 11	Label 0	Number of d 0 1	Block Type 0 Source Ip Source Ip	Creator 0 09_594_508_00 09_594_588_00	安全云旗章动化	Enestion Time © dar 04, 2024 11:38:43 GMT+06:00 dar 02, 2024 11:21:06 GMT+06:00	Operation Edit Batch Block Canc Edit Batch Block Canc		
		10 • Total Records: 2 < 1 >									

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

Figure 9-51	Workspace	management page
-------------	-----------	-----------------

SecMaster	Management ①				🕞 Process
Security Overview Workspaces Management Agencies	Create Writespace $\label{eq:product} \overline{V} \mbox{ Inter a same and layourd for seach}.$				C
Purchased Resources Security Governance(beta)	Constanting Constanti	 incidents 0 Assets 0 	Vulner 0	O Alerts 0 instan 0	Selected Spaces C

Step 4 In the navigation pane on the left, choose Risk Prevention > Policy management. Then, click the Emergency strategy tab to go to the emergency policy page.

rity Situation 👻	Line of Defense Strategy	icy strategy 8								
Prevention 0 🔺	Number of delivered policies (D		Top 3 Operation	Connections			Top 5 Blocking Areas 💿	Statistics by week	
Unerabilities	VPC WAF	1	3	rank	Operation Connect	ion	Number of			
mergency Unerability Notices	CFW		1	1			4		1	0
vinerability Notices				2			3			
at Operations				3			1	-	2	
rity Orchestration 🔻										
195 v										
	Add Batch Delete Q. By detault, data is searched by key	rerd.								С
	Block Object 0	Label 0		Number of d 0	Block Type 0	Creator 0	Reason Descri Cr	eation Time 0	Operation	
	1 151	label		1	Source Ip	ep_svc_ssa_cc	安全安接真动化	ar 04, 2024 11:39:43 GMT+08:00	Edit Batch Block Cancel Blocking in Ba	tches Delete
	issues:114	label		1	Source Ip	60.5VC.558.CC	安全云明目动化	er 02, 2024 11:21:06 GMT+06:00	Edit Batch Block Cancel Blocking in Ba	tches Delete

Figure 9-52 Emergency strategy 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

10 Threat Operations

10.1 Incident Management

10.1.1 Viewing Incidents

Scenario

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

This topic describes how to view incident information.

Procedure

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

Figure 10-1 Workspace management page

SecMaster	Management ③				🕞 Process
Security Overview Workspaces	Could Hiphigan				C
Purchased Resources Security Governance(beta)	Constant except	Incidents 0 Assets 0	♥ Vuiner 0 Securl 0	● Alerts 0 linstan 0	Selected Spaces C ⊗ Mindicat 0 S Playbo 0

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

Figure 10-2 Incidents

nhandled incidents							Auto		,	Manual Incident		Incidents Number		
6			6		• F • F • L • T	tigh 2 ow 1	6			12		24		
Add Import	Balch Close	Batch Delete									Feb 01, 2024 00:00:0	0 — Feb 07, 2024 23 59 59	• •	c
Q Enter a keyword. E	y default, the search	is performed by nam	ne or a combination of	search criteria.										đ
Incident	Incident ID	Incident	Status	Verificati	Owner	Creation	First Occ	Last Occ	Planned	Description	Data Sou	Operation		
Closed	ab9a54dd-17	O High	Closed H	Unknown	i	2024/02/06 11	2024/02/05 1				Database Sec	Edit Close Delete		
Closed	3049e754-37	O High	O Closed H	Unknown		2024/02/06 0	2024/02/05 1	-	-		Detabase Sec	Edit Close Delete		
Closed	92045070-31	O High	O Closed H	Unknown		2024/02/05 1	2024/02/04 1				Database Sec	Edit Close Delete		
Closed	92d7c3bb-76	O Low	O Closed H	Unknown		2024/02/05 1	2024/02/05 11	-	-		Host Security	Edit Close Delete		
	2151315e-1152	O Tes	Open Un	Unknown		2024/02/03 1	2024/02/03 1	-	-		Host Security	Edit Close Delete		
5 - Total Recon		2 2 4 5	> 01											

Step 5 On the **Incidents** page, view incident details.

Figure 10-3 Viewing an Incident

Unhandled incidents							Auto		М	anual Incident		Incidents Number	
6			6		● 5 ● H ● U ● T	igh 2 ow 1	6			12		24	
Add Import	Batch Close	Batch Delete								0	Feb 01, 2024 00:00.0	0 – Feb 07, 2024 23:59:59	
Q. Enter a keyword	By default, the search	is performed by nar	e or a combination of	search criteria.									0
Incident	Incident ID	Incident	Status	Verificati	Owner	Creation	First Occ	Last Occ	Planned	Description	Data Sou	Operation	
Closed	ab9a54dd-17	O High	O Closed H	Unknown	ş	2024/02/06 11	2024/02/05 1	-	-		Database Sec	Edit Close Delete	
Closed	3049e754-37	O High	O Closed H	Unknown		2024/02/06 0	2024/02/05 1	-	-		Detabase Sec	Edt Close Delete	
Closed	920a5b70-31	O High	O Closed H	Unknown		2024/02/05 1	2024/02/04 1				Database Sec	Edit Close Delete	
Closed	92d7c3bb-76	O Low	O Closed H	Unknown		2024/02/05 1	2024/02/05 11				Host Security	Edit Close Delete	
	2151315e-1152	O Tes	Open Un	Unknown		2024/02/03 1	2024/02/03 1		-		Host Security	Edit Close Delete	
5 • Total Rec	rds: 24 🦳 🤆 🚺	2 3 4 5	> Go										

Table 10-1 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	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.
	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.
	• 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

10.1.2 Adding or 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-4 Workspace management page

SecMaster	Management ()				Process
Security Overview Workspaces	$\begin{tabular}{c} \hline \end{tabular} \hline \end{tabular} $				C
Purchased Resources Security Governance(beta)	Grand scores G	Incidents 0 Assets 0	Vulner 0	O Alerts 0 ◎ Instan 0	Selected Spaces C 🛞

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

Figure 10-5 Incidents

handled Incide	ents						Auto		,	Manual Incident		Incidents Number	
6		(6		 6 6 6 7 	igh 2 ow 1	6			12		24	
Add	Import Batch Cir	se Batch Dele	10								Feb 01, 2024 00:00.0	10 - Feb 07, 2024 23:59:59	c
Q. Enter a kx	ryword. By default, the se	arch is performed by na	ame or a combination o	f search criteria.									Ċ
_ Incide	int Incident I	Incident	Status	Verificati	Owner	Creation	First Occ	Last Occ	Planned	Description	Data Sou	Operation	
Close	d ab9a54dd-1	O Hon	O Closed H	Unknown		2024/02/06 11	2024/02/05 1				Database Sec	Edt Close Delete	
Close	d 3549e754-3	O High	O Closed H	Unknown		2024/02/06 0	2024/02/05 1	-	-		Database Sec	Edt Close Delete	
Citere	d 920a5670-3	O High	O Closed H	Unknown		2024/02/05 1	2024/02/04 1	-	-		Detabase Sec	Edit Close Delete	
Close	d 92d7c3bb-7f	Low	O Closed H	Unknown		2024/02/06 1	2024/02/05 11	-			Host Security	Edit Close Delete	
	2151315e-115	2 O Tips	Open Un	Unknown		2024/02/03 1	2024/02/03 1	-	-		Host Security	Edit Close Delete	
	al Records: 24 <		5 - 00										

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

Parameter		Description
Basic Informati on	Incident Name	 Custom incident name. The value must contain: Only uppercase letters, lowercase letters, digits, and the special characters: () A maximum of 255 characters
	Incident Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Level	Severity level. The options are Tips , Low , Medium , High , and Fatal .
	Status	Incident status. The options are Open , Blocked , and Closed .
	Data Source Name	Data source name
	Data Source Type	Type of the data source. The options are Huawei , Third-party , and Tenant .
	(Optional) Owner	Primary owner of the incident.

 Table 10-2 Parameters for adding an incident

Paramete	r	Description
Timeline	First Occurrence Time	Time when the incident occurred first time.
	(Optional) Last Occurrence Time	Time when the incident occurred last time.
	(Optional) Planned Closure Time	Time to close the incident.
Other	(Optional) Verification Status	Verification status of the incident to identify the accuracy of the incident. The options are Unknown , Positive , and False positive .
	(Optional) Stage	 Incident phase. Preparation: Prepare resources to process incidents. Detection and analysis: Detect and analyze the cause of an incident. Contain, extradition, and recovery: Handle an incident. Post Incident Activity: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging
	(Optional) Label	Label of the incident.
	Description	 Incident description. The value can contain: Only uppercase letters, lowercase letters, digits, and the special characters: () A maximum of 1,024 characters.

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

----End

Editing an Incident

Step 1 Log in to the management console.

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

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

Figure 10-6 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Crede Workspace T fator a name and layound for search.				C
Purchased Resources Security Governance(beta)	Current Account D: AddR077 Media12 Region Project- Mars Not handed	 Incidents 0 ○ Assets 0 	 Vuiner 0 ⊜ Securi 0 	Alerts 0	Selected Spaces C 😒 🗠 Indicat 0 🗈 Playbo 0

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

Figure 10-7 Incidents

nhandled incide	ints						Auto		м	anual Incident		Incidents Number		
6			6				6			12		24		
Add	mport Balch Clos	e Baltch Delet									Feb 01, 2024 00:00:0	- Feb 07, 2024 23:59:59	8 6 C	6
Q. Enter a ke	yword. By default, the sea	rch is performed by na	me or a combination of	search criteria.										G
Incide	nt Incident ID	Incident	Status	Verificati	Owner	Creation	First Occ	Last Occ	Planned	Description	Data Sou	Operation		
Close	d ab9a54dd-17		O Closed H	Unknown		2024/02/06 11	2024/02/05 1				Database Sec	Edit Close Delete		
Close	d 3649e754-37	O High	O Closed H	Unknown		2024/02/06 0	2024/02/05 1	-	-		Database Sec	Edit Close Delete		
Citose	d 920a5670-31	O High	O Closed H	Unknown		2024/02/05 1	2024/02/04 1	-	-		Detabase Sec	Edit Close Delete		
Close	d 92d7c30b-76	e Lou	O Closed H	Unknown		2024/02/05 1	2024/02/05 11	-			Host Security	Edit Close Delete		
	2151315e-1152	О Тря	Open Un	Unknown		2024/02/03 1	2024/02/03 1	-	-		Host Security	Edit Close Delete		
5 v Tota	al Records: 24	1 2 3 4 5	→ 00											

- **Step 5** In the incident list, locate the row that contains the target incident and click **Edit** in the **Operation** column.
- **Step 6** On the **Edit** page that is displayed, edit incident parameters.

Table 10-3 Parameters	for editing an incident
-----------------------	-------------------------

Paramete	er	Description
Basic Informa tion	Incident Name	 Custom incident name. The value must contain: Only uppercase letters, lowercase letters, digits, and the special characters: () A maximum of 255 characters
	Incident Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Level	Severity level. The options are Tips , Low , Medium , High , and Fatal .
	Status	Incident status. The options are Open , Blocked , and Closed .
	Data Source Name	Name of the data source, which cannot be changed
	Data Source Type	Type of the data source, which cannot be changed

Paramet	er	Description
	(Optional) Owner	Primary owner of the incident.
Timelin e	First Occurrence Time	Time when the incident occurred first time.
	(Optional) Last Occurrence Time	Time when the incident occurred last time.
	(Optional) Planned Closure Time	Time to close the incident.
Other	(Optional) Verification Status	Verification status of the incident to identify the accuracy of the incident. The options are Unknown, Positive , and False positive .
	(Optional) Phase	 Incident phase. 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: Only uppercase letters, lowercase letters, digits, and the special characters: () A maximum of 1,024 characters.

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

----End

10.1.3 Importing and Exporting Incidents

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

Figure 10-8 Workspace management page

SecMaster	Management 💮	Process
Security Overview Workspeces	Deals Histopea T firster a same and lepsond for search.	C
Agencies Purchased Resources Security Governance(beta)	Constrained Setted Space: Setted Space: Setted Space: Setted Space: O Atem 1 Image: Setted Space: Setted Space: O Atem 2 Image: Setted Space: O Atem 3 C Marcin: O Atem 3 C Image: Setted Space: O Atem 3 C Image: Setted Space: O Atem 3 C Atem 3 Atem 3	

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

Figure 10-9 Incidents

Anhandled Inc	cidents							Auto			Manual Incident		Incidents Number		
6				6				6			12		24		
Add	Import	Batch Close	Batch Dente									Feb 01, 2024 00:00.0	0 - Feb 07, 2024 23:59:59	С	۲
Q. Enter a	a keyword. By i	default, the search i	is performed by nam	e or a combination of	search criteria.										٢
_ Inc	cident	Incident ID	Incident	Status	Verificati	Owner	Creation	First Occ	Last Occ	Planned	Description	Data Sou	Operation		
C)	losed	ab9a54dd-17	O High	O Closed H	Unknown		2024/02/06 11	2024/02/05 1	-			Database Sec	Edit Close Delete		
(c)	losed	3549e754-37	O High	O Closed H	Unknown		2024/02/06 0	2024/02/05 1		-		Database Sec	Edit Close Delete		
(c)	losed	920a5070-31	O High	Closed H	Unknown		2024/02/05 1	2024/02/04 1				Detabase Sec	Edit Close Delete		
C (C)	losed	92d7c3bb-76	O Low	O Closed H	Unknown		2024/02/05 1	2024/02/05 11	-			Host Security	Edit Close Delete		
		2151315e-1152	O Tes	Open Un	Unknown		2024/02/03 1	2024/02/03 1	-			Host Security	Edit Close Delete		
5 +	Total Records:	24 < 1	2 3 4 5	> 00											

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

Figure 10-10 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	$\begin{tabular}{lllllllllllllllllllllllllllllllllll$				C
Purchased Resources Security Governance(beta)	Grand score) Grand score) Grand score) Grand score) Grand score) Grand score) Ket torold.	Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 instan 0	Selected Spaces C

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

Figure 10-11 Incidents

handled incidents							Auto			Manual Incident		Incidents Number		
6		6				iatal 2 tigh 2 .ow 1 tips 1	6			12		24		
Add Import	Batch Close	Balch Delete									Feb 01, 2024 00:00:0	- Feb 07, 2024 23:59:59	C C	:) (4
Q. Enter a keyword. D	y default, the search is pe	normed by name or	a combination of s	earch criteria.										¢
Incident	Incident ID	Incident	Status	Verificati	Owner	Creation	First Occ	Last Occ	Planned	Description	Data Sou	Operation		
Closed	ab9a54dd-17	High O	Closed H	Unknown	į.,	2024/02/06 11	2024/02/05 1	-	-		Database Sec	Edit Close Delete		
Closed	3042e754-37	High O	Closed H	Unknown		2024/02/06 0	2024/02/05 1	-	-		Database Sec	Edt Close Delete		
Closed	920a5670-31 0	High O	Closed H	Unknown		2024/02/05 1	2024/02/04 1				Database Sec	Edit Close Delete		
Closed	92d7c3bb-76	Low 0	Closed H	Unknown		2024/02/05 1	2024/02/05 11	-	-		Host Security	Edit Close Delete		
											Host Security			

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

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

Step 7 Click OK.

The system automatically downloads the Excel to your local PC.

----End

10.1.4 Closing or Deleting Incidents

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 left corner of the page and choose Security & Compliance > SecMaster.

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

Figure 10-12 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspeces	Credit Workspace If form a name and keyword for seach.				C
Agencies Purchased Resources Security Governance(beta)	Control control Control control Control control Control Kel houring	 E Incidents 0 ○ Assets 0 	♥ Vulner 0⊜ Securl 0	O Alerts 0 S Instan 0	Selected Spaces C 🛞 indicat 0 Playbo 0

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

Figure 10-13 Incidents

Unhandled incidents							Auto		м	anual Incident		Incidents Number	
6			6		• 5 • H • L • T	igh 2 w 1	6			12		24	
Add Impo	Batch Close	Batch Delete									Feb 01, 2024 00:00.0	0 - Feb 07, 2024 23:59:59	
Q. Enter a keywo	d. By default, the search	is performed by nan	e or a combination of	search criteria.									(
Incident	Incident ID	Incident	Status	Verificati	Owner	Creation	First Occ	Last Occ	Planned	Description	Data Sou	Operation	
Closed	a09a54dd-17	O High	O Closed H	Unknown		2024/02/06 11	2024/02/05 1	-	-		Database Sec	Edit Close Delete	
Closed	3b49e754-37	O High	O Closed H	Unknown		2024/02/06 0	2024/02/05 1		-		Database Sec	Edit Close Delete	
Closed	920a5b70-31	O High	Closed H	Unknown		2024/02/05 1	2024/02/04 1		-		Detabase Sec	Edit Close Delete	
Closed	92d7c3bb-76	O Low	O Closed H	Unknown		2024/02/05 1	2024/02/05 11				Host Security	Edit Close Delete	
	2151315e-1152	О тря	Open Un	Unknown		2024/02/03 1	2024/02/03 1				Host Security	Edit Close Delete	
5 • Total Re	cords: 24 < 1	2 3 4 5	> 00										

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

5	
Operation	Description
Closing an Incident	 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.
	 In the confirmation dialog box, select Reason for, enter Close Comment, and click OK.
Deleting an Incident	 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 .
	NOTE Deleted incidents cannot be restored. Exercise caution when deleting an incident.

Table 10-5 Managing incidents

----End

10.2 Alert Management

10.2.1 Viewing Alerts

Scenario

On the **Alerts** tab, you can query alerts in the last 360 days. You can view the alert details, including alert name, type, risk severity, and generation time. By customizing filtering conditions, such as the alert name, risk severity, and time, you can quickly query information about the specific alerts.

This section describes how to view alert information.

Procedure

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

Figure 10-14 Workspace management page

SecMaster	Management 💮	Process
Security Overview Workspaces Management Agencies	Oracle Windspace If later a name and leyword for search.	C
Purchased Resources Security Governance(beta)		Selected Spaces C ⑧ № Indicat 0 Playbo 0

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

Figure 10-15 Alerts

								Teelay	This work This	manih	Castorn
handloc	I Alerts				Auto		Mercual		Alerts Number		
	7		7	 High 5 Median Tipe 1 	0		0		7		
Add		Batch Close More *									0
	Type :	And Name (Atarm Severity :	Source IP Address		35e0ae 0	Data Source Prod	Owner :	Creation Time (Operation	(
	Web attacks	[CountillySectionies]	O High		Linkesser	Open Handled au	Haal Desarity Device		2024/02/07 10 33:00 8	Operation +	
	Web attacks	[CoundByTecklaster]	O High		Uninseen	O Open : Handled au	Haal Desarity Device		2024/02/07 10:27:58.4	Operation •	
	Web shell	[CrossedBy/SectAssier]	O Hoh		Unknown	O Open : Handled au	Host Security Service		2624/02/07 10:22:58.8	Operation -	
	Web attacks		O High		Unknown	Open Unhandled	Host Security Service		2024/02/07 10:10:50.5	Operation •	
0	Abserval user behavio		O High		Unknown	Open Unnarded	Host Security Service	-	2024/02/05 16:27:47.6	Operation +	
	Encrypted camency m Matware		O Medice		Uninsees	• Open Unnanded	Hani Desarity Device		2624/02/05 16 27 07 2	Operation +	
•	DNS protocol attacks DDOG attacks		O Ter		Uninsees	Open: Unhandled	Hani Desarity Device		2024/02/04 16 26 16 8	Operation +	
10 *	Total Records: 7										

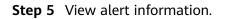


Figure 10-16 Viewing Alerts

									Today	This week This n	ronth Cush	dom
ndled Ale	lerts		-			Auto		Manual		Alerts Number		
-	7	(7	 High 5 Mediar Tips 1 		0		0		7		
Add Alarm Se	Associated Event	Batch Close More •	fer a keyword. By default, the	search is performed by name	or a combination of search (utheia					C	
	npe 0	Alert Name :	Alarm Severity :	Source IP Address	Destination IP Ad		Status :	Data Source Prod	Owner :	Creation Time :	Operation	
	eb atlacks	[CicsedBySecMaster]	O High	-	-	Unknown	O Open Handled au	Host Security Service		2024/02/07 10:33:00.5	Operation •	
	eb attacks	[CiceedBySecMaster]	O High	-	-	Unknown	O Open Handled au	Host Security Service		2024/02/07 10:27:59.4	Operation +	
	eb attacks	[ClosedBySecMaster]	O mpn	-	-	Unknown	O Open Handled au	Host Security Service		2024/02/07 10:22:58.8	Operation •	
	eb atlacks		O High	-	-	Unknown	Open Unhandled	Host Security Service	-	2024/02/07 10:18:58.3	Operation +	
	icious use of token promal user behavio		O mon	-	-	Unknown	Open Unhardled	Host Security Service	0	2024/02/05 16:27:47.6	Operation +	
	rypled ourrency mi alware		() Medium	-	-	Unknown	Open Unhandled	Host Security Service		2024/02/06 16:27:07.2	Operation •	
	S protocol attacks DoS attacks		O Tes	-	-	Unknown	Open Unhardled	Host Security Service		2024/02/06 16:26 16:8	Operation +	
	Total Records: 7	1 > 00										

Table 10-6 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 AlertsThis 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.	
Unhandled Alerts	handled within the specified time range in the current workspace. The unhandled alerts are displayed by
	automatically by playbooks within the specified time
	manually within the specified time range in the current
Alerts	This area displays how many alerts that are reported within the specified time range in the current workspace.

Parameter	Description
Alarm list	The list displays more details about each alert.
	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.
	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:
	• 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.
	 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

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

Scenario

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

Converting an Alert to an Incident

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-17 Workspace management page

SecMaster	Management 🛞	Process
Security Overview Workspaces Management Agencies	Chelle Wantgace If fortie a name and leyword for search.	C
Purchased Resources Security Governance(beta)	0 Address 0 Address 0 Address 0 Address 0 Address 0 Address 0 Matrix 0 Matrix	Selected Spaces C (2) Minimization 0 Playbo 0

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

Figure 10-18 Alerts

nandio	d Alerta				Auto		Manual		Alerts Number		
	7	(7	 High 5 Modia Tipe 1 	0		0		7		
A00	Associated Event	Math Close More -	nter a keyward. By default, the								0
	Type: :	Alert Name :	Alarm Severity :	Source IP Asidress	Verification Status	Sistura :	Data Source Prod	Owner :	Creation Time :	Operation	
	Web attacks	CiceedBySecMaster1	O High		Unknown	Open Handled au	Host Security Service		2024/02/07 10:33:00.5	Operation +	
	Web attacks	CiceedBySecMaster1	O High		Unknown	Open Handled au	Host Security Service		2024/02/07 10:27:59.4	Operation +	
	Web attacks	[CircumithySecklassier]	O High		Unimpers	Open Handled au	Heat Security Service		2024/02/07 10:22:55.6	Operation .	
	Web alles in		O trigh		Unknown	Open: Unhandled	Heat Security Service		2024/02/07 10 18:55 3	Operation +	
	Makaous use of lokan Akenersal user behavio		O High		Unknown	Open: Unhandled	Heat Security Service	-	2024/02/05 16:27:47.6	Operation +	
	Encrypted currency mi Matware		O Medice		Unknown	Open: Unhandled	Hust Encartly Service		2024/02/06 16 27 07 2	Operation +	
	DNS protocol attacks		O Ten		University	Onen Unhandled	Hant Reports Revise		2024/02/04 16 26 16 8		

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

Figure 10-19 Workspace management page

SecMaster	Management ①				🕞 Process
Security Overview Workspaces	Credit Wantspece IF lister a name and keywood for search.				C
Purchased Resources Security Governance(beta)	convertions convertence convertence convertence convertence converten	S Incidents 0 Assets 0	♥ Vulner 0 Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ └ Indicat 0 IP Playbo 0

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

Figure 10-20 Alerts

									Teelay	This week This i	sanih -	Castornie
randio	d Alerta					Auto		Manual		Alerts Number		
	7	· · · · · (7	 High 5 Modia Tipe 1 		0		0		7		
A00		Mark Chies										C C
Al Alar	en linearity) Al Baha • (0.6	nter a keyword. By default, the	search is performed by norm	e or a combination of search	critoria.						0
	Type :	Alert Name :	Alarm Sevenity :	Source IP Address	Destination IP Ad	Verification Status	Steture :	Data Source Pred	Owner :	Creation Time :	Operation	
	Web attacks	[CrosedBySecMaster]	O man			Unknown	O Open Handled au	Host Security Service		2024/02/07 10:33:00.5	Operation +	
	Web attacks	[CrosedBySecMaster]	O High			Unknown	Open Handled au	Heat Security Service		2024/02/07 10:27:59.4	Operation +	
	Web attacks	{ClosedBySecklaster}	O High			Unimpun	Open Handled au	Heat Security Service		2024/02/07 10:22:58.8	Operation •	
	Web allocks		O High			Unknown	Open: Unhandled	Heat Security Service		2024/02/07 10 18:58.3	Operation v	
	Makazan use of token Abnormal user behavior		O High			Unknown	Open: Unhandled	Heat Security Service	-	2024/02/05 16:27:47.6	Operation v	
	Encrypted currency mi Matware		O Medice			Unknown	Open: Unhandled	Hust Decardy Device		2024/02/04 16 27:07 2	Operation +	
	DNS protocol attacks		O Tes			University	Open Unhandled	Hand Descript Dervice		2024/02/08 16 26 16 8	Operation +	

- **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**.

----End

10.2.3 Adding or 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-21 Workspace management page

SecMaster	Management 🕥			Process
Security Overview Workspaces Management Agencies	Credit Workspace $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $	C		
Purchased Resources Security Governance(beta)				₩ Indicat 0

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

Figure 10-22 Alerts

ndio	d Alerta					Auto		Manual		Alerts Number		
	7	(7	 High 5 Modia Yips 1 		0		0		7		
A80												с
	Type :	Alert Name :	Alarm Severity :	Source IP Address	Destination IP Ad		Status :	Data Source Pred	Owner :	Creation Time :	Operation	
	Web attacks	[CiceedBySecMaster]	O High			Unknown	O Open Handled au	Host Security Service		2024/02/07 10:33:00.5	Operation +	
	Web allocks	CrossdBySecMaster2	O High			Unknown	Open Handled au	Host Security Service		2024/02/07 10:27:59.4	Operation +	
	Web attacks	[Circumity/Sechiaster]	O High			Unimpore	Open Handled au	Hoal Security Service		2624/02/07 10:22:58.8	Operation .	
0	Web allacks		O High			Unimpore	Open Unhandled	Heat Security Service		2024/02/07 10 18:58.3	Operation +	
0	Address use of token Absorval user listbatto		O High			Unimpure	Open: Unhandled	Heat Security Service	-	2024/02/05 16:27:47.6	Operation +	
-	Encrypted currency mi Matware		O Modern			University	Open: Unhandled	Haal Resardy Bervice		2024/02/04 16 27:07 2	Operation +	
	ONS protocol attacks		• Ten			Unknown	Onen Unbestieri	Hant Desardy Device		2024/02/04 16 26 16 8		

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

Paramete	r	Description
Basic informat ion	Alert Name	 User-defined alert name. The value must contain: 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	Data source name
	Data Source Type	Type of the data source. The options are Huawei , Third-party , and Tenant .
Timeline -	First Occurrence Time	Time when an alert is generated for the first time.
	(Optional) Last Occurrence Time	Last time when an alert was generated
	(Optional) Planned Closure Time	Time when the alert plan is disabled.
Other	(Optional) Labels	Alert labels.
	(Optional) Debugging data	Whether to enable simulated debugging.
	(Optional) Verification Status	Verification status of the alert to identify the accuracy of the incident. The options are Unknown, Positive , and False positive .
	(Optional) Stage	 Alert phase. 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.

 Table 10-7
 Alert parameters

Paramete	r	Description
	Description	Alert description. The value can contain:
		 Only uppercase letters, lowercase letters, digits, and the special characters: ()
		• A maximum of 1,024 characters.

Step 6 Click OK.

----End

Editing an Alert

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

Figure 10-23 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	Craft Wintgace $$\ensuremath{\mathbb{T}}$ fortor a name and layound for seach.				C
Purchased Resources Security Governance(beta)	Constant events 0 add9777 dedar2 Region Paged- Max Not hold.	Dincidents 0 Assets 0	♥ Vuiner 0 Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ি indicat 0 B Playbo 0

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

Figure 10-24 Alerts

ando	1 Alerts					Auto		Manual		Alerts Number		
	7	(7	 High 5 Median Tipe 1 		0		0		7		
A66	Associated Event	Dath Gloss More +	der a browned. By default, the	enough in configurated by comes	or a continuition of second	coloria.						•
	Type 0	Anthene (Alarm Severity :	Source IP Address		Vertication Status	Matter 0	Data Source Prod	Owner (Creation Time (Operation	
•	VND attacks	{ClosedBylleuMaster}	O High			Uninseen	Open Handled au	Hand Resardy Revise		2024/02/07 10 33:00 8	Operation +	
	Web attacks	[ClosedByBeuMasler]	O then			Unknown	O Open Handled au	Hast Desarity Device		2024/02/07 10 27:08.4	Operation +	
	Web attacks	[CrosedDySecMaster]	O men			Unknown	O Open Handled av	Host Security Service		2024/02/07 10:22:58.0	Operation +	
	Web attacks		O High			Unknown	Open Unhandled	Host Security Service		2024/02/07 10 10:58.5	Operation +	
	Absense use of taken Abserval user behavio		O High			Unknown	Open Unnanded	Host Security Service	-	2024/02/05 16:27:47.6	Operation +	
	Encrypted camency m Matware		0 10000			Uninesses	Open Unnanded	Hani Desarity Dervice		2024/02/06 16 27:07 2	Operation +	
	DNS protocol attacks		• Ter			Unineses	Open Unhandled	Hand Research Revine		2024/02/01 10 20 10 8		

- **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 10-8**.

Table 10-8 Alert parameters

Parameter	,	Description
Basic Informati on	Alert Name	 User-defined alert name. The value must contain: 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 incident. The options are Unknown , Positive , and False positive .
	Stage	 Alert phase. 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
Descri	ption	 Alert description. The value can contain: Only uppercase letters, lowercase letters, digits, and the special characters: () A maximum of 1,024 characters.

Step 7 Click OK.

----End

10.2.4 Importing and Exporting Alerts

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

Figure 10-25 Workspace management page

SecMaster	Management 💿	🕞 Process
Security Overview Workspaces	Credit WithSpace To fine a name and layout for seach.	C
Purchased Resources Purchased Resources Security Governance(beta)	0 add9777 \$46412 Rejon 3 Project- Mare ☐ Incidents 0 @ Vulner 0 Ø Aleris 0	ected Spaces C 🛞 dicat 0 laybo 0

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

Figure 10-26 Alerts

								_		
ndie	ed Alerts				Auto		Manual		Alerts Number	
	7		7	 Hight Modil Tips 1 	0		0		7	
A00			Criter a keyward. Dy default, By		 					
	Type :	Alert Name :	Alarm Severity :	Source IP Address	Verification Status	Stature ::	Data Source Prod	Owner :	Creation Time :	Operation
	Web attacks	[ClosedBySecMaster]	O High		Unknown	O Open Handled au	Host Security Service		2024/02/07 10:33:00.5	Operation +
	Web attacks	[CrosedBySecMaster]	O rego		Unknown	Open Handled au	Host Security Service		2024/02/07 10:27:59.4	Operation +
	Web attacks	[ClosedBySecklaster]	O rego		Unimpun	Open Handled au	Haat Security Service		2624/02/07 10:22:58.6	Operation -
	Web allocks		O triph		Unknown	Open: Unhandled	Heat Security Service		2024/02/07 10 18:55 3	Operation +
	Makazan use of token Abnormal user behavior		O High		Unknown	Open: Unhandled	Heat Security Service		2024/02/05 16:27:47.6	Operation +
	Encrypted camency mi Matware		O Median		Unknown	Open: Unhandled	Hust Recardy Revice		2024/02/06 16 27 07 2	Operation +
	DNS protocol attacks		0 Terr		Unknown	Open Unhandled	Hand Research Revise		2026/02/04 16 26 16 8	

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

Figure 10-27 Workspace management page

SecMaster	Management 💿				Process
Security Overview Workspaces	Credit WithStapped $eq:started_started$				C
Purchased Resources Security Governance(beta)	Commit account in the second of the second o	Incidents O Assets O	♥ Vuiner 0 ⊜ Securi 0	Alerts O Instan	Selected Spaces C 🛞 Mindicat 0 Playbo 0

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

Figure 10-28 Alerts

									Teeley	This week This	manih i	Castornice
Inhandio	d Alerts					Auto		Menual		Alerts Number		
	7		7	 High 5 Median Tips 1 		0		0		7		
	Associated Event	Datch Olose More +	er a brywird. By default, De									•
	туре с	And Name ()	Alarm Severity :	Source IP Address	Destination IP Ad		Status 0	Data Jource Prod	Owner (Creation Time (Operation	Ŵ
	VND attacks	[CoundByEnsMaster]	O High			Uninseen	Open Handled au	Hand Emissily Device		2024/02/07 10 33:00 8	Operation +	
	Web shell	[CoundByTecMaster]	O High			University	O Open : Handled au	Hard Recardy Revice		2024/02/07 10 27:59.4	Operation +	
	Web shell	[CrossedBy/SecMaster]	O Hoh			Unknown	O Open : Handled au	Host Security Service		2024/02/07 10:22:58.8	Operation +	
	Web attacks		O High			Unknown	Open Unhandled	Host Security Service		2024/02/07 10 18:58.5	Operation +	
	Absornal user behavior		O High			Unknown	Open Unnarded	Host Security Service	-	2024/02/06 16:27:47.6	Operation +	
	Encrypted currency m Matware		O Medice			Linkowers	• Open Unnanded	Hani Desarity Dervice		2024/02/06 16 27:07.2	Operation +	
	DNS protocol attacks DDog attacks		O Ter			Uninsees	Open: Unhandled	Hani Emarity Enviro		2024/02/06 16 26 16 8	Operation +	
10 ×	Total Records: 7	< 1 > 00										

- **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 10-9	Exporting	alerts
------------	-----------	--------

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

Step 7 Click OK.

The system automatically downloads the Excel to your local PC.

----End

10.2.5 Closing or Deleting an Alert

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

Figure 10-29 Workspace management page

SecMaster	Management 💮				🗇 Process
Security Overview Workspaces	Crede Workspeen $\overline{V} \mbox{ Items and keyword for search}.$				C Q
Purchased Resources Security Governance(beta)	Conversional Conve	S Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	 O Alerts O Instan O 	Selected Spaces C 🛞

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

Figure 10-30 Alerts	

								Teelay	This week This e	sanih Castornie
handloc	d Alerta		_		Auto		Manual		Alerts Number	
	7	•		 High 5 Modian Tips 1 	0		0		7	
A80	Associated Event	More -	Criter a keyword. By default, the							00
	Type :	Alert Name :	Alarm Severity :	Source IP Address		Status :	Data Source Prod	Owner :	Creation Time :	Operation
	Web attacks	[CrossdBySecMaster]	O High		Unknown	O Open Handled au	Host Security Service		2024/02/07 10:33:00.5	Operation +
	Web attacks	CrosedBySecMaster2	O High		Unknown	Open Handled au	Host Security Service		2024/02/07 10:27:59.4	Operation +
	Web attacks	[CiessedBy/Secklasier]	O High		Unimpun	Open Handled au	Host Security Service		2024/02/07 10:22:58.6	Operation •
0	Web allocks		trigh		Unknown	Open: Unhandled	Heat Security Service		2024/02/07 10:18:58.3	Operation +
	Absorvations for the second		O mph		Unknown	O Open: Unhandled	Heat Security Service	-	2024/02/05 16:27:47.6	Operation +
- 1	Encrypted currency mi Matware		O Modern		Unknown	Open: Unhandled	Hast Recardy Revice		2024/02/04 16 27 07 2	Operation +
- 1	DNS protocol attacks DDx01 attacks		0 Ter		University	Open Unhandled	Hant Emissity Service		2024/02/04 16 26 16 8	Operation +
10 Y	Total Records: 7									

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

Operation	Description	
Closing an alert	 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. 	
	 In the confirmation dialog box, select Reason for, enter Close Comment, and click OK. 	
Deleting an alert	 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. 	
	2. In the displayed dialog box, click OK .	
	NOTE Deleted alerts cannot be restored. Exercise caution when deleting an alert.	

----End

10.2.6 Handling Alerts based on Suggestions

During data integration, SecMaster can automatically convert cloud service logs to alerts. SecMaster provides the following suggestions for handling such concerted alerts.

Abnormal System Behavior/High-risk Command Execution

Data Source	HSS alert logs
Alert Presentation	[dangercmd] [HSS] Host: {{ipList}} Run dangercmd, {{time}}
Monitoring Scenario	High-Risk commands executed on servers
Alert Field	To view corresponding high-risk command alerts in SecMaster, take the following steps:
	 Go to the Security Orchestration page of the target workspace. Then, choose Objects > Classify&Mapping.
	 Click the name of the HSS Alert Categorization and Re- Mapping to go to the details page. The high-risk command execution corresponds to msg.appendInfo.event_type=3015.

Investigation Guideline and Handling Suggestion	 Go to the Threat Operations > Security Analysis page in SecMaster, expand the target data space, and click pipeline sec-hss-alarm. The query and analysis page of ssec-hss- alarm is displayed on the right. Search for the log details for the current alert based on the values of the appendInfo.event_type,time, and ipList fields to confirm the meaning and purpose of the command. Use the appendInfo.process_info field to check whether the current high-risk command (process_cmdline) and its parent process command (parent_process_cmdline) are suspicious. 	
	 You can use sec-hss-log to query the host (ipList) behavior in a similar period of time, and use appendInfo.pid_link (sec-hss-log) and appendInfo.process_info.parent_process_pid(sec-hss-alarm) to sort the process sequence. Then, you can make informative decisions to find out suspicious processes and commands. For those processes and commands, you can scan for further hacking behavior, such as viewing sensitive data, viewing network environments, privilege escalation, network proving, and PoC execution. 	
	 If it is confirmed that the fault is triggered by attacks, contact the resource owner immediately. 	
High-Risk Command	 The high-risk commands involved in alerts are as follows: strace: captures and records all system calls of a specified process and all received signals. rz: used to upload files from a local computer to a remote server. It is usually used in SSH sessions. sz: used to download files from a remote server to a local computer. This command is usually used in SSH sessions. tcpdump: used to probe data packets and capture data packets flowing on network adapters. nmap: used to scan and probe networks. nc/ncat: or netcat, used to implement many network-related functions, such as listening and connecting ports. 	

Web Attacks (SQL Injection)

• Corresponding Alert Field

To view corresponding SQL inject alerts in SecMaster, take the following steps:

- a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.
- b. Click the name of the **WAF Alert Categorization and Re-Mapping** to go to the details page.

The **msg.attack** for SQL injection is **sqli**.

• Troubleshooting Methods and Handling Suggestions

- a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-waf-attack**. The query and analysis page of sec-waf-attack is displayed on the right.
- b. Search for the log details for the current alert based on the values of the **attack**, **__time**, and **sip** fields. The key parameters are as follows:
 - **hit_data**: attack packet or link.
 - uri: request URL.
 - **action**: processing action
 - **cookie**: request cookie information.
- c. Check attack packets to see how the SQL injection is made and check whether there is any vulnerability in the application.

If there is, rectify the fault in time by using parameterized query, input verification, and software update and patching.

Web Attacks/Vulnerability Exploits

• Corresponding Alert Field

To view corresponding vulnerability exploit alerts in SecMaster, take the following steps:

- a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.
- b. Click the name of the **WAF Alert Categorization and Re-Mapping** to go to the details page.

The **msg.attack** value for vulnerability exploits is **vuln**.

- Troubleshooting Methods and Handling Suggestions
 - a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-waf-attack**. The query and analysis page of sec-waf-attack is displayed on the right.
 - b. Search for the log details for the current alert based on the values of the **attack**, **__time**, and **sip** fields. The key parameters are as follows:
 - hit_data: attack packet or link.
 - uri: request URL.
 - **action**: processing action
 - **cookie**: request cookie information.
 - **header**: request header information.
 - c. Confirm the vulnerability exploit type based on the attack packet and detect vulnerabilities in attacked assets.

If there is a vulnerability, fix it in a timely manner to prevent attackers from exploiting this vulnerability to attack the system or applications.

Web Attacks/Command Injection

• Corresponding Alert Field

To view corresponding command injection alerts in SecMaster, take the following steps:

In SecMaster, choose **Security Orchestration** > **Objects** > **Classify&Mapping**. Click **WAF Alert Categorization and Re-Mapping** to go to the details page. The **msg.attack** value for command injection attacks is **cmdi**.

• Troubleshooting Methods and Handling Suggestions

- a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-waf-attack**. The query and analysis page of sec-waf-attack is displayed on the right.
- b. Search for the log details for the current alert based on the values of the **attack**, **__time**, and **sip** fields. The key parameters are as follows:
 - hit_data: attack packet or link.
 - uri: request URL.
 - **action**: processing action
 - **cookie**: request cookie information.
 - **header**: request header information.
- c. Check attack packets to see how the command injection is made and check whether there is any vulnerability in the application.
 - If there is any vulnerability, fix it as soon as possible and update the related software or database version.
 - Perform a comprehensive check on the system to see if there are other vulnerabilities or backdoors.
 - Restrict system access permissions. For example, you can disable the root account and restrict access from some IP addresses to reduce possible intrusion paths.

Abnormal System/Process Behavior

Locate the affected assets, services, and workloads based on the corresponding alerts.

• Corresponding Alert Field

To view corresponding abnormal system or process behavior alerts in SecMaster, take the following steps:

- a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.
- b. Click the name of the **HSS Alert Categorization and Re-Mapping** to go to the details page.

Abnormal process behavior: msg.appendInfo.event_type=3007

• Troubleshooting Methods and Handling Suggestions

- a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-hss-alarm**. The query and analysis page of sec-hss-alarm is displayed on the right.
 - i. Search for the log details for the current alert based on the values of the **appendInfo.event_type**, **__time**, and **ipList** fields.
- b. Check the information about the current process and parent process in **appendinfo. process_info** to determine whether the process is abnormal. If the process is abnormal, contact the corresponding resource owner.
 - Immediately stop affected processes or services to avoid further attacks or other damage.
 - Investigate the causes and sources of abnormal behavior by all means, for example, viewing logs, monitoring the system, and analyzing the process memory, to determine the specific symptoms and possible root causes of exceptions.
 - Based on the nature and severity of the abnormal behavior, take proper measures, such as restarting processes, rectifying software errors, rectifying system faults, and replacing hardware devices.
 - Comprehensively check the affected system to see if there are other vulnerabilities or backdoors.

Abnormal System Behavior/Key File Directory Modifications

Locate the affected assets, services, and workloads based on the corresponding alerts.

• Corresponding Alert Field

To view corresponding key file directory modification alerts in SecMaster, take the following steps:

- a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.
- b. Click the name of the **HSS Alert Categorization and Re-Mapping** to go to the details page.

Key file directory modification: msg.appendInfo.event_type=3005

- Troubleshooting Methods and Handling Suggestions
 - a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-hss-alarm**. The query and analysis page of sec-hss-alarm is displayed on the right.
 - b. Search for the log details for the current alert based on the values of the appendinfo.event_type, __time, and ipList fields.
 In the preceding information, appendinfo.file_info indicates the file directory information. Check whether the file directory information is normal. If the file directory information is abnormal, contact the
 - corresponding resource owner.
 Determine the impact scope of the change. First, determine the files that are affected by the directory change and the impact of the files on services. If the impact scope is large, immediate measures must

be taken to prevent further losses.

- Restore key files: If directories or files are changed abnormally, restore them in a timely manner. If a file is deleted or damaged, you need to restore it from a backup. If the files are not backed up, stop related operations immediately and take data restoration measures to restore the files to the status before the change.
- Update related configurations: For some programs and systems that require configuration file paths, update related configurations in a timely manner to ensure that these programs and systems can correctly access key files.
- Review the change reason: Review and check the reason for the directory change. If the change was caused by human misoperations, correct the fault and strengthen management in a timely manner. If the change was made by the system, evaluate the necessity and impact of the change and ensure that the change is reasonable and secure.
- Enhance security measures: For security management of key files, measures must be enhanced to ensure that files cannot be mistakenly deleted, maliciously tampered with, or disclosed. Measures such as encryption, backup, and access control can be taken to ensure file integrity and availability.

10.2.7 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. **Table 10-12** lists recommended settings. You can also block a single attack source based on the comprehensive investigation of multiple alerts.

Alert Type	Defense Layer	Recommended Policy		
HSS alerts	Server protection	VPC policies are recommended to block traffic.		
WAF alerts	Application protection	WAF policies are recommended to block traffic.		
CFW alerts	Network protection	CFW policies are recommended to block traffic.		
IAM alerts	Identity authentication	IAM policies are recommended to block traffic.		
OBS and DBSS alerts	Data protection	You can use VPC or CFW policies based on actual attack scenarios and investigation results to disconnect attack sources from protected resources.		

 Table 10-12 Recommended blocking policies

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

Figure 10-31 Workspace management page

SecMaster	Management (1)	Process
Security Overview Workspaces Management Agencies	Coalt Wanspace © Enter a name and layout for search.	C
Purchased Resources Security Governance(beta)	0 add9177 Notified Prajed More Ill Incidents 0 Or Vallner0 O Add915 Incidents 0 Prajed More Not Anoted O Add917 Notified O Add917 Notified Incidents 0 O Add917 Incidents 0 Incidents 0	

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

Figure 10-32 Alerts

nhandla								Marriad	Teslay		reach	Castonice
nhandio	d Alerts					Auto		Menual		Alerts Number		
	7		7	 High 5 Media Tige 1 		0		0		7		
Ass	Associated Event	Dath Glose More +	der a bevoord. By default, De									00
	Type 0	Ant Name (Atarm Severity :	Source IP Address	Destination IP Ad		Status 0	Data Jource Prod	Owner ()	Creation Time	Operation	W
	Web attacks	[ConsidyIsuMasise]	O regn			University	Open: Handled au	Hast Desarity Dentise		2024/02/07 10 33:00 6	Operation +	
	Web shell	[ClosedByIlesMaster]	O Hoh			Linknowe	O Open : Handled av	Haal Recardy Device		2024/02/07 10 27:58.4	Operation +	
	Web shell	[CrossedDy/SecMaster]	O High			Unknown	O Open : Handled au	Host Security Service		2024/02/07 10:22:58.8	Operation -	
	Web attacks		O High			Unknown	Open: Unhandled	Host Security Service		2024/02/07 10:10:50.3	Operation •	
	Abserval user behavior		O High			Unknown	Open: Unnanded	Host Security Service		2024/02/05 16:27:47.6	Operation •	
	Encrypted camency m Matware		O 100000			Linkower	O Open : Unnandled	Hani Security Service		2024/02/06 16 27:07 2	Operation +	
	DND protocol attacks		O Tes			University	Open: Unhandled	Hant Emarity Environ		2024/02/06 16 26 16 8	Operation +	

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.

Parameter	Description
Block Object	• 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 (,). Example:
	– Single IP address: 192.168.0.0
	 IP address range: 192.168.0.0/12
	• If you select IAM for Blocked Object Type , enter IAM user names.
	• A maximum of 50 IP addresses, IP address ranges, or IAM users can be blocked by an emergency policy once.
Label	Label of the custom emergency policy.
Operation Connection	Select the operation connections for the policy.
Block Aging	Check whether the policy needs to be stopped.
	• 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.
Reason Description	Description of the custom policy.

Table 10-13 One-click blocking

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

Figure 10-33 Workspace management page

SecMaster	Management 💿				D Process
Security Overview Workspaces Management Agencies	Creals Wonspace $\label{eq:prod} \overline{V} \mbox{ into a name and layourd for search}.$				C
Purchased Resources Security Governance(beta)	Constanting Constanti	incidents 0 Assets 0	 ◊ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 indicat 0 Playbo 0

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

Figure 10-34 Alerts

mila	d Alerts				derto.		Marrial		Alerta Number		
	7	(7	 High 5 Median Tipe 1 	0		0		7		
Add	Associated Event	Datch Olose More +	der a brywied. By default, the								٥
	Type 0	Ant Name 1	Atarm Severity :	Source IP ADS1988	Vertication Status	Stature 0	Data Source Prod	Owner 0	Creation Time (Operation	
	VND sheet	[CountillyInsMaster]	O regn		Uninseen	Open Handled au	Haal Desarity Device		2024/02/07 10 33:00 8	Operation +	
	Web shell	[CountillyInsMaster]	O High		Uninseen	O Open : Handled au	Haal Desarity Device		2024/02/07 10:27:89.4	Operation •	
	Web shot	[CrossdDySecMaster]	O man		Unknown	O Open Handled as	Host Security Service		2024/02/07 10:22:58.0	Operation +	
	Web shell Web attacks		O regin		Unknown	Open: Unhandled	Host Security Service		2024/02/07 10:10:50.5	Operation +	
	Meloisus use of lokes Abserval user behavio		O regn		Unknown	Open: Unhandled	Host Security Service	-	2024/02/05 16:27:47.6	Operation +	
	Encrypted currency m Matware		O Medice		Uninsees	• Open Unnanded	Hani Desarity Device		2024/02/05 16 27 07 2	Operation +	
	DND protocol attacks		O 101		University	Open Unhandled	Hand Departy Device		2024/02/05 16 26 16 8		

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

10.3 Indicator Management

10.3.1 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-35 Workspace management page

SecMaster	Management 🕥				🕞 Process
Security Overview Workspeces	Credit Workspace $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	O AddR077 Sedat2 Region Not hoted.	 incidents 0 ○ Assets 0 	♥ Vulner () ⊜ Securl ()	 Alerts () Instan () 	Selected Spaces C i Indicat 0 Playbo 0

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

Figure 10-36 Indicators

< / Indicators																						
Security Situation Resource Manager Risk Prevention Thread Operations Incidents Alerts Indicators Indicators	Ir	ndicator	Type ®)		• lpvt 1		verdue Indic	ator				Indicato	r Status ®)		Open 1			0		Black 7 Gray 4
Intelligent Modeling Security Analysis Security Orchestration		Add Q E	nter a kaya		I, the search is	performed by r	hame or a con	ibination of sea	arch críberia.									Feb 0	1, 2024 00:00 1	00 - Feb 07, 2024 23 59 59	m) C	0
Settings •			lsdi	Indi 5a04201	Thr Black	Type ipv4	Stat Open	Con 00	0w	Firs 2024/02	Cre 2024/02	Exp	Clo	Cre	Gra First tim	Upd 2024/02	Value	Dat Databa	Det Cloud S	Operation Edt Close Delete		
	1		10	ad1537 893bb4	Gray Black	ipv4 ipv4	Open Open	80 80	-	2024/02	2024/02			-	First tim	2024/02	1 . 1 .	Cloud F		Edit Close Delete		

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

Table 10-14 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: ()
Туре	Indicator type.
Threat Degree	Select a threat degree level.
	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 Huawei , Third- party , and Tenant .
Status	Indicator status. Possible values are Open , Closed , and Revoked .
(Optional) Confidence	Reliability of the selected indicator. The value ranges from 80 to 100.
(Optional) Owner	Primary owner of the indicator.
(Optional) Labels	Label of a user-defined counter.
First Occurrence Time	First occurrence time of the indicator.
Last Occurrence Time	Latest occurrence time of the indicator.
(Optional) Expiration Time	Expiration time of the indicator.
Invalid or not	Whether to invalidate the indicator. The default value is No .

Parameter	Description
Granularity	Granularity of the indicator. The options are First time observed , Self-produced data , To be purchased , and Query from external network .
Other parameters	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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-37 Workspace management page
--

SecMaster	Management ③				Process
Security Overview Workspeces	Credit Wonspec				C
Purchased Resources Security Governance(beta)	Granit count 0 add077 Sele12 Region Project- Itore Not hoted	 Incidents () Assets () 	♥ Vulner 0 i Securi 0	O Alerts 0 instan 0	Selected Spaces C iv Indicat 0 B Playbo 0

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

Figure 10-38 Indicators

< / Indicators																					
Security Situation • Resource Manager •	Ind	icator 1	ype 🕲				c	verdue India	ator 🕲				Indicato	r Status 🛈				Th	reat Degree	0	
Risk Prevention Threat Operations Incidents		(11)		e ipv4 1	n (0						11)		Open 11		(11	Black 7 Gray 4
Alerts																					
Intelligent Modeling Security Analysis		Add		a)														Feb 01	, 2024 00:00 1	00 - Feb 07, 2024 23 59:59	: C 🖲
lecurity Analysis		Q, E	der a keywo	rd. By default	, the search is	performed by i	name or a con	ibination of sev	arch criteria.												•
ietings T			Indi	Indi	Thr	Type	Stat	Con	Ow	Firs	Cre	Ехр	C10	Cre	Gra	Upd	Value	Dat	Det	Operation	
			14	6404501	Black	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	1	Databa	Cloud S	Edit Close Delute	
			10	ad1537	Gray	ipv4	Open	80		2024/02	2024/02	-	-	-	First tim	2024/02	1	Cloud F	Cloud S	Edit Close Delete	
			1	893554	Black	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	1	Cloud F	Cloud S	Edit Close Debite	

- **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.

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: ()
Туре	Indicator type.
Threat Degree	 Select a threat degree level. 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, Self-produced data, To be purchased, and Query from external network.
<i>Other parameters</i>	You need to set the parameters based on the selected type. Set the parameters as prompted. For example, if you select ipv6 for Type , you also need to configure the IP address, email account, and region.

Step 7 Click OK.

----End

10.3.2 Disabling and Deleting an Indicator

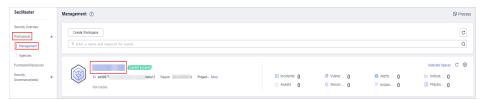
Scenario

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

Figure 10-39 Workspace management page



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

Figure 10-40 Indicators

< / Indicators																					
Security Situation Resource Manager Rick Prevention	Ind	icator Type 🕲					Dverdue India	ator 🕲				Indicato	or Status 🕲				T	ireat Degree	0		
Threet Operations		11)		● ipv41		0						11)		Open 1		C	")	Black 7 Gray 4	
Indicators 😝		Add Imp	of														Feb 0	1, 2024 00:00.0	0 - Feb 07, 2024 23 59 59	30	۲
Security Analysis Security Orchestration V		C), Enter a keywo	ord. By default,	the search is	performed by I	name or a co	mbination of se	arch criteria.													٢
Settings +		11di	Indi 6x04b0f		Type ips4	Stat Open	Con 80	Ow	Firs 2024/02	Cre 2024/02		Cio	Cre	Gra First tim	Upd 2024/02	Value	Dat	Det Cloud S	Operation Edit Close Debte		
4			ad1537	Gray	ipv4	Open	80		2024/02	2024/02	-	-	-	First tim	2024/02	1	Cloud F	Cloud S	Edit Close Delete		
			893564	Black	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	t .	Cloud F	Cloud S	Edit Close Dekte		

Step 5 On the **Indicators** page, close or delete an indicator.

Table 10-16	Indicator	parameters
-------------	-----------	------------

Operation	Description
Close	 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.

Operation	Description
Delete	 On the Indicators page, locate the target indicator and click Delete in the Operation column.
	2. In the dialog box displayed, click OK .
	NOTE Deleted indicators cannot be restored. Exercise caution when performing this operation.

10.3.3 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-41 Workspace management page

SecMaster	Management ③				🕼 Process
Security Overview Workspaces Management Agencies	Credit Wantgace If loter a name and layered for seach.				C
Purchased Resources Security Governance(beta)	O add/01/7 Sediar2 Report Not tould	 Incidents 0 Assets 0 	♥ Vulner 0 Securl 0	 o Alerts <lio alerts<="" li=""> o Alerts o Alerts o A</lio>	Selected Spaces C 🛞 iv Indicat 0 Playbo 0

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

Figure 10-42 Indicators

/ Indicators																						
Resource Manager		dicator 1	ype 🕲				c	verdue India	ator 🕲				Indicato	r Status 🛈				Π	ireat Degree	0		
isk Prevention			11			• ipv4 1		h						11			Open 11		(11		Black 7
incidents			Ü					J						Ü			- open re				•	Gray 4
Alerts																						
Indicators 😢																						
Intelligent Modeling		Add		a)														Feb 0	, 2024 00.00.0	00 - Feb 07, 2024 23.59:59	8	5 C (
Security Analysis ourity Orchestration		Q, E	der a keywo	rd. By default	the search is	performed by	name or a con	ibination of sev	arch oriteria.													(
tings •			Indi	hdi	Thr	Type	Stat	Con	Ow	Firs	Cre	Ехр	Clo	Cre	Gra	Upd	Value	Dat	Det	Operation		
			0	6404505	Black	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	1	Databa	Cloud S	Edit Close Dehite		
	4		0	ad1537	Gray	ipv4	Open	80		2024/02	2024/02	-	-	-	First tim	2024/02	1	Cloud F	Cloud S	Edit Close Delete		
				893004	Black	ipv4	Open	83	-	2024/02	2024/02	-	-	-	First tim	2024/02	1	Cloud F	Cloud S	Edit Close Debite		

- **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.

Exporting Indicators

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

Figure 10-43 Workspace management page

SecMaster	Management (?)				D Process
Security Overview Workspaces Management Agencies	$\begin{tabular}{cccc} \hline \begin{tabular}{cccc} \hline \begin{tabular}{ccccc} \hline \begin{tabular}{ccccc} \hline \begin{tabular}{ccccc} \hline \begin{tabular}{ccccc} \hline \begin{tabular}{ccccc} \hline \begin{tabular}{cccccccccc} \hline \begin{tabular}{cccccccccccccccccccccccccccccccccccc$				C Q
Purchased Resources Security Governance(beta)	0 #00077 Vedel2 Region 1 Prijed- Mare Nid hotod. <td< th=""><th> Incidents 0 △ Assets 0 </th><th>♥ Vulner 0 ⊜ Securl 0</th><th>O Alerts 0 instan 0</th><th>selected Spaces C ⑧ ↓ Indicat 0 Playbo 0</th></td<>	 Incidents 0 △ Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 instan 0	selected Spaces C ⑧ ↓ Indicat 0 Playbo 0

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

/ Indicators																					
y Situation v ico Managor v invention Operations A idants	Indicat	or Type ®)		 Ipv4 3 		Wendue India	ator 🕲				Indicato	r Status ®)		Open 11			0		Black 7 Gray 4
rts icatore 🚭 Illigent Modeling curity Analysis			port	, the search is	performed by n	ama or a cor	rbination of sea	arch críbaria.									Feb 0	1, 2024 00:00 (10 — Feb 07, 2024 23 59 59	8	1 C (
ty Orchestration 💌 25 💌) hd	Indi 5a04501	Thr Black	Type ipv4	Stat Open	Con	Ow	Firs	Cre	Exp	Clo	Cre	Gra First tim	Upd	Value 1	Dat Databa	Dat Cloud S	Operation Edt Close Delete		
1) ====	ad1537	Gray	ipv4	Open Open	90 92	-	2024/02	2024/02			-	First tim	2024/02	1	Cloud F		Edit Close Delote		

Figure 10-44 Indicators

- **Step 5** On the **Indicators** page, select the indicators you want to export and click \square in the upper right corner of the list. The **Export** dialog box is displayed.
- **Step 6** In the **Export** dialog box, set parameters.

Table 10-17	Exporting	indicators
-------------	-----------	------------

Parameter	Description
Format	By default, the indicator list is exported into an Excel.

Parameter	Description
Columns	Select the indicator parameters to be exported.

Step 7 Click OK.

The system automatically downloads the Excel to your local PC.

----End

10.3.4 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-45 Workspace management page

SecMaster	Management ③				🕞 Process
Security Overview Workspaces	Credit Watapace $\label{eq:state} \overline{V} \mbox{ Inter a name and keyworld for search}.$				C Q
Purchased Resources Security Governance(beta)	Constant const O add977 fedarit2 Repor Frepd More Not holdd	Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	 Alerts () Instan () 	Selected Spaces C ⑧ ↓ Indicat 0 B Playbo 0

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

Figure 10-46 Indicators

< / Indicators																	
Security Stuation • Resource Manager •	Indicator Type 🕲		Overdue In	dicator ®				Indicator	r Status 🕲				Th	reat Degree	0		
Risk Prevention Threat Operations Incidents	11	 ipv4.11 	0						11)		Open 11		("	Black 7 Gray 4	
Alerts Indicators	(Add (inpat)												Feb 01	, 2024 00 00 0	20 - Feb 07, 2024 23 59 59	60	۲
Security Analysis Security Orchestration 💌	Q. Enter a keyword. By default, th	e search is performed by n	ame or a combination of	search criteria.													۲
Settings	Indi Indi	Thr Type	Stat Con	Ow	Firs	Cre	Ехр	Clo	Cre	Gra	Upd	Value	Dat	Dat	Operation		
	1 6a04b0f	Black ipv4	Open 80		2024/02	2024/02	-	-	-	First tim	2024/02	1 .	Databa	Cloud S	Edit Close Delete		
	ad1537	Gray ipv4	Open 80	-	2024/02	2024/02	-	-		First tim	2024/02	1	Cloud F	Cloud S	Edit Close Delete		
	1 1 293004	Black ipv4	Open 83	-	2024/02	2024/02	-		-	First tim	2024/02	t	Cloud F	Cloud S	Edit Close Dehite		



icator T	Type 🕲				c	verdue Indic	ator 🕲				Indicato	r Status 🕲				Th	reat Degree	9			
(11)		ipvi 1	1	0						11)		Open 11		(1)		Black Gray 4	
Add		ort														Feb 01,	2024 00:00.0	0 – Feb 07, 2024 23.59.59	•	3 0	
Q, Er	nter a keywi	ord. By default,	the search is	performed by r	iame or a cor	rbination of sea	arch criteria.														0
	Indi	Indi	Thr	Type	Stat	Con	Ow	Firs	Cre	Exp	Clo	Cre	Gra	Upd	Value	Dat	Dat	Operation			
	1(6s04b0f	Black	ipv4	Open	80	-	2024/02	2024/02	-		-	First tim	2024/02	1	Databa	Cloud S	Edit Close Delete			
	1	ad1537	Gray	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	1	Cloud F	Cloud S	Edit Close Delete			
	10	893664	Black	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	1	Cloud F	Cloud S	Edit Close Delete			
	192	a30903	Gray	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	192.168	Databa	Cloud S	Edit Close Delete			
	10	f7bbe8e	Błack	ipv4	Open	80	-	2024/02	2024/02	-	-	-	First tim	2024/02	1	Databa	Cloud S	Edit Close Delete			
5 +	Total R	ecords: 11	< 1	2 3 >	G0																

Table 10-18 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	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.
	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.
	 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

10.4 Intelligent Modeling

10.4.1 Viewing Available Model Templates

Scenario

SecMaster uses models to scan log data in pipelines. If the data is not within the model range, an alert is generated. 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-48 Workspace management page



Step 4 In the navigation pane on the left, choose Threat Operations > Intelligent Modeling. On the displayed page, click the Model Templates tab.

Figure 10-49 Model Templates tab

< / Intelligent	Modeling					
Security Situation 🔹						
Resource Manager 🔹 💌	Available Models Model Templates	0				
Risk Prevention	Model Template Statistics		Severity			
Threat Operations	Available templates	Active templates				_
Incidents	50	20	 Critical 1 High 	14 • Medium 28 • Low I	Informative 7	
Nets						
Indicators	V Search by name.					Q 🛞 C
Intelligent Modeling	Severity 0	Name	Model Type	Updated 🖕	Created 0	Operation
Security Analysis	Wedam	Network - External malicious IP address scannin				
				Jul 05, 2023 17:39:38 GMT+08:00	Jun 27, 2023 11:09:09 GMT+08:00	Details
Security Orchestration 💌						
Security Orchestration 💌 Settings 💌	Wedum	Application - Possible Java framework common		Jul 05, 2023 17:38:38 GMT+06:00 Jul 05, 2023 17:38:07 GMT+06:00	Jun 27, 2023 11:08:09 GMT+08:00 Jun 20, 2023 17:38:55 GMT+08:00	Details Details

Step 5 On the Model Templates tab, view available model templates.

Table 10-19	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 .

Parameter	Description
Template list	• 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.

10.4.2 Creating and Editing a Model

Scenario

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

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

- Creating an Alert Model Using a Template
- Creating a Custom Alert Model
- Editing a Model

Limitations and Constraints

- A maximum of 100 alert models can be created in a single workspace under a single account in a single region.
- The running interval of an alert model must be greater than or equal to 5 minutes, and the time range for querying data must be less than or equal to 14 days.

Creating an Alert Model Using a Template

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

Figure 10-50 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Credit Workspace $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Contract access C	Incidents 0	♥ Vulner 0 i Securl 0	O Alerts 0 instan 0	Selected Spaces C 🗟

Step 4In the navigation pane on the left, choose Threat Operations > Intelligent
Modeling. On the displayed page, click the Model Templates tab.

Figure 10-51 Model Templates tab

< / Intellige	nt Modeling					
Security Situation 🔹						
Resource Manager 🛛 💌	Available Models Model Templates	: 😖				
Risk Prevention 💌	Model Template Statistics		Severity			
Threat Operations	Available templates	Active templates				
Incidents	DE 50	DE(3) 20	Critical 1	High 14 • Medium 28 • Low	0 Informative 7	
Alerts						
Indicators	V Search by name.					Q 🛞 C
Intelligent Modeling 🧐	Severity 0	Name	Model Type	Updated \$	Created ©	Operation
Security Analysis Security Orchestration V	Medum	Network - External malicious IP address scannin	ng Rule model	Jul 05, 2023 17:39:38 GMT+08:00	Jun 27, 2023 11:09:09 GMT+08:00	Details
ietings 👻	Meckum	Application - Possible Java framework common	co Rule model	Jul 05, 2023 17:38:07 GMT+08:00	Jun 20, 2023 17:36:55 GMT+08:00	Details

- **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 10-20**.

Parameter	Description
Pipeline Name	Select the execution pipeline of the alert model.
Model Name	Name of the alert model.
Severity	Severity of the alert model. You can set the severity to Critical , High , Medium Low , or Informative .
Alarm Type	Alarm type displayed after the alert model is triggered.
Model Type	The default value is Rule model .
Description	Description of the alert model
Status	Indicates whether to enable the alert model.
	• C: indicates that the model is enabled. This is the default status.
	• Construction: Experimental states that the model is disabled.
	The status set here can be changed after the entire alert model is set successfully.

 Table 10-20
 Basic alert model parameters

- **Step 8** After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.
- **Step 9** Set the model logic. For details about the parameters, see **Table 10-21**.

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click Run and view the running result.
Query Plan	Set an alert query plan.
	• 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	 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	Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.
	If there are multiple triggers, click Add .
Alarm Trigger	The way to trigger alerts for queried results. The options are as follows:
	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.
	• C: indicates that the query stops after an alert is generated.
	• : indicates that the query is not stopped after an alert is generated.

Table 10-21 Configure Model Logic

- **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.

Creating a Custom Alert Model

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

Figure 10-52 Workspace management page

SecMaster	Management () (7 Process
Security Overview Workspaces	Order Windsages C T finter a name and layoutd for asach. Q
Purchased Resources Security Governance(beta)	Select Space - New Select Space - New Select Space - New Select Space - New Select Space - O - Alerts O - Merts O - Alerts O - Alert

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

Figure 10-53 Available Models



- Step 5 Click Create Model in the upper left corner of the Available Models tab.
- **Step 6** On the **Create Model** slide-out panel displayed, configure basic information about the alert model. For details about the parameters, see **Table 10-22**.

Table	10-22	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.

Parameter	Description
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. indicates that the model is enabled.
	This is the default status.
	• Construction: indicates that the model is disabled.
	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 10-23**.

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 .
Query Plan	 Set an alert query plan. 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.

Table 10-23 Configure Model Logic

Parameter	Description
Advanced Alarm Settings	 Extended information about a user-defined alert. Click Add, and set the Key and Value information.
	Alarm Details: Enter the alarm name, description, and handling suggestions.
Trigger Condition	Setting alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.
Alarm Trigger	The way to trigger alerts for queried result. The options are as follows:
	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.
	• constraints that the query stops after an alert is generated.
	• : indicates that the query is not stopped after an alert is generated.

- **Step 9** After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.
- **Step 10** After confirming that the preview is correct, click **OK** in the lower right corner of the page.

Editing a Model

Only custom models can be edited.

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

Figure 10-54 Workspace management page

SecMaster	Management ()	🕞 Process
Security Overview Workspaces Management Agencies	Own Workspoor To find a more and layoned for search.	C
Purchased Resources Security Governance(beta)	D ad5977 Salat2 Repon Preject- Mars D Monter. 0 O Aleris 0 M	Selected Spaces C 🛞 Indicat 0 Playbo 0

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

Figure 10-55 Available Models

< I Intelligen	nt Modeling									
Security Situation 💌										
Resource Manager 💌	Available Models 1	itodel Templates								
Rick Prevention •	Model Statistics				Severity					
Thread Operations 🔺	Available V		Active models							
Incidents	97	S10	93		Critical 1	High 25 • Medi	um 59	Low 12 0 Inf	formative 0	
Alets										
Indicators	Create Model	inable Disable Delete	V Search by	name.						Q 🕘 C
Intelligent Modeling	Severity 0	Naroe-TD	Status	Debugging	Pipeline Name	Model Type	Built-in	Updated a	Created 0	Operation
Security Analysis Security Orchestration V	- O Hot	97315122-0083-46%-8x24-71	🔮 Enable	O Disable	sec-rip-affact	Rule model	No	Jun 03, 2023 10:50:53 GMT+	Jun 02, 2023 16:14:20 GMT+	Disable Edit Delete

- **Step 5** In the available model list, click **Edit** in the **Operation** column of the target model.
- **Step 6** On the **Edit Model** slide-out panel, configure basic information about the alert model. For details about the parameters, see **Table 10-24**.

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

 Table 10-24
 Basic alert model parameters

- **Step 7** After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.
- **Step 8** Set the model logic. For details about the parameters, see **Table 10-25**.

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click Run and view the running result.
Query Plan	 Set an alert query plan. 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 day, 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
Advanced Alarm Settings	 from 0 to 5 minutes. 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	Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx. If there are multiple triggers, click Add .
Alarm Trigger	The way to trigger alerts for queried results. The options are as follows:One alert for all query resultsOne alert for each query result
Debugging	Sets whether to generate debugging alarms.
Suppression	 Specifies whether to stop the query after an alert is generated. indicates that the query stops after an alert is generated.

Table 10-25 Configure Model Logic

- **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.

10.4.3 Viewing Available Models

Scenario

This topic describes how to view available models.

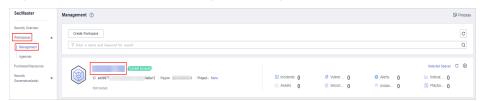
Prerequisites

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

Figure 10-56 Workspace management page



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

Figure 10-57 Available Models

< I Intelliger	nt Modeling										
Security Situation •											
Resource Manager 🔹 💌	Available Models M	/odel Templates									
Rick Prevention 💌	Model Statistics				Severity						
Threat Operations 🔺	Available Mo	otes 🔊	Active models								
Incidents	97	90	93		Critical 1	High 25 • Med	um 59	Low 12	formative 0		
Alets											
Alerts Indicators	Create Model Er	nable Disable Delete	V Search b	y name.							Q @ C
	Create Model En	nable Disable Delete	97 Search by Status	y name. Debugging	Pipeline Narse	Model Type	Built-in	Updated o	Created o	Operation	Q@C
Indicators					Pipeline Name sec-nip-attack	Model Type Rule model	Built-in No	Updated	Created () Jun 10, 2023 16:14:20 GMT+		



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.

10.4.4 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-58 Workspace management page

SecMaster	Management ①				Process
Security Overview Workspeces Management Agencies	Credit Writigate T later a name and keyword for search.				C
Purchased Resources Security Governance(beta)		 Encidents 0 ○ Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C └ Indicat 0 S Playbo 0

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

Figure 10-59 Available Models

<		t Nodeling										
Security Situation	*											
Resource Manager	*	Available Models Model Ter	nplates									
Risk Prevention	*	Model Statistics				Severity						
Threat Operations		Available Models 97		Active models								
Incidents		V 97	<u> (0)</u>	93		Oritical 1	High 25 • Mediu	m 59	Low 12 • Inf	formative 0		
Alets												
Indicators		Create Model Enable	Deable Defete	V Search b	y name.						c	1 @ C
Indicators	8			V Search b Status	y name. Debugging	Pipeline Name	Model Type	Built-in	Updated g	Created 0	Operation	1 🛛 C
Indicators		Create Model Enable				Pipeline Name sec-nip-attack	Nodel Type Rule model	Built in No	Updated Jun 03, 2023 16:50:53 GMT+	Created () Jun 02, 2023 10:14 20 GMT+		

Step 5 On the **Available Models** tab, manage models.

Operation	Description
Enable	In the model list, click Enable in the Operation column of the target model.
	NOTE To enable models in batches, select all models you want to start and click Enable in the upper left corner of the list.
	If the model status changes to Enable , the model is successfully started.
Disable	In the model list, locate the row that contains the target model and click Disable in the Operation column.
	NOTE To disable models in batches, select all models and click Disable in the upper left corner of the list.
	When the alert model status changes to Disable , the model is disabled.
Delete	1. In the model list, locate the row that contains the target model and click Delete in the Operation column.
	NOTE To delete models in batches, select all models to be deleted and click Delete in the upper left corner of the list.
	2. In the displayed dialog box, click OK .

Table 10-27 Managing models

----End

10.5 Security Analysis

10.5.1 Security Analysis Overview

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

Cloud services and logs that can be interconnected with SecMaster

SecMaster can integrate logs of multiple Huawei Cloud services, such as Web Application Firewall (WAF), Host Security Server (HSS), and Object Storage Service (OBS). You can search for and analyze all collected logs in SecMaster. By default, the logs are stored for 7 days.

For details, see Log Access Supported by SecMaster.

Limitations and Constraints

- A maximum of 500 results can be returned for a single analysis query.
- A maximum of 50 shortcut queries can be created in a pipeline. That is, a maximum of 50 query analysis criteria can be saved as shortcut queries.
- If there are over 50,000 results for a single query, the accuracy may decrease. In this case, you can select a short time range or apply more filter criteria to reduce the number of query results.
- In aggregation queries (for example, GROUP BY statement) based on several fields, the default number of buckets for the second field is 10. If more than 10 buckets are generated, part of qualified data will be lost. In this case, the query results are not accurate.

10.5.2 How to Use Security Analysis

Table 10-28 shows the process of using the security analysis function.

Step	Description
Adding a Workspace	Add a workspace for resource isolation and control.
Integrating Data	Configure the data to be accessed.
	SecMaster can integrate log data of multiple Huawei Cloud 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.

Table 1	10-28	Process
---------	-------	---------

Step	Description
Configuring Indexes	Configure indexes to narrow down the query scope. By default, indexes have been configured for some reserved fields in the accessed cloud service logs. For details, see Log Fields .
Querying and Analyzing Data	Query and analyze the accessed data.
Downloading Logs	Allows you to download raw logs or queried and analyzed logs.
Querying Analysis Results in Charts and Tables	After you run query and analysis statements, SecMaster can display the query and analysis results in charts and tables.
	Currently, data can be displayed in tables, line charts, bar charts, and pie charts.

10.5.3 Log Fields

If you access WAF, HSS, CFW, CTS, and IPS logs through the console, SecMaster adds information such as log sources and timestamps to these logs in the form of key-value pairs.

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 10-29 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.na me	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
[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

Parameter	Field Type	Description
[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 10-30 sec-waf-attack

Field	Туре	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	Туре	Description
attack	String	 Attack type The value can be: 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	Туре	Description
action	String	 Processing action. The value can be: 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. 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		Туре	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_se	nt	String	Total number of bytes of the response body sent to the client.
upstream_resp	oonse_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 10-31 describes the fields in WAF access logs.

Table 10-31 sec-waf-access

Field	Туре	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_ti me	String	Response time of the backend server
upstream_status	String	Response code of the backend server
upstream_connect_tim e	String	Duration for connecting to the backend server

Field	Туре	Description
upstream_header_tim e	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 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	10-32	sec-obs-access
Tuble	10 52	Jee obj access

Field	Туре	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	Туре	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: 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	Туре	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.
huawei_cloud_service	String	 Whether the request is a CDN request. CDN_F: Authentication failed. CDN: Authentication succeeded.
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_typ e	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_coun t	String	Number of times that data is read.
vpc_id	String	ID of the VPC to which the request client belongs.
access_with_security_t oken	String	Access using the STS token.
copy_size	String	Copy size.

Field	Туре	Description
vpcep_traffic	String	Transmission through VPCEP.
access_key	String	AK.

sec-nip-attack

Fields in IPS attack logs

Table 10-33 sec-nip-attack

Field	Туре	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.
Dstlp	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.

Field	Туре	Description
Target	String	 Object attacked by the packet detected by a signature. The value can be: server: The attack object is the server. client: The attack object is the client. both: The attack objects are both the server and client.
Severity	String	Severity of the attack caused by the packet detected by a signature. The value can be: • information • low • medium • high
Os	String	OS attacked by the packet detected by a signature. The value can be: 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. 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

Field	Туре	Description
uid	String	User ID
un	String	Username
did	String	Domain ID
dn	String	Domain name
src	String	Request domain name
opl	String	Operation level
ор	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

Table 10-34 sec-iam-audit

sec-hss-vul

Fields in HSS vulnerability scanning results

Table 10-35 sec-hss-vul

Field	Туре	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.

Field		Туре	Description
occurTime	occurTime		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.
hostlp		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	vulld	String	Official vulnerability ID.
	type	Int32	Vulnerability type. The value can be:
			• 0: Linux
			 1: Windows 2: Web CMS
repairNecessit y status		Int32	 Necessity level of vulnerability fixing. The value can be: 1: low-risk 2&3: medium-risk 4: high risk
		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.

Field		Туре	Description
	severityLevel	String	Vulnerability severity. The options are as follows: • Critical • High • Medium • Low
	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 .
	agentld	String	UUID of the associated host agent.
	projectId	String	ID of the affected tenant.

sec-hss-alarm

Fields in HSS alert logs

Table 10-36 sec-hss-alarm

Field		Туре	Description
agentUuid		String	Agent UUID.
alarmCsn		String	Alert UUID.
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.
alarmVersio	on	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.
hostlp		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.
enterpriseP	rojectId	String	ID of the affected enterprise tenant.
appendInfo		Object	Alert details.
appendInf	agent_id	String	Agent ID.
0	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.

F : 14		Turne	Description	
Field			Туре	Description
	occur_time		Long	Occurrence time (accurate to second).
	recent_time		Long	Last occurrence time (accurate to second).
	event_cateo	Jory	Integer	Incident category.
	event_type		Integer	Incident type.
	event_coun	t	Integer	Number of incidents.
	severity		Integer	Severity.
	attack_phas	se	Integer	Attack phase.
	attack_tag		Integer	Attack tag.
	confidence		Integer	Confidence.
	action		Integer	Action.
	detect_moc	lule	String	Detection module.
	report_sour	ce	String	Report source.
	related_eve	nts	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 user_info		list	Process information.
			list	User information.
	file_info		list	File information.
	geo_info		Object	Geographic information.
	malware_in	fo	Object	Malware information.
	forensic_info		String	Evidence collection field.
	recommend	lation	String	Handling suggestions.
	extend_info)	String	Extended incident information.
	resource_i	project_id	String	Project ID.
r	nfo	region_na me	String	Region name.
		vpc_id	String	VPC ID.

Field			Туре	Description
		host_nam e	String	Host name.
		host_ip	String	Host IP address.
		host_id	String	Host ID (ECS ID).
		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_versio n	String	OS version.
	network_i nfo	local_add ress	String	Local address.
		local_port	Integer	Local port.
		remote_a ddress	String	Remote address.
		remote_p ort	Integer	Remote port.
		src_ip	String	Source IP address.
		src_port	Integer	Source port.
		src_domai n	String	Source domain.
		dest_ip	String	Destination IP address.
		dest_port	Integer	Destination port.
		dest_dom ain	String	Destination domain.
		protocol	String	Protocol.
		app_proto col	String	Application layer protocol.

Field	Field			Description
		flow_direc tion	String	Flow direction.
	app_info	sql	String	Executed SQL statement.
		domain_n ame	String	DNS domain name.
		url_path	String	URL.
		url_meth od	String	URL method.
		req_refer	String	URL request referrer.
		email_sub ject	String	Email subject.
		email_sen der	String	Email sender.
		email_rec eiver	String	Email recipient.
		email_key word	String	Email keyword.
	process_in fo	process_n ame	String	Process name.
		process_p ath	String	Process file path.
		process_pi d	Integer	Process ID.
		process_ui d	Integer	Process user ID.
		process_u sername	String	Process username.
		process_c mdline	String	Process file command line.
		process_fi lename	String	Process file name.
		process_st art_time	Long	Process start time.
		process_gi d	Integer	Process group ID.
		process_e gid	Integer	Effective process group ID.

Field			Туре	Description
		process_e uid	Integer	Effective process user ID.
		parent_pr ocess_na me	String	Parent process name.
		parent_pr ocess_pat h	String	Parent process file path.
		parent_pr ocess_pid	Integer	Parent process ID.
		parent_pr ocess_uid	Integer	Parent process user ID.
		parent_pr ocess_cm dline	String	Parent process file command line.
		parent_pr ocess_file name	String	Parent process file name.
		parent_pr ocess_star t_time	Long	Parent process start time.
		parent_pr ocess_gid	Integer	Parent process group ID.
		parent_pr ocess_egi d	Integer	Effective parent process group ID.
		parent_pr ocess_eui d	Integer	Effective parent process user ID.
		child_proc ess_name	String	Subprocess name.
		child_proc ess_path	String	Subprocess file path.
		child_proc ess_pid	Integer	Subprocess ID.
		child_proc ess_uid	Integer	Subprocess user ID.
		child_proc ess_cmdli ne	String	Subprocess file command line.

Field			Туре	Description
		child_proc ess_filena me	String	Subprocess file name.
		child_proc ess_start_ time	Long	Subprocess start time.
		child_proc ess_gid	Integer	Subprocess group ID.
		child_proc ess_egid	Integer	Effective subprocess group ID.
		child_proc ess_euid	Integer	Effective subprocess user ID.
		virt_cmd	String	Virtualization command.
		virt_proce ss_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_nam e	String	Username.
		user_grou p_name	String	User group name.
		user_hom e_dir	String	User home directory.
		login_ip	String	User login IP address.
		service_ty pe	String	Login service type.
	service_p ort	Integer	Login service port.	
		login_mo de	String	Login mode.
		login_last time	Long	Last login time of a user.

Field			Туре	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_war n_left_day s	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_mtim e	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_sha25 6	String	File SHA256 value.
		file_type	String	File type.
	file_conte nt	String	File content.	
		file_attr	String	File attribute.
		file_opera tion	String	File operation type.
		file_chang e_attr	String	Old/New attribute.

Field			Туре	Description
		file_new_ path	String	New file path.
		file_desc	String	File description.
		file_key_w ord	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_i nfo	monitor_ process	String	Monitoring process.
		escape_m ode	String	Escape mode.
		abnormal _port	String	Abnormal port.
	geo_info	src_countr y	String	Source country/region.
		src_city	String	Source city.
		src_latitu de	Long	Source latitude.
		src_longit ude	Long	Source longitude.
		dest_coun try	String	Destination country/region.
		dest_city	String	Destination city.
		dest_latit ude	Long	Destination latitude.
		dest_longi tude	Long	Destination longitude.
	malware_ info	malware_ family	String	Malware family.
		malware_ class	String	Malware classification.
	system_in	pwd_valid	Boolean	Whether the password is valid.
	fo	pwd_min_ len	Integer	Password length.

Field			Туре	Description
		pwd_digit _credit	Integer	Digits contained in the password.
		pwd_upp ercase_let ter	Integer	Uppercase letters contained in the password.
		pwd_lowe rcase_lett er	Integer	Lowercase letters contained in the password.
		pwd_speci al_charact ers	Integer	Special characters contained in the password.
	extend_in	hit_rule	String	Hit rule.
	fo	rule_nam e	String	Rule name.
		rulesetna me	String	Rule set name.
		report_ty pe	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_ti me	Long	First detection time.
		ti_last_ti me	Long	Last detection time.

sec-hss-log

Fields in HSS security logs

Table 10-37 sec-hss-log

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

Field		Туре	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.
alarmVersio	on	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.
hostlp		String	Communication IP address of the affected host.
ipList	ipList		List of IP addresses of affected hosts.
cloudId		String	Cloud agent SN.
region	region		Region where the affected host is located.
projectId		String	ID of the affected tenant.
enterpriseP	rojectId	String	ID of the affected enterprise tenant.
appendInfo)	Object	Alert details.
appendInf	agent_id	String	Agent ID.
0	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			Туре	Description
	event_cate	Jory	Integer	Incident category.
	event_type		Integer	Incident type.
	event_coun	t	Integer	Number of incidents.
	severity		Integer	Severity.
	attack_pha	se	Integer	Attack phase.
	attack_tag		Integer	Attack tag.
	confidence		Integer	Confidence.
	action		Integer	Action.
	detect_mod	lule	String	Detection module.
	report_sour	ce	String	Report source.
	related_eve	ents	String	Related incident ID.
	resource_in	fo	Object	Resource information.
	network_in	fo	Object	Network information.
	app_info		Object	Application information.
	system_info		Object	System information.
	process_inf	0	list	Process information.
	user_info		list	User information.
	file_info		list	File information.
	geo_info		Object	Geographic information.
	malware_ir	ifo	Object	Malware information.
	forensic_inf	ō	String	Evidence collection field.
	recommend	dation	String	Handling suggestions.
	extend_info		String	Extended incident information.
	resource_i	project_id	String	Project ID.
nfo	region_na me	String	Region name.	
		vpc_id	String	VPC ID.
		host_nam e	String	Host name.
		host_ip	String	Host IP address.
		host_id	String	Host ID (ECS ID).

Field			Туре	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_versio n	String	OS version.
	network_i nfo	local_add ress	String	Local address.
		local_port	Integer	Local port.
		remote_a ddress	String	Remote address.
	remote_p ort	Integer	Remote port.	
		src_ip	String	Source IP address.
		src_port	Integer	Source port.
		src_domai n	String	Source domain.
		dest_ip	String	Destination IP address.
		dest_port	Integer	Destination port.
		dest_dom ain	String	Destination domain.
		protocol	String	Protocol.
		app_proto col	String	Application layer protocol.
		flow_direc tion	String	Flow direction.
	app_info	sql	String	Executed SQL statement.

Field			Туре	Description
		domain_n ame	String	DNS domain name.
	url_path	String	URL.	
		url_meth od	String	URL method.
		req_refer	String	URL request referrer.
		email_sub ject	String	Email subject.
		email_sen der	String	Email sender.
		email_rec eiver	String	Email recipient.
		email_key word	String	Email keyword.
	process_in fo	process_n ame	String	Process name.
		process_p ath	String	Process file path.
		process_pi d	Integer	Process ID.
		process_ui d	Integer	Process user ID.
		process_u sername	String	Process username.
		process_c mdline	String	Process file command line.
		process_fi lename	String	Process file name.
		process_st art_time	Long	Process start time.
		process_gi d	Integer	Process group ID.
		process_e gid	Integer	Effective process group ID.
		process_e uid	Integer	Effective process user ID.

Field			Туре	Description
		rent_pr ess_na	String	Parent process name.
		rent_pr ess_pat	String	Parent process file path.
		rent_pr ess_pid	Integer	Parent process ID.
		rent_pr ess_uid	Integer	Parent process user ID.
		rent_pr ess_cm ne	String	Parent process file command line.
		rent_pr ess_file me	String	Parent process file name.
	oce	rent_pr ess_star ime	Long	Parent process start time.
		rent_pr ess_gid	Integer	Parent process group ID.
		rent_pr ess_egi	Integer	Effective parent process group ID.
		rent_pr ess_eui	Integer	Effective parent process user ID.
		ld_proc _name	String	Subprocess name.
		ld_proc _path	String	Subprocess file path.
		ld_proc _pid	Integer	Subprocess ID.
		ld_proc _uid	Integer	Subprocess user ID.
		ld_proc _cmdli	String	Subprocess file command line.

Field			Туре	Description
		child_proc ess_filena me	String	Subprocess file name.
		child_proc ess_start_ time	Long	Subprocess start time.
		child_proc ess_gid	Integer	Subprocess group ID.
		child_proc ess_egid	Integer	Effective subprocess group ID.
		child_proc ess_euid	Integer	Effective subprocess user ID.
		virt_cmd	String	Virtualization command.
		virt_proce ss_name	String	Virtualization process name.
	user_info	escape mode	String	Escape mode.
		escape cmd	String	Command executed after the escape.
		user_id	Integer	User ID.
		user_gid	Integer	User GID.
		user_nam e	String	Username.
		user_grou p_name	String	User group name.
		user_hom e_dir	String	User home directory.
		login_ip	String	User login IP address.
		service_ty pe	String	Login service type.
		service_p ort	Integer	Login service port.
		login_mo de	String	Login mode.
		login_last time	Long	Last login time of a user.

Field			Туре	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_war n_left_day s	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_mtim e	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_sha25 6	String	File SHA256 value.
		file_type	String	File type.
		file_conte nt	String	File content.
		file_attr	String	File attribute.
		file_opera tion	String	File operation type.
		file_chang e_attr	String	Old/New attribute.

Field			Туре	Description
		file_new_ path	String	New file path.
		file_desc	String	File description.
		file_key_w ord	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_i nfo	monitor_ process	String	Monitoring process.
		escape_m ode	String	Escape mode.
		abnormal _port	String	Abnormal port.
	geo_info	src_countr y	String	Source country/region.
		src_city	String	Source city.
		src_latitu de	Long	Source latitude.
		src_longit ude	Long	Source longitude.
		dest_coun try	String	Destination country/region.
		dest_city	String	Destination city.
		dest_latit ude	Long	Destination latitude.
		dest_longi tude	Long	Destination longitude.
	malware_ info	malware_ family	String	Malware family.
		malware_ class	String	Malware classification.
	system_in	pwd_valid	Boolean	Whether the password is valid.
	fo	pwd_min_ len	Integer	Password length.

Field			Туре	Description
		pwd_digit _credit	Integer	Digits contained in the password.
		pwd_upp ercase_let ter	Integer	Uppercase letters contained in the password.
		pwd_lowe rcase_lett er	Integer	Lowercase letters contained in the password.
		pwd_speci al_charact ers	Integer	Special characters contained in the password.
	extend_in fo	hit_rule	String	Hit rule.
		rule_nam e	String	Rule name.
		rulesetna me	String	Rule set name.
		report_ty pe	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_ti me	Long	First detection time.
		ti_last_ti me	Long	Last detection time.

sec-ddos-attack

Fields in Anti-DDoS attack logs

Table 10-38 sec-ddos-attack

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

Field	Туре	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	Туре	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	Туре	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 10-39 sec-cts-audit

Field	Туре	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	Туре	Description
trace_name	String	Operation name.
trace_rating	String	 Level of an operation incident. The options are as follows: 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: 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	Туре	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

Field	Туре	Description
event_time	Date	Attack time
action	String	Response action of CFW permit deny
арр	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	Туре	Description
attack_type	String	Type of the attackVulnerability exploitVulnerability scanTrojanWormsPhishingWeb attacksApplication DDoSBuffer overflowPassword attacksMailAccess controlHacking toolsHijackingProtocol exceptionSpamSpywareDDoS floodSuspicious DNS activitiesOther 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 CRITICAL HIGH MIDDLE LOW
source	String	 Defense for the detected attack 0: basic defense 1: virtual patch
src_ip	String	Source IP address
src_port	String	Source port number

Field	Туре	Description
direction	String	Flow direction
		out2in: inbound
		 in2out: outbound

sec-cfw-flow

Fields in CFW traffic logs

Table 10-41	sec-cfw-flow
-------------	--------------

Field	Туре	Description
арр	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 10-42 sec-cfw-block

Field	Туре	Description
hit_time	Date	Time of access

Field	Туре	Description
action	String	Response action of CFW
		• permit
		• deny
арр	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

Field	Туре	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	Туре	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_tim e	String	Time required for a remote connection.
upstream_header_tim e	String	Time required for receiving the header at the remote end.
upstream_response_ti me	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 10-44 dbss-alarm

Field	Туре	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		Туре	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.

Field	Туре	Description
log_type	String	Alert type
region_id	String	Region
domain_id	String	Account ID.
project_id	String	Project ID
leakage_ak	String	АК
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

 Table 10-45
 AK SK leakage (aksk_leakage)

Field	Туре	Description
leakage_user_name	String	Sub-username of the leakage
leakage_domain_id	String	Leaked account ID.
leakage_domain_nam e	String	Leaked account name.
url	String	Website URL of the leakage

Table 10-46 Risky OBS bucket files (obs_risk)

Field	Туре	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<stri ng,String>></map<stri 	List of matched rules
keyword	String	Keyword for matching sensitive data rules
available_zone	String	AZ
encrypted	String	Whether to encrypt data

Field	Туре	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_i d	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<stri ng,String>></map<stri 	List of matched rules
keyword	String	Keyword for matching sensitive data rules

 Table 10-47
 Sensitive data fields (db_risk)

10.5.4 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**.

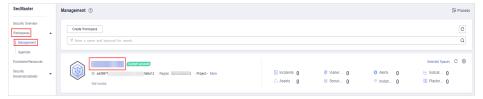
Limitations and Constraints

Custom index can be configured only for new custom pipelines. For details, see **Creating a Pipeline**.

Configuring Field Indexes

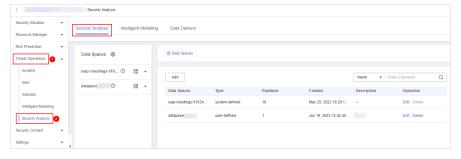
- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-60 Workspace management page



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

Figure 10-61 Accessing the Security Analysis tab page



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

Figure 10-62 Pipeline data page

Data Spaces 🐵	⊗ Data Spaces × Kase-waf-attack ×	
isap-cloudlogs-cc2 ⑦ 88 ▲	sec-waf-attack Dark Overy	Index Bettings Serve As Quick Query Add Ak Q] Last 15 minutes v Overy/Analyze
	count 2 1.5 0.5 0.5 Dec 07, 202 17:45:00 Dec 07, 202 17:47:40 Dec 07, 202 17:50:00 Oe DEC 07, 202 17:50:000 OE DEC 07, 202 17:	Dec 07, 2022 17.45.67 Dec 07, 2022 18.60.07 C

Step 6 On the pipeline page, click **Index Settings** in the upper right corner.

Step 7 On the **Index Settings** page, configure index parameters.

1. Enable the index status.

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

2. Configure index parameters. For details about the parameters, see **Table 10-48**.

Parameter	Description
Field	Log field (key)
Туре	Data type of the log field value. The options are text, keyword, long, integer, double, float, date, and json.
Includes Chinese	Indicates whether to distinguish between Chinese and English during query. This parameter needs to be specified when Type is set to text .
	 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.
	Example: The log content is user:WAF log user Zhang San .
	 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.

Table 10-48 Parameters for index settings

Step 8 Click OK.

----End

10.5.5 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.

- Entering Query Criteria for Query and Analysis
- Using Existing Fields for Query and Analysis
- Managing Query Analysis Results

Prerequisites

Data access has been completed. For details, see **Data Integration**.

Entering Query Criteria for Query and Analysis

Step 1 Log in to the management console.

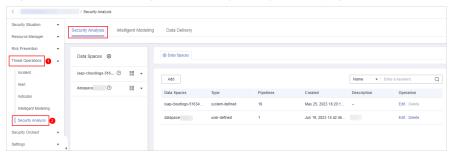
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-63 Workspace management page

SecMaster	Management 💮	🕞 Process
Security Overview Workspaces	Onthe Writegace IP forthe a number and happened for search.	C
Purchased Resources Security Governance(beta)	Constant and a constant a cons	Selected Spaces C indicat 0 Playbo 0

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

Figure 10-64 Accessing the Security Analysis tab page



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

Figure 10-65 Pipeline data page

Analyze & Query Intelligent Modeling	
Data Spaces 🐵	© Data Spaces x 🛛 🔁 sec-wsf-attack x
isap-cloudlogs-cc2 ⑦	sec-weif-ettack Index Settings Save As Quick Query Add Alam Quick Query • Enter a search ortheria Quick Query • Coordinates • Coordinates
	Count C C C C C C C C C C C C C

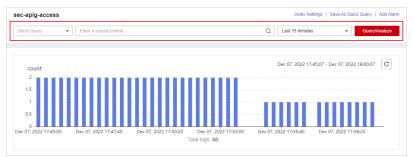
Step 6 On the pipeline data retrieval page, enter the query analysis statement.

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.

Figure 10-66 Query/Analyze



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

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

Step 8 Click Query/Analyze and view the results.

----End

Using Existing Fields for Query and Analysis

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

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

Figure 10-67 Workspace management page

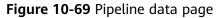
SecMaster	Management ③				Process
Security Overview Workspaces	Crede Workspect T later a name and layouth for search.				C
Purchased Resources Security Governance(beta)	B add077 dda12 Repor Net hold:	Incidents 0 Assets 0	♥ Vulner 0 i Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞

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

Figure 10-68 Accessing the Security Analysis tab page

<	/ Security Analysis							
Security Situation 🔹	Security Analysis Intelligent Modeling	Data Delivery						
Resource Manager 🔹	Security Analysis Intelligent Modeling	Data Delivery						
Risk Prevention 👻								
Threat Operations 1	Data Spaces 💿	Data Spaces						
Incident	isap-cloudlogs-516 🕐 🚦 👻							
Alert	datapace 🕜 🔡 👻	Add				Name 🔻 Ei	nter a keyword.	Q
Indicator		Data Spaces	Туре	Pipelines	Created	Description	Operation	
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete	
Security Analysis 2		datapacer	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete	
Security Orchest 🔹								
Settings •	4							

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.



Analyze & Query Intelligent Modeling		
Data Spaces 🕲	O Data Spaces x Fa sec-waf-attack x	
isap-cloudlogs-cc2 ⑦	sec-waf-attack Ouck Overy	Index Settings Save As Quick Query Add Alarm Q Last 15 minutes
	Count 2 1.5 0 0 0 0 0 0 0 0 0 0 0 0 0	Dee 07, 2022 17:45:07 Dee 07, 2023 18:00:07 C

Step 6 Set search criteria.

For details about the existing fields in the access data, see Log Fields.

NOTE

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

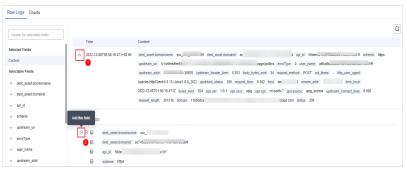
Click
 ✓ before an optional field on the left and click
 ^① (adding a field value)
 or
 [○] (removing a field value) next to the target field. The matched fields are
 displayed in the query box.

Figure 10-70 Filtering a Field Value (1)

c-apig-access				Index Settings Save As Quick Query Add
luick Query 👻	dest_asset.domainname=MATCH_QUERY('soc_soc_	0	X Q Las	t 15 minutes • Ouery/Analyz
count			Dec 0	18, 2022 09:37:31 - Dec 08, 2022 09:52:31
1				
Dec 08, 2022 09:37:20	Dec 08, 2022 09:39:20 Dec 08, 2022 09:	41:20 Dec 08, 2022 09:43:20 Dec 08, 2022 09:45:20 Total logs: 45	Dec 08, 2022 09:47:20 Dec 08, 2022 09:49:2	20 Dec 08, 2022 09:51:20
_				
Search for selectable fields.	Time	Content		
Search for selectable fields.	Time 2022-12-60109 52:16.385-66.0	Content	.74 stat4 aprjj£ 500ee opsetsa erro7rpa: 0 uner_nama: ad0	lac31f scheme: https
_		Content O derd_atest.domaname_esc		lac31f scheme: https
Search for selectable fields. Rected Fields	✓ 2022-12-06T09 52:16.385+08.0	Content 9 derd, jasel dimensione: esc. 9 derd, jasel dimension genteum_uter: Volterante genteum_uter: 3000 upteum_besicit, time: 0.303 Austachterffichter(45:33) zumit 8,2,473 upteum_utities: 200 mages	ebolitics errorType: 0 user_name. add body_bytes_sent 34 request_method: POST out_tin ent_time: 0.352 host ae 5 remote_addr 1	lac31f scherne: https Datboi nes: - http_user_agent: 1 30 time_locat
Search for selectable fields. lected Fields intent lectable Fields	✓ 2022-12-06T00 52:16.385+08:0	Content O dest_asset_domainsame_stor) dest_asset_domainsame_stor updatemadd to 2005 updatembases_films = 0.333	ebolitics errorType: 0 user_name. add body_bytes_sent 34 request_method: POST out_tin ent_time: 0.352 host ae 5 remote_addr 1	lac31f scherne: https Datboi nes: - http_user_agent: 1 30 time_locat

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

Figure 10-71 Filtering a Field Value (2)



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

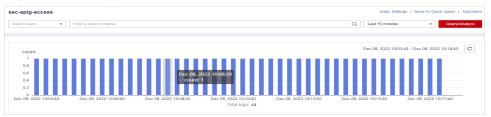
Managing Query Analysis Results

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.

Figure 10-72 Log distribution bar chart



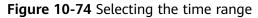
• Raw Logs

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

Figure 10-73 Raw Logs

Search for selectable fields.		
	Time	Content
Selected Fields	✓ 2022-11-17T19:26:19.311+08:00	dest_asset domainname: scc9 dest_asset domainid: ac743 e8bf4 api_id:
Content		50c 51ac31f scheme: https
Selectable Fields		upstream_uri: /v1/infers/fee59dc6-17e ation/image/politics errorType: 0 user_name:
 dest_asset.domainname 		ado: '296119 upstream_addr: :30935 upstream_header_time: 0.353 body_bytes_sent: 34
 dest asset.domainid 		request_method: POST out_times: - http_user_agent: Apache-HttpClient/4.5.13 (Java/1.8.0_262) upstream_status: 200
- 1		request_time: 0.352 host: 2 7 status: 200
✓ api_id		
√ scheme	2022-11-17T19:26:19.311+08:00	dest_asset.domainname: scc_s) dest_asset.domainid: ac743 8bf4 apl_id:
✓ upstream_uri		50deea81591 :31f scheme: https
✓ errorType		upstream_uri: /v1/infers/fee 4-469858/b5608/v1.0/moderation/image/politics errorType: 0 user_name:
		ad0a0bc '2961f9 upstream_addr: i:30935 upstream_header_time: 0.353 body_bytes_sent: 34

- 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.





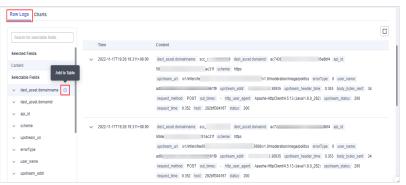
■ To view data of all fields at a specified time, click ✓ in front of the time in the table to expand all data. By default, data is displayed in a table.

To view data in JSON format, click the **JSON** tab. Data in JSON format is displayed on the page.

Figure 10-75 Expand to display data

Search for selectable fields.		Ľ
	Time Content	
Selected Fields	A 2022-11-17T19-26:19.311+08:00 dest_asset.domainname: scc) dest_asset.domainid: ac7438b6 ie&bf4 api_jd:	
Content	50: ac31f scheme. https	
Selectable Fields	upstream_uri: /v1/imfers/fee 1.0/moderation/image/politics errorType: 0 user_name:	
 dest_asset.domainname 	ad0a(11111111111111111111111111111111111	1
 dest_asset.domainid 	request_method. POST out_times: - http_user_agent: Apache-HttpCtient/4.5.13 (Java/1.8.0_262) upstream_status: 200	
o dest_assec domains	remark time: 0.262 best: 2026#204467 status: 200	
	request_time: 0.352 host: 292btf304167 status: 200	
 deal_assec_domains api_id scheme 	request_lime: 0.352 Noti: 22200504467 intel:: 200	
√ api_id	Table JSON	
→ api_id	Table JSCN dist_asset domainmanic_acc	
 api_id scheme upstream_uni errorType 	Table JSON	
 api_id scheme upstream_unt error1ype user_name 	Table 2501	
 → api_id → scheme > upstream_uri 	Table JSON Image: Set of domainsment sect_set Image: Sect_set sect_set	

Figure 10-76 Selected fields to be displayed



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.

Figure 10-77 Adjusting field display sequence

Search for selectable fields					Ľ
	Time	dest_asset.domainname	dest_asset.domainid 💶 🛪	api_id ◀ ► ×	scheme 🔹 🛪
ielected Fields	✓ 2022-11-17T19:26:19.311+08:00	500,	ac74: šeb		https
✓ api_id	√ 2022-11-17719.26.19.311+08.00	800_	ac74: 04eb		https
✓ dest_asset.domainname ⊙	✓ 2022-11-17T19.25:59.300+08.00	scc.	ac74: eb	50c ±10	https
∽ scheme ⊙	✓ 2022-11-17719:25:59:300+08:00	sce,	ac74: eb	50de 10	https
v upstream_uri	✓ 2022-11-17719:25:39:290+08:00	scc	ac74 ieb		https
 upsream_un errorType 	✓ 2022-11-17719:25:39.290+08:00	scc	ac74 sb		https
v user_name	✓ 2022-11-17719:25:19.280+08:00	scc_	ac7 b		https
v upstream_addr	✓ 2022-11-17T19:25:19.280+08:00	sci	ac7 leb		https
 upstream_header_time body_bytes_sent 	✓ 2022-11-17719:24:59.270+08:00	scc	ac7- 3b	50)	https
 request_method 	✓ 2022-11-17T19:24:59.270+08:00	SCC.	ac7(https

 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.

Figure 10-78 Cancel

Search for selectable fields.											ſ
Selected Fields	1 -	Time 2022-11-17T19:26:		dest_asset.do	mainname 🕨 🗙	dest_asset.domainid 4	-	api_id 4 F ×			
v api_id ⊙	- I -										
√ dest_asset.domainid Θ	- I - I	 2022-11-17T19:26: 	19.311+08.00	800,		ac7	leb	50	0	https	
✓ dest_asset.domainname ⊖		✓ 2022-11-17T19:25:	59.300+08:00	500_		ac74	eb	51	1	https	
\vee scheme Θ		2022-11-17T19:25	59.300+08:00	scc.		ac7-	o	51	0	https	
Selectable Fields		2022-11-17719:25	39.290+08:00	500,		ac		5(0	https	
 upstream_uri errorType 		 2022-11-17T19:25: 	39.290+08:00	scc,		ac7	b	50	b	https	
✓ user_name		2022-11-17T19:25:	19.280+08:00	scc		ac7-		5		https	
✓ upstream_addr		✓ 2022-11-17T19:25:	19.280+08:00	500		ac7-		50d		https	
 upstream_header_time body bytes sent 		 2022-11-17T19:24: 	59.270+08:00	scc_		ac7		504		https	
v request_method		2022-11-17719:24:	59 270+09-00	100		ac7438	leb	50c		https	

- To export logs: On the **Raw Logs** tab page, click ^C in the upper right corner of the page. The system automatically downloads raw logs to the local PC.
- Charts

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

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

Alarm

In the upper right corner of the **Analyze & Query** tab, click **Add Alarm** to add alert models. You can set alert rules for generating alerts for query and analysis results hit the rules. For details, see **Quickly Adding a Log Alarm Model**.

• Quick Query

In the upper right corner of the query analysis page, click **Save as Quick Query** to save search criteria as a quick query. For details, see **Quick Query**.

10.5.6 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-79 Workspace management page



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

Figure 10-80 Accessing the Security Analysis tab page

<	/ Security Analysis							
Security Situation • Resource Manager •	Security Analysis Intelligent Modeling Data Delivery							
Risk Prevention Threat Operations	Data Spaces 🔞	Data Spaces						
Incident	isap-cloudlogs-516 ⑦ 🖁 🗸 🔻	Add				Name 👻 Enter	a keyword.	Q
Indicator	datapace 🕜 🔐 🕶	Data Spaces	Туре	Pipelines	Created	Description	Operation	
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete	
Security Analysis		datapace	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete	
Security Orchest 👻								
Settings •								

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

Figure 10-81 Pipeline data page

Analyze & Query Intelligent Modeling		
Data Spaces 🐵	⊗ Data Spaces × Rs tec-waf-attack ×	
isap-cloudiogs-cc2 ⑦ 88 ▲	sec-waf-attack Ounch Owny Enter a search orders Qu 	Index Settings Save As Quick Query Add Alarm L Last 15 minutes Query/Analyze
	Count 2 1.5 1.5 0 0 0 0 0 0 0 0 0 0 0 0 0	Dec 07, 2022 17.4567 - Dec 07, 2022 1860607 (C)

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 \square . The system downloads logs to the local PC.
- Chart logs: On the **Charts** tab page, click **Download**. The system downloads the logs to the local PC.

----End

10.5.7 Query and Analysis Statements - SQL Syntax

10.5.7.1 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

Statement Type	Description
Query Statement	A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.
Analysis Statement	An analysis statement is used to calculate and collect statistics on query results.

Table 10-49 Basic syntax

10.5.7.2 Limitations and Constraints

• Query statements do not support mathematical operations, such as (age + 100) ≤ 1000 .

- Aggregate functions support only fields and do not support expressions, for example, avg(log(age)).
- Multi-table association is not supported.
- Subqueries are not supported.
- A maximum of 500 records can be returned on the page.
- A maximum of 10,000 groups can be returned by GROUP BY.

10.5.7.3 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 10-50 Operator descriptions

Operator	Description
=	Queries logs in which the value of a field is equal to a certain value.
\Leftrightarrow	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.

Operator	Description
IN	Queries the logs whose field values are within a specified value range.
BETWEEN	Queries the logs whose field values are in the specified range.
LIKE	Searches for logs of a field value in full text.
IS NULL	Queries logs whose field value is NULL.
IS NOT NULL	Query logs whose field value is NOT NULL.

Examples

Table 10-51 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'
Logs about successful GET or POST requests	(request_method = 'GET' OR request_method = 'POST') AND status BETWEEN 200 AND 299
Logs of GET or POST request failures	(request_method = 'GET' OR request_method = 'POST') NOT status BETWEEN 200 AND 299
Logs of successful GET requests (status code: 200 to 299) whose request time is greater than or equal to 60 seconds.	request_method = 'GET' AND status BETWEEN 200 AND 299 AND request_time >= 60
Logs whose request time is 60 seconds.	request_time = 60

10.5.7.4 Syntax of Analysis Statements

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
```

[ORDER BY expression [ASC | DESC] [, ...]] [LIMIT size OFFSET offset]

10.5.7.5 Analysis Statements - SELECT

Specifies the field to be queried.

Using * to query all fields.

SELECT *

Table 10-52 Using * to query all fields

account _numbe r	firstn ame	gend er	city	balanc e	emplo yer	state	lastna me	age
1	Amb er	М	Broga n	39225	Pyrami	IL	Duke	32
16	Hatti e	М	Dante	5686	Netag y	TN	Bond	36
13	Nane tte	F	Nogal	32838	Quility	VA	Bates	28
18	Dale	М	Orick	4180	null	MD	Adams	32

Querying a Specified Field

SELECT firstname, lastname

Table 10-53 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 10-54 Using AS to define field aliases

num
1

num	
16	
13	
18	

Using the DISTINCT Statement

SELECT DISTINCT age

Table 10-55 Using the DISTINCT statement

age	
32	
36	
28	

Using SQL Functions

For details about functions, see Functions.

SELECT LENGTH(firstname) as len, firstname

Table 10-56 Using SQL functions

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

10.5.7.6 Analysis Statements - GROUP BY

Groups data by field value.

Grouping by Field Value

SELECT age GROUP BY age

Table 10-57 Grouping by field value

age	
28	
32	
36	

Grouping by Field Alias

SELECT account_number AS num GROUP BY num

Table 10-58 Grouping by field alias

num	
1	
16	
13	
18	

Grouping by Multiple Fields

SELECT account_number AS num, age GROUP BY num, age

Table 10-59 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 10-60 Using SQL functions

len	count
4	2
5	2

10.5.7.7 Analysis Statements - HAVING

Filters data based on grouping and Aggregate Functions.

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

Table 10-61 The HAVING function

age	MAX(balance)
28	32838
32	39225

10.5.7.8 Analysis Statements - ORDER BY

Sorts data by field value.

Sorting Data by Field Value

SELECT age ORDER BY age DESC

Table 10-62 Sorting by field value

age	
28	
32	
32	
36	

10.5.7.9 Analysis Statements - LIMIT

Specifies the number of returned data records.

Specifying the Number of Returned Records

SELECT * LIMIT 1

account _numb er	first nam e	gende r	city	balan ce	emplo yer	state	lastna me	age
1	Amb er	М	Broga n	39225	Pyrami	IL	Duke	32

Table 10-63 Specifying the number of returned records

Specifying the Number of Returned Records and Offsets

SELECT * LIMIT 1 OFFSET 1

Table 10-64 Specifying the number of returned records and offsets

account _numb er	first nam e	gende r	city	balan ce	emplo yer	state	lastna me	age
16	Hatti e	М	Dante	5686	Netag y	TN	Bond	36

10.5.7.10 Analysis Statements - Functions

Mathematics Functions

Table 10-65 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
е	Natural base number e	e() -> double	SELECT e() LIMIT 1
ехр	Power of the natural base number e	exp(number T) -> T	SELECT exp(0.5) LIMIT 1

Function	Purpose	Description	Example Value
expm1	Subtract one from the power of the natural base number e.	expm1(number T) -> T	SELECT expm1(0.5) LIMIT 1
floor	Rounded down	floor(number T) -> T	SELECT floor(0.5) AS Rounded_Down LIMIT 1
ln	Returns the natural logarithm.	ln(number T) -> double	SELECT ln(10) LIMIT 1
log	Logarithm with T as the base	log(number T, number) -> double	SELECT log(10) LIMIT 1
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	Multiplicatio n	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
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

Function	Purpose	Description	Example Value
/	Division	number / number -> number	SELECT 1 / 100 LIMIT 1
%	Remainder	number % number -> number	SELECT 1 % 100 LIMIT 1

Trigonometric Functions

Table 10-66	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	lnverse 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

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_for mat	Obtains the date value based on the format.	date_format(date, string) -> string	SELECT date_format(date, 'Y') LIMIT 1	
day_of_m onth	Month	day_of_month(date) -> integer	SELECT day_of_month(date) LIMIT 1	
day_of_w eek	Day of a week	day_of_week(date) -> integer	SELECT day_of_week(date) LIMIT 1	
day_of_ye ar	Number of days in the current year	day_of_year(date) -> integer	SELECT day_of_year(date) LIMIT 1	
hour_of_d ay	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_o f_hour	Number of minutes in the current hour	minute_of_hour(date) -> integer	SELECT minute_of_hour(date) LIMIT 1	
minute_o f_day	Number of minutes on the current day	minute_of_day(date) - > integer	SELECT minute_of_day(date) LIMIT 1	
monthna me	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	
timestam p	Date	timestamp(date) -> date	SELECT timestamp(date) LIMIT 1	

Function	Purpose	Description	Example Value
year	Year	year(date) -> integer	SELECT year(date) LIMIT 1

Text Functions

Table 10-68 Text functions

Function	Purpose	Description	Example Value
ascii	ASCII value of the first character	ascii(string T) -> integer	SELECT ascii('t') LIMIT 1
concat_w s	Connection String	concat_ws(separator, string, string) -> string	SELECT concat_ws('-', 'Tutorial', 'is', 'fun!') LIMIT 1
left	Obtain a character string from left to right.	left(string T, integer) - > T	SELECT left('hello', 2) LIMIT 1
length	length	length(string) -> integer	SELECT length('hello') LIMIT 1
locate	Search for a string	locate(string, string) -> integer	SELECT locate('o', 'hello') LIMIT 1
replace	Replace strings	replace(string T, string, string) -> T	SELECT replace('hello', 'l', 'x') LIMIT 1
right	Obtain a character string from right to left.	right(string T, integer) -> T	SELECT right('hello', 1) LIMIT 1
rtrim	Remove the empty character string on the right.	rtrim(string T) -> T	SELECT rtrim('hello ') LIMIT 1
substring	Obtaining a Substring	substring(string T, integer, integer) -> T	SELECT substring('hello', 2,5) LIMIT 1
trim	Remove empty character strings on both sides.	trim(string T) -> T	SELECT trim(' hello ') LIMIT 1

Function	Purpose	Description	Example Value
upper	Convert all letters to uppercase letters.	upper(string T) -> T	SELECT upper('helloworld') LIMIT 1

Other

Table 10-69 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

10.5.7.11 Analysis Statements - Aggregate Functions

Table 10-70 Aggrega	te functions
---------------------	--------------

Function	Purpose	Description	Example Value
avg	Average value	avg(number T) -> T	SELECT avg(age) LIMIT 1
sum	Sum	sum(number T) -> T	SELECT sum(age) LIMIT 1
min	Specifies the minimum value.	min(number T) -> T	SELECT min(age) LIMIT 1
max	Maximum value	max(number T) -> T	SELECT max(age) LIMIT 1

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

10.5.8 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-82 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Create Wontgace Totate a name and keyword for search.				C
Agencies Purchased Resources Security Governance(beta)	Contract Access 0 445977 (Mart 2 Report Paged - Mars Not hold	⊡ incidents 0 ○ Assets 0	 Q Vulner 0 ⊜ Securi 0 	 Alerts Instan 0 	Selected Spaces C ⑧ ↓ Indicat 0 Playbo 0

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

Figure 10-83 Accessing the Security Analysis tab page

<	/ Security Analysis							
Security Situation • Resource Manager •	Security Analysis Intelligent Modeling Data Delivery							
Risk Prevention Threat Operations	Data Spaces 🔞	Data Spaces						
Incident	isap-cloudlogs-516 🕐 🚦 👻	Add				Name 💌 E	nter a keyword.	Q
Indicator	datapace ③ 📅 🔻	Data Spaces	Туре	Pipelines	Created	Description	Operation	
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1		Edit Delete	
Security Analysis		datapace	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete	
Security Orchest Settings	4							

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

Figure 10-84 Pipeline data page

Analyze & Query Intelligent Modelin	9	
Data Spaces 🐵	O Data Spaces × Ca sec-wall-attack ×	
isep-cloudlogs-cc2 ⑦ 88 ▲ sec-waf-attack ⑦ ④ More	sec-waf-attack Quick Overy Enter a search criteria 	Index Settings Save As Quick Query Add Alarr Q. Last 15 minutes
	count 2 1.5	Dec 07, 2022 17:45:07 - Dec 07, 2022 18:00:07
	1 0.5 Dec 07, 2022 17:45:60 Dec 07, 2022 17:45:40 Dec 07, 2022 17:45:60 Dec 07, 2022 1	ec 07, 2022 17:5540 Dec 07, 2022 17:5820

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 10-71
 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 $\overline{}$ in the quick query search box on the pipeline data query and analysis page and select the target quick query name to use the quick query.

----End

10.5.9 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

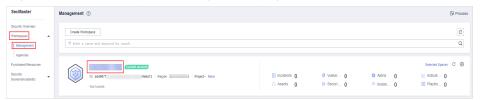
Data access has been completed. For details, see **Data Integration**.

Procedure

Step 1 Log in to the management console.

- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-85 Workspace management page



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

Figure 10-86 Accessing the Security Analysis tab page

<		/ Security Analysis							
Security Situation	٠	Security Analysis Intelligent M	adaliaa	Data Delivery					
Resource Manager	*	Security Analysis Intelligent M	Juening	Data Delivery					
Risk Prevention	*								
Threat Operations		Data Spaces 🛞		Data Spaces					
Incident		isap-cloudlogs-516 ⑦ 🔠	Ŧ						
Alert		datapace ()		Add				Name 👻 Enter a	a keyword. Q
Indicator				Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling				isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1		Edit Delete
Security Analysis				datapace/	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
Security Orchest	*								
Settings	•								

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

Figure 10-87 Pipeline data page

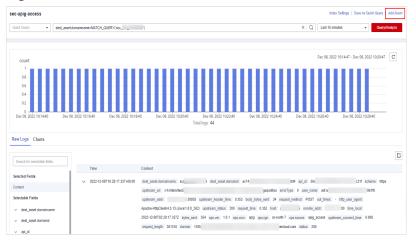
Analyze & Query Intelligent Modeling		
Data Spaces 🐵	Ø Data Spaces × Cale-waf-attack ×	
isap-cloudlogs-cc2 (2) 88	sec-waf-attack	Index Settings Save As Quick Query Add Alarm
sec-waf-attack (2) More	Quick Query	Last 15 minutes
	count 2 1.5 1. 0.5 0 0 0 0 0 0 0 0 0 0 0 0 0	Dee 07, 2022 17.45.07 - Dee 07, 2022 18.00.07 C

Step 6 Enter the query analysis statement, set the time range, and click **Query/Analyze**. The query analysis result is displayed.

For details, see Querying and Analyzing Data.

Step 7 Click **Add Alarm** in the upper right corner of the page. The **Create Alarm Model** page is displayed.

Figure 10-88 Add Alarm



Step 8 Configure basic alarm information by referring to **Table 10-72**.

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.			
	• C: indicates that the model is enabled. This is the default status.			
	•: indicates that the model is disabled.			
	You can change the alarm model status after the model is configured.			

 Table 10-72
 Basic parameters of an alarm model

- **Step 9** After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.
- **Step 10** Set the model logic. For details about the parameters, see **Table 10-73**.

Table 10-73 Configure Model I	_ogic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click Run and view the running result.
Query Plan	Set an alert query plan.
	• 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	 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	Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.
	If there are multiple triggers, click Add .
Alarm Trigger	The way to trigger alerts for queried results. The options are as follows:
	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.
	• C: indicates that the query stops after an alert is generated.
	• Construction: indicates that the query is not stopped after an alert is generated.

- **Step 11** After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.
- **Step 12** After confirming that the preview is correct, click **OK** in the lower right corner of the page to confirm the configuration.

----End

10.5.10 Charts

10.5.10.1 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

10.5.10.2 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-89 Workspace management page

SecMaster	Management () (Process
Security Overview Workspaces	Crede Winkspace C 7 Totar a more and legened for samedy. Q
Purchased Resources Security Governance(beta)	Contractions C @ 0 _ addrift _ bdaf2 0 _ addrift _ paged- Mare It totald: _ Paged- Mare

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

Figure 10-90 Accessing the Security Analysis tab page Intelligent Mo Data Deliver Data Spaces 💿 ② Data Spaces gs-516... ⑦ 🔠 🗸 Add 0 88 • Data Spaces Туре Created Operation May 25, 2023 18:20:1... Edit | Delete Jun 19, 2023 14:42:45... Edit De

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

Figure 10-91 Pipeline data page

Analyze & Query Intelligent Modeling	
Data Spaces 🐵	Obla Spaces × Falsec-waf-attack ×
Isap-cloudlogs-cc2 ⑦	sec-waf-attack Index Settings Save As Oulds Courry Add Alarm
	Ouldk Ouery • Enter a search criteria Q Last 15 minutes • Ouery/Analyze
	Count

- **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 \blacksquare .

Figure 10-92 Charts

Raw I	ogs Charts				
Preview				Download Hide Configuration	✓ Chart Type
	response_code JΞ	request_time ↓Ξ	upstream_header_time ↓Ξ		≣⊻ĿO
	200				
	202				✓ Base Settings Title
	200				Enter a title.
	202				✓ Chart Settings
	200				Hidden Fields
	202				Select at least one field.
	200				

Step 8 Set parameters in the table.

Table 10-74 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

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.10.3 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-93 Workspace management page

SecMaster	Management () Process
Security Overview Workspeces	Center Produces C If there a name and largened for sameh. Q
Purchased Resources Security Governance(beta)	0 add0017 646147 646147 646147 646147 6

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

<	/ Security Analysis									
Security Situation • Resource Manager •	Security Analysis Intel	ligent Modelii	ng D	iata Delivery						
Risk Prevention Threat Operations	Data Spaces 🔞		© (Data Spaces						
Incident	isap-cloudlogs-516 ()	88 *		Add				Name +	Enter a keyword.	(
Alert	datapace (?)	88 ▼	Da	ta Spaces	Туре	Pipelines	Created	Description	Operation	
Intelligent Modeling			isa	p-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete	
Security Analysis 2			dal	tapace	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete	
ecurity Orchest 🔹										
Settings •										

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

Figure 10-95 Pipeline data page

Analyze & Query Intelligent Modeling	
Data Spaces 🐵	© Data Spaces × 1% sec-wal-attack ×
isap-cloudlogs-cc2 ⑦	sec-wsf-attack Index Bettings Save As Guick Query Add Alarm Could Query •] Enter a search ortiens Q Last 15 minutes • Q Last 15 minutes
	Count 2 1.5 0 0 0 0 0 0 0 0 0 0 0 0 0

- **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 **M**.

Figure 10-96 Line chart statistics



Step 8 Set line chart parameters.

Category	Parameter	Description
Base Settings	Title	Customized line chart title
Chart Settings	X-Axis Title	Customized title of the X axis

Category	Parameter	Description		
	Y-Axis Title	Customized title of the Y axis		
	X-Axis Field	Field to be displayed on the X axis		
	Y-Axis Field	Field to be displayed on the Y axis		
Legend	Show Legend	Determine whether to display the legend.		
	Position	This parameter is mandatory when the legend display function is enabled.		
		Position of the legend in the chart. The options are Top , Bottom , Left , and Right .		

After the chart is configured, you can preview the configured data analysis result on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click Add as Indicator Card in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click Save.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.10.4 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 left corner of the page and choose Security & Compliance > SecMaster.

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

Figure 10-97 Workspace management page

SecMaster	Management (2)	Process
Security Overview Workspaces	Cente Writippez T inter a name and lapsend for search.	C
Purchased Resources Security Governance(beta)		-

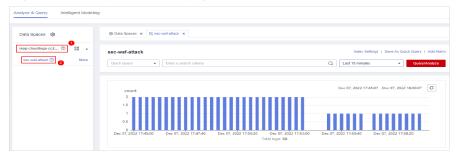
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-98 Accessing the Security Analysis tab page

<	/ / Security Analysis									
Security Situation										
Resource Manager										
Risk Prevention Threat Operations A	Data Spaces 🔞	Data Spaces								
Incident	isap-cloudlogs-516 🕜 📲 🔻	Add				Name v Enter a	a keyword. Q			
Indicator	datapace 🕜 🔡 🕶	Data Spaces	Туре	Pipelines	Created	Description	Operation			
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete			
Security Analysis		datapace	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete			
Security Orchest •										
Settings •										

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

Figure 10-99 Pipeline data page



- **Step 6** Enter the query and analysis statement, set the time range, and click **Query**/ **Analyze**.
- **Step 7** Click the **Charts** tab. In the **Chart Type** area on the right of the page, click Ш.

Figure 10-100 Bar chart statistics



Step 8 Set bar chart parameters.

Table 10-76 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

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.

• Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.10.5 Pie Charts

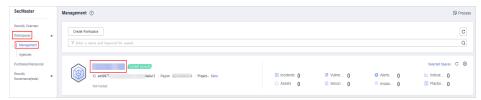
The query and analysis results can be displayed in a pie chart.

The pie chart is used to show the proportion of different categories. Different categories are compared by radian.

Procedure

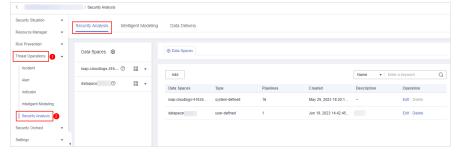
- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-101 Workspace management page



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

Figure 10-102 Accessing the Security Analysis tab page



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

Figure 10-103 Pipeline data page

Analyze & Query Intelligent Modeling	
Data Spaces 🐵	© Data Spaces × R sec-waf-attack ×
isap-cloudlogs-cc2 ⑦	sec-waf-attack Index Settings Sev As Qualk Query Add Alam Quick Query • Enter a search orderia Q Last 15 minutes • Covery/Analyze
	Count 2 1.5 0 0 0 0 0 0 0 0 0 0 0 0 0

- **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 ${f \Theta}$.



Figure 10-104 Pie chart statistics

Step 8 Set pie chart parameters.

Table	10-77	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

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click Add as Indicator Card in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click Save.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.11 Managing Data Spaces

10.5.11.1 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.

Limitations and Constraints

• A maximum of five data spaces can be created in a workspace in a region for a single account.

Procedure

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

Figure 10-105 Workspace management page

SecMaster	Management ①			Process
Security Overview Workspaces	Credit Wintspace 7 Enter a name and layered for stands.			C
Purchased Resources Security Governance(beta)	add977 Sela12 Report Propo- Mare Adds1 Report Adds1 Report	 ♥ Vulner 0 ⊜ Securi 0 	 O Alerts O Mistan O 	Selected Spaces C ⊗ ✓ Indicat 0 Playbo 0

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

<	/ Security Analysis						
Security Situation • Resource Manager •	Security Analysis Intelligent Modeling	Data Delivery					
Risk Prevention Threat Operations	Data Spaces 🛞	Data Spaces					
Incident	isap-cloudlogs-516 🧿 🚦 🔻	Add				Name - Enter	a keyword. C
Indicator	datapace ③ 🔠 🔻	Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis		datapa ce/	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
Security Orchest •							
Settings •							

Figure 10-106 Accessing the Security Analysis tab page

Step 5 In the upper left corner of the data space list, click **Add**. The **Adding Data Spaces** page is displayed on the right.

Figure 10-107 Creating a data space

Analyze & Coerry Inteligent Modeling									
Data Spaces 🔞		Data Spaces							
. 0	00 v	Add					Name + Enter a keyword. Q		
0	00 v	Data Spaces	Туре	Pipelines	Created	Description	Operation		
isap-c) 4 ()	DD v		user-defined	20	Nov 30, 2022 16:23:50 GMT+08:00	-	Edit Delete		
10	00	t 2	user-defined	4	Dec 08, 2022 14:08:09 GMT+08:00		Edit Delete		
		isap-cloud -44	system-defined	t	Jan 16, 2023 15:25:07 GMT+08:00	-	Edt Delete		

Step 6 On the **Adding Data Spaces** page, set the parameters for the new data space. For details about the parameters, see **Table 10-78**.

Parameter	Description
Data Space	Data space name. It must meet the following requirements:
	• 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 on Huawei Cloud and cannot be the same as any other data space name.
Description	You can make remarks on the data space. This parameter is optional.

Step 7 Click OK. The data space is added.

After the data space is added, you can view the new data space in the data space list.

----End

10.5.11.2 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-108 Workspace management page

SecMaster	Management () (Process
Security Overview Workspaces	Cesh Hintpace C T form a name and layered for search. Q
Purchased Resources Security Governance(beta)	construction construction<

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

Figure 10-109	Accessing the	e Security	Analysis tab	page

<	/ Security Analysis						
Security Situation							
Resource Manager 🔹							
Risk Prevention •	Data Spaces 💿	Data Spaces					
Incident	isap-cloudlogs-516 ⑦ 🔡 🔻						
Alert	datapace 💿 🖁 🕶	Add				Name v Enter a	keyword. Q
Indicator	0000000 0 86 1	Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis		datapace	user-defined	t	Jun 19, 2023 14:42:45		Edit Delete
Security Orchest 🔹							
Settings •	4						

Step 5 On the **Data Spaces** page, view all data space information. **Table 10-79** describes related parameters.

Table 10-79 Data spa	ace parameters
----------------------	----------------

Parameter	Description	
Data Spaces	Data space name	
Туре	 Type of data in the data space. It may be: System-defined: data space created by the system by default during data access. User-defined: data space created by users. 	

Parameter	Description
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 ⑦ next to a data space name to view the details about the data space.

Figure 10-110 Data space details

oata Spaces 🛛 🕲		Data Spaces					
и	88	Add					Name
? (T)	80	Data Spaces	Type	Pipelines	Created	Descriptio	n Operation
ap-cloudlogs-034 💮	88	н	user-defined	1	Nov 30, 2022 16:23:50 GMT	-	Edit Delete
		2	user-defined		Dec 08, 2022 14:08:09 GMT		Edit Delete

Step 7 In the Data **Space Details** area, you can view details about a data space. For details about the parameters, see **Table 10-80**.

Table 10)-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

10.5.11.3 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 left corner of the page and choose Security & Compliance > SecMaster.

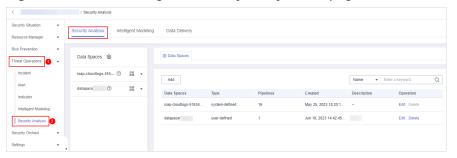
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-111 Workspace management page

SecMaster	Management 💮			Process
Security Overview Workspaces	Cente Writigues $\Psi \mbox{ for a none and layouth for search}. \label{eq:prod}$			C
Purchased Resources Security Governance(beta)		 ♥ Vuiner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

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

Figure 10-112 Accessing the Security Analysis tab page



- **Step 5** Locate the row that contains the data space to be edited, and click **Edit** in the **Operation** column.
- **Step 6** In the displayed **Edit Data Space** dialog box, modify the data space information.
- Step 7 Click OK.

----End

10.5.11.4 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 left corner of the page and choose Security & Compliance > SecMaster.

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

Figure 10-113 Workspace management page

SecMaster	Management ③				🕞 Process
Security Overview Workspeces	Chell Workpace If form a more and keyword for search.				C
Agencies Purchased Resources Security Governance(beta)	O add0177 federal Region Project- More Not honded	i Incidents 0 Assets 0	 ◊ Wulner 0 ⊜ Securl 0 	O Alerts 0 instan 0	Selected Spaces C ⑧ iv Indicat 0 is Playbo 0

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

Figure 10-114 Accessing the Security Analysis tab page

<	/ Security Analysis										
Security Situation	٠	Security Analysis Intelli	igent Modeli	ina	Data Delivery						
Resource Manager	*		gent moden		Data Dontory						
Risk Prevention	•										
Threat Operations	•	Data Spaces 💿			Data Spaces						
Incident		isap-cloudlogs-516 (2)	88 v								
Alert		datapace (2)	88 ¥		Add				Name v Enter a	a keyword. Q	
Indicator		uatapace ()	00 ¥		Data Spaces	Туре	Pipelines	Created	Description	Operation	
Intelligent Modeling					isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete	
Security Analysis					datapace	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete	
Security Orchest	÷										
Settings	÷ ,										

- Step 5 In the row containing the desired database, click **Delete** in the **Operation** column.
- **Step 6** In the dialog box that is displayed, click **OK**. The data space is 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.

----End

10.5.12 Managing Pipelines

10.5.12.1 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.

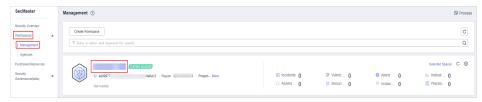
Limitations and Constraints

• A maximum of 20 pipelines can be created in a data space in a region for a single account.

Procedure

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

Figure 10-115 Workspace management page



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

Figure 10-116 Accessing the Security Analysis tab page

<	/ Security Analysis						
Security Situation • Resource Manager •	Security Analysis Intelligent Modeling	Data Delivery					
Risk Prevention Threat Operations	Data Spaces 🛞	Data Spaces					
Incident Alert	isap-cloudlogs-516 ⑦ 🔐 🕶	Add				Name • Enter	a keyword. Q
Indicator		Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1		Edit Delete
Security Analysis		datapace	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
Security Orchest •							
Settings •	4						

Step 5 In the data space navigation pane on the left, click **B** on the right of the data space name and select **Create Pipeline** from the drop-down list box. The **Create Pipeline** page is displayed on the right.

Figure 10-117 Creating a pipeline

Security Analysis Data Delivery						
Data Space 🛞	Data Spaces					
isap-cloudlogs-960 ⑦ BB ♥	Add				Name 👻 Ent	er a keyword. Q.
Pipeline 🗳	Data Space	Туре	Pipelines	Created	Description	Operation
	isap-cloudlogs-9601d6e	system-defined	7	Feb 26, 2024 14:26:43	-	Edit Delete

Step 6 On the **Create Pipeline** page, configure pipeline parameters. For details about the parameters, see **Table 10-81**.

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:
	• The name contains 5 to 63 characters.
	 The value can contain letters, numbers, and hyphens (-). The hyphen (-) cannot be used at the beginning or end, or used consecutively. The name must be unique in the data space.
Shards	The number of shards of the pipeline. The value range is 1 to 64.
Lifecycle	Life cycle of data in the pipeline. Value range: 7-180
Description	Remarks on the pipeline. This parameter is optional.

Step 7 Click OK.

After the pipeline is created, you can click the data space name or \checkmark next to the data space to view the created pipeline.

----End

10.5.12.2 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-118 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	$\begin{tabular}{ c c c c } \hline \begin{tabular}{c c c c } \hline \hline & \end{tabular} tabu$				C
Purchased Resources Security Governance(beta)	D 405077 24412 Report Pope- More Not tooled	Incidents O Assets O	♥ Vulner 0 i Securi 0	O Alerts 0 ◎ Instan 0	Selected Spaces C 🛞

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

Figure 10-119 Accessing the Security Analysis tab page

<	/ Security Analysis						
Security Situation •	Security Analysis Intelligent Modeling	Data Delivery					
Resource Manager 🔹							
Risk Prevention 💌		Data Spaces					
Threat Operations 1	Data Spaces 🛞	Data Spaces					
Incident	isap-cloudlogs-516 ⑦						
Alert	datapace ()	Add				Name 👻 Enter	a keyword. Q
Indicator	uatapate 🕜 👩 🔻	Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis 2		datapace [,]	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
Security Orchest •							
Settings •	4						

Step 5 In the data space navigation tree on the left, click the data space name or ^{*} to view the created pipeline.

Figure 10-120 Viewing pipeline details

Analyze & Query Intelligent Modeling							
Data Spaces 🔞	Data Spaces						
dataspace 🕜 📴 🔽	Add				Name v E	Enter a keyword. Q	λ
	Data Spaces	Туре	Pipelines	Created	Description	Operation	
	dataspace	user-defined	1	Nov 28, 2022 16:35:42 G	x	Edit Delete	

Step 6 Click ⑦ next to a pipeline name you want to view. The pipe details are displayed in the right pane.

Table 10-82	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.

Parameter Description	
Pipeline ID	ID of the current pipeline.
Shards	Number of shards of the pipeline.
Lifecycle	Retention period of data in the pipeline.
Created	Time when a pipe is created
Description	Description of the pipeline

----End

10.5.12.3 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-121 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspeces	$$\ensuremath{\mathbb{T}}$$ Crede Workspace $$\ensuremath{\mathbb{T}}$$ Inter a name and layered for search.				C
Purchased Resources Security Governance(beta)	Ormer source O	Incidents 0	♥ Vulner () ⊜ Securl ()	 Alerts Instan 0 	Selected Spaces C ⑧ ↓ Indicat 0 19 Playbo 0

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

	/ Security Analysis						
ecurity Situation • esource Manager •	Security Analysis Intelligent Modelin	g Data Delivery					
rreat Operations	Data Spaces 🛞	Data Spaces					
Incident	isap-cloudlogs-516 ⑦ 🔐 👻	Add				Name + Enter	r a keyword. 🛛 🤇
Indicator	datapace 🕜 🔠 🔻	Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis 2		datapacer	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
ecurity Orchest 🔹							
ettings -							

Figure 10-122 Accessing the Security Analysis tab page

Step 5 In the data space navigation tree on the left, click the data space name or ^{*} to view the created pipeline.

Figure 10-123 Viewing pipeline details

Analyze & Query Intelligent Modeling	9						
Data Spaces 🔞	Data Spaces						
dataspace 🕥 🚦 🔻	Add				Name	 Enter a keyword. 	Q
	Data Spaces	Туре	Pipelines	Created	Description	Operation	
	dataspace	user-defined	1	Nov 28, 2022 16:35:42 G	х	Edit Delete	

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

nalyze & Query	Intelligent Modeling	,	for ear	ung u p	.petile			
Data Spaces 💿		Data Spaces						
dataspace ⑦	₩ ▲ ❷	Add				Name	▼ Enter a keyword.	
pipe1 (?)	More 3	Data Spaces	Туре	Pipelines	Created	Description	Operation	
	Edt 4 Consume Monitoring	dataspace	user-defined	1	Nov 28, 2022 16:35:42 G	х	Edit Delete	
	Delete							

Figure 10-124 Entry for editing a pipeline

Step 7 On the **Edit Pipeline** page, set pipeline parameters. For details about the parameters, see **Table 10-83**.

Table 10-83 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

10.5.12.4 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-125 Workspace management page

SecMaster	Management ③				🕞 Process
Security Overview Workspaces	$\label{eq:rescaled} \fboxtime the second secon$				C
Purchased Resources Security Governance(beta)	Contract C	 Incidents 0 Assets 0 	Vulner 0 ⊜ Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⊛ indicat 0 Playbo 0

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

Figure 10-126	Accessing	the Security	/ Analysis	tab page
---------------	-----------	--------------	------------	----------

<	/ Security Analysis						
Security Situation • Resource Manager •	Security Analysis Intelligent Modeling	Data Delivery					
Risk Prevention Threat Operations	Data Spaces 🛞	Data Spaces					
Incident	isap-cloudlogs-516 ⑦ 🐰 👻	Add				Name V Enter	a keyword. Q
Indicator	datapace (?)	Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis 2		datapa cer	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
Security Orchest 🔹							
Settings •							

Step 5 In the data space navigation tree on the left, click the data space name or [•] to view the created pipeline.

Figure 10-127 Viewing pipeline details

Analyze & Query Intelligent Modeling							
Data Spaces 🔞	Data Spaces						
dataspace 🕜 🛛 🖁 💌	Add				Name	 Enter a keyword. 	Q
	Data Spaces	Туре	Pipelines	Created	Description	Operation	
	dataspace	user-defined	1	Nov 28, 2022 16:35:42 G	x	Edt Delete	

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

Figure 10-128 Deleting a pipeline

Analyze & Query	Intelligent Modeling							
Data Spaces 🔞		Data Spaces						
dataspace ⑦	BB 🔺 🥝 More 🕄	Add				Name	 Enter a keyword. 	Q
	Edt	Data Spaces	Туре	Pipelines	Created	Description	Operation	
	Consume	dataspace	user-defined	1	Nov 28, 2022 16:35:42 G	x	Edit Delete	
	Monitoring							
1	Delete							

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

----End

10.6 Data Consumption

Data consumption refers to the process during which third-party software or cloud products consume the log data in real time through a client. It is a sequential read/write from/into full data.

SecMaster provides the data consumption function and supports real-time data consumption through the client.

Enabling Data Consumption

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-129 Workspace management page

SecMaster	Management ()	🕞 Process
Security Overview Workspeces Management Agencies	Create Writespace IF latter a same and layout for search.	Q
Purchased Resources Security Governance(beta)	A defition A defit A defit	• •

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

	/ Security Analysis							
Security Situation Resource Manager	Security Analysis Intell	igent Modeling	Data Delivery					
Risk Prevention +	Data Spaces 💿		Data Spaces					
Incident	isap-cloudlogs-516 (2)	88 •	Add				Name v Enter	r a keyword. C
Indicator	datapace 🕜		Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling			isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis			datapacer	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
ecurity Orchest 👻								
Settings 👻								

Figure 10-130 Accessing the Security Analysis tab page

Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Consume**.

Figure 10-131 Accessing the data consumption page

Security Analysis Data Delivery							
Data Spaces 🐵	Data Spaces						
isap-cloudlogs-c7c ③ 器 🔺 sec-cfw-block ④ More 2	Add				Name	Enter a keyword.	Q
sec-chu-flow @ Edit	Data Spaces	Туре	Pipelines	Created	Description	Operation	
sec-cfw-risk () Consume	isap-cloudlogs-c7c98da5-d	system-defined	17	Feb 16, 2023 20:03:01 GM	-	Edit Delete	
sec-cts-audit C Deliver		user-defined	4	Mar 30, 2023 14:50:09 GM	-	Edit Delete	
sec-doss-alarm Delete		user-defined	1	Sep 06, 2023 10:29:24 GM		Edit Delete	
sec-ddos-attack More							

Step 6 On the Data Consumption page, click **Interview of Consumption** next to Current Status to enable data consumption.

After the function is enabled, the consumption configuration information is displayed, as shown in **Table 10-84**.

Table 10-84 Data consumption parameter	ſable 10-84 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, which determines how data is transmitted to consumers.
Access Node	Access node of the current data.

----End

Related Operations

After data consumption is enabled, you can click \frown next to **Status** on the Data Consumption page to disable data consumption.

10.7 Data Delivery

10.7.1 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

- To deliver data to OBS, ensure there is an available bucket whose bucket policy is **Public Read and Write**. For details, see **Creating an OBS Bucket**.
- To deliver data to LTS, ensure there is an available log group and log streams. For details, see Managing Log Groups and Managing Log Streams.

Limitations and Constraints

When performing cross-account delivery, the data can only be delivered to the pipelines instead of cloud services of other accounts.

Creating a Data Delivery

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

Figure 10-132	Workspace	management	page
---------------	-----------	------------	------

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	Create Hittingson $\label{eq:constraint} \overline{\mathcal{V}} \mbox{ forther a name and keyword for search}.$				C
i Agencies Purchased Resources Security Governance(beta)	Convertience C	 ⊡ Incidents 0 ○ Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 Instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

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

	/ Security Analysis							
ecurity Situation • esource Manager •	Security Analysis Intelligent Mo	deling	Data Delivery					
isk Prevention 🔹	Data Spaces 🔞		Data Spaces					
Incident	isap-cloudlogs-516 ()		Add				Name • Enter	r a keyword.
Indicator	datapace ⑦ 🖁		Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling			isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis			datapacer	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
ecurity Orchest 🔹								
ettings 👻								

Figure 10-133 Accessing the Security Analysis tab page

Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Deliver**.

Figure 10-134 Accessing data delivery settings page

Security Analysis Data Delivery							
Data Spaces 🛞	② Data Spaces						
isap-cloudlogs-c7c ()	Add				Name	 Enter a keyword. 	Q
sec-cfw-flow @ Edit	Data Spaces	Туре	Pipelines	Created	Description	Operation	
sec-cfw-risk (2)	isap-cloudlogs-c7c98da5-d	system-defined	17	Feb 16, 2023 20:03:01 GM	-	Edit Delete	
Monitoring sec-cts-audit (Deliver		user-defined	4	Mar 30, 2023 14:50:09 GM	-	Edit Delete	
sec-dbss-alarm Delete		user-defined	4	Sep 06, 2023 10:29:24 GM		Edit Delete	
sec-ddos-attack () More							

Step 6 (Optional) Authorization of the destination type is required for the first delivery. If the authorization has been performed, skip this step.

Confirm the authorization information, select Agree to authorize and click OK.

- **Step 7** On the **Create Delivery** page, set data delivery parameters.
 - 1. Configure basic information.

Table 10-85 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 10-86 Data so	purce 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	

Parameter	Description
Data Spaces	Data space to which the current pipeline belongs
Pipeline	Pipeline name
Data Read Policy	Data read policy of the current pipeline
Read By	Identity of the data source reader

- 3. Configure the delivery destination.
 - **PIPE**: Deliver the current pipeline data to other pipelines of the current account or pipelines of other accounts. Set this parameter as required.
 - Current: Deliver the current pipeline data to another pipeline of the current account. For details about the parameters, see Table 10-87.

Parameter	Description
Account Type	Account type of the data delivery destination. Select Current .
Delivery Type	Delivery type. Select PIPE .
Workspace	Workspace where the destination PIPE is located
Data Spaces	Data space where the destination PIPE is located
Pipeline	Pipeline where the destination PIPE is located
Written To	The value is generated by default and does not need to be configured.

Table 10-87 Destination parameters - Current account pipeline

 Cross-account delivery: Deliver the current pipeline data to the pipeline of another account. For details about the parameters, see Table 10-88.

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

Parameter	Description
Workspace ID	ID of the workspace where the destination PIPE is located. For details about how to query the workspace ID, see Step 6 .
Data Space ID	ID of the data space where the destination PIPE is located. For details about how to query the data space ID, see Step 6 .
Pipeline ID	ID of the pipeline where the destination PIPE is located. For details about how to query the pipeline ID, see Step 6 .
Written To	The value is generated by default and does not need to be configured.

LTS: Deliver the pipeline data to LTS. For details about the parameter settings, see Table 10-89.

To deliver data to LTS, ensure there is an available log group and log streams. For details, see **Managing Log Groups** and **Managing Log Streams**.

Parameter	Description
Account Type	Account type of the data delivery destination. When delivering data to LTS, only the Current account type can be selected.
Delivery Type	Delivery type. Select LTS .
Log Group	Destination LTS log group
Log Stream	Destination LTS log stream
Written To	The value is generated by default and does not need to be configured.

Table 10-89 Destination parameters - LTS

OBS: Deliver the pipeline data to OBS. For details about the parameter settings, see Table 10-90.

To deliver data to OBS, ensure there is an available bucket whose bucket policy is **Public Read and Write**. For details, see **Creating an OBS Bucket**.

Table 10-90	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.

Parameter	Description	
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**.

10.7.2 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 execute 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-135 Workspace management page

SecMaster	Management 💮				🕞 Process
Security Overview Workspaces	Credit Watspace $\label{eq:credit} \overline{\nabla} \mbox{ Inter a name and largenced for search}.$				C
Purchased Resources Security Governance(beta)	constant constant	Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	O Alerts O ⊗ InstanO	Selected Spaces C 🛞 Mindicat 0 Playbo 0

- Step 4 In the navigation pane on the left, choose Threat Operations > Security Analysis. On the Security Analysis page that is displayed, click the Data Delivery tab. The Data Delivery page is displayed.
- **Step 5** On the **Data Delivery** page, click the **Cross-tenant Permissions** tab. On the page that is displayed, click **Accept** in the **Operation** column of the target delivery task.

To accept authorization in batches, select all tasks to be authorized and click **Accept** in the upper left corner of the list.

Figure 10-136 Data delivery authorization

< / Da	ta Delivery								
Security Situation	•	Analyze & Query I	ntelligent Modeling Data D	elivery					
Resource Manager	· •		L	0					
Risk Prevention	-	-							
Threat Operations	0 •	Delivery Tasks	Cross-Tenant Permissions						
Incident		Accept Reje							
Alert			Destination All	* Del	ivery Status All	Authorization Status	Al	Enter a data so	urce keyword Q
Incidator		Name/ID	Data Source	Destination	Delivery Status	Authorization Status	Requested	Handled	Operation
Intelligent Mod	eing	A(>5 ^c	b PIPE	1 Delivering	Authorized	Mar 13, 2023 15:14:08		Accept Reject Cancel
Security Analys	0		212-e C	b		Unauthorized	Feb 13, 2023 20:02:17	-	Accept Reject
Settings									

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.

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.

Table 10-91 Cross-tenant permission authorizati	on options
---	------------

Operation	Description
Cancel	 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.

10.7.3 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-137 Workspace management page

SecMaster	Management (3)				🕞 Process
Security Overview Workspeces Management Agencies	Create Wontspace				C
Purchased Resources Security Governance(beta)	Generation Generation	 ⊡ Incidents 0 ○ Assets 0 	♥ Vulner 0 ⊜ Securl 0	 Alerts Instan 0 	Selected Spaces C ⑧ i Indicat 0 ∋ Playbo 0

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

Figure 10-138 Accessing the Security Analysis tab page

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

Figure 10-139 Pipeline data page

Analyze & Query Intelligent Modeling	
Data Spaces 🐵	⊗ Data Spaces × 🕞 sec-waf-attack ×
isap-cloudlogs-cc2 ⑦ 88 ▲ sec-waf-attack ⑦ 29 More	sec-waf-attack Index Bettings Save As Quick Query Add Alam
sec-waf-attack (2) More	Quick Query Enter a search criteria Q Last 15 minutes Query/Analyze
· · · · · · · · · · · · · · · · · · ·	
	Count Der 07, 2022 17:45:07 - Dre 97, 2022 18:00:07 C 1

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 \checkmark before to the log group name.

- **Step 4** Click the name of the log stream selected during data delivery. The log stream details page is displayed.
- **Step 5** On the log stream details page, view the delivered log information.

----End

10.7.4 Managing Data Delivery

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

Figure 10-140 Workspace management page

SecMaster	Management 🕥 🖗 Proces
Security Overview Workspeces Management Agencies	Could Windpace C If first a same and layout for such. Q
Purchased Resources Security Governance(beta)	Image: Construct sector C Sector Sector

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

Figure 10-141	Accessing	the data	delivery	page
---------------	-----------	----------	----------	------

< / / Data Delivery							
Security Situation •	Analyze & Query Intelligent Modeling Data Delivery						
Resource Manager 🔹 👻							
Risk Prevention -							
Threat Operations 1	Delivery Tasks Cross-Tenant Permissions						
Incident	Delete Search by name.	Q @ C					
Alert	NameID Data Source Consumption Policy Destination Type Destination Monitoring	Status Created Operation					
Incidator	□ 197. 56c 3ee Latest LTS c 😅	A Delivering Mar 13, 2023 15:16: Suspend Delete					
Intelligent Modeling	- 400 - Lanst PIPE	I Delivering Mar 13, 2023 15:14: Suspend Delete					
Security Analysis	- 40;						
Security Orchest •							
Settings -							

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

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.

Table 10-92 Delivery task parameters

----End

Suspending a Delivery Task

After a data delivery task is added and authorized, the delivery task status changes to **Delivering**. To stop the delivery, you can suspend the target delivery task.

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

Figure 10-142 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Create Workspace				C
Agencies Purchased Resources Security Governance(beta) ▼	General security Gene	 ⊡ Incidents 0 ○ Assets 0 	♥ Vulner 0 Securl 0	O Alerts 0 instan0	Selected Spaces C ⑧ ↓ Indicat 0 Playbo 0

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

Figure 10-143 Accessing the data delivery page

< / / Data Delivery									
Security Situation +	Analyze & Query	Intelligent Modeling	Data Delivery						
Resource Manager 🔹 👻		mangen modeling	(3						
Risk Prevention •		8							
Threat Operations 🚺 🔺	Delivery Tasks	Cross-Tenant Permission	ŝ						
Incident	Delete		Search by name.						Q 🚳 C
Alert	Name/ID	Data Source	Consumption Policy	Destination Type	Destination	Monitoring	Status	Created	Operation
Incidator	167 56c	30 (Latest	LTS	c		Delivering	Mar 13, 2023 15:16:	Suspend Delete
Intelligent Modeling Security Analysis	405	a01 ¢	Latest	PIPE	¢	8	Delivering	Mar 13, 2023 15:14:	Suspend Delete
Security Orchest •									
Settings 👻									

Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Suspend** in the **Operation** column.

After a delivery task is suspended, the delivery task status changes to **Suspended**, indicating that the delivery task is suspended successfully.

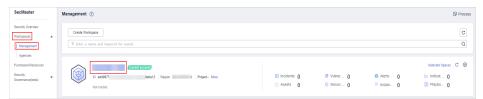
----End

Starting a Delivery Task

You can restart a suspended delivery task.

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

Figure 10-144 Workspace management page



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

Figure 10	-145 Accessi	ng the	data	delivery	page
-----------	--------------	--------	------	----------	------

< / / Data Delive	iry									
Security Situation	•	Analyze & Query	Intelligent Modeling	Data Delivery						
Resource Manager	•			8						
Risk Prevention	-		0							
Threat Operations		Delivery Tasks	Cross-Tenant Permission	15						
Incident		Delete		Search by name.						Q 🛞 C
Alert		Name/ID	Data Source	Consumption Policy	Destination Type	Destination	Monitoring	Status	Created	Operation
Incidator		1187 56c	зе С	Latest	LTS	c		Delivering	Mar 13, 2023 15:16:	Suspend Delete
Intelligent Modeling Security Analysis		400	e01 C	Løtest	PIPE	¢	•	1 Delivering	Mar 13, 2023 15:14:	Suspend Delete
Security Orchest	-									
Settings										

Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Start** in the **Operation** column.

After a delivery task is restarted, the delivery task status changes to **Delivering**, indicating that the delivery task is successfully started.

----End

Deleting a Delivery Task

If a data delivery task is no longer needed, you can delete it.

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

Figure 10-146 Workspace management page

SecMaster	Management 💿			Process
Security Overview Workspaces	Orest Virtuges ♀ Entr a same and hopped for seach.			C Q
Purchased Resources Security Governance(beta)		ð Vulner 0	 O Alerts O Instan O 	Selected Spaces C 🛞 indicat 0 Playbo 0

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

Figure 10-147 Accessing the data delivery page

/ Data Delivery										
Security Situation •	Analyze & Que	v Intelliner	nt Modeling	Data Delivery						
Resource Manager 🔹 💌	Foranyze & Goe	y menger	in modeling	3						
Risk Prevention 👻										
Threat Operations 🕕 🔺	Delivery Ta	sks Cross-Te	enant Permissions	5						
Incident	Delete			Search by name.						Q 🛞 C
Alert	Nam	a/ID	Data Source	Consumption Po	licy Destination Type	Destination	Monitoring	Status	Created	Operation
Incidator	56c	34	e (Latest	LTS	¢		Delivering	Mar 13, 2023 15:16:	Suspend Delete
Intelligent Modeling Security Analysis	409		c c	Latest	PIPE	(Delivering	Mar 13, 2023 15:14:	Suspend Delete
Security Orchest 👻										
ettings -										

Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Delete** in the **Operation** column and click **OK** in the displayed dialog box.

----End

10.7.5 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 decisionmaking 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. For details, see Managing Log Groups and Managing Log Streams.

Procedure

Creating a Data Delivery

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

Figure 10-148 Workspace management page

SecMaster	Management ③				D Process
Security Overview Workspaces	Could Hompson $\overline{V} \mbox{ Inter a name and legended for search}.$				Q
Purchased Resources Security Governance(beta)	Consideration and Consideration Project- Mana Not handled	Incidents 0 Assets 0	♥ Vuiner 0 ⊜ Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ └ Indicat 0 S Playbo 0

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

Figure 10-149 Accessing the Security Analysis tab page

<	/ Security Analysis						
Security Situation 🔹	Security Analysis Intelligent Modeling	Data Delivery					
Resource Manager 🔹	intelligent wordeling	Data Delivery					
Risk Prevention 🔻		Data Spaces					
Threat Operations 1	Data Spaces 💿	© Data Spates					
Incident	isap-cloudlogs-516 🕐 🚦 👻	Add				Name - Enter	a kauward
Alert	datapace 🕜 🔠 🕶	7100				Hand - Chief	
Indicator		Data Spaces	Туре	Pipelines	Created	Description	Operation
Intelligent Modeling		isap-cloudlogs-51634	system-defined	16	May 25, 2023 18:20:1	-	Edit Delete
Security Analysis		datapace	user-defined	1	Jun 19, 2023 14:42:45		Edit Delete
Security Orchest 👻							
Settings •	4						

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**.

Security Analysis Data Delivery								
Data Spaces 🛞	Data Spaces							
isap-cloudlogs-c7c (2) 38 🔺 sec-cfw-block (2) More 👩	Add					Name -	Enter a keyword.	Q
sec-cfw-flow @ Edit	Data Spaces	Туре	Pipelines	Created	Descrip	otion	Operation	
sec-cfw-risk (2) Consume	isap-cloudlogs-c7c98da5-d	system-defined	17	Feb 16, 2023 20:03:01 GM	-		Edit Delete	
sec-cts-audit (2 Deliver 6		user-defined	4	Mar 30, 2023 14:50:09 GM	-		Edit Delete	
sec-dbss-alarm Delete		user-defined	1	Sep 05, 2023 10:29:24 GM			Edit Delete	
sec-ddos-attack () More								

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. If no log group is available, create one. For details, see **Creating an LTS Log Group**.
 - Log Stream: Select a destination LTS log stream. If no log stream is available, create one. For details, see Creating an LTS Log Stream.

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

Step 8 Under Access Authorization, view the permissions granted in Step 6.

A delivery requires the read and write permissions to access your cloud resources. A delivery task cannot access your cloud resources unless the access is authorized by you.

Step 9 Click OK.

Data Delivery Authorization

Step 10 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.

Figure 10-151 Data delivery authorization

< / / Data Delivery		
Security Situation +	Analyze & Query Intelligent Modeling Data Delivery	
Resource Manager +		
Risk Prevention 👻		
Threat Operations	Delvery Tasks Cross-Tenant Permissions	
Incident	Accept Reject Cancel	
Alert	Destination Al • Defivery Status Al • Autorization Status Al • Enter a data source keyword Q 6	ĝ C
Incidator	Name1D Data Source Destination Delivery Status Authorization Status Requested Handled Operation	
Intelligent Modeling	8	ancel
Security Analysis	Unautholized Feb 13, 2023 20 52:17	
Settings •		

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 11** Click in the upper left corner of the page and choose **Management &** Governance > Log Tank Service.
- **Step 12** In the log group list on the **Log Management** page, locate the log group for which you want to add data delivery and click \checkmark before the log group name.

- **Step 13** Click the name of the log stream selected during data delivery. The log stream details page is displayed.
- **Step 14** On the log stream details page, view the delivered log information.

----End

10.8 Data Monitoring

SecMaster can monitor metrics such as the production rate, production volume, and total consumption rate of the upstream and downstream SecMaster pipelines. You can check the service status based on the monitoring results.

Basic Concepts

- A producer is a logical object used to construct data and transmit it to the server. It stores data in message queues.
- A subscriber is used to subscribe to SecMaster pipeline messages. A pipeline can be subscribed to by multiple subscribers. SecMaster distributes messages through subscribers.
- A consumer is a running entity that receives and processes data. It consumes and processes messages in the SecMaster pipeline through subscribers.
- A message queue is the container for data storage and transmission.

Viewing Metrics

Step 1 Log in to the management console.

- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-152 Workspace management page

SecMaster	Management () (2 Proc	288
Security Overview Workspaces	Contributionspina C T Enter a new and topood for seech. Q	
Agencies Purchased Resources Security Governance(beta)	Count count Sector 2 Report Paget- Mars © Vulter © Alerts © Vulter © Alerts © Vulter © Alerts © Vulter © Alerts © Inscient 6 Image: 1 Paget Image: 1 Paget	1

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

Intellic Data Deliver Data Spaces 🐵 Data Spaces ogs-516... ⑦ 🔠 🗸 Add ce ⑦ 88 -Data Spaces Created Descr Operation May 25, 2023 18:20:1... Edit | Delete san.cloudlons.61634 Jun 19, 2023 14:42:45...

Figure 10-153 Accessing the Security Analysis tab page

Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Monitoring**.

Figure 10-154 Accessing the data monitoring page

ata Spaces 🐵	Data Spaces						
ap-cloudlogs-c7c ⑦ 88 🔺 sec-cfw-block ⑦ More 🖉	Add				Name	 Enter a keyword. 	C
sec-chu-flow @ Edit	Data Spaces	Туре	Pipelines	Created	Description	Operation	
sec-cfw-risk (2)	isap-cloudlogs-c7c98da5-d	system-defined	17	Feb 16, 2023 20:03:01 GM		Edt Delete	
sec-cts-audit (Deliver		user-defined	4	Mar 30, 2023 14:50:09 GM	-	Edt Delete	
sec-dbss-alarm Delete		user-defined	1	Sep 06, 2023 10:29:24 GM	_	Edit Delete	

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

Overview	Producer	Pipeline	Subscriber			
	•	0.00Alarms/second		0.00Alarms/second 0.00B/s	0.00Alarms/second 0.00Alarms/second 0.00B/s	0.00Alarms/second
	icers available oducer)			alert-rule-test (Pipeline Name)	Subscriber1 2c971c	5760fca8e44aee4dfc5693cbd2c6cc94540fb0757 (Consumer)

Figure 10-155 Viewing monitored data

- **Overview**: Displays information such as the production rate between producers, pipelines, subscribers, and consumers in the current pipeline.
- Producer: Displays metrics of the producer, such as current production TPS, current production rate, current production volume, and current message storage size.
- **Pipeline**: Displays the pipeline message size (MB), producer-to-pipeline message size (MB), producer-to-pipeline messages, message size consumed by pipelines (MB), messages consumed by pipelines, unacknowledged message size (MB), pipeline production rate, pipeline consumption rate, average message size (KB), and offloaded message size (B) in a specified period (last 2/6/12/24 hours, last 7 days, or a customized period).

• Subscriber: displays the total consumption rate of subscribers, consumed data volume (B), consumed messages, and active consumers in a specified period (last 2/6/12/24 hours, last 7 days, or a user-defined period).

----End

11 Security Orchestration

11.1 Security Orchestration Overview

Security orchestration combines security functions of different systems or components in a system involved in security operations of enterprises and organizations based on certain logical relationships to complete a specific security operations process and procedure. It aims to help security teams of enterprises and organizations quickly and efficiently respond to network threats and implement efficient and automatic response and handling of security incidents.

It provides the following functions:

- Playbook management: you can use the built-in automatic response playbooks or customize playbooks.
- Workflow: Allows you to draw a playbook triggering flowchart.
- Instance management: allows you to monitor and manage running instances and view records.
- Security Orchestration, Automation and Response (SOAR): You can orchestrate workflows to let SecMaster automatically handle security incidents and suspicious incidents.

Limitations and Constraints

- In a single workspace of an account, the scheduling frequency of a single playbook is greater than or equal to 5 minutes.
- The maximum number of retries within a day for a single workspace of a single account is as follows:
 - Manual retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
 - API retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
- Restrictions on classification and mapping are as follows:
 - In a single workspace of a single account, a maximum of 50 classification & mapping templates can be created.

- In a single workspace of a single account, the proportion of a classification to its mappings is 1:100.
- A maximum of 100 classifications and mappings can be added to a workspace of a single account.

Basic Concepts

• Playbook

A playbook is a formal expression of the security operation workflow in the security orchestration system and is usually executed driven by the workflow engine in the orchestrator.

Orchestrating a playbook is to build the manual security operation workflow and software into a machine playbook.

Workflow

A workflow is a collaborative work mode that integrates various capabilities related to security operation, such as tools, technologies, workflows, and personnel. A workflow is the response flow when a playbook is triggered.

It combines API-enabled security capabilities, or applications, in SecMaster and manual checkpoints based on certain logical relationships to complete a specific security operations process and procedure.

11.2 Built-in Playbooks and Workflows

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

Built-in Playbooks

The following playbooks are enabled by default:

HSS alert status synchronization, automatic notification of high-risk vulnerabilities, historical handling information associated with host defense alarms, SecMaster and WAF address group association policy, historical handling information associated with application defense alarms, historical handling information associated with network defense alarms, automatic closure of repeated alarms, and alarm IP metric marking Asset protection status statistics notification, automatic alarm statistics notification, and automatic high-risk alarm notification

Securit y Layer	Playbook Name	Description	Data Class	
Server security	HSS alert synchronization	Automatically synchronizes HSS alerts generated for servers.	Alert	
	Automatic notification of high-risk vulnerabilities	Sends email or SMS notifications to specified recipients when vulnerabilities rated as high severity are discovered.	Vulner ability	

Table 11-1 Built-in playbooks

Securit y Layer	Playbook Name	Description	Data Class
	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.	Comm onCon text
	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
Applica tion security	SecMaster WAF Address Group Association Policy	Associates an address group specified by SecMaster with WAF blacklist (IP address group blacklist) rules for all enterprise projects to block IP addresses in the address group.	Comm onCon text
	WAF clear Non- domain Policy	Checks WAF protection policies at 09:00 every Monday and deletes policies with no rules included.	Comm onCon text
	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

Securit y Layer	Playbook Name	Description	Data Class
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
ldentity 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
Networ k 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
	Automatic disabling of repeated alerts	Associates the alerts with the same names and close the duplicated ones generated within the past seven 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 first 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.	Comm onCon text

Securit y Layer	Playbook Name	Description	Data Class
	Alert statistics Notify	Collects statistics on alerts that are not cleared at 19:00 every day and sends notifications to customers by email or SMS.	Alert
	Automatic security blocking of 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

Built-in Workflows

Table	11-2	Built-in	workflows
-------	------	----------	-----------

Securit y Layer	Workflow Name	Description	Data Class
Server security	HSS alert synchronization	Automatically synchronizes HSS alerts generated for servers.	Alert
	Automatic notification of high-risk vulnerabilities	Sends email or SMS notifications to specified recipients when vulnerabilities rated as high severity are discovered.	Vulner ability
	Vulnerability handling	Invokes the HSS Interface for fixing vulnerabilities.	Vulner ability
	Policy management – Security group blocking	Adds the target IP address to all security groups.	Policy
	Policy management – Security group blocking cancellation	Removes the target IP address from all security groups.	Policy
	One-click host isolation	Isolates all ports on the target server.	Alert
	One-click host de-isolation	Releases the target servers from the isolation security group.	Alert

Securit y Layer	Workflow Name	Description	Data Class
	Attack link analysis alert notification	Analyzes attack link and generates alerts when attacks found on websites running on the affected servers.	Alert
	Server vulnerability notification	Checks servers with EIPs bound on the resource manager page and notifies of discovered vulnerabilities.	Comm onCon text
	HSS isolation and killing of malware	Automatically isolates and kills malware.	Alert
	Host Defense Alarms Are Associated With Historical Handling Information	Parent workflow. This workflow determines which type of child workflow needs to be invoked based on HSS alerts. The workflow also associates new alerts with historical alerts and adds handling details to the comment area. The following child workflows may be invoked: Host defense alarms are associated with historical handling information - Threat Modeling - Process, Host defense alarms are associated with historical handling information - Threat Modeling - Login, and Host defense alarms are associated with historical handling information - Automatic conversion to alerts.	Alert
	Host defense alarms are associated with historical handling information - Threat Modeling - Process	A child workflow. This workflow associates process alerts constructed in threat modeling with historical handling details and adds them to the comment area for the alerts.	Alert
	Host defense alarms are associated with historical handling information - Threat Modeling - Login	A child workflow. This workflow associates login alerts constructed in threat modeling with historical handling details and adds them to the comment area for the alerts.	Alert

Securit y Layer	Workflow Name	Description	Data Class
	Host Defense Alarms Are Associated With Historical Handling Information - Automatic conversion to alerts.	A child workflow. This workflow associates HSS alerts that are automatically converted to SecMaster alerts with historical handling details and add them to the comment area for such SecMaster alerts.	Alert
	Host isolation - Malware	If suspicious malware (such as ransomware and mining) was detected on a server, a manual review is triggered. The malware details (such as the type, affected server, process command, and file path) are displayed for operation personnel to review. If the malware is confirmed, affected servers will be isolated automatically.	Alert
Applica tion	One-click WAF blocking	Blocks target IP addresses in all policies in WAF in the current account.	Alert
security	One-click WAF unblocking	Unblocks the target IP addresses from a specific policy group in the WAF in the current account.	Alert
	Policy management – WAF blocking	Adds target IP addresses to a WAF blacklist.	Policy
	Policy management – Cancel WAF blocking	Removes target IP addresses from a WAF blacklist.	Policy
	WAF address group policy	Applies WAF whitelist or blacklist rules to WAF address groups specified by SecMaster.	Comm onCon text
	Application Defense Alarms Are Associated With Historical Handling Information	Associates WAF alerts with alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
	WAF clear Non- domain Policy	Checks WAF protection policies at 09:00 every Monday and deletes policies with no rules included.	Comm onCon text

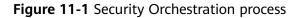
Securit y Layer	Workflow Name	Description	Data Class
Networ k	One-click CFW blocking	Adds target IP addresses to a CFW blacklist.	Alert
security	One-click CFW unblocking	Removes target IP addresses from a CFW blacklist.	Alert
	Policy management – CFW blocking	Adds target IP addresses to a CFW blacklist.	Policy
	Policy management – Cancel CFW blocking	Removes target IP addresses from a CFW blacklist.	Policy
	Network Defense Alarms Are Associated With Historical Handling Information	Associates CFW alerts with alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
Identity authen tication	Identity Defense Alarms Are Associated With Historical Handling Information	Associates IAM alerts with alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
	Policy Management – IAM blocking (IAM interception for policy delivery)	Triggers emergency policies and changes the status of an IAM user to Disabled.	Policy
	Policy management – Cancel IAM blocking (Policy Delivery IAM Decapsulation)	Triggers emergency policies and changes the status of an IAM user to Enabled.	Policy
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, verifies them the IP addresses against Threat Book, sets the confirmed malicious IP addresses as threat indicators, and associates indicators with alerts.	Alert

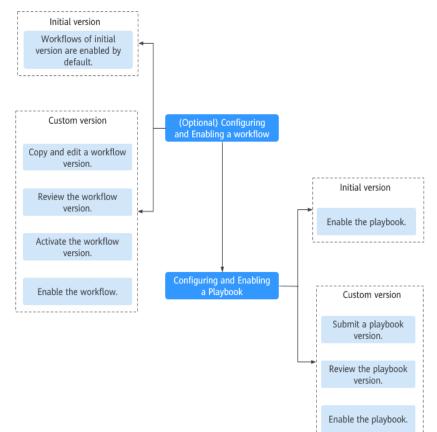
Securit y Layer	Workflow Name	Description	Data Class
	Automatic disabling of repeated alerts	Associates the alerts with the same names and close the duplicated ones generated within the past seven days.	Alert
	Automatic renaming of alert names	Generates custom alert names by combining specified key fields.	Alert
	Adding IP address to alert	Adds attack source IP address and attacked IP address labels for alerts.	Alert
	One-click unblocking	Applies unblocking workflows based on alert data source products.	Alert
	One-click blocking	Applies blocking workflows based on alert data source products.	Alert
	IP intelligence association	Associates alerts with SecMaster intelligence first 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.	Comm onCon text
	Alert statistics Notify	Collects statistics on alerts that are not cleared at 19:00 every day and sends notifications to customers by email or SMS.	Alert
	Automatic security blocking of 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.	Comm onCon text
	Real-time Close Alert Automatically	Clears the current alert.	Comm onCon text
	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

Securit y Layer	Workflow Name	Description	Data Class
	Querying historical alarms	Associates an alert with the child workflow that is used to handle similar alerts before.	Comm onCon text
		Queries comments for historical alerts for a specified period of time and returns de-duplicated comments.	

11.3 Security Orchestration Process

This topic describes how Security Orchestration works.





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 disabling of repeated alerts . Most of playbooks are enabled by default. The following playbooks are enabled by default: HSS alert status synchronization, automatic notification of high-risk vulnerabilities, historical handling information associated with host defense alarms, SecMaster and WAF address group association policy, historical handling information associated with application defense alarms, historical handling information associated with network defense alarms, automatic closure of repeated alarms, and alarm IP metric marking Asset protection status statistics notification, automatic alarm statistics notification, and automatic high-risk alarm notification If you want to use a playbook that is not enabled, you can enable the initial version of the playbook (V1, activated by default), or modify the playbook and then enable it.

Table 11-3 Process

11.4 (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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-2 Workspace management page

SecMaster	Management ()	Process
Security Overview Workspaces Management Agencies	Credit Withspace IF fates a same and layword for search.	C
Purchased Resources Security Governance(beta)		Selected Spaces C 🛞 Indicat 0 Playbo 0

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

Figure 11-3 Workflows tab page

	/ Playb	ooks / Workflours													
Security Stuation Resource Manager	* *	Playbooks Workflows	altoridas Voidtous Asset connection Instance Management												
Risk Prevention Threat Operations Security Orchestration	•	Penc	ling review 0			Not enable	d 14			Enabled	20				
Objects Playbooks @		Narrie		Dataclass	Warking 5	Workflo 5	7 Current	Crosted	Crowlad	Status	All Updated At	Name Description	Enter a keyword. Operation	Q C Ľ	
Plugins Settings	•		a attack link analysis 3a617167	Alert	Enabled	General	y current	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:40 G		Disable Version Mar	rapement	
		Dne-click release ae141	b2e902f	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:41 G	-	Enable Version Man	agement i Delete	

Copying a workflow version

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-4 Version Management page

 Add
 Import
 Status
 Add
 Name
 Control
 Operation

 Operation
 Database
 Windles
 Vindles
 Vindles
 Control
 Database
 <

- **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 displayed dialog box, click **OK**.

Editing and submitting a workflow version

- **Step 8** 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 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.

Param	eter		Description
Basic	Basic Node	StartEvent	The start of a workflow. Each workflow can have only one start node. The entire workflow starts from the start node.
		EndEvent	The end of a workflow. Each workflow can have multiple end nodes, but the workflow must end with an end node.
		UserTask	When the workflow execution reaches this node, the workflow is suspended and a to-do task is generated on the Task Center page.
			After you complete the task, the subsequent nodes in the workflow continue to be executed. Table 11-5 describes the UserTask parameters.
		SubProcess	Another workflow is started to perform cyclic operations. It is equivalent to the loop body in the workflow.
	System Gatew ay	ExclusiveGa teway	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.
		ParallelGate way	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.)
		InclusiveGat eway	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.)
Workfl	ows		You can select all released workflows in the current workspace.
Plug-in	S		You can select all plug-ins in the current workspace.

 Table 11-4 Resource Libraries 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.
	 On the Access Authorization slide-out panel displayed, select Agree and click OK.

Table 11-5 UserTask parameters

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.

Figure 11-5 Version Management page

lidd Import							Status	AL	• Name •	Enter a keyword.	QC	C
Name	Dataclass	Workflo 🏆	Workflo 🏆	Current	Created	Created	Updated	Updated At	Description	Operation		
One click host isolation 55ec9432-fc83-3fc1-e139-f93606410e58	Alert	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:58	-	Disable Version Management]	
HostDefenseAlarmsAreAccocciatedWithHistoricaHan 3e93c325 0f5a-359c ac72-563abeb9864	Alert	Enabled	General	vt	system	Feb 26, 2024 14:28:56	system	Feb 26, 2024 14:27:11	-	Disable Version Management		
Policy Management - Policy Delivery IAM Decapsulat 20/20250-0705-0578-0646-1105x/2014005	Policy	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:57	-	Disable Version Management		

- **Step 12** On the **Version Management** slide-out panel, 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, in the version information area, locate the row containing the desired workflow version, and click **Activate** in the **Operation** column.
- Step 15 In the displayed dialog box, click OK.

Enabling a workflow

- **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

11.5 (Optional) Configuring and Enabling a Playbook

By default, SecMaster provides playbooks such as **Fetching Indicator from alert**, **Synchronization of HSS alert status**, and **Automatic disabling of repeated alerts**. Most of playbooks are enabled by default. The following playbooks are enabled by default:

HSS alert status synchronization, automatic notification of high-risk vulnerabilities, historical handling information associated with host defense alarms, SecMaster and WAF address group association policy, historical handling information associated with application defense alarms, historical handling information associated with network defense alarms, automatic closure of repeated alarms, and alarm IP metric marking Asset protection status statistics notification, automatic alarm statistics notification, and automatic high-risk alarm notification

If you want to use a playbook that is not enabled, you can enable the initial version of the playbook (V1, activated by default), or modify the playbook and then enable 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-6 Workspace management page

SecMaster	Management ③				🕞 Process
Security Overview Workspaces Management Agencies	$\label{eq:state} \fbox$ Under thistopee				C
Purchased Resources Security Governance(beta)	Contraction Contracti	 Incidents 0 ○ Assets 0 	 ♥ Vulner 0 ⊜ Securl 0 	O Alerts 0 instan 0	Selected Spaces C 🛞 indicat 0 Playto 0

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

Figure 11-7 Accessing the Playbooks tab

< //	Playbox	oks / Playbook														
Security Stuation	- I P	Claubander	Playbooks Workflows Asset connection Instance Management													
Resource Manager		Hajoods Worktows Asset connection instance Management														
Risk Prevention																
Threat Operations			Pendin	g review 0			1	lot enabled	10		Enabled 1					
Security Orchestration	•															
Objects											Status Al					
Playbooks 👩											Sidius	* Name	Enter a keyword			C (
Layouts		N	arre	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description		Operation		
Plugins			dd the IP indica	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23 42 32 GMT+06:00	-		Enable More		
Settings •	·		lert notification	Alert	Not enabled	vt	Ø	system	2023/06/08 23 42:32 GWT+08:00	system	2023/06/08 23 42 32 GWT+06:00	-		Enable More		

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

Figure 11-8 Workspace management page

SecMaster	Management 🕥	Process
Security Overview Workspaces	Onder Hippingsea If later a name and layound for search.	C
Purchased Resources Security Governance(beta)	0 addet? 6xdet? Region Paged- Mare It Incidents 0 Valent 0 A Arents 0 Not homed. C Addets 0 It strate 0 It st	Selected Spaces C

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

Figure 11-9 Accessing the Playbooks tab

< / P	laybooks / Playbooks												
Security Situation	Playbooks Workflows	Asset corner	elies Jacobs	nce Manager									
Resource Manager 🔹	Baybooks Nothions	Asset Colliner	LUUTI TIISUI	ince Manager	neni.								
Risk Prevention 🔻													
Threat Operations	Pendi	ng review 0			1	lot enabled	10		Enabled 1				
Security Orchestration													
Objects Playbooks									Status Al	* Name	 Enter a keyword. 	QC	3 O
Layouts	Name	Detaclass	Playbo 🍞	Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operati		
Plugins	Add the IP indica	Alef	Not enabled	vt	ø	system	2023/06/08 23 42:32 GMT+08:00	system	2023/06/06 23:42:32 GMT+06:00	-	Enable	Mare 🕶	
Settings •	Alert notification	Alef	Not enabled	vt	ø	system	2023/08/08 23 42:32 GWT+08:00	system	2023/06/06 23 42 32 GMT+06:00	-	Enable	Mare 🕶	

Copying a Playbook Version

Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-10 Version Management slide-out panel

 Name
 Datactass
 PL
 C
 Corr
 Mont
 Created (b)
 Updated (b)
 Update

- **Step 6** 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 7** In the displayed dialog box, click **OK**.

Editing and Submitting a Playbook Version

- **Step 8** 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 9** On the page for editing a playbook version, edit the version information.
- Step 10 Click OK.

Reviewing a Playbook Version

Step 11 After the playbook version is edited and submitted, the playbook management page is displayed. On the **Playbooks** page, click **Version Management** in the **Operation** column of the target playbook.

Figure 11-11 Version Management slide-out panel

Name	Dataclass	PI	7	Cur	Monit	Created By	Created	Updated By	Updated At	Description	Operation
Capture a	Commo	Not e		-	Ø	system	2023/06/24 14:35:51 GMT+08:00	system	2023/05/24 14:35:51 GMT+08:00	-	Enable More 🔺
CFW First	Commo	Not e		-	Ø	system	2023/06/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	-	Version Management
Automatic	Alert	Not e			⊠	system	2023/06/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	-	Delete

- **Step 12** On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target playbook.
- Step 13 In the displayed dialog box, set Comment to Passed and click OK.

Enabling a Playbook

- **Step 14** On the **Version Management** slide-out panel, click **Enable** in the **Operation** column of the target playbook.
- **Step 15** In the slide-out panel, select the playbook version you want to enable and click **OK**.

----End

11.6 Operation Object Management

11.6.1 Data Class

11.6.1.1 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-12 Workspace management page

SecMaster	Management ()
Security Overview Workspaces Management Agencies	Create Wintspace C IF Enter a same and leptond for search. Q
Purchased Resources Security Governance(beta)	Carrier Science C @ 0 addet7 region Project- Nove 10 addet7 region Project- Nove 11 incodents 0 © Vaner. 0 Alerts 1 Incodents 0 Project. 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. The **Data Class** tab page is displayed by default.

Figure 11-13 Accessing the Data Class tab

Security Situation 🔹										
Resource Manager 🔹 🔻	Data Class Type Mar	nagement Classify&Ma	ipping							
Risk Prevention 💌										
Threat Operations								C 💿		
Security Orchestration	▼ Search by name							Q		
Objects 2	Name	Business Code	Built-in	Created By	Created	Updated	Description	Operation		
Playbooks	Policy	Policy	Yes	system	2023/08/08 23:38:36 GMT+08:00	2023/08/08 23:38:36 GMT+08:00	Built-in policy data class	View Topology Edit Delete		
Layouts Plugins	PolicyRecord	PolicyRecord	Yes	system	2023/08/08 23:38:36 GMT+08:00	2023/08/08 23:38:36 GMT+08:00	Built-in policy record data class	View Topology Edit Delete		
Settings 💌	Resource	Resource	Yes	system	2023/04/26 14:19:03 GMT+08:00	2023/08/08 21:06:44 GMT+08:00	Built-in resource data class	View Topology Edit Delete		
	Alert	Alert	Yes	system	2023/04/26 14:19:03 GMT+08:00	2023/08/08 21:06:44 GMT+08:00	Built-in alert data class	View Topology Edit Delete		

Step 5 In the data class list, view the existing data class information.

If there are many data classes, you can use a filter, such as data class name, code, built-in or not, or description, enter a keyword in the search box, and click Q to quickly search for a specified data class.

Parameter	Description
Name	Name of a data class.
Business Code	Business code of the data type.
Built-in	Indicates whether the data class is a built-in data class.
Created By	Creator information of the data class.
Created	Time when a dataset is created.
Updated	Time when a dataset is updated.
Description	Description of a data class
Operation	You can edit and delete data classes.

Table 11-6 Data Information

Step 6 To view details about a data class, click the name of the target data class. The details page of the target data class is displayed on the right.

----End

11.6.2 Type Management

11.6.2.1 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-14 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-15 Type Management page

< / 08	ojects / Ty	pe Management										
Security Situation	•		-									
Resource Manager	-	ata Class Type Manageme	<u> </u>	Classifya	Mapping							
tisk Prevention												
hreat Operations	-	Alert Types Event Types	Threat Inf	elligence	Vulnerability Type Cust	am Type						
lecurity Orchestration		Type Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword.	Q	С
Objects 2		AI •	<u>2</u> 1≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🍞	SLA	Description	Operation		
Playbooks Layouts		Abnormal network behavior(22	9		Abnormal access frequency (IP Access Frequency Abnorm		Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins dings		Abnormal system behavior(31)			Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable	-	Abnormal IP address switch	Associated Layout Edit Delete		
1		Abnormal user behavior(38)			First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete		

- **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 11-7**.

If there are many subtypes, you can select the **Sub Type** or **Associated Layout** and enter the corresponding keyword for search.

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 Enabled: The current type has been enabled. Disabled: The current type has been disabled. 				

 Table 11-7 Alert type parameters

Parameter	Description					
SLA	SLA processing time of an alert type.					
Description	Description of an alert type					
Operation	You can edit and delete alert or incident types.					

----End

Adding an Alert Type

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

Figure 11-16 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Credit Withington $\label{eq:starting} \overline{V} \mbox{ Inter a name and keyword for search}.$				C
Purchased Resources Security Governance(beta)		 Incidents 0 Assets 0 	 Vulner 0 Securt 0 	O Alerts 0 ◎ Instan 0	Selected Spaces C ⑧ № Indicat 0 Playbo 0

Figure 11-17 Type Management page

< / 00	C / Cojecis / Type Management									
oreany orearen	Data Class Type Management Classify&Mapping									
		Alert Types Event Types Threat	Intelligenc	ce Vulnerability Type Custo	am Type					
Security Orchestration	2	Type Name	A	dd Batch enable	Batch Disable			Sub Type	 Enter a keyword. 	QC
Playbooks		Al v Åt		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation	
Layouts		Abnormal network behavior(22)	1	Abnormal access frequency (IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete	
Plugins Settings		Abnormal system behavior(31)		Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable		Abnormal IP address switch	Associated Layout Edit Delete	
	1	Abnormal user behavior(38)		First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete	

- **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 11-8 Parameters for	r adding an alert type
---------------------------	------------------------

Parameter	Description
Type Name	Customize the name of the new alert type.

Parameter	Description
Туре Тад	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 .
Sub Type TagEnter the alert subtype ID. The keyword must comply with the upper camel case naming rules, for example, SubTypeName.Startup StatusIndicates whether an alert type is enabled.	
	• C: indicates that the alert type is enabled.
	• Construction: Experimental structure indicates that the type is disabled.
SLA	Set the SLA processing time of the alert.
Description	Description of a user-defined alert type

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

Figure 11-18 Workspace management page

SecMaster	Management ③	C Process C Q Sector Space: C @ c- tave II Incorets: 0 @ Vuiner 0 @ Avers. 0 Er Incoret 0 C Asets: 0 II Sector 0 II Prepto 0		
Security Overview Workspaces	$\begin{tabular}{c} \hline \end{tabular} \hline $$ Total a name and layout for seach. \end{tabular}$			
Purchased Resources Security Governance(beta)	O def877 fease count for the last fease fease fease fease fease			i⊻ Indicat 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-19 Type Management page

Security Situation	*													
Resource Manager	*	Data	Data Class Type Management Classify6Mapping											
Risk Prevention	*													
hreat Operations			Alert Types	Event Types	Threat Inte	ligence	Vulnerability Type Cust	tom Type						
Security Orchestration	0			Type Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword.	Q	С
Objects			AL	•	¢1≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 😨	SLA	Description	Operation		
Playbooks Layouts			Abnorm	al network behavior(22			Abnormal access frequency o IP Access Frequency Abnorm		Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins Settings 💌			Abnormal system behavior(31)				Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable	-	Abnormal IP address switch	Associated Layout Edit Delete		
		•	1.	al user behavior(38)			First login from an IP address	Alert Detail	Enable		First login from an IP address	Associated Layout Edit Delete		

- **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 layout to be associated.
- Step 8 Click OK.

----End

Editing an Alert Type

NOTE

- Currently, the built-in alert type cannot be edited.
- After a customized alert type is added, the **Type Name**, **Type Tag**, and **Sub Type Tag** parameters cannot be modified.
- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-20 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Could Workspace $\overline{\nabla} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Comme accel	Incidents 0 Assets 0	♥ Vulner 0 Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ indicat 0 B Playbo 0

Figure 11-21 Type Management page

< 1 / 0	bjects /	Type M	lanagement								
Security Situation	Ŧ	Data C	Class Type Managemer			Mapping					
Resource Manager	•	Data C	Jass Type Managemer	. 6	Liassitya	mapping					
Risk Prevention	*										
Threat Operations		1	Alert Types Event Types	Threat Inte	elligence	Vulnerability Type Cus	lom Type				
Security Orchestration	-		Type Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword. Q C
Objects 📀			Al ×	2 ‡≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation
Playbooks Layouts			Abnormal network behavior(22)			Abnormal access frequency of IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete
Plugins Settings	-		Abnormal system behavior(31)			Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable		Abnormal IP address switch	Associated Layout Edit Delete
	1		Abnormal user behavlor(38)			First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete

- **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.

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.
	• C: indicates that the type is enabled.
	• Construction: Experimental structure indicates that the type is disabled.
SLA	Set the SLA processing time of the alert.
Description	Description of a custom alert type

Table 11-9 Parameters for editing an alert type

Step 9 In the lower right corner of the page, click **OK**.

----End

Managing an Alert Type

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

Figure 11-22 Workspace management page

SecMaster	Management ③				🗇 Process
Security Overview Workspaces	$\fboxlabel{eq:response} \fboxlabel{eq:response} \fboxlabel{eq:response} \fboxlabel{eq:response} \fboxlabel{eq:response} \fboxlabel{eq:response} \vspace{-1.5} \rain the transformation of the response of the response$				C
Purchased Resources Security Governance(beta)	Generation Generation	Incidents 0 Assets 0	Vuiner 0 ⊜ Securi 0	O Alerts 0 ≋ Instan 0	Selected Spaces C indicat 0 Playbo 0

Figure 11-23 Type Management page

< / / Object	s / Type	e Management											
Security Situation													
Resource Manager 🔹 👻	Dat	a Class	Type Managemen		Classify	&Mapping							
Risk Prevention 💌													
Threat Operations		Alert Types	Event Types 1	hreat Int	elligence	Vulnerability Type Cust	om Type						
Security Orchestration		1	Type Name		Ad	d Batch enable	Batch Disable			Sub Type	Enter a keyword.	Q	С
Objects		AI	×	21≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation		
Playbooks Layouts		Abnormal	network behavior(22)			Abnormal access frequency o IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins Settings 💌		Abnormal	system behavior(31)			Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable		Abnormal IP address switch	Associated Layout Edit Delete		
	1	Abnormal	user behavior(38)			First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete		

- **Step 5** On the **Type Management** page, click the **Alert Type** tab.
- **Step 6** On the **Alert Types** tab, manage alert types.

Operation	Description
Enable NOTE The built-in alert types are enabled by default. You do not need to manually enable them.	 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.
uem.	 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 NOTE Currently, the built-in alert types cannot be disabled.	 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.
	 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.

 Table 11-10
 Managing an alert type

Operation	Description
Delete NOTE Currently, built-in alert types cannot be deleted.	 On the alert type management page, select the type to be deleted and click Delete in the Operation column. In the displayed dialog box, click OK.

----End

11.6.2.2 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-24 Workspace management page

SecMaster	Management ③				
Security Overview Workspaces	Could Workspace $\overline{V} \mbox{ Inter a more and layered for search}.$				
Purchased Resources Security Governance(beta)	Construction C	S incidents 0 Assets 0	♥ Vuiner 0		🗠 Indicat 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-25 Type Management page

< /	Objects	/ Type I	Management										
Security Situation	*												
Resource Manager	*	Data	ata Class Type Management Classify&Mapping										
Risk Prevention	Ŧ												
Threat Operations			Alert Types Event Typ	es Threat I	ntelligen	ce Vulnerability Type Cust	om Type						
Security Orchestration	•		Type Nan	e		dd Batch enable	Batch Disable			Sub Type	Enter a keyword.	Q	С
Objects 2			AI •	<u></u> _‡≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation		
Playbooks Layouts			Abnormal network beh			Abnormal access frequency o IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins ettings			Abnormal system beha	vior(31)		Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable		Abnormal IP address switch	Associated Layout Edit Delete		
		Abnormal user behavior(38)			First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete		_	

- **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 11-11**.

Parameter	Description
Type Name	Name of an incident type
Sub Type/Sub Type Tag	Name and ID of an incident subtype
Associated Layout	Layout associated with the incident type
Startup Status	Indicates whether an incident type is enabled.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.

 Table 11-11 Incident type parameters

----End

Adding an Incident Type

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

Figure 11-26 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspeces	Credit Workspace $\label{eq:static_static} \overline{\mathbb{Y}} \mbox{ for a name and keyword for search}.$				C
Purchased Resources Security Governance(beta)	Cannot Except 0 defet17 defet12 Report Project- Note Not house.	 ⊡ Incidents 0 ○ Assets 0 	♥ Vulner 0 ⊜ Securl 0	Alerts O Instan	Selected Spaces C 🛞

Figure 11-27 Type Management page

< / / Objects	s / Type Management													
Security Situation 🔹	Data Class Type Management Classify&Mapping													
Resource Manager 🔹 👻	Uara class lype Management Classify Malapong													
Risk Prevention 💌	ak Preventon 🔹													
Threat Operations	tread Operations Altert Types Event Types Thread Intelligence Valinerability Type Costom Type													
Security Orchestration	Type Name Add Batch enable Batch Disable Sub Type + Enter a keyword. Q C	3												
Objects 2	Al Sub Type/Sub Type Tag Associated Lay Startup Status SLA Description Operation													
Playbooks Layouts	Abnormal access frequency c Associated Layout Edit Detel IP Access Frequency Annum Access frequency of Associated Layout Edit Detel													
Plugins Settings •	Athromal system behavior(31) Athromal P address selfch Alert Detail Enable – Athromal IP address selfch Associated Layout Edit Deteile													
	Abnormal user behavior(3) Perst togin from an IP address Alext Detail Enable - First togin from an IP address Associated Layout [Edit Detail													

- **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.

Parameter	Description
Type Name	Customized name of an incident type. The name must comply with the upper camel case naming rules, for example, TypeName .
Туре Тад	Enter the incident type ID. The keyword must comply with the upper camel case naming rules, for example, TypeTag .
Sub Type	Enter the subtype of the incident type. The name must comply with the upper camel case naming rules, for example, SubType .
Sub Type Tag	Enter the incident subtype ID. The keyword must comply with the upper camel case naming rules, for example, SubTypeName .
Startup Status	Indicates whether an incident type is enabled.
	• C: indicates that the type is enabled.
	• Construction: indicates that the alert type is disabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

 Table 11-12 Incident type parameters

After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Step 7 In the lower right corner of the page, click OK.

After the incident type is added, you can view the new incident type in **Type Name** on the **Event Type** page.

----End

Associating an Incident Type with a Layout

NOTE

By default, built-in incident types are associated with existing layouts. You cannot customize associated layouts.

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

Figure 11-28 Workspace management page

SecMaster	Management () Proces
Security Overview Workspaces	Onth Windpace C To find a value and layered for seach. Q
Purchased Resources Security Governance(beta)	Construction C @ 0 addet17 Made 2 Paget-Max ☐ Incidents 0 0 Addet - 0 Paget - Max ☐ Incidents 0 0 Addet - 0 ☐ Incidents

Step 4 In the navigation pane on the left, choose Security Orchestration > Objects. On the displayed page, click the Type Management tab.

Figure 11-29 Type Management page

< / 0	bjects /	Type N	Aanagement											
Security Situation	Ŧ	Data Class Type Management Classify&Mapping												
Resource Manager	*	Lata Crass lype Management Crassny 6 Mapping												
Risk Prevention	Ŧ													
Threat Operations			Alert Types E	Event Types	Threat Inf	elligence	Vulnerability Type Cust	tom Type						
Security Orchestration	-		Тур	e Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword.	Q	С
Objects 2			AI +		21≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🍞	SLA	Description	Operation		
Playbooks Leyouts			Abnormal netr	vork behavior(22	,		Abnormal access frequency of IP Access Frequency Abnorm		Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins Settings	-	Abnormal system behavior(31)			Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable		Abnormal IP address switch	Associated Layout Edit Delete				
	1		Abnormal user	r behavior(38)			First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete		

- **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 layout to be associated.
- Step 8 Click OK.
 - ----End

Editing an Incident Type

NOTE

- Currently, the built-in incident type cannot be edited.
- After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.
- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-30 Workspace management page

SecMaster	Management 💿	E	Process
Security Overview Workspaces	Credit Wonspace T fotor a name and layound for search.		C
Purchased Resources Security Governance(beta)	Committeened C		C ⊕

Figure 11-31 Type Management page

< / / 0	bjects /	Type Mar	tremeger											
Security Situation	Ŧ	Pada Class Tues Management Classified Manajas												
Resource Manager	*	Data Class Type Management Classify&Mapping												
Risk Prevention	Ŧ													
Threat Operations		Atert Types Event Types Threat Intelligence Vulnerability Type Custom Type												
Security Orchestration	-		Type Nam	e	A	dd Batch enable	Batch Disable			Sub Type	Enter a keyword.	Q	С	
Objects			u +	21=		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation			
Playbooks Layouts			Abnormal network beha	vior(22)		Abnormal access frequency of IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete			
Plugins Settings	-	Abnormal system behavior(31) Abnormal user behavior(38)		ior(31)		Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable	-	Abnormal IP address switch	Associated Layout Edit Delete			
	4				First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete				

- **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 11-13 Incident type parameters

Parameter	Description
Type Name	Name of an incident type, which cannot be modified.
Туре Тад	Incident type ID, which cannot be modified.

Parameter	Description
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. indicates that the type is enabled. indicates that the alert type is disabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

Step 9 In the lower right corner of the page, click **OK**.

----End

Managing Existing Incident Types

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

Figure 11-32 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspeces	Could Wonspece $\overline{V} \ \ \text{for search}.$				C
Purchased Resources Security Governance(beta)	D add0777 deda12 Report Not hoted	 Incidents 0 Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts O Se Instan O	Selected Spaces C 🛞 iv Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-33 Type Management page

<	Objects	/ Type	e Management											
Security Situation	٣	Dat	a Class	Type Managemer	2	Chereity	Manning							
Resource Manager	٠		Data Class Type Management Classify&Mapping											
Risk Prevention	٣													
Threat Operations	,		Alert Types	Event Types	fhreat In	telligence	Vulnerability Type Cust	om Type						
Security Orchestration	•		1	Type Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword.	QC	
Objects			AI	*	21≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation		
Playbooks Layouts			Abnormal	network behavior(22)			Abnormal access frequency o IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins Settings	÷		Abnormal system behavior(31)				Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable		Abnormal IP address switch	Associated Layout Edit Delete		
		1	Abnormal	user behavior(38)			First login from an IP address IP First Access	Alert Detail	Enable		First login from an IP address	Associated Layout Edit Delete		

Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 On the incident type tab, manage incident types.

Operation	Description
Enable NOTE The built-in incident types are enabled by default. You do not need to manually enable them.	 On the type management page, select the type to be enabled and click Batch Enable. Alternatively, locate the row containing the incident type to be enabled, click Disable in the Status column. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the status of the
	target type changes to Enable , the target type is enabled successfully.
Disable NOTE Currently, the built-in incident types cannot be disabled.	 On the Event Type page, select the type to be disabled and click Batch Disable. Alternatively, locate the row containing the incident type to be disabled, click Enable in the Status column.
	 In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the Status of the target type changes to Disable, the target type is disabled successfully.
Delete NOTE Currently, built-in incident	 On the incident type management page, select the type to be deleted and click Delete in the Operation column.
types cannot be deleted.	2. In the displayed dialog box, click OK .

 Table 11-14 Managing existing incident types

----End

11.6.2.3 Viewing Threat Intelligence Types

Scenario

This section describes how to view threat intelligence types.

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.

Viewing Threat Intelligence Types

Step 1 Log in to the management console.

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

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

Figure 11-34 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspaces Management Agencies	$\begin{tabular}{c} \hline \label{eq:rescaled} \hline $$ Total Writigate $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$$				C
Purchased Resources Security Governance(beta)	United access 0 ex56977 Melai2 Region (1997) Project Mark Not fixed.	incidents 0 Assets 0	 ♥ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ № Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-35 Type Management page

< /	Objects	/ Type I	Aanagement											
Security Situation	*													
Resource Manager	•	Data	Class	Type Managemen	6	Jassiya	SMapping							
Risk Prevention	Ŧ													
hreat Operations	<u> </u>		Alert Types	Event Types 1	Threat Int	elligence	Vulnerability Type Cus	tom Type						
lecurity Orchestration	•			Type Name		Add	Batch enable	Batch Disable			Sub Type	 Enter a keyword. 	Q	С
Objects 2			AI	*	21≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation		
Playbooks Layouts			Abnorma	el network behavior(22)	- 1		Abnormal access frequency o IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins ettings			Abnorma	il system behavior(31)			Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable	-	Abnormal IP address switch	Associated Layout Edit Delete		
	4		Abnorma	I user behavior(38)	- 1		First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete		

- **Step 5** On the **Type Management** page, click the **Threat Intelligence** tab.
- **Step 6** On the **Threat Intelligence** page, view details. For details about the parameters, see **Table 11-15**.

Table 11-15 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: Enabled: The current type has been enabled. Disabled: The current type has been disabled.
Evpired Time	
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

11.6.2.4 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-36 Workspace management page

SecMaster	Management 💿				Process
Security Overview Workspeces Management Agencies	Creals Workspace $\label{eq:product} \overline{\nabla} \mbox{ Intra a name and largered for search}.$				C
Purchased Resources Security Governance(beta)	Commit accord 0 405077 36422 Rigon Paged- Mare Not hand:	 Incidents 0 Assets 0 	 ♥ Vulner 0 Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ ↓ Indicat 0 ▷ Playbo 0

Figure 11-37 Type Management page

< / Object	ts / Type Management						
Security Situation 🔹	Data Class Type Management	Classify&Mapping					
Resource Manager 🛛 🔻	Type Management	Classily&Mapping					
Risk Prevention 💌							
Threat Operations	Alert Types Event Types Three	Intelligence Vulnerability Type Cu	istom Type				
Security Orchestration	Type Name	Add Batch enable	Batch Disable		Sub Type	Enter a keyword. Q	С
Objects	Al v A	Sub Type/Sub Type Tag	Associated Lay Startup Status	⊽ SLA	Description	Operation	
Playbooks Layouts	Abnormal network behavior(22)	Abnormal access frequency IP Access Frequency Abnor	r Klert Detail Enable	-	Abnormal access frequency of	Associated Layout Edit Delete	
Plugins Settings •	Abnormal system behavior(31)	Abnormal IP address switch IP Switch Abnormal	Alert Detail Enable	-	Abnormal IP address switch	Associated Layout Edit Delete	
	Abnormal user behavlor(38)	First login from an IP addre	88 Alert Detail Enable	-	First login from an IP address	Associated Layout Edit Delete	

- **Step 5** On the **Type Management** page, click the **Vulnerability Type** tab.
- **Step 6** On the **Vulnerability Type** tab page, view details about existing vulnerability types. For details about the parameters, see **Table 11-16**.

Table 11-16 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: Enabled: The current type has been enabled. Disabled: The current type has been disabled. 					
Built-in	Indicates whether the vulnerability is a built-in vulnerability type.					
Description	Description of a vulnerability type					
Operation	You can edit and delete vulnerability types.					

----End

Adding a Vulnerability Type

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

Figure 11-38	Workspace	management	page
--------------	-----------	------------	------

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	Could Writingson $\label{eq:static} \overline{\mathcal{V}} \mbox{ Inter a name and layouth for search}.$				C
Purchased Resources Security Governance(beta)	definition definition definition definition definition definition definition	incidents 0 Assets 0	Ø Vulner 0 ⊜ Securl 0	O Alerts 0 instan 0	Selected Spaces C indicat 0 ⊡ Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-39 Type Management page

< / / 0	Objects (/ Type Management										
Security Situation	¥		_									
Resource Manager	*	Data Class Type Managem	ent 🚯	Classify8	Mapping							
Risk Prevention	Ŧ											
Threat Operations	÷	Alert Types Event Types	Threat In	elligence	Vulnerability Type Cust	form Type						
Security Orchestration		Type Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword.	Q	С
Objects 2		AI *	21≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation		
Playbooks		Abnormal network behavior(2	12)		Abnormal access frequency o IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete		
Plugins Bettings	-	Abnormal system behavior(3	1)		Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable	-	Abnormal IP address switch	Associated Layout Edit Delete		
	4	Abnormal user behavior(38)			First login from an IP address IP First Access	Alert Detail	Enable	_	First login from an IP address	Associated Layout Edit Delete		

- **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** slideout panel, set type parameters.

Parameter	Description
Type Name	Name of the vulnerability type to be added. The name must comply with the upper camel case naming rules, for example, TypeName .
Туре Тад	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: indicates that the type is enabled. indicates that the type is disabled.
Description	Description of a user-defined vulnerability

Table 11-17 Vulnerability type parameters

D 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

D NOTE

Currently, built-in vulnerability types do not support customized layouts.

Step 1 Log in to the management console.

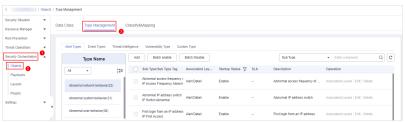
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-40 Workspace management page

SecMaster	Management ①				Process
Security Overview Workspaces Management Agencies	$$\ensuremath{\mathbb{V}}$$ Create Withingtons $$\ensuremath{\mathbb{V}}$$ Enter a name and layound for search.				C
Purchased Resources Security Governance(beta)	General count 0 add977 Sele12 Region Project- Nove Not Instance	 S incidents 0 ○ Assets 0 	 ♥ Vulner 0 ⊜ Securl 0 	 Alerts Instan 0 	Selected Spaces C 🛞 // Indicat 0 Playto 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-41 Type Management page



- Step 5 On the Type Management page, click the Vulnerability Type tab.
- **Step 6** On the **Vulnerability Type** page, select the vulnerability type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type.
- **Step 7** In the **Binding/Changing Layouts** box, select the layout to be associated.
- Step 8 Click OK.

----End

Editing a Vulnerability Type

D NOTE

- Currently, the built-in vulnerability types cannot be edited.
- After a user-defined vulnerability type is added, the type ID cannot be modified.
- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-42 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Create Workspace $\label{eq:states} \overline{V} \mbox{ Inter a name and keyword for search}.$				C
Purchased Resources Security Governance(beta)	Grand score Grand sco	3 Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	O Alerts O instan O	Selected Spaces C 🛞 iv Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-43 Type Management page

< / / Objects / Type Management											
Security Stuation											
Resource Manager 🔹	Type Management	Classify&Mapping									
Risk Prevention 💌											
Threat Operations	Alert Types Event Types Threat In	tellgence Vulnerability Type Custom Type									
Security Orchestration	Type Name	Add Batch enable Batch Disable	Sub Type								
Objects 2	Al + ÅI	Sub Type/Sub Type Tag Associated Lay Startup Status 😨 S	SLA Description Operation								
Playbooks Layouts	Abnormal network behavior(22)	Abnormal access frequency < Alert Detail Enable -	- Abnormal access frequency of Associated Layout Edit Delete								
Plugins Settings •	Abnormal system behavior(31)	Abnormal IP address switch IP Switch Abnormal Alert Detail Enable -	- Abnormal IP address switch Associated Layout Edit Delete								
1	Abnormal user behavior(38)	First login from an IP address IP First Access Alert Datail Enable	- First login from an IP address Associated Layout Edit Delete								

- **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.

Parameter	Description
Type Name	Name of a user-defined vulnerability type
Туре Тад	Vulnerability type ID, which cannot be modified.
Startup Status	Set the enabling status of the vulnerability type:
	• C: indicates that the type is enabled.
	• Construction: Experimental structure indicates that the type is disabled.
Description	Description of a user-defined vulnerability

Step 8 In the lower right corner of the page, click **OK**.

----End

Managing a Vulnerability Type

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

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

Figure 11-44 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspaces Management Agencies	$\begin{tabular}{c} \hline \label{eq:rescaled} \hline $$ Total Writigate $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$$				C
Purchased Resources Security Governance(beta)	0 editif? Weided Project Nove Not fictured	incidents 0 Assets 0	 ♥ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ № Indicat 0 Playbo 0

Figure 11-45 Type Management page

< / / Objects	s / Type	Management									
Security Situation 🔹			1.								
Resource Manager 🛛 🔻	Data	Class Type Management	•	assirya	Mapping						
Risk Prevention 💌											
Threat Operations		Alert Types Event Types T	hreat Inte	lligence	Vulnerability Type Cust	om Type					
Security Orchestration		Type Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword.	QC
Objects		AI •	2 1≡		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation	
Playbooks Layouts		Abnormal network behavior(22)			Abnormal access frequency o IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete	
Plugins Settings 💌		Abnormal system behavior(31)			Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable	-	Abnormal IP address switch	Associated Layout Edit Delete	
	4	Abnormal user behavior(38)	- 1		First login from an IP address	Alert Detail	Enable		First login from an IP address	Associated Layout Edit Delete	

- **Step 5** On the **Type Management** page, click the **Vulnerability Type** tab.
- **Step 6** On the vulnerability type tab, manage vulnerability types.

Table 11-19 Managing a vulnerability type	Table	11-19	Managing	a vulnerability type
---	-------	-------	----------	----------------------

Operation	Description
Enable NOTE Built-in vulnerability types are enabled by default. You do not need to manually enable them.	 On the Vulnerability Type page, select the type to be enabled and click Batch Enable. Alternatively, locate the row containing the vulnerability type to be enabled, click Disable in the Status column.
	 In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the status of the target type changes to Enable, the target type is enabled successfully.
Disable NOTE Currently, the built-in vulnerability types cannot be disabled.	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.
	 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 NOTE Currently, the built-in vulnerability types cannot be deleted.	 On the Vulnerability Type tab, select the vulnerability type to be deleted and click Delete in the Operation column. In the displayed dialog box, click OK.

----End

11.6.2.5 Viewing Custom Types

Scenario

This section describes how to view custom threat intelligence types.

Limitations and Constraints

Built-in types and sub-types cannot be associated with layouts, edited, deleted, enabled, or disabled.

Viewing Custom Types or Subtypes

Step 1 Log in to the management console.

- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-46 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Credet Workspace $\overline{V} \mbox{ Inter a more and keyword for search}.$				C
Purchased Resources Security Governance(beta)	Constitution and Consti	3 Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	● Alerts 0 linstan 0	Selected Spaces C 🛞 iv Indicat 0 Playbo 0

Figure 11-47 Type Management page

< //	Objects	/ Type	Managemen	4									
Security Situation	٠												
Resource Manager	*	Data	ata Class Type Management Classify&Mapping										
Risk Prevention	Ŧ												
Threat Operations	r I		Alert Types	Event Types 1	Threat Int	elligence	Vulnerability Type Cust	om Type					
Security Orchestration	^			Type Name		Add	Batch enable	Batch Disable			Sub Type	Enter a keyword.	QC
Objects 2			AI	*	ģ‡≣		Sub Type/Sub Type Tag	Associated Lay	Startup Status 🖓	SLA	Description	Operation	
Playbooks			Abnorma	al network behavior(22)			Abnormal access frequency o IP Access Frequency Abnorm	Alert Detail	Enable	-	Abnormal access frequency of	Associated Layout Edit Delete	
Plugins Settings	÷		Abnorma	al system behavior(31)			Abnormal IP address switch IP Switch Abnormal	Alert Detail	Enable	-	Abnormal IP address switch	Associated Layout Edit Delete	
		1	Abnorma	al user behavior(38)			First login from an IP address IP First Access	Alert Detail	Enable	-	First login from an IP address	Associated Layout Edit Delete	

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
```

11.6.3 Classification & Mapping

11.6.3.1 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-48 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspeces	Could Workspece $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	O add0177 deds12 Region Proct- Non Not hoted.	Incidents 0 Assets 0	 ♥ Vulner 0 ⊜ Securi 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ Indicat 0 ∋ Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-49 Classify&Mapping tab page

(Dijects / Cases/jAlkaparg										
Security Situation Resource Manager	Data	a Class Type Management C	Classify&Mapping							
Risk Prevention Threat Operations		Create					Start Date End Date	a)	QEBC	
Security Orchestration		Name	Data Class	Enable Status 🍞	Progress	Number of asso	Created	Description	Operation	
Objects 2		CFW Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration CFW Alert Categorization and R_{\cdots}	Cione	
Layouts		MTD Alert Calegorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration of MTD Alert Categorization and	Cione	
Plugins Settings v		HSS Alert Calegorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration of HSS Alert Calegorization and	Clone	

Step 5 On the **Classify&Mapping** tab, view details about the created categorical mappings.

Parameter	Description
Name	Name of a categorical mapping.
Data Class	Type of the data class to which the categorical mapping belongs.
Enable Status	 Status of a categorical mapping. Enable: The current categorical mapping is enabled. Disable: The current categorical mapping has been disabled.
Progress	The progress of creating the categorical mapping.
Associated instances	Total number of plug-in instances associated with the categorical mapping.
Created	Time the categorical mapping was created.
Description	Description of the categorical mapping.

Step 6 To view details about a categorical mapping, click the name of the target categorical mapping. The categorical mapping details page is displayed.

----End

11.6.3.2 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.

Limitations and Constraints

- In a single workspace of a single account, a maximum of 50 classification & mapping templates can be created.
- In a single workspace of a single account, the proportion of a classification to its mappings is 1:100.
- A maximum of 100 classifications and mappings can be added to a workspace of a single account.

Creating a Categorical Mapping

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-50 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Credit Workspece If Enter a name and layword for search.				C
Agencies Purchased Resources Security Governance(beta)		Incidents 0 Assets 0	 Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⊗ i Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-51 Classify&Mapping tab page

< / / Opints / CestifyMaging										
Security Situation	۳	Data Class Type Management	Classify&Mapping							
Resource Manager	۳	Data Class Type management	vezon/arvehhnið	F						
Risk Prevention	۳									
Threat Operations	,	Create					Start Date End Date	ä	Q = III C	
Security Orchestration	•	Name	Data Class	Enable Status 🏼	Progress	Number of asso	Created	Description	Operation	
Dijects 2		CFW Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration CFW Alert Categorization and R	Clone	
Layouts		MTD Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration of MTD Alert Categorization and	Clone	
Settings	Ŧ	HSS Alert Calegorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Buil-In Configuration of HSS Alert Categorization and	Cione	

- **Step 5** On the **Classify&Mapping** page, click **Create**.
- **Step 6** On the **Create Categorical Mapping** page, set categorical mapping parameters.

Figure 11-52 Create Categorical Mapping page

asic Parameters	Classify Mapping Pretreatment							
Vame Classify								
Data Catagory Incident +	Classi	Classification Method						
Description	General classification	Custom classification						
01,000	This method is applicable for data processing in most scenarios.	If you have special data processing requirements, you can create a custom data class to meet your needs.						
A d Data Source								
* Data Source Select inst *								
* Instance CFW -								
A II JSON File								
Jpload JSON file								
- + + \ssim \ssim d A^- A^+ Enter a keyword. Q								
	ок	OK						

1. In the **Basic Parameters** area on the left, configure basic information about the categorical mapping. For details about the parameters, see **Table 11-21**.

Parameter	Description		
Name	Name of a user-defined categorical mapping.		
Data Category	Select the corresponding data type.		
Description	Description of the custom categorical mapping.		

Table 11-21 Configuring basic information

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 page on the right, set preprocessing mapping parameters.
- 8. Click \square 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-53 Workspace management page

SecMaster	Management ①		Process
Security Overview Workspaces	Condit Websigned IF for a name and keyword for search.		C
Purchased Resources Security Governance(beta)		Alerts 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-54 Classify&Mapping tab page

<	/ Objec	ds / (Sassify&Mapping							
Security Situation	۳	Da	ta Class Type Management C	lassify&Mapping						
Resource Manager	۳	Ua	ia ciaso Type management	iasonyawapping)					
Risk Prevention	Ŧ									
Threat Operations			Create					Start Date End Date	±	Q = 88
Security Orchestration	•		Name	Data Class	Enable Status 🍞	Progress	Number of asso	Created	Description	Operation
Objects 2			CFW Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration CFW Alert Categorization and R	Clone
Layouts			MTD Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23 42 32 GMT+08/00	Built-in Configuration of MTD Alert Categorization and	Clone
Plugins Settings	Ŧ		HSS Alert Calegorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08.00	Built-in Configuration of HSS Alert Categorization and	Cione

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

Figure 11-55 Workspace management page

SecMaster	Management 💿				Process
Security Overview Workspaces	Credit Workspace $\overline{V} \mbox{ Inter a name and keyword for search}.$				C
Purchased Resources Security Governance(beta)	D add077 dda12 Repor	Incidents O Assets O	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-56 Classify&Mapping tab page

< / 0b)	/ Objects / Classify/Magying												
Security Stuation • Resource Manager •	Da	ata Class Type Management C	Classify&Mapping)									
Risk Prevention Threat Operations		Create					Start Date — End Date	a	QEHC				
Security Orchestration		Name	Data Class	Enable Status 🍞	Progress	Number of asso	Created	Description	Operation				
Objects 2		CFW Alert Calegorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration CFW Alert Categorization and R	Cione				
Layouts		MTD Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23:42:32 GMT+08:00	Built-in Configuration of MTD Alert Calegorization and	Cione				
Plugins Settings •		HSS Alert Calegorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23 42 32 GMT+08:00	Built-in Configuration of HSS Alert Calegorization and	Cione				

- **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 11-21**.

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

11.6.3.3 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-57 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspaces	Create Wanspece				C
Purchased Resources Security Governance/beta)	Conventioned	i incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	O Alerts O instan O	Selected Spaces C 🛞 M Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-58 Classify&Mapping tab page

	/ Object	ls / Classify&Mapping											
Security Situation	۳	Data Class Type Management	Chara & O Managina										
Resource Manager	۳	Data Class Type Management	Classify&Mapping)									
Risk Prevention	۳												
Threat Operations	•	Create						Start Date End Date	ė]	Q	Ξ	С
Security Orchestration	-	Name	Data Class	Enable Status γ	Progress	Number of asso	Created		Description		Operation	i -	
Objects 2		CFW Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23	1.42.32 GMT+08.00	Built-in Configuration CFW.	Alert Categorization and R	Clone		
Layouts		MTD Alert Categorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23	142.32 GMT+08.00	Built-in Configuration of MT	D Alert Categorization and	Clone		
Plugins Settings	Ŧ	HSS Alert Calegorization and Re-Mapping	Alert	Enable	Basic In Classify Mapping	1	2023/08/08 23	142.32 GMT+08.00	Built-in Configuration of HS	S Alert Calegorization and	Clone		

Step 5 On the **Classify&Mapping** tab, manage categorical mappings.

Operation	Description				
Enable NOTE	Locate the row containing the target categorical mapping and click Disable in the Status column.				
Custom categorical mappings cannot be enabled.	If the status changes to Enable , the categorical mapping has been enabled.				
Disable NOTE	Locate the row containing your desired categorical mapping and click Enable in the Status column.				
Custom categorical mappings cannot be disabled.	If the status changes to Disable , the categorical mapping has been disabled.				
Delete NOTE	 Click Delete in the Operation column of the target categorical mapping. 				
Currently, the built-in categorical mappings cannot be deleted.	 In the displayed pane on the right, click Delete. NOTE 				
	 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. 				

 Table 11-23 Managing categorical mappings

----End

11.7 Playbook Orchestration Management

11.7.1 Playbooks

11.7.1.1 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

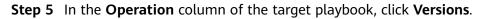
Figure 11-59 Workspace management page

SecMaster	Management ③				📝 Process
Security Overview Workspaces Management Agencies	Create Wanapace				C
Purchased Resources Purchased Resources Security Governance(beta)	Constitution Const	incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	 Alerts Instan 0 	Selected Spaces C 🛞 M Indicat 0 Playbo 0

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

Figure 11-60 Accessing the Playbooks tab

K Play	/ Paytoos / Paytoos														
Security Situation		Playbooks Workflows Asset connection Instance Management													
Resource Manager 🛛 🔻	мау	Hajrooks Wontows Asset connection Instance watagement													
Risk Prevention 🔹															
Threat Operations	Pending review 0					1	Not enabled 10 Enabled 1								
Security Orchestration															
Objects										Status Al					
Playbooks										Sidius	* Name	Enter a keyword		Q C	00
Layouts		Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description		Operation		
Plugins		Add the IP indica	Alert	Not enabled	v1	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+06:00	-		Enable More	•	
Settings 💌		Aiert notification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GWT+08:00	system	2023/08/08 23 42 32 GMT+08:00	-		Esable More		



Name	Dataclass	PI 7	7 Cur	Monit	Created By	Created	Updated By	Updated At	Description	Operation
Capture a	Commo	Not e	-	2	system	2023/06/24 14:35:51 GMT+08:00	system	2023/05/24 14:35:51 GMT+08:00	-	Enable More 🔺
CFW First	Commo	Not e	-	Ø	system	2023/06/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	-	Version Management
Automatic	Alert	Not e	-	Ø	system	2023/08/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	-	Delete

- **Step 6** On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Submit** in the **Operation** column.
- **Step 7** In the confirmation dialog box, click **OK** to submit the playbook version.

NOTE

- After the playbook version is submitted, **Version Status** changes to **To be reviewed**.
- After a playbook version is submitted, it cannot be edited. If you need to edit it, you can create a version or reject it during review.

----End

Follow-up Operations

A submitted playbook version needs to be reviewed. For details, see **Reviewing a Playbook Version**.

11.7.1.2 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-62 Workspace management page

SecMaster	Management 💮				🕞 Process
Security Overview Workspaces	Could Wonspec $\overline{V} \mbox{ for search}.$				C
Purchased Resources Security Governance(beta)	Conserve Source Or addition Or addition Or addition Or addition Or addition Or addition Or addition	incidents Assets 0	♥ Vulner 0 ⊜ Securl 0	 Alerts Instan O 	Selected Spaces C ⑧ iv Indicat 0 S Playbo 0

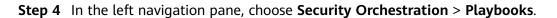


Figure 11-63 Accessing the Playbooks tab

< / Pa	ajboaka	s / Playbooks													
Security Situation 🔹 💌		avbooks Workflows	Asset connect	line lead											
Resource Manager 🔹 🔻	-	Workflows	Violatious Asset connection Instance Management												
Risk Prevention 🔹															
Threat Operations		Pendin	g review 0			1	lot enabled	10		Enabled 1					
Security Orchestration															
Objects										Status AI	* Name	Enter a keyword.			[] ⊚
Playbooks 2										olano Al	• 1418	 Dist a neywork. 	C.	96	
Layouts		Name	Detacless	Playbo 1	7 Current	Monitoring	Created By	Created	Updated By	Updated At	Description	(operation		
Plugins Satians		Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/06 23:42:32 GWT+06:00	-	E	inable More 🔻		
Settings •		Alert notification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42 32 GMT+08:00	system	2023/06/08 23 42 32 GMT+08:00	-	6	inable More +		

Figure 11-64 Version Management slide-out panel

Name	Dataclass	PI	7	Cur	Monit	Created By	Created	Updated By	Updated At	Description	Operation
Capture a	Commo	Not e				system	2023/06/24 14:35:51 GMT+08:00	system	2023/05/24 14:35:51 GMT+08:00	-	Enable More 🔺
CFW First	Commo	Not e			ø	system	2023/06/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	-	Version Management
Automatic	Alert	Not e			Ø	system	2023/06/24 14:35:51 GMT+08:00	system	2023/08/24 14:35:51 GMT+08:00		Delete

- **Step 6** On the **Version Management** slide-out panel, click **Review**.
- **Step 7** On the **Review Playbook Version** page, enter the review information. **Table 11-24** describes the parameters for reviewing a playbook version.

Parameter	Description
Comments	Select the review conclusion.
	 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	This parameter is mandatory when the review comment is Reject.
	Enter the review comment. This parameter is mandatory when Reject is selected for Review Comment.

 Table 11-24
 Parameters for reviewing a playbook version

NOTE

If the current playbook has only one version, the version is in the activated state by default after being approved.

Step 8 Click **OK** to complete the playbook version review.

----End

Follow-up Operations

An approved playbook version needs to be enabled. For details, see **Enabling a Playbook**.

11.7.1.3 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-65 Workspace management page

SecMaster	Management 💮	📝 Process
Security Overview Workspaces	Credit Wintspace 9 Enter a name and leyonoid for search.	C
Purchased Resources Purchased Resources Security Governance(beta)	Construct construct Sender figures S	

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

Figure 11-66 Accessing the Playbooks tab

K / Playb	iooks / Playbooks												
Security Situation 🔹	Decksele Maddeus	Asset corne	ation Jacobse										
Resource Manager 🔹 🔻	Playbooks Workflows	Worldow Asset connection Instance Management											
Risk Prevention 💌													
Threat Operations	Pendi	ng review 0			1	lot enabled	10		Enabled 1				
Security Orchestration													
Objects													
Playbooks 👩									Status All	* Name	Enter a keyword	q	CĽ⊗
Layouts	Name Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description		Operation	
Plugins	Add the IP indica.	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+08:00	-		Enable More 🔻	
Sellings 💌	Alert notification	Alert	Not enabled	vt	Ø	system	2023/06/08 23 42:32 GMT+08:00	system	2023/06/08 23 42 32 GMT+06:00	-		Enable More 🔻	

- **Step 5** In the **Operation** column of the target playbook, click **Enable**.
- **Step 6** After selecting the playbook version to be enabled, click **OK**.

----End

11.7.1.4 Managing Playbooks

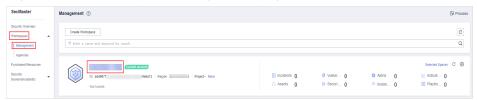
Scenario

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

Figure 11-67 Workspace management page



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

Figure 11-68 Accessing the Playbooks tab

<	Plajboo	oks / Playbooks											
Security Situation	•												
Resource Manager	•	Playbooks Workflows	Asset conner	ction Insta	ince Manage	ment							
Risk Prevention	•												
Threat Operations		Pendir	ng review 0				Not enabled	10		Enabled 1			
Security Orchestration													
Objects													
Playbooks 🕗										Status All	* Name	Enter a keyword.	1 C 🕻 🛛
Layouts		Name Name	Detacless	Playbo 7	7 Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operation	
Plugins		Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+06:00	-	Enable More	
Settings	•	Alert notification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GMT+08:00	system	2023/08/08 23 42 32 GMT+08:00	-	Enable More	

Step 5 On the **Playbooks** tab page, view playbook information.

Figure 11-69 Viewing playbook information

Play	books	Workfle	ows As	set connec	tion	Instance	Management					
		Pending review 0 Not enabled 7					enabled 7		Enabled 1			
	Add	Import							Status All	•	Name Enter a keywor	d Q C 🖸 🗐
		Name	Dataclass	Pl 77	Cur	Monit	Created By	Created	Updated By	Updated At	Description	Operation
		Synchroni,	Alert	Not e		Ø	system	2023/05/07 09:53:30 GMT+08:00	system	2023/05/07 09:53:30 GMT+08:00		Enable More +
		Automatic	Vulnera	Not e	-	۵	system	2023/06/07 09:53:30 GMT+08:00	system	2023/06/07 09:53:30 GMT+08:00		Enable More +
		Automatic	Alert	Not e	-	Ø	system	2023/06/07 09:53:30 GMT+08:00	system	2023/06/07 09:53:30 GMT+08:00	-	Enable More 👻
		Automatic	Alert	Not e		Ø	system	2023/08/07 09:53:30 GMT+08:00	system	2023/05/07 09:53:30 GMT+08:00	-	Enable More 💌
		Capture a	Commo	Enabled	vt	8	system	2023/05/07 09:53:30 GMT+08:00	system	2023/05/07 09:54:55 GMT+08:00	**	Disable Version Management
		Automatic	Alert	Not e	-	۵	system	2023/06/07 09:53:30 GMT+08:00	system	2023/06/07 09:53:30 GMT+08:00	-	Enable More +
		Fetching I	Alert	Not e	-	Ø	system	2023/06/07 09:53:30 GMT+08:00	system	2023/06/07 09:53:30 GMT+08:00	-	Enable More 👻
		Automatic	Alert	Not e		⊠	system	2023/06/07 09:53:30 GMT+08:00	system	2023/05/07 09:53:30 GMT+08:00		Enable More 💌

- The numbers of **Pending review**, **Not enabled**, and **Enabled** playbooks are displayed above the playbook list.
- View the information about existing playbooks.

When there are a large number of playbooks, you can use the search function to quickly search for a specified playbook with search filters such as the status, name, description, or data class of the playbook. Enter a keyword in the search box, and click Q.

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	 Click to view the playbook running monitoring information. 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. Average running duration = Total running duration of instances. Instance Status Statistics: allows you to view the total number of running instances, the number of 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

Table 11-25 Playbook parameters

Step 6 To view details about a playbook, click the name of the playbook.

----End

Exporting Playbooks

D NOTE

SecMaster supports the export of playbooks whose **Status** is **Enabled**.

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

Figure 11-70 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	$$\ensuremath{\mathbb{C}}\xspace$ Total Yanguca $$\ensuremath{\mathbb{V}}\xspace$ for same and layered for same.				C
Purchased Resources Security Governance(beta)		incidents Assets 0	♥ Vulner 0 ⊜ Securl 0	Alerts O Instan	Selected Spaces C 🗟

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

Figure 11-71 Accessing the Playbooks tab

$\langle \cdot \cdot \rangle$	/ Playbo	ooks / Playbooks												
Security Situation	٠	Playbooks Workflows	Asset conner	dian lands	Marana									
Resource Manager	٠		ybooks Workflows Asset connection Instance Management											
Risk Prevention	٠													
Threat Operations	1	Pendi	ng review 0			1	lot enabled	10		Enabled 1				
Security Orchestration	4													
Objects										814 m				
Playbooks 2										Status All	* Name	Enter a keyword	Q	0 ∐ ⊚
Layouts		Name Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description		Operation	
Plugins		Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+06:00	-		Enable More 🔻	
Settings	۳	Alert addition	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GMT+08:00	system	2023/06/08 23 42 32 GMT+08:00	-		Enable More 🔻	

- **Step 5** Select the playbooks to be exported and click \square in the upper right corner of the list. The dialog box for confirming the export is displayed.
- **Step 6** In the dialog box that is displayed, click **OK** to export the playbooks to the local host.

----End

Disabling a Playbook

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

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

Figure 11-72 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspeces	Could Workspace $\overline{\nabla} \mbox{ Inter a name and largered for search}.$				C
Purchased Resources Security Governance(beta)	0 extent to the first to the fi	S Incidents 0 Assets 0	♥ Vulner 0	O Alerts 0 instan 0	Selected Spaces C ⑧ № Indicat 0 9 Playbo 0

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

Figure 11-73 Accessing the Playbooks tab

< / Pie	ajbooks / Playbooks												
Security Situation 🔹 🔻	Playbooks Workflows	Asset conner	ation Instead	ce Manageri									
Resource Manager 🔹 🔻		Asset Colliner	LUUT TIISIM	ce Managen	ien.								
Risk Prevention 🔹													
Threat Operations	Pendi	ng review 0			t i	lot enabled	10		Enabled 1				
Security Orchestration													
Objects									Status Al	* Name			
Playbooks 2									Sidius	* Name	 Enter a keyword 	u u	CĽ⊗
Layouts	Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description		Operation	
Plugins	Add the IP indica.	Alert	Not enabled	٧l	Ø	system	2023/06/08 23 42:32 GWT+08:00	system	2023/06/06 23:42:32 GMT+06:00	-		Enable More 🔻	
Settings •	Alert notification	Alef	Not enabled	v1	Ø	system	2023/06/08 23 42:32 GMT+08:00	system	2023/06/08 23 42 32 GMT+08:00	-		Enable More 🕶	

- **Step 5** In the **Operation** column of the target playbook, click **Disable**. A confirmation dialog box is displayed.
- **Step 6** In the displayed dialog box, click **OK**.

----End

Deleting a Playbook

NOTE

To delete a playbook, the following conditions must be met:

- The playbook is not enabled.
- No activated playbook version exists in the current playbook.
- No running playbook instance exists.
- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-7	4 Workspace	management page	
-------------	-------------	-----------------	--

SecMaster	Management ①				Process
Security Overview Workspaces	Could Workspace $\overline{V} \mbox{ Inter a name and layoutd for search}.$				C
Purchased Resources Security Governance(beta)	Convert accest in additif7, befari2 Region Project- More Not holded.	incidents 0 Assets 0	♥ Vuiner 0 Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⊗ indicat 0 Playbo 0

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

Figure 11-75 Accessing the Playbooks tab

< / P	Playboo	oks / Playbooks													
Security Situation	- I E	Claubanter	Workflows	Asset connect	ing lands										
Resource Manager 🔹		Playbooks 8	nonuons	Asset connect	011 115/2	ice Manager	neni								
Risk Prevention															
Threat Operations			Pendin	g review 0			1	lot enabled	10		Enabled 1				
Security Orchestration	•														
Objects											Status Al		 Enter a keyword. 	0.0	60
Playbooks 💡											Sidilis Al	* Name	 Enter a keywore. 	u c	
Layouts		Nam	e	Detaclass	Playbo D	Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operat	и	
Plugins		A00	the IP indica	Alert	Not enabled	vt	Ø	system	2123/06/08 23:42:32 GMT+06:00	system	2023/06/08 23 42 32 GMT+06:00	-	Enable	More 🔻	
Settings •	, 	Aler	notification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42 32 GMT+08:00	system	2023/06/08 23 42 32 GMT+08:00	-	Enable	More 🔻	

- **Step 5** In the **Operation** column of the playbook to be deleted, click **Delete**.
- **Step 6** In the dialog box that is displayed, click **Confirm** to delete the playbook.

By default, all playbook versions in the current playbook are deleted. The deletion operation cannot be undone. Exercise caution when performing this operation.

----End

11.7.1.5 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

D NOTE

The draft version cannot be previewed.

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

Figure 11-76 Workspace management page

SecMaster	Management ()				Process
Security Overview Workspaces Management Agencies	$$\ensuremath{\mathbb{T}}$$ Crete Workspace $$\ensuremath{\mathbb{T}}$$ Teters a name and largeoid for search.				C
Purchased Resources Security Governance(beta)	D 445977 defa12 Region Peged- More Not holded	 incidents 0 ○ Assets 0 	♥ Vulner 0 Securi 0	o Alerts 0 instan 0	Selected Spaces C 🛞 indicat 0 Flaybo 0

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

Figure 11-77 Accessing the Playbooks tab

<	/ Playb	books / Playbooks											
Security Situation	۳	Playbooks Workflows	Asset corne	ation Inches									
Resource Manager	٠	Playbooks Workflows	Asset Conne	LUOII IIISI2	ince Manage	inen.							
Risk Prevention	٠												
Threat Operations		Pend	ing review 0				lot enabled	10		Enabled 1			
Security Orchestration	•												
Objects													
Playbooks 😕										Status All	* Name	 Enter a keyword. 	QCL
Layouts		Name	Detaclass	Playbo 7	7 Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operatio	6
Plugins		Add the IP indica.	Alert	Not enabled	vt	ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/06 23:42:32 GMT+06:00	-	Enable	Mare 🕶
Settings	۳	Alert notification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GWT+08:00	system	2023/08/08 23 42 32 GWT+08:00	-	Enable	More +

Figure 11-78 Version Management slide-out panel

Name	Dataclass	PI 🏹	Cur	Monit	Created By	Created	Updated By	Updated At	Description	Operation
Capture a	Commo	Not e	-		system	2023/06/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	-	Enable More 🔺
CFW First	Commo	Not e	-	⊠	system	2023/08/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00		Version Management
Automatic	Alert	Not e	-		system	2023/06/24 14:35:51 GMT+08:00	system	2023/05/24 14:35:51 GMT+08:00	-	Delete

- **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

Only playbook versions whose version status is **Unsubmitted** can be edited.

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

Figure 11-79 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspaces	Credit Watapen To fater a name and layword for search.				C
Purchased Resources Security Governance(beta)	Comme accest 6 deterti? belari2 Region Prijed- Mare Not home.	S Incidents 0 Assets 0	♥ Vulner 0	O Alerts 0 instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

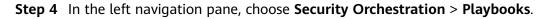


Figure 11-80 Accessing the Playbooks tab

$\langle \cdot \cdot \rangle$	/ Playt	books / Pla	ybooks													
Security Situation	٠	Charles	oks Workflows	Asset connec	tion Inches											
Resource Manager	٠	Playbor		Asset connet	2011 111512	nce Manage	ITRIT.									
Risk Prevention	٠															
Threat Operations	a l		Pendi	ng review 0				Not enabled	10		Enabled 1					
Security Orchestration	*															
Objects											Status Al			0		
Playbooks 💡											Sidius	* Name	Enter a keyword.	ų	С	90
Layouts			Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description	0	iperation		
Plugins Settinos	Ţ		Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/08/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+06:00	-	E	nable More 🔻		
semals	*		Alert notification	Alert	Not enabled	vt	8	system	2023/08/08 23 42:32 GWT+08:00	system	2023/06/08 23 42 32 GMT+06:00	-	E	nable More 🕶		

Figure 11-81 Version Management slide-out panel



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

Figure	11-82	Workspace	management	page

SecMaster	Management ①				🕞 Process
Security Overview Workspaces	Crede Workspace $\overline{V} \mbox{ Iters a name and layound for search}.$				C
Purchased Resources Security Governance(beta)	Conserver Conserver	 Incidents 0 △ Assets 0 	♥ Vulner 0 ⊜ Securi 0	 Alerts Instan 0 	Selected Spaces C (*) V Indicat () Playbo ()

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

Figure 11-83 Accessing the Playbooks tab

$\langle \cdot \cdot \rangle$	/ Playb	ooks / Play	books												
Security Situation	٠	Charles	ks Workflows	Asset connec	tion Inches										
Resource Manager	*	Playboo	3 100000	Asset connet	2011 111512	ince Manage	ment								
Risk Prevention															
Threat Operations	a l		Pendir	ng review 0			1	Not enabled	10		Enabled 1				
Security Orchestration	•														
Objects											Status Al	v Name	 Enter a keyword. 	Q C	
Playbooks 💡											Janua M	• Natio	 Dian a neywork. 	U	JUJ
Layouts			Name	Detaclass	Playbo 7	7 Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operat	08	
Plugins			Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/08/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+06:00	-	Enable	More +	
Settings	*		Alert notification	Alert	Not enabled	vt	۲	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+08:00	-	Enable	More +	

Figure 11-84 Version Management slide-out panel



Step 6 On the **Version Management** page, in the version information area, locate the row containing the desired playbook version, and click **Activate** or **Deactivate** in the **Operation** column.

----End

Copying a Playbook Version

NOTE

Only playbook versions in the **Activated** or **Inactive** state can be copied.

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

Figure 11-85 Workspace management page

SecMaster	Management () (P Pix	icess
Security Overview Workspaces	Center Windpaper C If later and adjusted for search. C	2
Purchased Resources Security Governance(beta)	Control Baseco Control Baseco C Selected Taseco C C Selected Taseco C C Selected Taseco C C Selected Taseco Selected Taseco Selected Tasecoo Sel	9

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

Figure 11-86 Accessing the Playbooks tab

<	/ Playboo	oks / Playbo	oks												
Security Situation Resource Manager		Playbooks	Workflows	Asset connec	tion Insta	nce Manager	nent								
Risk Prevention Threat Operations Security Orchestration	,		Pendin	ng review O			Ν	lot enabled	10		Enabled 1				
Objects Playbooks											Status Al	* Name	• Enter a keyword.	Q	c 🛯 🛛
Layouts Plugins			Name Add the IP indica	Detacless Alert	Playbo 7	Current	Monitoring	Created By system	Created 2023/06/08 23 42:32 GMT+08:00	Updated By system	Updated At 2023/08/08 23 42 32 GMT+08:00	Description		iperation nable More +	
Settings	٠		Alert notification	Alert	Not enabled	vt	Ø	system	2023/06/08 23 42:32 GMT+08:00	system	2023/08/08 23 42 32 GMT+08:00	-	6	nable More 🔻	

Figure 11-87 Version Management slide-out panel

Name	Dataclass	Pl 77	Cur	Monit	Created By	Created	Updated By	Updated At	Description	Operation
Capture a	Commo	Not e		ø	system	2023/06/24 14:35:51 GMT+08:00	system	2023/05/24 14:35:51 GMT+08:00	-	Enable More .
CFW First	Commo	Not e	-	ø	system	2023/06/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	-	Version Management
Automatic	Alert	Not e	-		system	2023/08/24 14:35:51 GMT+08:00	system	2023/06/24 14:35:51 GMT+08:00	- !	Delate

- **Step 6** On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Copy** in the **Operation** column.
- **Step 7** In the dialog box that is displayed, click **OK**.

----End

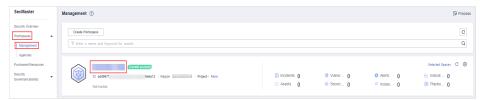
Deleting a Playbook Version

NOTE

To delete a playbook version, the following conditions must be met:

- The playbook version is inactivated.
- No running playbook version instance exists.
- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-88 Workspace management page



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

Figure 11-89 Accessing the Playbooks tab

< / Playb	icks / Playbooks											
Security Situation 🔹	Playbooks Workflows	Asset corne	elies Jacobs									
Resource Manager 🔹 🔻	Playbooks Workflows	Asset conne	ction insta	nce Manage	nent							
Risk Prevention 🔻												
Threat Operations	Pendi	ng review 0			1	Not enabled	10		Enabled 1			
Security Orchestration												
Objects												
Playbooks									Status	* Name	 Enter a keywo 	n. Q C E
Layouts	Name Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description		Operation
Plugins	Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+08:00	-		Enable More •
Settings 💌	Alert redification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GMT+08:00	system	2023/06/08 23 42 32 GMT+08:00	-		Enable More 💌

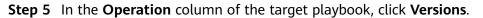


Figure 11-90 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Delete** in the **Operation** column.

NOTE

After a playbook version is deleted, it cannot be retrieved. Exercise caution when performing this operation.

----End

11.7.2 Workflows

11.7.2.1 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-91 Workspace management page



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

Figure 11-92 Workflows tab page

	/ Playb	coks / Workflow	15														
Security Stuation Resource Manager	* *	Playbooks	Workflows	Asset connection	Instance Manage	ement											
Risk Prevention Threat Operations Security Orchestration	, J		Pending	g review O			Not enable	d 14			Enable	d 20					
Objects Playbooks											Status		• Name	¥		Q	c Ľ
Layouts Plugins Settings	¥		Name Alert notification via att ef9423	tack link analysis 3a617167	Dataclass	Workflo 7 Enabled	7 Workflo Y General	7 Current	Created	Created 2023/08/08 23:42:38 G	Update system	Updated At 2023/08/08 23:42:40 G	Description		Operation Disable Version Manager	vent	
			One-click release ae14t	62e902f	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:41 G	-		Enable Version Managerr	ent Dele	He

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-93 Version Management page

dd Import							Status	AL	v Name v	Enter a keyword. Q	СС
Name	Dataclass	Workflo 🍞	Workto	Current	Created	Created	Updated	Updated At	Description	Operation	
One-click host isolation 55ec0432-fc83-3fc1-8139-8360e410a68	Alert	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:58		Disable Version Management	
HastDefenseAlarmsAreAssociatedWithHistoricaHan 3e83c325-b8ta-350c-ac72-583abet/8864	Alert	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:27:11		Disable Version Management	
Policy Management - Policy Delivery IAM Decapsulat 20(2025b-07d5-3570-b046-110bs/2b1x005	Policy	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:57	-	Disable 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 11-26** describes the parameters.

Parameter	Description
Comments	 Select the review conclusion. If the workflow version is approved, the status of the workflow version changes to Activated.
	 Reject. After the workflow version is rejected, the status of the workflow version changes to Rejected. You can edit the workflow version and submit it again.
Reason for rejection	Enter the review comment. This parameter is mandatory when Reject is selected for Review Comment.

Table 11-26 Workflow review parameters

NOTE

- You can edit a rejected workflow version. For details, see Managing Workflow Versions.
- Workflow version status change:

If the current workflow has only one workflow version, the status of the approved workflow **version** is **Activated** by default.

Step 8 Click OK to complete the workflow version review.

----End

Follow-up Operations

An approved workflow version needs to be enabled. For details, see **Enabling a Workflow**.

11.7.2.2 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-94 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspaces Management Agencies	Could Workspace If force a name and layword for watch.				C
Purchased Resources Security Governance(beta)	Convert econor	 Incidents 0 Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 indicat 0 Playbo 0

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

Security Situation	٠	Discharder	Workflows	Asset connection												
Resource Manager	٠	Playbooks	WORNOWS	Asset connection	Instance Manag	ement										
Risk Prevention	*															
Threat Operations	<u>,</u>		Pending	review 0			Not enable	ed 14			Enabled	20				
Security Orchestration	•															
Objects																
Playbooks 👔											Status	All	* Name	 Enter a keywo 	rd. Q	С
Layouts		. N	ame		Dataclass	Workflo	Vorkflo	V Current	Created	Created	Update	Updated At	Description	Operation		
Plugins lettings			lert notification via att 19423	ack link analysis 3a617167	Alert	Enabled	General	vt	system	2023/08/08 23:42:38 G	system	2023/06/06 23:42:40 G	-	Disable Ve	rsion Management	
			ne-click release e14t	026902	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/06/06 23:42:41 G	-	Enable Ver	sion Management G	Delete

Figure 11-95 Workflows tab page

Step 5 In the row containing the target workflow, click **Enable** in the **Operation** column.

Figure 11-96 Enabling a workflow

							Status	Al	*	Name	 Enter a keyword. 	Q	С	C
Name	Dataclass	Workflo 7	Workflo 7	Current	Created	Created	Update	Updated At	Descrip	tion	Operation			
WAF interception 5e578242-2119-365-9d2b-6f317ba7d6e8	Alert	Not enabled	General	v1	system	2023/06/24 14:35:56 G	system	2023/06/24 14:38:59 G	-		Enable Version Management	Delete		
VPC Asset Connector 8548eaba-3d5c-3076-011b-afd969ba6f3e	CommonC	Not enabled	General	vt	system	2023/06/24 14:35:56 G	system	2023/06/24 14:38:57 G	-		Enable Version Management I	Delata		
CFW First External Alarm 8ca18/75-5987-3bd4-a1cf-a17e4f55bd1e	CommonC	Not enabled	General	vt	system	2023/06/24 14:35:56 G	system	2023/06/24 14:36:58 G	-		Enable Version Management I	Delate		

Step 6 In the slide-out panel that is displayed, select the workflow version to be enabled and click **OK**.

----End

11.7.2.3 Managing Workflows

Scenario

This section describes how to manage workflows, including **Viewing Workflows**, **Exporting Workflows**, **Deleting Workflows**, and **Disabling a Workflow**.

Viewing Workflows

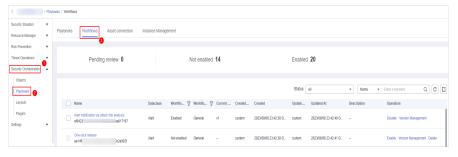
- **Step 1** Log in to the management console.
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-97 Workspace management page

SecMaster	Management () (Process
Security Overview Workspaces	Centri Vinnapes C If for a name and lapsed for reach. Q
Purchased Resources Security Governance(beta)	Image: Construction Second Space C O 0 add0077 Media12 Paged-Mare III Incodents 0 O Alerts 0 Imaged-Mare D Incodents 0 Alerts 0 Biscodents 0 Imaged-Mare D

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

Figure 11-98 Workflows tab page



Step 5 On the Workflow Management page, view the information about the created workflow.

Figure 11-99 Viewing workflows

Pending review 0		N	ot enabled	10			Enabled	15				
						Status	All	•	Name •	Enter a keywo	d. Q	C
Name	Dataclass	Workfl 🍸	Workfl	Curren	Create	Created	Updat	Updated At	Description	Operatio	on	
Automatic renaming of alarm names 02b1b5d8-20a3-32dc-a02c-044db9a2e232	Alert	Not enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:54		Enable	Version Management	Delete
Automatic security blocking of WAF attacks 2c8958aa-84db-36c2-8992-6c7f16d33e49	Alert	Not enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:54	-	Enable	Version Management	Delete
ECS Assel Connector 2fbe000-80c8-3c3e-993e-50f0183ecd17	Common	Enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:55	-	Disable	Version Management	
Vulnerability fixing 463def0b-9539-37f2-bbdd-761c9c59264f	Vulnerability	Not enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:55	-	Enable	Version Management	Delete
WebSite Asset Connector 4b2535b7-d17b-37ec-a631-a36fe0420062	Common	Enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:55	-	Disable	Version Management	
RDS Asset Connector 6919dc48-d534-3723-b38f-76091a00e5fb	Common	Enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:55		Disable	Version Management	
WAP interception 90219a8e-1b64-316e-aa88-3f028cb4de0f	Alert	Not enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:55		Enable	Version Management	Delete
EIP Asset Connector 99143tdf-82a4-3da2-a076-23ed63020c88	Common	Enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:55		Disable	Version Management	
Automatic notification of high-risk alerts 9bc890dd-066a-3486-8121-6077e1fb4bd2	Alert	Not enabled	General	vt	system	2023/06/07 09:54:52	system	2023/06/07 09:54:54		Enable	Version Management	Delete

- The numbers of **Pending review**, **Not enabled**, and **Enabled** workflows are displayed above the workflow list.
- View information about existing workflows in the workflow list.

If there are a large number of workflows, you can select the workflow status, name, description, or data class, enter a keyword in the search box, and click Q to quickly search for a specified workflow.

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.

Table 11-27 Workflow parameters

Step 6 To view details about a workflow, click the name of the workflow to access its details page.

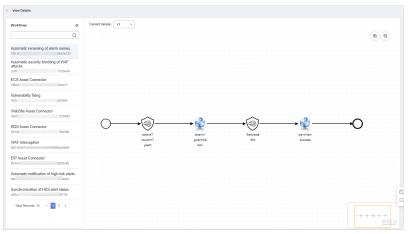


Figure 11-100 Workflow details

----End

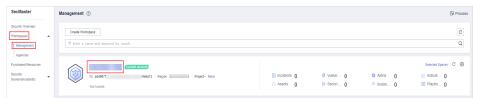
Exporting Workflows

NOTE

Workflows in the **Enabled** state can be exported.

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

Figure 11-101 Workspace management page



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

Figure 11-102 Workflows tab page

\leq	1 Phylocia / Hordows															
Security Situation Resource Manager	* *	Playbooks	Workflows	Asset connection	Instance Manag	ement										
Risk Prevention Threat Operations Security Orchestration	•		Pendin	g review O			Not enable	d 14			Enable	1 20				
Objects Playbooks											Status		• Name	¥		Q C E
Layouts Plugins Settings	¥		arme lert notification via at 9423	tack link analysis 3a617167	Dataclass Alert	Workflo 1	Workflo ۲ General	7 Current	Created	Created 2023/08/08 23:42:38 G	Update system	Updated At 2023/08/08 23:42:40 G	Description		Operation Disable Version Manageme	nt
			ne-click release e14t	b2e902f	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:41 G	-		Enable Version Management	nt Delete

- **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

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

Figure 11-103 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	$\begin{tabular}{ c c c c } \hline \mbox{Cruth Woltspace} \\ \hline \end{tabular} $				Q
Purchased Resources Security Governance(beta)	California concel 0 ex66977 Media2 Region Project- More Not feeded.	Incidents 0 Assets 0	 ♥ Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

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

Figure 11-104 Workflows tab page

<	/ Playt	books / Workflows													
Security Situation	٠	Playbooks	Workflows	Asset connection	Instance Manao	amont									
Resource Manager	٠	riayuuusa		Asser connection	matarice manag	unon									
Risk Prevention	٠														
Threat Operations	o		Pending	g review 0			Not enabled	14			Enable	d 20			
Security Orchestration	1														
Objects											Status		* Name	 Enter a keyword. 	QCI
Playbooks 2											010103	~	• Isane	 Enter a Neywork. 	
Layouts		Na Na	ame		Dataclass	Workflo	7 Workflo 7	Current	Created	Created	Update	Updated At	Description	Operation	
Plugins Settings	Ŧ		lert notification via att 9423	lack link analysis 3a617167	Alert	Enabled	General	vt	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:40 G	-	Disable Version Manaj	gement
			ne-click release e14t	62e902f	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/06/06 23:42:41 G	-	Enable Version Manag	ement Delete

- **Step 5** On the **Workflows** tab page, locate the row containing the target workflow and click **Delete** in the **Operation** column.
- Step 6 Click OK to delete the workflow.

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

Figure 11-105 Workspace management page



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

Figure 11-106 Workflows tab page

<	/ Playb	ooks / Workflours													
Security Stuation Resource Manager	* *	Playbooks	Workflows	Asset connection	Instance Manage	ement									
Risk Prevention Threat Operations Security Orchestration	Ţ		Pending	g review O		P	lot enabled	14			Enabled	20			
Objects Playbooks 2		Na	urna		Dataclass	Washing 🗸	Workflo 7	Current	Crowlad	Crowlad	Status	All Updated At	• Name Description	Enter a keyword. Operation	QCĽ
Plugins Settings	•	A	ert notification via att 9423	ack link analysis 3a617167	Alert	Enabled	General	v1	system	2023/08/08 23:42:38 G	system	2023/06/06 23:42:40 G		Disable Version Mane	gement
			ne-click release r14t	626902/	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:41 G	-	Enable Version Manaj	pement Delete

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

11.7.2.4 Managing Workflow Versions

Scenario

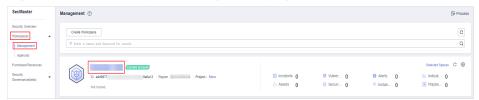
This section describes how to manage workflow versions, including **Copying a Workflow Version**, **Editing a Workflow Version**, **Submitting a Workflow Version**, **Activating/Deactivating a Workflow Version**, and **Deleting a Workflow Version**.

Copying a Workflow Version

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-107 Workspace management page



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

Figure 11-108 Workflows tab page

$\langle \cdot $	/ Playb	coks / Workflous													
Security Situation Resource Manager	• •	Playbooks	Workflows	Asset connection	Instance Manag	ement									
Risk Prevention	٠														
Threat Operations	ď		Pendin	ig review 0			Not enabled	14			Enabled	20			
Security Orchestration	•														
Objects											Status		* Name	 Enter a keyword. 	QCC
Playbooks											oraius	All	• Name	 Enter a keyword. 	Q C D
Layouts		N	ame		Dataclass	Workflo)	Workflo 7	Current	Created	Created	Update	Updated At	Description	Operation	
Plugins Settings	•		lert notification via at 19423	tack link analysis 3a617167	Alert	Enabled	General	vt	system	2023/08/08 23:42:38 G	system	2023/06/06 23:42:40 G	-	Disable Versi	on Management
			ne-click release e14t	b2e902f	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:41 G	-	Enable Versio	n Management Dalete

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-109 Version Management page

A	d Import							Status	Al	• Name •	Enter a keyword.	o c Ľ
	Name	Dataclass	Workflo P	Workflo 5	Current	Created	Created	Updated	Updated At	Description	Operation	
	One-click host isolation 55ec9432-tc83-3tc1-8139-#350b410e68	Alert	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:58		Disable Version Management	ut.
	HostDefenseAlarmsAnaAccociatedWithHistoricaHan 3e93c325-b95a-359c-ac72-5fc3abeb9864	Alert	Enabled	General	vt	system	Feb 25, 2024 14:25:55	system	Feb 25, 2024 14:27:11	-	Disable Version Manageme	n
	Policy Management - Policy Delivery IAM Decapsulat 20x2025b-07d5-3578-b846-110bx2b1x005	Policy	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:57		Disable Version Manageme	n

- **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

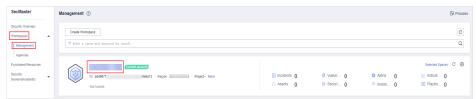
NOTE

You can only edit a workflow version whose version status is **To be submitted** or **Rejected**.

Step 1 Log in to the management console.

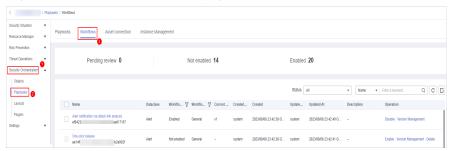
- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-110 Workspace management page



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

Figure 11-111 Workflows tab page



Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-112 Version Management page



- **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.

Param	eter		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.

Param	ator		Description					
Paralli			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 11-29 describes the UserTask parameters.					
		SubProcess	Another workflow is started to perform cyclic operations. It is equivalent to the loop body in the workflow.					
	System Gatew ay	ExclusiveGa teway	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.					
		ParallelGate	During line distribution, all lines are executed.					
					way	During line aggregation, the subsequent nodes are executed only when all the lines arrive. (If one line fails, the entire workflow fails.)		
		InclusiveGat eway	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.)					
Workfl	Workflows		You can select all released workflows in the current workspace.					
Plug-in	Plug-ins		You can select all plug-ins in the current workspace.					

Table 11-29 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.
	 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-113 Workspace management page

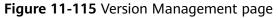
SecMaster	Management 🕥				Process
Security Overview Workspeces Management Agencies	Owned Wanspaces If father a name and keywood for search.				C
Purchased Resources Security Governance(beta)	Constant scores	⊡ Incidents 0 ○ Assets 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞

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

Figure 11-114 Workflows tab page

< / P	Asybo	oks / Workflows											
Security Situation Resource Manager Risk Prevention		Playtoolis Notifices Asset connection Instance Management											
Threat Operations	·	Pending review 0			Not enable	d 14			Enabled	20			
Objects Playbooks									Status	AL	• Name	 Enter a keyword. 	CC
Layouts		Name	Dataclass	Workflo 7	7 Workflo	Current	Created	Created	Update	Updated At	Description	Operation	
Plugins Settings v		Alert notification via attack link analysis ef9423 isa617167	Alert	Enabled	General	vt	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:40 G	-	Disable Version Management	
		One-click release ae141 b2e902r	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/06/08 23:42:41 G	-	Enable Version Management	Delete

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.



Add	Import							Status	Al	• Name •	Enter a keyword.	QCL
- N	lame	Dataclass	Workflo 🍞	Workflo	Current	Created	Created	Updated	Updated At	Description	Operation	
	ine-click host isolation 5ec9432-fc83-3fc1-8139-f93606410e58	Alert	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:58	-	Disable Version Managemen	3
	lostDefense Alarms Are Accorciate dWItH Istorica Han e93c325 6/5a-359c-ac72-5fs3abeb9k64	Alert	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:27:11	-	Disable Version Managemen	
	olicy Management - Policy Delivery IAM Decapsulat ox2025b-07d5-3578-b046-110bx2b1x005	Policy	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:57	-	Disable Version Managemen	

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.

Version Man	agement					×
Basic Informa	tion					
Workflow name			Dataclass	PolicyRecor	rd	
Workflow type	General		Workflow status	Enabled		
Created By			Created	2023/10/24	09:17:10 GMT+08:00	
Updated By			Updated At	2023/10/24	09:17:47 GMT+08:00	
Version Inform	nation					
Version	Status	Resu	Ilts Descriptio	on	Operation	
Draft Version	TDraft	-	-		Edit Submit Delete	
v1	Activate	ed	-		Deactivate Clone	

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.

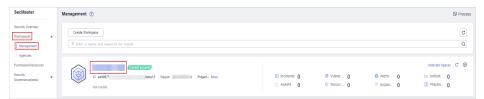
----End

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

Figure 11-117 Workspace management page



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

Figure 11-118 Workflows tab page

<	/ Playb	ooks / Workflows													
Security Stuation Resource Manager	•	Playbooks	Payboxs Transform Asset connection Instance Management												
Risk Prevention Threat Operations Security Orchestration	•		Pending	g review O		ľ	Not enabled	14			Enabled	20			
Objects Playbooks											Status	AL	* Name	💌 Enter a keyword.	QCĽ
Layouts Plugins Settings			ert notification via att 9423	lack link analysis 3a617167	Dataclass Alert	Workflo 7	Workflo 🖓 General	Current	Created	Created 2023/08/08 23:42:38 G	Update system	Updated At 2023/08/08 23:42:40 G	Description	Operation Disable Versio	n Management
Guarge			ne-click release 141	62e902f	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:41 G	-	Enable Versio	n Management Delete

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-119 Version Management page

Add Import							Status	Al	* Name *	Enter a keyword. Q
Name	Dataclass	Workflo 🍞	Workflo 🍞	Current	Created	Created	Updated	Updated At	Description	Operation
One-click host isolation 55ec9432-fc63-3tc1-8139-93506410e58	Aiert	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:58	-	Disable Version Management
HastDakmanAarmaAvaAasociatedWithHistoricaHan 3e93c325 065e-359c ec72-563abet9864	Alert	Enabled	General	vt	system	Feb 25, 2024 14:25:55	system	Feb 26, 2024 14:27:11	-	Disable Version Management
Policy Management - Policy Delivery IAM Decapsulat 20x2025b-07d5-3578-b846-110bx2b1x005	Policy	Enabled	General	vt	system	Feb 26, 2024 14:26:56	system	Feb 26, 2024 14:26:57	-	Disable 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.

Figure 11-120 Example deactivating a workflow version

Version Man	agement					
Basic Informa	tion					
Workflow name		Da	taclass	Alert		
Process type	Common	Pro	ocess status	Unabled		
Created By		Cre	eated	2022/11/30 16:43	3:12 GMT+08:00	
Modified By		Up	dated	2022/11/30 16:4	5:44 GMT+08:00	
Version Inforn	nation					
Version	Version Status	Debug	Descriptio	n O	peration	
Draft Version	To be submitted	i		E	dit Submit Delete	
v1	Activated			D	eactivate Clone	

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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.
 - Figure 11-121 Workspace management page

SecMaster	Management ()				Process
Security Overview Workspaces Management Agencies	Crede Workspace $\label{eq:states} \overline{\mathcal{V}} \mbox{ Inter an and layouth for search}.$				C
Purchased Resources Security Governance(beta)		incidents 0	 ◊ Vulner 0 ⊜ Securl 0 	O Alerts O instan O	Selected Spaces C

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

Figure 11-122 Workflows tab page

	/ Playb	coks / Workflours												
Security Situation	٠	Playbooks Workflow	Asset connection	Instance Manag	amant									
Resource Manager	۳	Holinon	3	materice menag	periodit.									
Risk Prevention	۳													
	ŏ	Pen	ding review 0			Not enable	14			Enable	d 20			
	*													
Objects										Status	40	* Name	 Enter a keyword. 	QCD
Playbooks 2														
Layouts		Name		Dataclass	Workflo 7	7 Workflo Y	Current	Created	Created	Update	Updated At	Description	Operation	
Plugins Settings	•	er9423	ia attack link analysis sa617167	Alert	Enabled	General	vt	system	2023/08/08 23:42:38 G	system	2023/06/06 23:42:40 G	-	Disable Version Man	agement
		One-click release ae14t	6269021	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/06/06 23:42:41 G	-	Enable Version Man	agement Dalete

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-123 Version Management page

 Add
 Tapot
 Status
 Add
 File
 Status
 Construct
 CO
 CC
 C

Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Delete** in the **Operation** column. In the dialog box displayed, click **OK**.

D NOTE

Deleted workflow versions cannot be retrieved. Exercise caution when performing this operation.

----End

11.7.3 Asset Connections

11.7.3.1 Adding an Asset Connection

Scenario

This topic describes how to create an asset.

Procedure

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

Figure 11-124 Workspace management page

SecMaster	Management 💿			Process
Security Overview Workspaces	$\label{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \vspace{-1.5} \rspace{-1.5} \vspace{-1.5} \vspace$			C
Purchased Resources Security Governance(beta)] Incidents 0 ♥ Vulne Assets 0	•	

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-125 Asset connection tab

< / / Playbook Mar	nagemi	ent / Asset connection											
Security Situation	•	Plavbooks Workflo	ws Asset conner	tion Instance Ma	anagement								
Resource Manager	•		· • • • • • • • • • • • • • • • • • • •										
Risk Prevention	×	Add								С			
Threat Operations	٠	V Search by name								Q			
Security Orchest	•	Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation				
Object Management		Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation				
Playbook		Alert handling meth	SecMasterBiz	system	2023/06/24 14:35:52 GMT	-	-	Alert handling method set	Edit Delete				
Management		VPC authentication	ACL	system	2023/06/24 14:35:52 GMT	-	-	VPC authentication	Edit Delete				
Layout management		SMN notification to	нттр	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for operat	Edit Delete				
		SecMaster authenti	HTTP	system	2023/06/24 14:35:52 GMT			SecMaster authentication token	Edit Delete				
	•	CFW authentication	HTTP	system	2023/06/24 14:35:52 GMT	-		CFW authentication token	Edit Delete				

- **Step 5** On the **Asset Connection** tab page, click **Add**. The slide-out panel **Add** is displayed on the right.
- **Step 6** On the panel, set asset connection parameters. For details about the parameters, see **Table 11-30**.

Parameter	Description
Connection Name	Enter an asset connection name. The naming rules are as follows:
	 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 .
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.

Table 11-30 Asset connection parameters

Step 7 Click **OK**. You can query the created asset connection in the asset connection list. ----**End**

11.7.3.2 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 left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-126 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Crede Watspace T fatter a name and layword for search.				C Q
Purchased Resources Security Governance(beta)	Order const	incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ Indicat 0 El Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-127 Asset connection tab

< / / Playbook Management / Asset connection												
Security Situation	•	Playbooks Workflows Asset connection Instance Management										
Resource Manager												
Risk Prevention	*											
Threat Operations	-	Add								С		
Security Orchest 📵		V Search by name								0		
Object Management		Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation			
Playbook		Alert handling meth	SecMasterBiz	system	2023/06/24 14:35:52 GMT	-	-	Alert handling method set	Edit Delete			
Management		VPC authentication	ACL	system	2023/06/24 14:35:52 GMT	-		VPC authentication	Edit Delete			
Layout management		SMN notification to	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for operat	Edit Delete			
Plugin Management Settings		SecMaster authenti	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SecMaster authentication token	Edit Delete			
		CFW authentication	HTTP	system	2023/06/24 14:35:52 GMT	-	-	CFW authentication token	Edit Delete			

Step 5 On the **Asset connection** tab page, view information about existing asset connections.

If there are a large number of asset connections, you can use the search function to quickly search for a specified asset connection: Filter asset connections by connection name, plug-in, creator, creation time, person who modified the connection, update time, or description of an asset connection, enter a keyword in the search box, and click Q.

Figure 11-128 Viewing asset connections

Add								С
𝒫 Search by name								Q
Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation	
Alert handling meth	SecMasterBiz	system	2023/06/24 14:35:52 GMT	-	-	Alert handling method set	Edit Delete	
VPC authentication	ACL	system	2023/06/24 14:35:52 GMT	-	-	VPC authentication	Edit Delete	
SMN notification to	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for operat	Edit Delete	
SecMaster authenti	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SecMaster authentication token	Edit Delete	
CFW authentication	HTTP	system	2023/06/24 14:35:52 GMT	-	-	CFW authentication token	Edit Delete	
SMN notification to	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for handl	Edit Delete	
WAF authentication	HTTP	system	2023/06/24 14:35:52 GMT	-	-	WAF authentication token	Edit Delete	
DBSS authenticatio	DBSS	system	2023/06/24 14:35:52 GMT	-	2023/04/13 22:28:25 GMT	DBSS authentication token	Edit Delete	
HSS authentication	HSS	system	2023/06/24 14:35:52 GMT			HSS authentication token	Edit Delete	
ECS authentication	ECS	system	2023/06/24 14:35:52 GMT			ECS authentication token	Edit Delete	
10 💌 Total Recor	ds: 17 🛛 < 🚺 2 🍑							

 Table 11-31
 Asset connection parameters

Parameter	Description					
Connection Name	Asset connection name					
Plug In	Plug-in corresponding to the asset connection					
Created By	User who creates an asset connection					
Created	Time when an asset connection is created					
User who last updated the information	User who modifies the asset connection last time					
Updated	Time when the asset connection was last updated					
Description	Description of the asset connection					

Parameter	Description
Operation	You can perform operations such as editing and deleting in the Operation column.

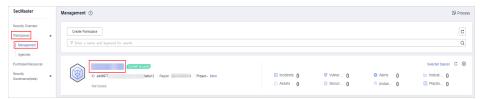
Step 6 To view details about an asset connection, click the name of the asset connection. The slide-out panel **Detail** is displayed.

----End

Editing an Asset Connection

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

Figure 11-129 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-130 Asset connection tab

< / / Playtook Management / Asset connection													
Security Situation	ation - Playbooks Workflows Asset connection Instance Management												
Resource Manager	•												
Risk Prevention	٠										С		
Threat Operations	٠		Add V Search by name								Q		
Security Orchest	*										ų		
Object Management			Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation			
Playbook 2			Alert handling meth	SecMasterBiz	system	2023/06/24 14:35:52 GMT	-	-	Alert handling method set	Edit Delete			
Management			VPC authentication	ACL	system	2023/06/24 14:35:52 GMT	-	-	VPC authentication	Edit Delete			
Layout management			SMN notification to	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for operat	Edit Delete			
Plugin Management Settings			SecMaster authenti	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SecMaster authentication token	Edit Delete			
			CFW authentication	HTTP	system	2023/06/24 14:35:52 GMT	-	-	CFW authentication token	Edit Delete			

- **Step 5** In the row containing a desired asset connection, click **Edit** in the **Operation** column. The slide-out panel **Edit** is displayed.
- **Step 6** On the **Edit** panel, edit asset connection parameters. For details about the parameters, see **Table 11-32**.

Parameter	Description
Connection Name	Enter an asset connection name. The naming rules are as follows:
	 Only uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and underscores (_) are allowed.
	A maximum of 64 characters are allowed.
Description	(Optional) Enter the asset connection description. The description can contain a maximum of 64 characters.
Plug In	Select the plug-in required for asset connection. For details about the plug-in, see Viewing Plug-in Details.
Created By	Creator of the asset connection. This parameter cannot be modified .
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.

 Table 11-32
 Asset connection parameters

Step 7 Click OK.

----End

Deleting an Asset Connection

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

SecMaster	Management ③				Process
Security Overview Workspeces	$\label{eq:product} \fbox{\begin{tabular}{lllllllllllllllllllllllllllllllllll$				C
Purchased Resources Security Governance(beta)	Constances O add0077 Adda12 Region Prijed- More Not hold:	Incidents 0 Assets 0	♥ Vulner 0	O Alerts 0 instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-132 Asset connection tab

< / / Playbook Ma	nagement	/ Asset connection								
Security Situation	•	Plavbooks Workflov	is Asset connec	tion Instance Ma	inagement					
Resource Manager	•			8						
Risk Prevention	*	Add								c
Threat Operations	*									
Security Orchest		V Search by name								Q
Object Management		Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation	
Playbook 2		Alert handling meth	SecMasterBiz	system	2023/06/24 14:35:52 GMT	-	-	Alert handling method set	Edit Delete	
managaman		VPC authentication	ACL	system	2023/06/24 14:35:52 GMT			VPC authentication	Edit Delete	
Layout management		SMN notification to	нттр	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for operat	Edit Delete	
		SecMaster authenti	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SecMaster authentication token	Edit Delete	
		CFW authentication	HTTP	system	2023/06/24 14:35:52 GMT	-		CFW authentication token	Edit Delete	

- **Step 5** Locate the row that contains a desired asset connection, click **Delete** in the **Operation** column.
- **Step 6** In the deletion confirmation dialog box that is displayed, click **OK** to confirm the deletion.

NOTE

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

----End

11.7.4 Instance Management

11.7.4.1 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.

Limitations and Constraints

The maximum number of retries within a day for a single workspace of a single account is as follows:

- Manual retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
- API retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-133 Workspace management page

SecMaster	Management () (Process
Security Overview Workspaces	Center Westspace C T fator a name and layout for search. Q
Purchased Resources Security Governance(beta)	Stelecter Spaces C @ D add0777, Stadar12 Region Project- More Not hold. Project- More C @ Valuer0 D Aterts 0 IM Indicat0 D Region0 D Regi

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Instance Management** tab.

Figure 11-	134 In	stance	Management	page

		/ Playt	book Management / Ins i	iance Management								
Security Situation	٠	Play	book Workflow	Asset connecti	on Instance Mar	nagement						
Resource Manager	٠											
Risk Prevention	٠					Instance	Creation Time	Start Date - End Date	Playbook Nat	me ▼ Entera	kevanri () C
Security Response	٠											
Security Orchest			Instance Name	Playbook Name	Data Class	Trigger Mode 🏼 🎖	Status 🎖	Context	Instance Creation Time	Instance End Time	Operation	
Object Management			-12-20		Alert	Event Trigger	Succeeder	1 -	2022/12/08 15:21:55 GM	2022/12/08 15:23:41 GM	Terminate Retry	
Playbook 2 Management			-v2-20		Alert	Event Trigger	🖉 Succeeder	i –	2022/12/08 15:21:55 GM	2022/12/08 15:23:41 GM	Terminate Retry	
Layout managemen			v2·20		Alert	Event Trigger	Succeeder	1 -	2022/12/08 15:20:15 GM	2022/12/08 15:20:20 GM	Terminate Retry	
Settings	•		-v2-20		Alert	Event Trigger	🖉 Succeeder	i –	2022/12/08 15:20:14 GM	2022/12/08 15:20:20 GM	Terminate Retry	
			-12-20		Alert	Event Trigger	Succeeder	i -	2022/12/08 15:18:34 GM	2022/12/08 15:20:20 GM	Terminate Retry	

Step 5 In the instance management list, view the instance name, playbook name, and data class. For details about the parameters, see **Table 11-33**.

Figure 11-135 Instances

			Instance C	reation Time Start Da	te End Date	Playbook Nam	e v Enter	a keyword. Q	0
Instance Name	Playbook Name	Data Class	Trigger Mode 🖓	Status 🍞	Context	Instance Creation Time	Instance End Time	Operation	
CSZMGJCF-v1-20		Alert	Event Trigger	Running		2022/11/30 16:48:35 GM	-	Terminate Retry	
GJCF1-v3-202211	1 V3	Alert	Event Trigger	Running	-	2022/11/30 15:28:40 GM	-	Terminate Retry	
GJCF1-v3-202211	+ t V3	Alert	Event Trigger	Running		2022/11/30 15:28:30 GM	-	Terminate Retry	
GJCF1-v3-202211	¥3	Alert	Event Trigger	Succeeded	-	2022/11/30 15:28:30 GM	2022/11/30 15:33:32 G	Terminate Retry	
GJCF1-v3-202211	1 13	Alert	Event Trigger	Running	-	2022/11/30 15:28:30 GM		Terminate Retry	
GJCF1-v3-202211	4 V3	Alert	Event Trigger	Running	-	2022/11/30 15:28:30 GM	-	Terminate Retry	
GJCF1-v2-202211	¥2	Alert	Event Trigger	Succeeded	-	2022/11/30 15:16:52 GM	2022/11/30 15:16:54 G	Terminate Retry	
0JCF1-v2-202211	1 2	Alert	Event Trigger	Succeeded	-	2022/11/30 15:16:50 GM	2022/11/30 15:28:34 G	Terminate Retry	
GJCF1-v2-202211	1 12	Alert	Event Trigger	Succeeded	-	2022/11/30 15:16:49 GM	2022/11/30 15:28:33 G	Terminate Retry	
10 • Total Reci	ords: 15 < 1 2	>							

Table 11-33 Parameters in the instance list	Table 1	1-33	Parameters	in	the	instance	list
---	---------	------	------------	----	-----	----------	------

Parameter	Description
Instance Name	Name of an instance
Playbook Name	Name of the playbook corresponding to the instance.

Parameter	Description
Data Class	Operation object of a playbook
Trigger Method	Triggering mode of an instance Timer Trigger Event Trigger
Status	 Status of an instance 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.

Step 6 To view details about an instance, click the instance name. On the displayed page, you can view the instance workflow and workflow node information.

----End

11.8 Layout Management

11.8.1 Viewing an Existing Layout Template

Scenario

The management page and details page templates for alert management, incident management, vulnerability management, analysis report, intelligence management, and large-screen security are available in the layout.

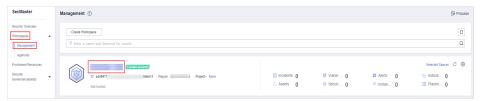
View an existing layout template.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-136 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Layouts**. On the displayed page, click the **Template** tab.

Figure 11-137 Layout template tab page

< / / Layout management	/ Layout			
Security Situation •	Layout Template			
Resource Manager +				
Risk Prevention +				
Threat Operations -		All Enter a keyword.	Q	Search
Security Orchest 0		I Indicator Large Screen Custom Resource		
Object Management	Page Type 🔠 Management Page Detail			
Playbook				
Management	Resource Details	Resource List	Vulnerability Details Detail	Vulnerability List D Management Page
Layout management	@ 2023/03/07 14:47:52 GMT+08:00	@ 2023/03/06 14:49:31 GMT+08:00	© 2022/11/26 14:24:05 GMT+08:00	@ 2022/11/26 14:20:37 GMT+08:00
Plugin Management	E Bull-inlayout,Resource Details	E Bult-Inlayout, Resource List	E Built-Inlayout, Vulnerability Details	E Bult-inlayout, Vulnerability List
Settings •	Built-in	Bull-in	Bull-t	Built-in
	Indicator Details	D Un classified	IPV6	IPV4
	1 Detail	Detail	(D Detail	1 Detail
	2022/11/17 17:03:19 GMT+08:00 IP Bult-inlavout.indicator Details	© 2022/11/17 17:03:19 GMT+08:00 Fi Bult-inlayout, Indicator-Un-classified	© 2022/11/17 17:03:19 GMT+08:00 Fi Bull-Inlayout.Indicator-IPV6	© 2022/11/17 17:03:19 GMT+08:00 (F) Bull+inlayout.Indicator-IPV4
	Bull-in		E CONTINUE CONTINUE OF TO	
	Datest	Buren	Soler .	Darrell

Step 5 On the **Template** tab page, view the template information.

You can search for a specified layout template by Layout Type or Page Type.

- You can view the name, page type, and creation time of an existing template.
- You can edit the name and layout of an existing template.
- You can delete an existing template.

----End

11.8.2 View Existing Layouts

Scenario

This topic describes how to perform the following operation: **Viewing an Existing Layout**.

Viewing an Existing Layout

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-138 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	$\label{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \fboxlabel{eq:rescaled} \vspace{-1.5}$				C
Purchased Resources Security Governance(beta)	0 459977 46442 Region Project- More Not honoid.	 incidents 0 ○ Assets 0 	♥ Vulner 0	O Alerts 0 instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Layouts**.

I Least dargement i Least

 Souch Stadier

 Souch Stadier

Figure 11-139 Layouts page

Step 5 On the layout management page, view existing layouts.

Hover your cursor over the target layout and click in the upper right corner of the layout. The layout configuration details page is displayed.

----End

11.9 Plug-in Management

11.9.1 Overview

SecMaster supports unified management of plug-ins used in the security orchestration process.

Terms

- **Plug-in**: an aggregation of functions, connectors, and public libraries. There are two types of plug-ins: custom plug-ins and commercial plug-ins. Custom plug-ins can be displayed in marts or used in playbooks.
- **Plug-in set**: a set of plug-ins that have the same service scenario.
- **Function**: an executable function that can be selected in a playbook to perform a specific behavior in the playbook.

- **Connector**: connects to data sources and sends security data such as alerts and incidents to SecMaster. Connectors are classified into incident-triggered connectors and scheduled connectors.
- **Public library**: a public module that contains API calls and public functions that will be used in other components.

11.9.2 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-140 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Create Watespace				C Q
Purchased Resources Security Governance(beta)	0 459977 494412 Region Project- Nov Not Includ.	Incidents 0 Assets 0	♥ Vulner 0 Secunt 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ indicat 0 ∋ Playbo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Plugins**.

Figure 11-141 Plugins page

curity Situation +	Plugin Management			
source Manager 🔹 👻	Q	â		
isk Prevention 🔹				
hreat Operations	- (18)	This is the built-in pi	lug-in set of I	
	+ () HSS Python			
Security Orchest	+ 🔮 HTTP Java			
Object Management	+ SecMasterBiz Python	Upgradable/System Plug-in	Custom plug-ins	Total number of plug-ins
Playbook	+ SecMasterUtilities Python	0/18	0	18
Management	+ () EIP Python	0/10	v	10
Layout management	+ © ECS Python			
Plugin Management 2	+ © RDS Python			
Plugin Management 2	+ © IAM Python			
ettings 🔻	+ © WAF Python			
	+ © Getthreatbookinfo Python			

Step 5 On the **Plugins** page, view plug-in details.

- The navigation pane on the left shows information about all built-in plug-in sets, plug-ins, and functions.
- To view details about a plug-in, click its name. Its details will be displayed in the right pane.

• To view details about a function, expand the plug-in and click the function name. The function details will be displayed in the right pane.

----End

12 Settings

12.1 Data Collection

12.1.1 Data Collection Overview

Data collection refers to the process of using Logstash to collect varied log data in many methods. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Limitations and Constraints

- Currently, the data collection agent can run only on Linux ECSs on x86_64 architecture. ECSs support the following OSs: Huawei Cloud EulerOS 2.5, Huawei Cloud EulerOS 2.9, EulerOS 2.5, EulerOS 2.9, and CentOS 7.9.
- If you want to view information in the console during Agent installation, logging in as an IAM user is mandatory.

Collector Specifications

In collection management, the collector specifications are as follows:

Specifications	Referenced Processing Capability
4U8G50G100G	2000 EPS @ 1KB
8U16G50G100G	5000 EPS @ 1KB
16U32G50G100G	10000 EPS @ 1KB

Table 12-1 Collector	⁻ Specifications
----------------------	-----------------------------

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.

12.1.2 Collecting Data

Scenario

This section describes how to collect data.

Step 1: Buy an ECS

For details, see **Purchasing an ECS**.

• Currently, the data collection agent can run only on Linux ECSs on x86_64 architecture. ECSs support the following OSs: Huawei Cloud EulerOS 2.5, Huawei Cloud EulerOS 2.9, EulerOS 2.5, EulerOS 2.9, and CentOS 7.9.

Note that you need to select the proper OSs and versions when you buying an ECS.

Figure 12-1 Selecting an OS version

Image	Public image	Private image	Shared image	Marketplace image	
	S EulerOS	* Public-C	AD-EulerOS-BaseTempla	te-2.5.9-x86_64-Standard for	•

ECSs are billed. For details about ECS pricing, see Billing Overview.
 If you do not need to collect log data later, you need to manually release the ECSs used. For details, see How Do I Release an ECS or VPC Endpoint?

Step 2: Install an Agent

- 1. Pre-check before installing an agent.
 - a. Run the **ps -ef | grep salt** command to check whether the salt-minion process exists on the host.
 - If yes, stop it first.
 - If no, go to 1.b.

Figure 12-2 Checking processes

[root@hos	t-192-1	68-0	~]#	ps -ef	grep salt	
root	18749	18315	0 09	:28 pts/0	00:00:00	grepcolor=auto salt
root	58881	1	0 Ap	r11 ?	00:00:00	/usr/bin/python3 /usr/bin/salt-minion
isap-sa+	58888	58881	0 Ap	rll ?	00:01:08	/usr/bin/python3 /usr/bin/salt-minion

b. Run the **df** -**h** command to check whether there are at least 50 GB of disk space reserved for the **root** directory disk or **opt** disk, two CPU cores, and 4 GB of memory.

Figure 12-3 Disks

[root@ecs-	.∼]# df	-h			
Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/vdal	40G	1.76	36G	5%	/
devtmpfs	7.8G	Θ	7.8G	0%	/dev
tmpfs	7.8G	Θ	7.8G	0%	/dev/shm
tmpfs	7.8G	129M	7.7G	2%	/run
tmpfs	7.8G	Θ	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	Θ	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. For details about capacity expansion, see **Modifying ECS Specifications**.

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

Figure 12-4 Workspace management page

SecMaster	Management ⑦				Process
Security Overview Workspeces	Crede Writipot To fine a name and knyword for search.				C
Purchased Resources Security Governance/beta)	Contract Contract Contrat Contract Con	 Incidents 0 Assets 0 	Vulner 0	O Alerts O ⊗ Instan O	Selected Spaces C indicat 0 Playbo 0

5. In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-5 Accessing the node management page

< / / Componen	tmanag	genetit / Noo Managenetit							
Security Situation		Node Management Component management							
Resource Manager	*								
Risk Prevention	٠								
Threat Operations	٠	Node management occupies the Netohali's directory. To avoid motivation deletion, you are advised not to store personal files in this directory.							
Security Orchest	*	Create	۲						
Settings	*	I Search by node name by default.	Q						
Collection Management		Node Name10 Health Status Region IP Address CPU Usage Memory Usage Disk Usage Network Speed Tag Heartbest Expination Disc Operation							
Component management									
Data Integration		•							
Checks		No data availatie.							
Catalog Customization									

- 6. On the **Node Management** tab page, click **Create**.
- 7. On the Create Node page, set parameters.

Figure 12-6 Create Node

_	e Node	tion (2	Script Ins Verificatio				
Networ	rk Channel (Configuration					
Netw	vork (?)	e-vpc		• C	8-vpc-01	• C	
Networ	rk Channel L	ist					
Туј	ре	Node Name		Node ID	Node Address	Status	Operation
Ma	anagement		salt01	-	-		Config Delete
Ma	anagement		;alt02		-		Config Delete
Da	ta		ирсер	-	-		Config Delete

- a. In the **Network Channel Configuration** area, select the VPC and subnet the network channel belongs to.
- b. In the network channel list, locate the row that contains the target channel and click **Config** in the **Operation** column. In the displayed confirmation dialog box, click **OK**.

NOTE

VPC endpoints you use for log collection are billed. For details about pricing, see **Billing Overview**.

If you do not need to collect log data later, you need to manually release the VPC endpoints used. For details, see **How Do I Release an ECS or VPC Endpoint?**

- 8. Click **Next** in the lower right corner of the page. On the page for verifying the script installation, click **I** to copy the command for installing the Agent.
- 9. Remotely log in to the ECS where you want to install the agent.
 - Huawei Cloud servers
 - Log in to the ECS console, locate the target server, and click **Remote** Login in the Operation column to log in to the server. For details, see Login Using VNC.
 - If your server has an EIP bound, you can also use a remote management tool, such as PuTTY or Xshell, to log in to the server and install the agent on the server as user **root**.
 - Non-Huawei Cloud servers

Use a remote management tool (such as PuTTY or Xshell) to connect to the EIP of your server and remotely log in to your server.

10. Run the **cd /opt/cloud** command to go to the installation directory.

The recommended installation path is **/opt/cloud**. This section also uses this path as an example. If you want to install the Agent in another path, change the path based on site requirements.

- 11. Run the command copied in 8 as user **root** to install the Agent on the ECS.
- 12. Enter the IAM username and password for logging in to the console when prompted.
- 13. If information similar to the following is displayed, the agent is successfully installed: install isap-agent successfully

Step 3: Create a Node

1. In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-7 Accessing the node management page

< / / Compone	int manag	percent	Nodo Management	
Security Situation Resource Manager	÷	NK	de l'Asnagement Composet management	
Risk Prevention	×		-	
Threat Operations	*		Node management occupies the vitabulit directory. To avoid mitriaken deletory, you are advised not to store personal files in this directory.	*
Security Orchest	*		Cenado	C
Settings 🕕	*		▼ Search by node name by default	Q
Collection Management			Node Name1D Health Status Region IP Address CPU Usage Memory Usage Disk Usage Network Speed Tag Heartbast Expiration Disc Operation	
Component management				
Data Integration		1		
Checks			No data availatio.	
Catalog Customization				

- 2. On the Node Management tab page, click Create.
- 3. On the **Create Node** page, set parameters.

Figure 12-8 Create Node

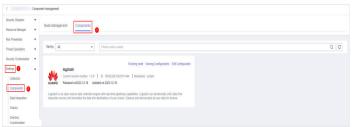
Configure Devic	ce (2) v	/erify Installe	d Script			
etwork Channel	Settings					
Network (?)	vpc-default		• C su	ibnet-default	• C	
etwork Channel	List					
Туре	Node Name		Endpoint ID	Endpoint Ad	Status	Operation
Type Management	Node Name	lt01	Endpoint ID bc162666-4d	Endpoint Ad	Status Accepted	Operation Config Delete
	Node Name	lt01 alt02				

- a. In the **Network Channel Configuration** area, select the VPC and subnet the network channel belongs to.
- b. In the network channel list, locate the row that contains the target channel and click **Config** in the **Operation** column. In the displayed confirmation dialog box, click **OK**.
- 4. Click **Next** in the lower right corner of the page to go to the **Script Installation Verification** page.
- 5. After confirming that the installation is complete, click **Confirm** in the lower right corner of the page.

Step 4: Configure Components

1. In the navigation pane on the left, choose **Settings** > **Components** and click the **Components** tab.

Figure 12-9 Accessing the Components tab page



- 2. On the **Components** tab page, click **Edit Configuration** in the upper right corner of the component to be viewed. The configuration management page of the component is displayed on the right.
- 3. 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**.
- 4. Click **Save and Apply** in the lower right corner of the page.

Step 5: Add a Data Connection

 In the navigation pane on the left, choose Settings > Collection Management.

Figure 12-10 Accessing the collections page

<	/ Coll	ection Management / Connection ma	anagement					
Security Situation Resource Manager	Ţ	Connection management	Parser Management	Collection channel manager	nent	Collection node m	anagement	
Risk Prevention	*	Add				Connect Title	*	Q C 0
Threat Operations Security Orchest		Connect Title	Connect Type	Connect Info	Channel		Description	Operation
Settings	•		Kafka	(topic_jd) json (codec)	0		1	Edit Delete
Management			File	/opt/cloud/ json_lines (codec)	(₀			Edit Delete
management Data Integration			Pipe	100	0		-	Edit Delete
Checks Catalog Customization		c	Pipe		1			Edit Delete

- 2. On the **Connection Management** tab page, click **Add**.
- 3. Add a data connection source.

In the **Source** column, select the source of the data source type and set parameters based on the selected type.

The following data source types are supported: **Transmission Control Protocol (TCP)**, **File**, **User Data Protocol (UDP)**, **Object Storage Service (OBS)**, **Message Queue (Kafka)**, and **SecMaster Pipeline**.

4. Add a data source connection destination.

Click the **Target** tab, select the destination of the data source type, and then set the parameters according to the selected type.

The following data source types are supported: File, Transmission Control Protocol (TCP), User Data Protocol (UDP), Message Queue (Kafka), Object Storage Service (OBS), and SecMaster Pipeline.

5. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

(Optional) Step 6: Configure the Parser

 In the navigation pane on the left, choose Settings > Collection Management. On the displayed page, click the Parsers tab.

Figure 12-11 Accessing the Parsers tab page

<	/ Collec	ction Management / Parsers									
Security Situation	*										
Resource Manager	٠	Connections Parsers Collection thannel management Collection Nodes									
Risk Prevention	-	•									
Threat Operations	÷	Patters Templates									
Security Orchestration											
Settings 0		Add Import Export			Name • Enter a name.	QC					
Collection		Name Name	Channel	Description	Operation						
Management		pace (1	-	Edt Delete						
Components		IVPC FLOWD			Edit Delete						
Data Integration											
Checks			0		Edit Daleta						
Directory Customization		ngiro.	0		Edit Delete						
		4 nd;	0	-	Edit Delete						

- 2. Customize a parser or create a parser from a template.
 - Customizing a parser
 - i. On the **Parsers** tab page, click **Add**.
 - ii. On the **Parsers** tab page, set parameters.

Parameter		Description				
Basic	Parser Name	Set a parser name.				
Information	Description	Enter the parser description.				
Rule list		Set the parsing rule of the parser. Perform the following steps:				
		1. Click Add and select a rule type.				
		 Parsing rules: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules. 				
		 Conditional control: Select the conditions for the parser. You can select If, Else, or Else if. 				
		2. Set parameters based on the selected rule.				

Table 12-2 Parameters for adding a parser

- iii. 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
 - i. On the **Parsers** tab page, click the **Templates** tab.
 - ii. On the displayed page, locate the row that contains the target template, click **Created by Template** in the **Operation** column.
 - iii. On the **Parsers** tab page, set parameters.

Paramete	r	Description
Basic Informat ion	Parser Name	Parser name, which is automatically generated by the system based on the template and can be changed.
	Descriptio n	Parser description, which is automatically generated by the system based on the template and can be modified.
Rule list		Parsing rule, which is automatically generated by the system based on the template and can be modified.
		To add a rule, click Add , select a rule type, and set parameters based on the selected rule.
		• Parsing rules : Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules.
		• Conditional control : Select the conditions for the parser. You can select If , Else , or Else if .

Table 12-3 Parameters for adding a parser

iv. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

Step 7: Add a Collection Channel

 In the navigation pane on the left, choose Settings > Collection Management. On the Collection Management page, click the Collection Channels tab.

Figure 12-12 Collection channel management tab page

Collection	Manager	nent / Collection channel managem	ent										
Security Situation	٠	Conrection management Parser Management Collection channel management Collection node management											
Resource Manager													
Risk Prevention	*												
Threat Operations	٠	Group list	Add								Enter a name a	and keyword k Q	C
Security Orchest	*	Enter a keyword.	Q	Connection information	Created By H	Health Status	Receive rate	Sending Rate	Configuratio	Channel Inst	Delivery Status	Operation	
Settings		All											
Collection Management		test2432						1					
Component								Q					
managament							No dela	au allahia					

- 2. Add a channel group.
 - a. On the collection channel management page, click 🕣 next to **Group list**.
 - b. Enter a group name and click \checkmark .

To edit or delete a group, hover the cursor over the group name and click the edit or deletion icon.

- 3. On the right of the group list, click **Add**.
- 4. On the displayed page, in the **Basic Configuration** phase, configure basic information.

Parameter		Description				
Basic	Name	User-defined collection channel name.				
Information	Channel grouping	Select the group the collection channel belongs to.				
	(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	Destination Name	Select the destination name of the collection channel.				
		After you select a source, the system automatically generates the information about the selected source				

Table 12-4 Basic configuration parameters

- 5. After the basic configuration is complete, click **Next** in the lower right corner of the page.
- 6. On the parser configuration page, select a parser to view its details.

If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see **Managing Parsers**.

- 7. After the parser is configured, click **Next** in the lower right corner of the page.
- 8. 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:
 - i. In the node list, locate the row that contains the target node, and click **Running Parameters** in the **Operation** column.
 - ii. Click Add Configuration and set Key and Value.
 - Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.
- 9. After the running node is selected, click **Next** in the lower right corner of the page.
- 10. On the **Channel Details Preview** page, confirm the configuration and click **OK**.

Related Operations

Troubleshooting the Agent Installation Failure

12.1.3 Collection Management

12.1.3.1 Managing Connections

Scenario

This topic describes how to perform the following operations: Adding a Connection, Viewing Connections, Editing a Data Connection, and Deleting a Data Connection.

Limitations and Constraints

• After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed.

Adding a Connection

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

Figure 12-13 Workspace management page

SecMaster	Management ⑦				🕞 Process
Security Overview Workspaces	Creatile With the paper of the second of the second for second. $\label{eq:second} \overline{V} \ \mbox{ Lotter } a \ \mbox{ career and large-second} \ \mbox{ second}.$				C
Purchased Resources Security Governance(beta)	Constant accord O additif?	 Incidents 0 ○ Assets 0 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 Mindicat 0 Playbo 0

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

Figure 12-14 Accessing the collections page

<	< / / Collection Management / Connection management									
Security Situation Resource Manager	Ţ	Connection management	Parser Management	Collection channel manage	ment	Collection node m	anagement			
Risk Prevention		Add				Connect Title	Ŧ	Q C 🐵		
Security Orchest	-	Connect Title	Connect Type	Connect Info	Channel		Description	Operation		
Settings	•		Kafka	(topic_id) json (codec)	0		1	Edit Delete		
Component			File	/opt/cloud/l json_lines (codec)	k(₀			Edt Delete		
management Data Integration			Pipe	100	0			Edit Delete		
Checks Catalog Customization		¢	Pipe		1			Edit Delete		

- Step 5 On the Connections tab, click Add.
- **Step 6** Add a data connection source.

In the **Source** column, select the source of the data source type and set parameters based on the selected type.

The following data source types are supported: **Transmission Control Protocol (TCP)**, **File**, **User Data Protocol (UDP)**, **Object Storage Service (OBS)**, **Message Queue (Kafka)**, and **SecMaster Pipeline**.

Step 7 Add a data source connection destination.

Click the **Target** tab, select the destination of the data source type, and then set the parameters according to the selected type.

The following data source types are supported: File, Transmission Control Protocol (TCP), User Data Protocol (UDP), Message Queue (Kafka), Object Storage Service (OBS), and SecMaster Pipeline.

Step 8 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

Viewing Connections

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

Figure 12-15 Workspace management page

SecMaster	Management (?)				Process
Security Overview Workspaces	Owned Wanspaces If father a name and keywood for search.				C
Purchased Resources Security Governance(beta)	Carrent access a defait? defait2 Region Project- Mars Net house.	i Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	o Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞 M Indicat 0 Playbo 0

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

Figure 12-16 Accessing the collections page

< / / Collection Management / Connection management									
Security Situation Resource Manager		Connection management	Parser Management	Collection channel manage	ement C	ollection node management			
Risk Prevention Threat Operations	* *	Add				Connect Title +	Q C 🕲		
Security Orchest		Connect Title	Connect Type	Connect Info	Channel	Description	Operation		
Settings	•		Kafka	(topic_id) json (codec)	0	1	Edit Delete		
Component			File	/opt/cloud/l json_lines (codec)	t(0		Edit Delete		
management Data Integration Checks			Pipe	100	0		Edit Delete		
Catalog Customization		•	Pipe		1		Edit Delete		

Step 5 On the **Connections** tab, view connection details.

Table 12-5 Connection parameters

Parameter	Description
Connection Name	Connection name
Connection Type	Connection type
Connection Info	Information about a connection

Parameter	Description
Reference Channels	Number of channels that are referenced by the connection
Description	Description of the connection
Operation	Operations such as editing or deleting connections

----End

Editing a Data Connection

NOTE

After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed.

For example, if you select **File** as the data source type when adding a data connection, you can modify only the parameters in the file type but cannot change the **File** type.

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

Figure 12-17 Workspace management page

SecMaster	Management ()				D Process
Security Overview Workspaces	Credit Workspace $\overline{V} \mbox{ for same and layout for sameh}.$				C
Purchased Resources Security Governance(beta)	Control Contro	Incidents 0 Assets 0	 ♥ Vuiner 0 ⊜ Securi 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C 😒 indicat 0 Playbo 0

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

Figure 12-18 Accessing the collections page

<	/ Colle	ction Management / Connection ma	anagement					
Security Situation Resource Manager		Connection management	Parser Management	Collection channel managem	ent	Collection node m	anagement	
Risk Prevention	•	Add				Connect Title	*	Q C 🛞
Security Orchest		Connect Title	Connect Type	Connect Info	Channel		Description	Operation
Settings	•		Kafka	(topic_id) json (codec)	0		1	Edit Delete
Component			File	/opt/cloud/l t json_lines (codec)	•			Edit Delete
management Data Integration			Pipe	100	0			Edit Delete
Checks Catalog Customization	•	¢	Pipe		1			Edit Delete

- **Step 5** On the Connections page, locate the row that contains the target connection and click **Edit** in the **Operation** column.
- **Step 6** On the **Select Data Source Type** page, edit the parameters of the data source type.

Step 7 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

Deleting a Data Connection

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

Figure 12-19 Workspace management page

SecMaster	Management ③				🕞 Process
Security Overview Workspeces Management Agencies	Could Wongoo $\label{eq:second} \overline{V} \mbox{ If the a name and legendre for search}.$				Q
Purchased Resources Security Governance(beta)	Connect Scotter	Incidents 0 Assets 0	♥ Vuiner 0	O Alerts 0 instan0	Selected Spaces C 🛞 indicat 0 Flaybo 0

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

Figure 12-20 Accessing the collections page

<	/ Collec	tion Management / Connection ma	nagement					
Security Situation	•	Connection management	Parser Management	Collection channel managem	ent	Collection node ma	inagement	
Risk Prevention	•							
Threat Operations	*	Add				Connect Title	¥	Q C 🛞
Security Orchest	*	Connect Title	Connect Type	Connect Info	Channel		Description	Operation
Settings	^		Kafka	(topic_id) json (codec)	0		-	Edit Delete
Component			File	/opt/cloud/i t (json_lines (codec)	0		_	Edit Delete
Data Integration			Pipe	100	0			Edt Delete
Catalog Customization		c	Pipe		1			Edt Delete

- **Step 5** On the Connections page, locate the row that contains the target connection and click **Delete** in the **Operation** column.
- **Step 6** In the displayed dialog box, click **OK**.

----End

12.1.3.2 Managing Parsers

Scenario

This topic describes how to perform the following operations: **Creating a Parser**, **Viewing Parsers**, **Importing a Parser**, **Editing a Parser**, **Exporting a Parser**, and **Deleting a Parser**.

Creating a Parser

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-21 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Centre Wantappea If later a name and layound for sounds.				C
Agencies Purchased Resources Security Governance(beta)	O #99977 #64412 Region Project- Mare Not hold.	Incidents 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 instan 0	Selected Spaces C

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-22 Accessing the Parsers tab page

< / / Co	C / Coldedon Management / Pasers					
Security Situation • Resource Manager •	Corrections Parson Collection channel management Collection Nodes					
Risk Prevention 💌	-					
Threat Operations 👻	Parsers Templates					
Security Orchestration V	Add Import Export		Name v I	Inter a name. Q		
Callection	Name	Charnel	Description	Operation		
Wanagement		1	-	Edit Delete		
Components	OPC FLOW)	0		Edt Delete		
Data Integration Checks		0		Edit Datete		
Directory Outperization	npino:	0		Edit Daleta		
	4 ndt.	0	-	Edit Daleta		

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 12-6 Parameters for adding a parser

Parameter		Description		
Basic	Parser Name	Set the parser name.		
Information	Description	Enter the parser description.		

Parameter	Description
Rule listSet the parsing rule of the parser. Perform the following steps:	
	1. Click Add and select a rule type.
	 Parsing rules: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules.
	 Conditional control: Select the conditions for the parser. You can select If, Else, or Else if.
	2. Set parameters based on the selected rule.

c. 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.

Parameter	r	Description
Basic Informati on	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.
Rule list		Parsing rule, which is automatically generated by the system based on the template and can be modified.
		To add a rule, click Add , select a rule type, and set parameters based on the selected rule.
		 Parsing rules: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules.
		 Conditional control: Select the conditions for the parser. You can select If, Else, or Else if.

Table 12-7 Parameters for adding a parser

d. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

Viewing Parsers

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

Figure 12-23 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspaces	Center Westspeet T later a name and largeoind for search.				C
Agencies Purchased Rescurces Security Governance(beta)	Butter & Stands Butter Butter Butter & Stands Butter & Stands	Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 instan 0	Selected Spaces C ⑧ iv Indicat 0 IP Playbo 0

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-24 Accessing	the	Parsers	tab	page
------------------------	-----	---------	-----	------

C / Collection Management / Parsers							
Security Situation							
Resource Manager 🔹 💌	Conections Passes Collection channel management Collection Nodes						
Risk Prevention 👻	-						
Threat Operations 🔹 💌	Parsers Templates	Parser Templates					
Security Orchestration	Add Import Export		Name	• Enler a name. Q C			
Settings 0	Name	Channel	Description	Operation			
Collection Management	ipace	1	-	Edt Delete			
Components Data Integration	(VPC FLOW)	0		Edt Delete			
Checks		0		Edit Delete			
Directory Customization	npix	0		Edit Dolete			
	4 nd;	0	-	Edit Delete			

Step 5 On the **Parsers** page, view the detailed information about parsers.

Table 12-8 Parsers parameters

Parameter	Description
Parser Name	Name of the parser.
Reference Channels	Number of channels referenced by the parser.
Description	Description of the parser.
Operation	You can edit and delete parsers.

Step 6 On the **Parsers** page, click the **Templates** tab.

Step 7 On the **Templates** tab displayed, view the parser template information.

Parameter	Description			
Template Name	Name of a parser template			
Description	Description of the parser template			
Operation	You can create a parser 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 left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

SecMaster	Management 💮				🕼 Process
Security Overview Workspaces	Credit Writigate T later a name and keyword for search.				C
Purchased Resources Security Governance(beta)		incidents Assets	♥ Vulner 0 ⊜ Securl 0	 O Alerts O ⊗ Instan O 	Selected Spaces C ⑧ i Indicat 0 B Playbo 0

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Security Staudon * Connections Farsen Collection channel management Collection Nodes								
Resource Manager 🔹 👻	Connections Parses Collection channel management Collection Nodes							
Risk Prevention 💌	-							
Threat Operations 🔹	Passars Templates							
Security Orchestration 🔹	Add Import Expert		Name	 Enter a name. 	C			
Settings 🚺 🔺								
Collection	Name	Channel	Description	Operation				
Management	i pace	1	-	Edit Delete				
Components	(VPC FLOW)	0		Edt Delete				
Data Integration								
Checks		0		Edt Delete				
Directory Customization	in ngino;	0		Edt Dalete				
	4 nd:	0	-	Edt Delete				

- **Step 5** On the **Parsers** tab, click **Import** in the upper left corner of the parser list.
- **Step 6** In the displayed **Import** dialog box, click **Select File** and select the JSON file you want to import.

- 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.

After the parsers are imported, you can view the imported parser information in the parser list.

----End

Editing a Parser

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

Figure 12-27 Workspace management page

SecMaster	Management 💿	Process
Security Overview Workspaces Management Agencies	Total Winspon Total reasons and lequal for search.	C
Purchased Resources Security Governance(beta)		•

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-28 Accessing the Parsers tab page

<	/ Collect	ion Management / Parsers							
Security Situation	٠								
Resource Manager	*	Connections Parses Collection channel management Collection Nodes							
Risk Prevention	*	-							
Threat Operations	*	Parsers Templates							
Security Orchestration	٠	Add Import Expert		Name	 Enter a name. 	QC			
Settings									
Collection		Name	Channel	Description	Operation				
Management		5000	1	-	Edit Delete				
Components		WPC FLOW	0		Edt Delete				
Data Integration									
Checks			0		Edit Delete				
Directory Customization		npinx.	0		Edit Daleta				
	4	10	0		Edit Delete				

- **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.

Parameter		Description		
Basic	Parser Name	Set the parser name.		
Information	Description	Enter the parser description.		
Rule list		Set the parsing rule of the parser. Perform the following steps: Click Add and select a rule type.		
		• Parsing rules : Select the parsing rule of the parser.		
		• Conditional control : Select the conditional control principle of the parser.		

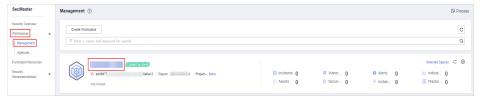
Step 7 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

Exporting a Parser

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

Figure 12-29 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-30 Accessing the Parsers tab page

< 1 / 0	C / Colector Mangement / Parens						
Security Situation		Collection Nodes					
Resource Manager		Lorecourt Nodes					
Risk Prevention	·						
Threat Operations	Parsers Templates						
Security Orchestration	Add Impart Expert		Nærre 💌 🗌 Enter a n	ana. Q C			
Collection	Name	Channel	Description	Operation			
Management	2000	4	-	Edit Dolete			
Components	(VPC FLOW)	0		Edt Delete			
Data Integration							
Checks		0		Edit Delete			
Directory Customization	ngiro:	0		Edit Daleta			
	4 ndt	0		Edit Delete			

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 the local PC.

----End

Deleting a Parser

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-31 Workspace management page

SecMaster	Management 💮	Process
Security Overview Workspaces	Craft WithSpace IF form a name and layout for search.	C
Agencies Purchased Resources Security Governance(beta)		

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-32 Accessing the Parsers tab page

C / Colector Mangaret / Paren										
Security Situation										
Resource Manager 🔹 💌	Connections Parsets Collection channel management Collection Nodes									
Risk Prevention 👻	-									
Threat Operations 💌	Parsers Templates									
Security Orchestration 👻	Add Import Expert		Name • Ente	caname. Q C						
Settings 🜒 🔺										
Collection	Name	Channel	Description	Operation						
Management	ipaca	1	-	Edit Delete						
Components	(VPC FLOW)	0		Edit Delete						
Data Integration		0		Edit Delete						
Checks		0		Dat Dates						
Directory Customization	n pire	0		Edit Daleta						
	4 1 102			Edit Delete						

- **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

12.1.3.3 Managing Collection Channels

Scenario

This topic describes how to perform the following operations: Adding a Collection Channel, Viewing Collection Channels, Editing a collection channel, Deleting a collection channel, and Enabling/Disabling/Restarting a Collection Channel.

Adding a Collection Channel

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-33 Workspace management page

SecMaster	Management 💮				🕞 Process
Security Overview Workspaces Management Agencies	Credit Withspace $\overline{ \ensuremath{\mathbb{T}}} \ensuremath{\mathbb{T}} \ensure$				C
Purchased Resources Security Governance(beta)	Come come Come Come come Co	 Incidents 0 Assets 0 	♥ Vulner 0	O Alerts 0 instan0	Selected Spaces C 🛞 indicat 0 S Playbo 0

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-34 Collection channel management tab page

< / / Collection	Manager	nent / Collection channel manageme	ent											
Security Situation	٠	Connection management Parser Management Collection channel management Collection node management												
Resource Manager						- 0								
Risk Prevention	٠													
Threat Operations	٠	Group list	۲	Add								Enter a name	and keyword k Q	C 🛞
Security Orchest	*	Enter a keyword.	Q	Name	Connection information	Created By	Health Status	Receive rate	Sending Rate	Configuratio	Channel Inst	Delivery Status	Operation	
Settings 🚯		AI												
Callection Management		18512432							!					
Component									Q					
management.								No data	available.					

Step 5 Add a channel group.

- 1. On the collection channel management page, click 🕣 next to **Group list**.
- 2. Enter a group name and click \checkmark .

To edit or delete a group, hover the cursor over the group name and click the edit or deletion icon.

- **Step 6** On the right of the group list, click **Add**.
- **Step 7** On the displayed page, in the **Basic Configuration** phase, configure basic information.

Parameter		Description					
Basic	Channel Name	User-defined collection channel name.					
Information	Channel grouping	Select the group to which the collection channel belongs.					
	(Optional) Description	(Optional) Enter the description of the collection channel.					

 Table 12-11
 Basic configuration parameters

Parameter		Description				
Source Configuration	Source Name	Select the source name of the collection channel.				
		After you select a source, the system automatically generates the information about the selected source.				
Destination	Destination Name	Select the destination name of the collection channel.				
		After you select a source, the system automatically generates the information about the selected source.				

- **Step 8** After the basic configuration is complete, click **Next** in the lower right corner of the page.
- **Step 9** On the parser configuration page, select a parser to view its details.

If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see **Managing Parsers**.

- **Step 10** After the parser is configured, click **Next** in the lower right corner of the page.
- **Step 11** On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node and click **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 set Key and Value.
 - Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.
- **Step 12** After the running node is selected, click **Next** in the lower right corner of the page.
- Step 13 On the Channel Details Preview page, confirm the configuration and click OK.

----End

Viewing Collection Channels

Step 1 Log in to the management console.

- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-35 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspeces Management Agencies	$$\ensuremath{\mathbb{C}}\xspace$ Total Wontgoon $$\ensuremath{\mathbb{C}}\xspace$ for search.				C
Purchased Resources Security Governance(beta)	Order Sector Order Sector Order Sector Order Sector Order Sector Not Noted	 Incidents 0 ○ Assets 0 	 ♥ Vulner 0 Securl 0 	 o Alerts 0 ⊗ Instan 0 	Selected Spaces C indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-36 Collection channel management tab page

Collection	Manager	ent / Collection channel managem	ert											
Security Situation	Connection management Parser Management Collection channel management Collection node management													
Resource Manager						_	en noor no noge							
Risk Prevention	٠													
Threat Operations		Group list	Θ	Add								Enter a name	and keyword k Q	C
Security Orchest		Enter a keyword.	Q	Name	Connection information	Created By	Health Status	Receive rate	Sending Rate	Configuratio	Channel Inst	Delivery Status	Operation	
Setings 🟮		All												
Callection Nanagement		18512432							!					
Component									Q					
managament								No data	available.					

Step 5 On the **Collection Channels** page, view the detailed information about collection channels.

Parameter	Description
Channel Groups	List of collection channel groups and group names.
Channel Name	Name of the collection channel.
Connection Information	Collect channel connection information
Created By	Creator of the collection channel
Health Status	Health status of the collection channel
Receive Rate	Receive rate of the collection channel
Transmit Rate	Transmit rate of the collection channel
Configuration Status	Configuration status of the collection channel
Channel Instances	Number of collection channels
Running Status	Running status of a collection channel
Operation	You can edit and stop collection channels.

 Table 12-12
 Collection channel parameters

----End

Editing a collection channel

Step 1 Log in to the management console.

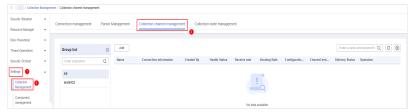
- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-37 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces	Credit Workspece If Enter a name and layword for search.				C
Agencies Purchased Resources Security Governance(beta)		Incidents 0 Assets 0	 Vulner 0 ⊜ Securl 0 	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⊗ i Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-38 Collection channel management tab page



- Step 5 In the collection channel list, locate the row that contains the target channel, click More > Edit in the Operation column. The Edit Collection Channel page is displayed.
- **Step 6** On the displayed page, in the **Basic Configuration** phase, configure basic information.

Parameter		Description				
Basic	Channel Name	User-defined collection channel name.				
Information	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.				

 Table 12-13 Basic configuration parameters

Parameter		Description
	Destination Name	Select the destination name of the collection channel.
		After you select a destination, the system automatically generates the information about the selected destination.

- **Step 7** After the basic configuration is complete, click **Next** in the lower right corner of the page.
- **Step 8** On the parser configuration page, select a parser to view its details.

If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see **Managing Parsers**.

- **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 set Key and Value.
 - Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.
- **Step 11** After the running node is selected, click **Next** in the lower right corner of the page.
- **Step 12** On the **Channel Details Preview** page, confirm the configuration and click **OK**.

----End

Deleting a collection channel

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

Figure 12-39 Workspace management page

SecMaster	Management ①				🕞 Process
Security Overview Workspaces	Credit Wantspece IF lister a name and keywood for search.				C
Purchased Resources Security Governance(beta)	c add9077 Bedst2 Regon Paged- Mars Not holds	S Incidents 0 Assets 0	♥ Vulner 0 Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ └ Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-40 Collection channel management tab page

C im / Colector Vanagement / Colector channel management													
Security Situation	*	Connection management Parser Management Collection channel management Collection node management											
Resource Manager	٠												
Risk Prevention	٠												
Threat Operations		Group list 🕘	Add								Enter a name a	nd keyword fr. Q	C
Security Orchest		Enter a keyword. Q	Name Con	section information	Created By H	lealth Status	Receive rate	Sending Rate	Configuratio	Channel Inst	Delivery Status	Operation	
Settings 🕚		AI											
Callection @		test2432					!						
Component				<u> </u>									
management							No data a	ovallable.					

- **Step 5** In the collection channel list, locate the row that contains the target channel, click **More** > **Delete** in the **Operation** column.
 - D NOTE

You can delete a collection channel only when it is stopped.

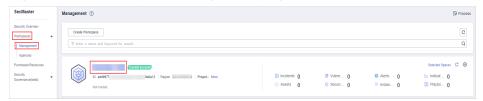
Step 6 In the displayed dialog box, click **OK**.

----End

Enabling/Disabling/Restarting a Collection Channel

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

Figure 12-41 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-42 Collection channel management tab page

< / / Collection	C i Colector Management / Colector Mannel management													
Security Situation	٠	Conrection management Parser Management Collector channel management Collection node management												
Resource Manager	٠		Connection management. Parser Management.											
Risk Prevention	٠													
Threat Operations		Group list	۲	Add								Enter a name i	and keyword k Q	C
Security Orchest	•	Enter a keyword.	Q	Name	Connection information	Created By	Health Status	Receive rate	Sending Rate	Configuratio	Channel Inst	Delivery Status	Operation	
Settings 🕕		All												
Collection Management		test2432							!					
Component														
managament								No data	available.					

Step 5 In the collection stream management list, locate the row that contains the target stream and click **Enable**, **Stop**, or **Restart** in the **Operation** column.

Step 6 In the displayed dialog box, click OK.

----End

12.1.3.4 Managing Collection Nodes

Scenario

This topic describes how to perform the Viewing Collection Nodes operation.

Viewing Collection Nodes

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

Figure 12-43 Workspace management page

SecMaster	Management () (2 Process
Security Overview Workspaces Management Agencies	Center transacta C If later a name and layound for search. Q
Purchased Resources Security Governance(beta)	0 #49977 0#6412 Pege- Mve I Incolents 0 © Wither_0 0 Alents 0 Ize Indoat_0 Not holdst 0 Alents 0 IS Report_0 It Indoat_0 III Protoc_0

Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the Collection Management page, click the **Collection Nodes** tab.

Figure 12-44 Accessing the collection nodes page



Step 5 On the **Collection Nodes** page, view the detailed information about collection nodes.

If there are a large number of nodes, you can select **Node Name** or **Node ID**, enter a keyword in the search box, and click Q to quickly search for a specified node.

Table 12-14 Collection no	de parameters
---------------------------	---------------

Parameter	Description			
Node Name/ID	Name or ID of a node			
Health Status	Node health status			

Parameter	Description
Region	Region where the node is located
IP Address	Node IP address
CPU Usage	CPU usage of the node
Memory Usage	Memory usage of the node
Disk Usage	Node disk usage
Network Speed	Network rate of a node
Label	Label information of a node
Heartbeat Expiration Mark	Indicates whether the node is disconnected due to heartbeat expiration.

Step 6 To view details about a node, click the node name.

----End

12.1.4 Component Management

12.1.4.1 Managing Collection Nodes

Scenario

This topic describes how to perform operations such as **Creating a Node**, **Viewing Nodes**, **Editing a Node**, and **Deregistering a Node**.

Creating a Node

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

Figure	12-45	Workspace	e management	page

SecMaster	Management (?)				🕼 Process
Security Overview Workspaces Management Agencies	Could Workspace $\overline{V} \mbox{ Iters a more and keyword for search}.$				C
Purchased Resources Security Governance(beta)	C add9077 dedat2 Region Pegad- Mon Not factored	Incidents 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ✓ Indicat 0 Playbo 0

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

Figure 12-46 Accessing the node management page



- **Step 5** On the **Nodes** tab, click **Create**. The **Create Node** page is displayed on the right.
- **Step 6** Click **Next** in the lower right corner of the page to go to the **Script Installation Verification** page.
- **Step 7** After confirming that the installation is complete, click **Confirm** in the lower right corner of the page.

If it is not installed, rectify the fault by referring to Step 2: Install an Agent.

----End

Viewing Nodes

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

Figure 12-47 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspeces Management Agencies	Create Withington $\label{eq:creation} \overline{\mbox{\forall Enter a more and layered for search}}.$				C
Purchased Resources Security Governance(beta)	Convert security O additr? Addit? Report Project- Mark Not hoted.	i Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C iv Indicat 0 B Playbo 0

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

Figure	12-48 Accessing	the node	management	page
--------	-----------------	----------	------------	------

< / / Component	nt manag	I hole Management	
Security Situation	-	Node Management Component management	
Resource Manager	÷		
Risk Prevention	٠		
Threat Operations	*	Node management occupies the relativalit directory. To avoid motalinen deviden, you are advised not to store personal lifes in this directory.	*
Security Orchest	٠	Consta	C
Bellings	-	▼ Search by node name by default.	Q
Collection Management		Node Neme/ID Health Status Region IP Address CPU Usage Memory Usage Cisk Usage Network Speed Tag Heartbest Expiration Disc Operation	
Component management			
Data integration			
Checks		ho data posizitia	
Catalog Customization		That Aller a Principles	

Step 5 On the Nodes tab, view the details about nodes.

If there are a large number of nodes, you can select **Node Name** or **Node ID**, enter a keyword in the search box, and click Q to quickly search for a specified node.

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.

 Table 12-15
 Collection node parameters

Step 6 To view details about a node, click the node name.

----End

Editing a Node

After a node is added, you can only modify the supplementary information about the node.

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

Figure 12-49 Workspace management page

SecMaster	Management ()
Security Overview Workspaces	Code Workspace C If fator a name and layout for search. Q
Purchased Resources Security Governance(beta)	0 Addr2 Region Paged- Mars Ill Incodents 0 © Varier

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

Figure 12-50 Accessing the node management page

< / / Compon	ent mana	erres.	nent / Node Management	
Security Situation	-			
Resource Manager	~	~	Node Management Component management	
Risk Prevention	*			
Threat Operations			Node management occupies the relovant/ directory. To avoid mislation deletion, you are advised not to shore personal lifes in this directory.	×
Security Orchest	*		Create	C®
Settings 🚯	+		T Search by node name by default.	a
Collection Management			Node Name/D Health Status Region IP Address CPU Usage Memory Usage Disk Usage Network Speed Tag Heartbest Expiration Disc Opera	ation
Component management	9			
Data Integration		۰.		
Checks			No data available.	
Catalog			The same and and an	

- **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.

Parameter	Description
Data Center	User-defined data center name
Network Plane	Select the network plane of the node.
Тад	Set the tag for the node.
Description	Description of a user-defined node.
Maintained By	Select a node owner.

 Table 12-16 Parameters of node information

Step 7 Click Confirm.

----End

Deregistering a Node

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

Figure 12-51 Workspace management page

SecMaster	Management ③		Process
Security Overview Workspaces	Could Wanspoor IF Enter a name and layeout for search.		C
Purchased Resources Security Governance(beta)		Alerts 0	Selected Spaces C ⊛ Indicat 0 Playbo 0

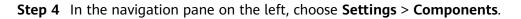


Figure 12-52 Accessing the node management page



- **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.

----End

12.1.4.2 Managing Components

Scenario

This topic describes how to **configure** and view a component.

Configuring a Component

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-53 Workspace management page

SecMaster	Management 💿				Process
Security Overview Workspaces Management Agencies	$\label{eq:rescaled} \fbox{\begin{tabular}{c} $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $$				C
Purchased Resources Security Governance(beta)	Generat economi D add0077 dedat2 Region Project-Nove Not hottock	incidents 0	♥ Vulner 0 ⊜ Securl 0	O Alerts O instan O	Selected Spaces C 🛞 iv Indicat 0 Playbo 0

Step 4 In the navigation pane on the left, choose **Settings** > **Components** and click the **Components** tab.

Figure 12-54 Accessing	l the	Components	tab
------------------------	-------	------------	-----

< / / Companent	15	
Security Stuation	Nodes Components	
Resource Manager		
Risk Prevention	•	
Threat Operations	Soft by AI Please enter a name.	Q C
Security Orchestration	· Bunnino Node View Settinos Ed	9 Californ
Settings 🜖	 logstash 	i ofeninge
Collection Management	Current Version 1.0.0 ID 1603635631920111444 Maintained By system Released 2022-12-16 Updated 2022-12-16	
Components 🕗	Logstash is an open source data collection engine with real-time pipelining capabilities. Logstash can dyn until data from disparate sources and normalize the data into destinations of your choice. Clearse and	samically
Data Integration	democratice all your data for diverse	
Checks		
Directory Customization		

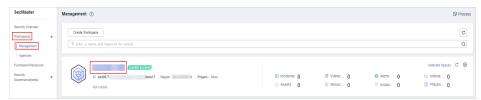
- **Step 5** On the **Components** tab page, click **Edit Settings** in the upper right corner of the component to be viewed. The configuration management page of the component is displayed on the right.
- **Step 6** In the **Node Configuration** area, click **Add** in the upper left corner of the node 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.

----End

Viewing Component Details

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

Figure 12-55 Workspace management page



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

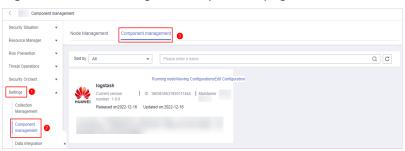


Figure 12-56 Accessing the components page

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 that is displayed, select a node and click OK.
 - Editing node parameters: Click
 vext to the node name to expand the node configuration information and edit the node parameters.
 - Running Parameter: Locate the row that contains the target node, click **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 to be removed and click Batch Remove in the upper left corner of the list.
 - To view historical versions, click **Historical Version** at the lower right corner of the panel.
- c. Click the **Apply** at the lower right corner of the page.

----End

12.2 Data Integration

12.2.1 Log Access Supported by SecMaster

SecMaster can integrate logs of multiple Huawei Cloud services, such as Web Application Firewall (WAF), Host Security Server (HSS), and Object Storage Service (OBS). You can search for and analyze all collected logs in SecMaster. By default, the logs are stored for 7 days.

Cloud Service	Log Description	Log	Log Lifecycle
Web Application Firewall	Attack logs	waf-attack	7 to 30 days
(WAF)	Access logs	waf-access	
SecMaster	Compliance baseline log	secmaster- baseline	7 to 10 days
Intrusion Prevention System (IPS)	Attack logs	nip-attack	7 to 30 days
Managed Threat Detection (MTD)	Alarm logs	mtd-alarm	7 to 30 days

Table 12-17 Log Access Supported by SecMaster

Cloud Service	Log Description	Log	Log Lifecycle
Host Security Service (HSS)	HSS alarms	hss-alarm	7 to 30 days
	HSS vulnerability scan results	hss-vul	7 days
	HSS security logs	hss-log	7 to 15 days
Cloud Trace Service (CTS)	CTS logs	cts-audit	7 to 30 days
Cloud Firewall (CFW)	Access control logs	cfw-block	7 to 30 days
	Traffic logs	cfw-flow	7 to 15 days
	Attack event logs	cfw-risk	7 to 30 days

12.2.2 Access Data

Scenario

SecMaster can access logs of Huawei Cloud services with your authorization, services such as Web Application Firewall (WAF), Host Security Server (HSS), and Object Storage Service (OBS). After you authorize the access, you can manage logs centrally and search and analyze all collected logs.

For details, see Log Access Supported by SecMaster.

This topic describes how to access logs and view where logs are stored.

Allowing SecMaster to Access Service Logs

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

Figure 12-57	Workspace	management page
--------------	-----------	-----------------

SecMaster	Management ③				🕞 Process
Security Overview Workspaces	Could Workspece $\overline{V} \ \ \ \ \ \ \ \ \ \ \ \ \ $				C
Purchased Resources Security Governance(beta)	Genetic accest Genetic accest	 Incidents 0 Assets 0 	Ø Vulner 0 ⊜ Securl 0	O Alerts 0 instan 0	Selected Spaces C 🗟

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

Figure 12-58 Data Integration page

< / Data In	legration							
Security Situation	•	Cloud Service Access						
Resource Manager								
Risk Prevention								
Threat Operations		Access Service Log						
Security Orchest		Cloud Service	Log	Region Level	Workspace	Storage Location (2)	Lifecycle	Automatically converts alarms
Settings	•	Web Application Firewall	WAF attack log 🕥	Region		/ isap-cloudlogs-0a60703a750093a92bac0	180 Days	
Collection Management		Net Application mental (1)	WAF accessing (?)	Region		/ isap-cloudlogs-0a60703a7500/3a92/bac0	180 Days	-
Component management		Object Storage Service (?)	Object Storage Service access log	Region		isap-cloudlogs-0a60703a750043a92bac0	180 Days	-
Data Integration		IPS	IPS attack log	Region		/ isap-cloudlogs-0a60703a7500f3a92tbac0	180 Days	-
Checks		Identity and Access Management	IAM audit log	Region		/ isap-cloudlogs-0a60703a7500f3a62/bac0	180 Days	-
Oustomization								

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 all cloud services in the current region, click **ODE** 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.

In the Automatically converts alarms column of your desired cloud products,

click **w** to enable the function of automatically converting cloud service logs to alerts when the logs meet certain alert rules and displaying the alerts on the **Alerts** page.

NOTE

- If this function is disabled, logs that meet certain alert rules will not be converted to alerts or displayed on the **Alerts** page.
- You can access host vulnerability scan results on the **Vulnerabilities** page of SecMaster. If such results have been accessed during data integration but this conversion function is disabled, the results will not be displayed on the **Vulnerabilities** page.
- Step 8 Click Save. In the displayed dialog box, click OK.

After the access completes, a default data space and pipeline are created.

----End

Viewing the Log Storage Location

- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
- Step 3 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.

< / / Data Integration									
Security Situation Resource Manager	• •	Cloud Service Access							
Risk Prevention	Ŧ								
Threat Operations	Ŧ	Ŧ							
Security Orchestration	*	Access Service Log							
Settings	*	Cloud Service	Log	Region Level	Workspace	Storage Location	0	Lifecycle	Automatically converts alarms
Components		Web Application Firewall (?)	WAF attack log 🕥	Region			/ isap-cloudlogs-5feee88	7 Days	
Data Integration		web Application Filewali	WAF access log (?)	Region			/ isap-cloudlog	7 Days	-
Directory Customization		Object Storage Service (2)	Object Storage Service acces	Region		L.	/ isap-cloudlog	7 Days	
	4	IPS	IPS attack log	Region			/ isap-cloudlog	7 Days	-

----End

Related Operations

- Canceling Data Access
 - a. In the **Log** column of the target cloud services, click **C** 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.

12.3 Checks

Scenario

This topic describes how to create baseline check plans. To use cloud service baseline inspection, you need to create check plans first.

Procedure

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

Figure 12-60 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	Credit Watapace $\label{eq:state} \overline{V} \mbox{ Inter a name and layouth for search}.$				C
Purchased Resources Security Governance(beta)	O #08977 694412 Report Not toold	Incidents O Assets O	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C 🛞

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

Figure 12-61 Checks page

< / / Checks		
Security Situation 💌		
Resource Manager 🔹 🔻	Region 🔍 👻	
Risk Prevention 🔻	Create Plan	
Threat Operations 🔹		
Security Orchestration 🔻	default(Default) Check Now	Check Now Edit Delete
Settings 🔺	C Schedule: every 3 days at 0:00-6:00	Schedule: every 1 days at 0:00-6:00
Collectors	Security Standards	Security Standards
Components	Cloud Security Compliance Check 1.0	DJCP 2.0 Level 3 Requirements
Data Integration		
Checks		
Directory Customization		

- **Step 5** On the **Checks** page, click **Create Plan**. The pane for creating a check plan is displayed on the right.
- **Step 6** Configure the check plan.
 - 1. Enter the basic information by referring to **Table 12-18**.

Parameter	Description
Name	Plan name
Schedule	Select how often and when the check plan is executed.
	 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

 Table 12-18
 Basic information about a check plan

2. Select a security standard for the plan.

Select the baseline check items to be checked.

Step 7 Click OK.

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

----End

12.4 Customizing Directories

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

Figure 12-62 Workspace management page

SecMaster	Management ③				Process
Security Overview Workspaces Management Agencies	Create Workspace If later a name and keyword for seach.				C Q
Agencies Purchased Resources Security Governance(beta)	Constant second 0 editr77 64642 Report Paged- Mare Not toolsd.	incidents 0 Assets 0	 ♥ Vulner 0 ⊜ Securl 0 	O Alerts 0 instan 0	Selected Spaces C ⊗ i Indicat 0 Playbo 0

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

Figure 12-63 Directory Customization page

<	/ Catalog	g Customization							
Security Situation	*								
Resource Manager	*						Level-1 Directory	Ŧ	Q C @
Risk Prevention		Level-1 Directory	Level-2 Directory	Status	Address		Layout	Publisher	Operation
Threat Operations	-	Threat Operations	Incident	Built-in	https://	. 0	Incident List Built-in	Huawei Cloud	Changing layout
Security Orchest		Resource	Resource	Built-in	https://v	. 0	Resource List Built-in	Huawei Cloud	Changing layout
Settings		Risk Prevention	Vulnerability	Built-in	https://v		Vulnerability List Built-In	Huawel Cloud	Changing layout
Collection Management		Threat Operations	Indicator	Built-in	https://		Indicator List Built-in	Huawei Cloud	Changing layout
Component		Threat Operations	Alert	Built-in	https://c	. 0	Alert List Built-in	Huawel Cloud	Changing layout
Data Integration									
Checks									
Catalog Customization	0								

Step 5 In the directory list, view the directory details.

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. The default publisher of a built-in directory is Huawei Cloud .
Operation	Operations you can do for the directory, such as changing the layout.

Table 12-19 Directory parameters

----End

Changing Layout

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-64 Workspace management page

SecMaster	Management ①				Process
Security Overview Workspaces	Credit Hittingues $\label{eq:constraint} \overline{V} \mbox{ forther a name and keyword for search}.$				C
Agencies Purchased Resources Security Governance(beta)	0 400077 64412 Region Project- Hore Not hold	3 Incidents 0 Assets 0	♥ Vulner 0 Securl 0	● Alerts 0 [®] Instan 0	Selected Spaces C indicat 0 Playbo 0

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

Figure 12-65	Directory	Customization	page
--------------	-----------	---------------	------

<	/ Catalog	Customization							
Security Situation	*								
Resource Manager	*						Level-1 Directory	*	Q C 🐵
Risk Prevention		Level-1 Directory	Level-2 Directory	Status	Address		Layout	Publisher	Operation
Threat Operations	-	Threat Operations	Incident	Built-in	https://v	. 0	Incident List Built-In	Huawei Cloud	Changing layout
Security Orchest	*	Resource	Resource	Built-In	https:///	. 0	Resource List Built-in	Huawei Cloud	Changing layout
Settings 1		Risk Prevention	Vulnerability	Built-in	https://v		Vulnerability List Built-in	Huawei Cloud	Changing layout
Collection Management		Threat Operations	Indicator	Built-in	https://	0	Indicator List Built-in	Huawei Cloud	Changing layout
Component		Threat Operations	Alert	Built-In	https://c		Alert List Built-in	Huawel Cloud	Changing layout
Data Integration									
Checks	4								
Catalog Customization	0								

- **Step 5** Click **Changing layout** in the **Operation** column of the target directory.
- **Step 6** On the **Changing layout** page, select the layout to be changed.
- Step 7 Click OK.
 - ----End

13 How to Use Playbooks

13.1 Overview

SecMaster automatically executes code written in playbooks to enable automatic response to alerts and incidents. While some playbooks still need some custom settings for custom data processing. Those playbooks include the ones for automatically updating alert names, reporting high-risk vulnerabilities, and reporting high-risk alerts.

This document describes how to customize settings and enable playbooks that require custom data processing.

Playbooks, Workflows, and Plug-ins

The relationships between playbooks, workflows, and plug-ins are as follows:

- A playbook is a combination of workflows. Playbooks are used for complex data processing in many ways.
- A workflow is composed of a combination of a series of plug-in nodes for complex data processing.
- A plug-in is the encapsulation of function code. It is the minimum unit of a playbook and implements specific functions.

13.2 Automatic Renaming of Alert Names

13.2.1 Overview

Scenario

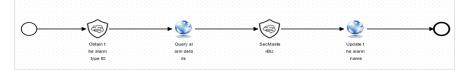
SecMaster provides a built-in playbook that can automatically rename alert names. You can customize alert names with this playbook to meet your needs.

How the Playbook Works

The **Automatic renaming of alarm names** playbook has matched the **Automatic renaming of alarm names** workflow. To configure this playbook, you need to configure the matched workflow and plug-ins the workflow uses.

The **Automatic renaming of alarm names** workflow has four plug-in nodes, one for obtaining alert type IDs, one for obtaining alert details, the SecMasterBiz node, and one for updating alert names. In this workflow, you only need to configure the SecMasterBiz node. This node is used to customize alert names.

Figure 13-1 Automatic renaming of alarm names workflow



Limitations and Constraints

Currently, only names for web shell attack alerts can be modified.

Verification

The following figure shows default alert names.

Figure 13-2 Before processing

(Aes				
Security Station 🛛 🔻				
kanalaap 🔹	Ligent handing of Alets 🕅	Epiet aer Ø	Aist State 🕅	Aers Notes 0
Rsi?eefin v				
Theil lpedors 🔒	0	()		
Includes	•	·		
, lets				
Indiatos				
ideliget Voteling	Adi Inpot Bath Case Bath Date	Azacidel Event		Derit Jahlowi-Derit Jakalese 🗒 🕻 🕻 🖗
Secutly Analysis	() Salas Deathel () Hat The			x ()
Seuri) Ordestalon 🛛 🔻	. Aert Name	Aktier., Aktige	Satus Allected., Venicad., Owner	Creation First Coc Last Coc Planned Latels Operation
Sting v				venne rente univer rente unte upon
	[H	Qisii Anoma'ebooki	H. Estel - Litom	203101

The following figure shows customized alert names.

Figure 13-3 After processing

eutitati v eutiteer v	Upertracting chies 🕸	Epistaer®			tested	Round							
iPasta 🔹													
st lipstite 🔺	0	0											
1088													
kS													
hists													
and the state													
	at hpt sitter i	asona Associated							k K ZS D	DI-3x1	15255	ŝ C	C
ikotų krajųs	At hpd Sattle 3 Q Sat Dated () actor	antione Assisted and							16 H, 25 H	DI-Dc1	35195		
Both Keise utij Loberation 🔹 🗸			in. Atla	Sta	Bal. KR	é. Over	Cedur.		16 K. 25 H				
inipet Indaiq Secul Kapis an) Eclestica 🔹 🔹	() Sala David () viciliar					é. Over	babr. 1870.	R#00.	iste.		105		C (

13.2.2 Configuring and Enabling the Playbook

Scenario

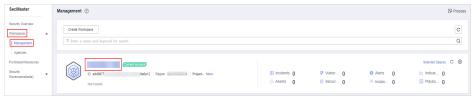
This topic walks you through on how to configure the SecMasterBiz node, enable the automatic renaming of alert name workflow, and enable the automatic renaming of alert name playbook.

Step 1: Configure and Enable the Workflow

Accessing the workflow management page

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

Figure 13-4 Workspace management page



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

Figure 13-5	Workflows	tab	page
-------------	-----------	-----	------

$\langle \cdot $	/ Play	books / Workflows	8														
Security Situation Resource Manager	* *	Playbooks	Workflows	Asset connection	Instance Manage	ement											
Risk Prevention Threat Operations Security Orchestration	•		Pendin	g review O			Not enabled	14			Enabled	1 20					
Objects Playbooks Layouts		N	ame		Dataclass	Workflo	7 Workflo 7	Current	Created	Created	Status [All Updated At	• Descript	• 8	inter a keyword.	Q C] []
Plugins Settings	¥		lert notification via at 19423	tack link analysis 3a617167	Alert	Enabled	General	vt	system	2023/08/08 23:42:38 G		2023/08/08 23 42 40 G	-		Disable Version Managero	ent	
			ne-click release e14t	62e902f	Alert	Not enabled	General	-	system	2023/08/08 23:42:38 G	system	2023/08/08 23:42:41 G	-		Enable Version Manageme	nt Delete	

Copying a workflow version

Step 5 Locate the row containing the **Automatic renaming of alarm names** workflow. In the **Operation** column, click **Version Management**.

Figure 13-6 Version Management page

Playbooks Wo	rkflows Asset connection I	nstance Managem	ent								
	Pending review 0			Disabled ()			Enabled	29		
Add	port							Status	All	• Name •	Enter a keyword. Q C
Name Name		Dataclass	Workflo 🍞	Workflo 🍞	Current	Created	Created	Updated	Updated At	Description	Operation
	ization of HSS alert status 1815-3433-8eef-285ea56ca601	Alert	Enabled	General	vt	system	2023/11/23 19:41:29 G	system	2023/11/23 19:41:33 G	-	Disable Version Management
	renaming of alarm names #038-32#e-9001-6884f4ccbb74	Alert	Enabled	General	vt	system	2023/11/23 19:41:29 G	system	2023/11/23 19:41:33 G	-	Disable Version Management
Cne-dick df20d4d0	release 1054-30de-a1e4-2885571c5410	Alert	Enabled	General	vt	system	2023/11/23 19:41:29 G	system	2023/11/23 19:41:34 G	-	Disable Version Management
	tion and killing of malware -7420-31cd-9090-3299add6d6a4	Alert	Enabled	General	vt	system	2023/11/23 19:41:29 G	system	2023/11/23 19:41:34 G	-	Disable Version Management

- **Step 6** On the **Version Management** page displayed, go to the **Version Information** area, locate the row where the initial version (v1) is listed, 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 **Automatic renaming of alarm names** workflow, go to the **Version Information** area, locate the row containing the copied workflow version, and click **Edit** in the **Operation** column.
- **Step 9** On the drawing page, click the **SecMasterBiz** plug-in and configure it in the **Node Parameters** pane displayed from the right.

For details about SecMasterBiz plug-in parameters, see What Is SecMasterBiz.

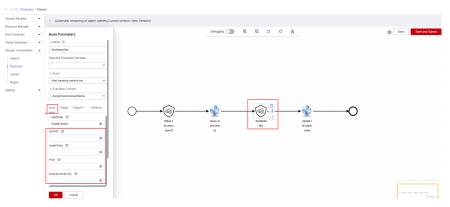


Figure 13-7 SecMasterBiz plug-in

Step 10 After the configuration is complete, click **Save and Submit** in the upper right corner. In the dialog box displayed, click **OK**.

Reviewing a workflow version

- **Step 11** On the **Workflows** page, locate the **Automatic renaming of alarm names** workflow and click **Version Management** in the **Operation** column.
- **Step 12** On the displayed **Version Management** page, locate the row that contains the edited workflow version, and click **Review** in the **Operation** column.

Step 13 In the displayed dialog box, set Comment to Passed and click OK.

Activating a workflow version

- **Step 14** On the **Version Management** page, locate the row that contains the reviewed workflow version and click **Activate** in the **Operation** column.
- Step 15 In the displayed dialog box, click OK.

After a workflow version is activated, the workflow is enabled by default.

----End

Step 2: Configure and Enable the Playbook

Step 1 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-8 Accessing the Playbooks tab

K / Pla	ybooks / Playbooks															
Security Situation	Playbooks Workflows		tion Inclus													
Resource Manager 🔹 💌		Usoftoss Asset connection Instance Management														
Risk Prevention 🔹																
Threat Operations	Pendi	ng review 0		N	lot enabled	10		Enabled 1								
Security Orchestration																
Objects									Status Al	*	Name	Enter a keyword.		0 0	C 0	
Playbooks 2														u lu		
Layouts	Name Name	Deteclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Descri	ption		Operation			
Plugins	Add the IP indica	Alert	Not enabled	vt	R	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23 42 32 GMT+06:00	-			sable More			
Setlings 💌	Alert solfication	Alert	Not enabled	vt	Ø	system	2023/06/08 23 42:32 GWT+08:00	system	2023/08/08 23:42:32 GMT+08:00	-			table More	•		

- **Step 2** On the **Playbooks**, locate the row that contains the playbook for automatically renaming alert names, and click **Enable** in the **Operation** column.
- **Step 3** In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

What Is SecMasterBiz

SecMasterBiz is a plug-in used in the workflow for automatically renaming alert names. It analyzes and processes web shell alert names. You can combine alert names in the way you want and let the system return the alert names as you configured.

The SecMasterBiz plug-in contains multiple actions. The **changeWebshellAlertName** action provides several input parameters for you to customize. Each input parameter indicates an analysis dimension.

You can select different dimension parameters as required to combine alert names. If a parameter is not selected, then it will not be returned in alert names by default. If you enter \mathbf{y} , this parameter is selected. If you enter \mathbf{n} , this parameter is not selected. If you leave this parameter blank, this parameter is not selected.

Parameter	Description	Value Range
severity	Indicates the alert severity.	y/n

Table 13-1 Parameter configuration

Parameter	Description	Value Range
createTime	Time the alert was created.	y/n
srclp	Attack source IP address.	y/n
sourceCountryCity	Country or city from where the attack source IP address originated.	y/n
destinationIp	IP addresses attacked	y/n
destinationCountryCity	Country or city where the attacked object locates.	y/n

13.2.3 Verifying the Playbook

Scenario

If the playbook for **Automatic renaming of alarm names** is enabled, you can verify the playbook status.

This topic describes how to verify a playbook.

Procedure

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

Figure 13-9 Workspace management page

SecMaster	Management ③				Proces
Security Overview Workspaces	Credit Workspace To fine a name and layered for seach.				C
Purchased Resources Security Governance(beta)	Contract Access 0 458977 (Mart 2 Report Peped- Mare Not hoted	i Incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	 Alerts Instan 0 	Selected Spaces C 🛞 indicat 0 Playbo 0

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

Figure 13-10 Alerts

							Teeley	This week This i	ayadh i	Castornie
andiod Alerts		-		Auto		Manual		Alerts Number		
7	(7	 High 5 Modia Tipe 1 	0		0		7		
AND Associated Event	1000 Close 1000 -	nier a keyword. By delault, Bu								0
Type :	Alert Name :	Alarm Severity :	Source IP Address		Stature :	Data Source Pred	Owner :	Creation Time :	Operation	
Vieto attactor	[CiceedBySecMaster]	O man		Unknown	O Open Handled au	Host Security Service		2024/02/07 10:33:00.5	Operation +	
Vieto allar ba	CrosedDySecMaster3	O High		Unknown	Open: Handled au	Host Security Service		2024/02/07 10:27:59.4	Operation +	
Web sheet	[ClearedBySecMaster]	O 1995		Unknown	Open Handled au	Host Security Service		2024/02/07 10:22:58 8	Operation -	
Web shell		O High		Unknown	Open Unhandled	Heat Security Service		2024/02/07 10 18:55.3	Operation v	
Matching use of loten Assessed user behavior		O righ		Unimpun	Open: Unhandled	Heat Security Service	-	2024/02/05 16:27:47.6	Operation +	
Encrypted currency mi Matware		O Motion		Underson	Open Unhandled	Hust Incarity Service		2024/02/06 16 27 07 2	Operation +	
DNS protocol attacks		O Terr		Unknown	Open Unhandled	Hand Research Revise		2024/02/04 16 26 16 8	Operation +	

Step 5 Click Add. Configure parameters in the Add slide-out panel.

- Alert Name: Enter a name for the alert.
- Alert Type: Select Web attacks and then Web shell.
- **Debugging data**: Select **Yes**.
- **Description**: Description of the custom alert.
- Retain the default values for other parameters.

Step 6 Click OK.

Step 7 Refresh the page and check whether alert names have been updated.

If the playbook is enabled, the playbook automatically processes new alerts and displays new alert names.

Figure 13-11 Output when no parameters are selected (default)

C / Alerta								
Security Shadon 🔹 Resource Manager 👻	Urgent handing of Alerts 👁	Expired arest @		Aiet States @		Alerts Number @		
Fish Prevention • Thread Operations •	0	0						
koderts Karta		•						
Induators Intelligent Madeling	Add Instit Extra Date Basis Deets Associated Freed					Dec / 6 1011 00 0	0.00 - Dec 11, 2023 23.59.58	
Decarity Analysis Decarity Octoebadan 💌	Q Status Roused @ AN THY							× 0
tating: •	Alexi Name Facil attackl Hackers bunched a tabl giber attack on tenant service	Alert Sevenity Alert Type O Field Absorbal bebrark b	Status Affected Assets Enabled -	Verification Status Owner Untroave	Creation Time First Occurrence Tu 2823/12/11 11:32:22 2623/12/11 11:32:16	Last Occurrence Tr., Panned Gosure Tr		Operation Operation +

Figure 13-12 Output when only severity is selected

C ANTO													
Security Situation •													
Emourie Manager •	Urgent handling of Alerts @	Expired alert @				Alert Status @				Alerts Number @			
Kos Proverbox W	-	-											
hreat Operations	0	0											
Incolanta													
AND .													
indicators													
Intelligent Madeling	Add Impot Extra Data State Associated Coard										Gast 05, 2023 80 96 98	- Dec 11, 2023 23 58 58	m 🖪 0
becurity Analysis	CL Server Develop (D) Ant Inter												*
letings -	Avent Name	Aint Severity	Alert Type	Status	Affected Assets	Verification Status	Owner	Creation Time	First Occurrence Tu-	Last Occurrence TL-	Planned Closure N	Labels	Operation
	Palai about Nasters launched a faid syleer allack on lenard sense.	O Foto	Almannal nationship	Evaluation		Gritmaum	_	2023/12/11 11 32 22	2823/12/11 11:32:46				Operation +

----End

13.3 Attack Link Analysis Alert Notification

13.3.1 Overview

Scenario

After a domain name was attacked, the attacker typically further attacked the backend servers. SecMaster provides an attack link analysis playbook that will automatically send alert notifications to specified operations personnel once it detects server attacks.

How the Playbook Works

The **Attack link analysis alert notification** playbook has been matched the **Attack link analysis alert notification** workflow. This workflow needs to use Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.

The **Attack link analysis alert notification** workflow queries the list of website assets associated with the assets affected by HSS alerts through asset associations. By default, a maximum of 3 website assets can be queried.

- If there are associated website assets, the workflow queries WAF alerts generated for each website asset from 3 hours ago to the current time. A maximum of 3 alerts can be queried. The alert types include XSS, SQL injection, command injection, local file inclusion, remote file inclusion, web shell, and vulnerability exploits.
- If there is an alert generated in WAF, the workflow associates the WAF alert with the corresponding HSS alert and sends a notification the email box you specified through SMN.

Empty Obtain t he affect Obtain he time Convert the form he curre rt notif Empty Emn Ş Ð Obtain Obtain t he asse he assoc site as iated as ets in a Analyze each assoc Empt Ŧ Ŧ T Ð Obtain t Put the Filter a Obtain t Associa e websit he asso alerts iated al n the I vebsite iated we =

Figure 13-13 Attack link analysis alert notification

Prerequisites

• You have enabled HSS and WAF alert access in SecMaster on the **Data** Integration page under the **Settings** pane in the current workspace. For details about how to enable HSS and WAF alert access in SecMaster, see **Data Integration**.

Figure 13-14 Alert access

< Data Inf	egration							
Security Situation Resource Manager	• •	Cloud Service Access						
Risk Prevention	-							
Threat Operations	Ŧ	•						
Security Orchestration	*	Access Service Logs						
Collection		Cloud Services	Logs	Region Level	Workspace	Storage Location (2)	Lifecycle	Automatically converts alarms
Management		Web Application Firewall (2)	WAF attack log ③	Region		/ isap-cloudlogs-0a60703a7500f	7 Days	
Data Integration		Neo Approach Priewall	WAF access log (?)	Region		-1-1-	7 Days	-
Checks		Object Storage Service (2)	Object Storage Service acce	Region		/ isap-cloudlogs-0a60703a7500f	180 Days	-
Customization	4	IPS	IPS attack log	Region		/ isap-cloudlogs-0a60703a7500f	180 Days	-
		Identity and Access Management	IAM audit log	Region		/ isap-cloudlogs-0a60703a7500f	180 Days	-
			HSS alarm	Region		/ isap-cloudlogs-0a60703a7500f	7 Days	
		Host Security Service (2)	HSS vulnerability scan result	Region		/ isap-cloudlogs-0a60703a7500f	180 Days	
			HSS log	Region			7 Days	-

• On the **Resource Manager** page in the current SecMaster workspace, click an asset name. On the asset details page displayed, associate the website asset with the server asset.

Figure 13-15 Associated Assets

< / / Resource Mana	iger / Resource Detail												
Security Situation 🛛 👻													
Resource Manager	Resource Name	ecs-,											
Resource Manager	Owner	-L Service system		-2		Departro	int	-2					
Risk Prevention •													
Threat Operations 👻	ECS status	ACTIVE	Ι,	Alert		Incide	nt			Vulnerability		Asset	
Security Orchestration 👻				0			0			()		2
Setiona 👻	Resource Information			0			0				,		~
Setingi 👻	Resource Type	doudservers	1	Associated Assets	Alert	Incident	Vulnerability						
	Resource Specifications	c7.targe.2.tinux	1.2										
	Resource ID	4200 305181											0 0 C 0
	05	Linux											• • • •
	Image Name	CentOS 7.6 64bit		Q Enter a kaywe	rd. By delault, the	search is parform	ed by name or a c	combination of sea	arch criberia				
				Resource	iarne		Resource Type			Name of the de	partment to which the a	Environment	Supplier Type
	Environment Information	n		vpc-			Virtual Private Cic	ud (VPC)		-		Cloud service	
	Region						ElasticIP			-		Cloud service	
	Environment	cloudservice					ENGOLIP					CAUSI SERVICE	
	AZ	A27											
	Enterprise project ID.	436052 7cbec8893											
	User ID	2522a 54aa000											

Verification

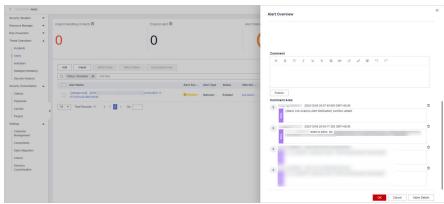
After the attack link analysis notification playbook is executed, server assets and the website assets will be associated based on corresponding HSS and WAF alerts.

Figure 13-16 Associated alerts

ecurity Situation					Alert Overvi	ew							
esource Manager 💌	Urgent handling of Alerts 🕲	Expired alert @		Alert Statu	Alarm Severity	Medun v					Owner		09_945
isk Prevention	0	0		(Disposal Sugg Recommended Method								
Alerts					Basic Informat	on							
Indicators					Alert Name		[dangercmd]						100
Intelligent Modeling	Add Import Eatch Close I	Batch Delete Associated Event			Alert ID		11957224-c866-	4950-9067-444		nment Account		awei Cloud	
Security Analysis	Q Status: IDisabled @ Add filter				Alert Type		Mahvare/Malici	ous Software	Data 5 Feidur	lource Product es	Hus	anel	
curity Orchestration	Alert Name		Alert Sev Alert Type	Status Affected	Stage		-		Data 5	iource Product	Name Ho	st Security Servi	DØ
Objects	(dangerond) (H	2023-11-	O Medium Malware/	Enabled ecs-test to	First Occurrent	ie Time	2023/11/23 11:3	13:36.000 GM	Last O	courrence Tim			
Playbooks	11716.04.43.000-06.00			Carro Contract	Time To Detect	ion			Time 1	o Response	-		
Layouts Plugins	10 v Total Records: 11 < 1 2 >	Ga			Associated in	dicators	Associated	Verts	Associated	Incidents	Payload		
ingi 🔺												9 0	C Θ
Collection					Alert N	Alert S	Alert T	Status	Last 0	First 0	Reaso	Labels	Creatio
Aanagement Components					Evuin.	O Low	Web att	Enabled	-	2023/1	-	(14)	2023/1
lata Integration					Duin.	O Low	Web att	Enabled	-	2023/1	-	-	2023/1
Jaca magraton Zhecks					Evuin.	O Low	Web att	Enabled	-	2023/1	-	()	2023/1
Directory					[[vuin	O Low	Web att.	Enabled		2023/1		-	2023/1
Directory Dustomization													
										c	K Ci	ancel A	arn Det

Comments on the corresponding alert added to the playbook

Figure 13-17 Comment



Alert notification email sent to specified personnel

Figure 13-18 Email notifications

2023/12/5 () 20 pmail smn			
SecMaster Aler			
	(Notifications		
牧件人 📕			
[Alert (ID=c Associated Alerts: ("id":"1b92be9c-c1 50fe-4744-b821-67]]: Attack link detected in	· · · ·	Handle the alert as soon as possible.
If you wish to stop receiving notific	ations from this topic, please click the link below to unsubs	cribe. This is a private link. Please keep it secure.	
	om/smn/unsubscribe.html?subscription_urn=urn:smn:		ster-Notification:050c3428fc904300a5d427fd3428734c&locale=en-us®ion=

13.3.2 Creating and Subscribing to a Topic

Scenario

The **Attack link analysis alert notification** workflow needs to use Simple Message Notification (SMN) to create and subscribe to a notification topic.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, click and choose **Management and Governance** > **Simple Message Notification**.
- **Step 3** Create a topic.
 - 1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

Figure 13-19 Create Topic

Simple Message Notification	Topics ③				Create	Topic
Dashboard Topic Management	You cannot search for topics by tag and oth Q Search or filter by keyword.	er search criteria at the same time, or the sear	ch results may be invalid.		c	۲
Topics	Name(ID \$		Enterprise Project \Leftrightarrow	Display Name 👙	Operation	
Subscriptions Message Templates	72d8155d93ba436da4f475efa7553342	um.smn.cn-south-1:0a60703a750013a	default		Publish Message Add Subscription More +	
	AUTO	um.smn.cn-south-1:0a60703a750013a	default		Publish Message Add Subscription More +	
	10 🔻 Total Records: 2 < 1	>				

- 2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.
 - Topic Name: SecMaster-Notification is recommended.
 - Display Name: SecMaster notification topic is recommended.
 - Retain the default values for other parameters.

Figure 13-20 Configuring a topic

Create Topic	×
★ Topic Name	SecMaster-Notification The name cannot be changed after the topic is created.
Display Name	SecMaster Notification Topic
	If a display name is specified, the email sender is presented in the format "Display name <username@example.com>" when email messages are delivered.</username@example.com>
★ Enterprise Project	default C Create Enterprise Project Enterprise Project Management Service (EPS) allows you to manage cloud resources and user groups by enterprise project.
CTS Log	
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags C To add a tag, enter a tag key and a tag value below.
	Enter a tag key Enter a tag value Add
	Tags you can still add: 10
	OK Cancel

Step 4 Add a subscription.

- 1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
- 2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
 - Protocol: Select Email.
 - Endpoint: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-21 Add Subscription

Add Subscrip	tion			
Topic Name	SecMaster-Notification			
* Protocol	Email	•		
★ Endpoint ⑦	Endpoints		Description	
	username@example.com			
	Add Endpoint			
	Batch Add Endpoints			

----End

13.3.3 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Attack link analysis alert notification** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **attack link analysis alarm notification** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Attack link analysis alert notification** playbook.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing** to a **Topic**.

Procedure

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

Figure 13-22 Workspace management page

SecMaster	Management 💮				Process
Security Overview Workspaces Management Agencies	Could Hippingson $\label{eq:generalized_state} T$ for a name and layered for search.				C
Purchased Resources Security Governance(beta)	Grand accel	incidents 0 Assets 0	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C ⑧ iv Indicat 0 ⊡ Playbo 0

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

Figure 13-23 Accessing the Playbooks tab

< // //	Playbool	ks / Playbooks										
Security Situation	•	Plantasta Maddaus	land and a	dias Jacob	Marca							
Resource Manager	•	Playbooks Workflows	Asset conner	ction Insta	nce Manager	nent						
Risk Prevention	•											
Threat Operations	•	Pendir	ng review 0			1	lot enabled	10		Enabled 1		
Security Orchestration	•											
Objects												
Playbooks 😕										Status Al	* Name	Enter a keyword. Q C G
Layouts		Name Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operation
Plugins		Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GWT+08:00	system	2023/06/08 23:42:32 GMT+06:00	-	Enable More +
Settings	*	Alert notification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GWT+08:00	system	2823/06/06 23 42 32 GMT+06:00	-	Enable More +

- **Step 5** On the **Playbooks** page, locate the row that contains the **Attack link analysis alert notification** playbook and click **Enable** in the **Operation** column.
- **Step 6** In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.4 Automatic Notification of High-Risk Vulnerabilities

13.4.1 Overview

Scenario

SecMaster provides a playbook that can automatically notify of high-risk server vulnerabilities to operations personnel.

How the Playbook Works

The **Automatic notification of high-risk vulnerabilities** playbook has been matched the **Automatic notification of high-risk vulnerabilities** workflow. This workflow needs to use Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.

If a high-risk vulnerability was reported by HSS, SMN sends a notification to operations personnel.

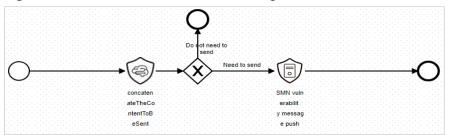


Figure 13-24 Automatic notification of high-risk vulnerabilities workflow

Prerequisites

You have enabled Host Security Service (HSS) alarm access on the **Data** Integration page under the **Settings** pane. For details, see **Data Integration**.

< / / Data Ir	tegration							
Security Situation Resource Manager	• •	Cloud Service Access						
Risk Prevention	*							
Threat Operations	*	•						
Security Orchestration	•	Access Service Logs						
Collection	1	Cloud Services	Logs	Region Level	Workspace	Storage Location (2)	Lifecycle	Automatically converts alarms
Management		Web Application Firewall (?)	WAF attack log (?)	Region	-		7 Days	
Data Integration		Theo Application Financial (2)	WAF access log (?)	Region			7 Days	-
Checks		Object Storage Service (2)	Object Storage Service acce	Region		/ Isap-cloudlogs-0a60703a7500f	180 Days	-
Customization	4	IPS	IPS attack log	Region		/isap-cloudlogs-0a60703a7500f	180 Days	-
		Identity and Access Management (?)	IAM audit log	Region		/ isap-cloudlogs-0a60703a7500f	180 Days	-
			HSS alarm	Region	-		7 Days	
		Host Security Service (?)	HSS vulnerability scan result	Region		/ isap-cloudlogs-0a60703a7500f	180 Days	
			HSS log	Region	-		7 Days	-

To view accessed data, choose **Risk Prevention** > **Vulnerabilities**.

Figure 13-26 Viewing alerts

ecurity Situation 💌								
esource Manager	VulnerabilityStatistics							
isk Prevention	Vuinerability Type Dist	ribution	Top 6 Vulnerabilities	Vulnerability ID	Vuinerability Type	Top 5 Vulnerable Resources		
Baseline Inspection			Name1D 😄	Affected		e High e Medium e Low		
Vulnerabilities		Einux Vulnerat	olity CVE-2018-25032	1				
Emergency Vulnerability Notices		Windows Vuln	erabilities CVE-2019-2708	1				
Policy management		36 Web-CMS Vul	nerability CVE-2020-35557	1		ecs-8d98		
ecurity Orchestration		Application Vu	Inerabilities CVE-2020-36558	1				
ettinga -			CVE-2021-0920	1				
	Linux Vulnerabilities	Windows Vulnerabilities Web	CMS Vulnerabilities Application Vul	erabilities				
	Linux Vulnerabilities Batch Repair	Windows Vulnerabilities Web-	CMS Vulnerabilities Application Vult	erabilities			C	
	Batch Repair			erabilities			C	1 C (
	Batch Repair	Import		Affected Assets	Vuinerability ID	Last Scanned	Landied Land	i c 4
	Batch Repair Q. Enter a keyword Vulnerability N	Import	a combination of search criteria.		Vumerability ID CVE-2021-45075	Last Scanned 2023/05/02 17:46/46 206 GMT+		I C 4
	Batch Repair Q Enter a keyword Vutnerability N Euler05-54-20	Import By default, the search is performed by name or Iame graded	a combination of search criteria.	Affected Assets		2023/03/02 17:40:46 206 GMT+	Handled Handled	i c e
	Batch Repair Q Enter a keyword Vutnerability N EsterOS-SA-20 EsterOS-SA-20	Import Dry default, the search is performed by name or ame graded 22-1317 Importa Medium	a combination of asarch others. ID Euler05-SA-2022-1317	Affected Assets	CVE-2021-45078	2023/03/02 17:46:46:266 GMT+ 21-203 2023/03/02 17:46:46:295 GMT+	Handled Handled Handled	
	Batch Repair Q Enter a keyword Valnerability N ExterOS-SA-20 ExterOS-SA-20 ExterOS-SA-20	Import Dy dufuell, the assurch is performed by name or anne praded 22-1377 Import © Medium 22-1328 Import © Medium	a combination of search orders. 10 Euler05-5A-2022-1317 Euler05-5A-2022-1328	Affected Assets	CVE-2021-45075 CVE-2021-0920,CVE-202	2023/03/02 17:46:46 206 GMT+ 2023/03/02 17:46:46 206 GMT+ 2023/03/02 17:46:46 206 GMT+ 21:4190 2023/03/02 17:46:46 206 GMT+	Handled Handled Handled	

13.4.2 Creating and Subscribing to a Topic

Scenario

The **Automatic notification of high-risk vulnerabilities** workflow uses Simple Message Notification (SMN) to send notifications. You need to create and subscribe to a topic for receiving notifications.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, click and choose **Management and Governance** > **Simple Message Notification**.
- **Step 3** Create a topic.
 - 1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

Figure 13-27 Create Topic

nple Message tification	Topics (?)	opics 💮								
ashboard opic Management	You cannot search for topics by tag and other Q. Search or filter by keyword.	r search criteria at the same time, or the searc	h results may be invalid.		c ø					
Topics	Name(1D \$	URN \$	Enterprise Project 💠	Display Name 💠	Operation					
Subscriptions Message Templates	72d885d93ba438da4f475efa7553342	um:smr:cn-south-1:0a60703a7500f3a	default	-	Publish Message Add Subscription More +					
Message Templates	AUTO^ 5b690e781be54432a51210s8bce30c92	um:smn:cn-south-1:0a50703a7500f3a	default		Publish Message Add Subscription More +					
	10 🔻 Total Records: 2 < 1	>								

- 2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.
 - **Topic Name: SecMaster-Notification** is recommended.
 - **Display Name**: **SecMaster notification topic** is recommended.

- Retain the default values for other parameters.

Figure 13-28 Configuring a topic

Create Topic	×							
* Topic Name	SecMaster-Notification							
	The name cannot be changed after the topic is created.							
Display Name	SecMaster Notification Topic							
	If a display name is specified, the email sender is presented in the format "Display name <username@example.com>" when email messages are delivered.</username@example.com>							
* Enterprise Project	default C Create Enterprise Project							
	Enterprise Project Management Service (EPS) allows you to manage cloud resources and user groups by enterprise project.							
CTS Log								
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags C To add a tag, enter a tag key and a tag value below.							
	Enter a tag key Enter a tag value Add							
	Tags you can still add: 10							
	OK Cancel							

Step 4 Add a subscription.

- 1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
- 2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
 - **Protocol**: Select **Email**.
 - **Endpoint**: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-29 Add Subscription

Add Subscrip	tion			
Topic Name	SecMaster-Notification			
* Protocol	Email	•		
★ Endpoint ⑦	Endpoints username@example.com		Description	
	Add Endpoint Batch Add Endpoints			

----End

13.4.3 Configuring an Asset Connection

Scenario

Before using the **Automatic notification of high-risk vulnerabilities** workflow, you need to configure the **SMN notification token for operational personnel** asset connection first.

This topic describes how to configure an asset connection.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

Procedure

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

Figure 13-30	Workspace	management page
--------------	-----------	-----------------

SecMaster	Management ①	Process
Security Overview Workspeces	Childs Workspace If Enter a mome and legenered for search.	C
Purchased Resources Security Governance(beta)	0 addm17 add#12 Rugon Project- Mare Ill incidents 0 Valmer 0 0 Atents 0 Not hoted. Interface Interface Ill incidents Ill incidents Ill incidents 0 Ill incidents 0 <t< th=""><th>Selected Spaces C 🛞 iv Indicat 0 Flaybo 0</th></t<>	Selected Spaces C 🛞 iv Indicat 0 Flaybo 0

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 13-31 Asset connection tab

Z												
< / / Playbook Mar	nageme	entry	vaset connection									
Security Situation	•	Dia	vbooks Workflow	vs Asset connec	tion Instance Ma	nanomont						
Resource Manager	÷	r ia)	laybooks Workflows Asset connection Instance Management									
Risk Prevention												
Threat Operations			Add								С	
	Ť		V Search by name								Q	
Security Orchest	*			-								
Object Management			Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation		
Playbook			Alert handling meth	SecMasterBiz	system	2023/06/24 14:35:52 GMT	-	-	Alert handling method set	Edit Delete		
Management			VPC authentication	ACL	system	2023/06/24 14:35:52 GMT		-	VPC authentication	Edit Delete		
Layout management			SMN notification to	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for operat	Edit Delete		
Plugin Management												
Settings	. 1		SecMaster authenti	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SecMaster authentication token	Edit Delete		
			CFW authentication	HTTP	system	2023/06/24 14:35:52 GMT	-	-	CFW authentication token	Edit Delete		

- Step 5 On the Asset connection page, locate the row that contains the SMN notification token for operational personnel connection and click Edit in the Operation column.
- **Step 6** On the **Edit** pane sliding out from the right, configure endpoint information.

Edit		>
★ Connection Name	SMN notification token for operational persor	
Description	SMN notification token for operational personnel	
★ Plug In	HTTP •	
Created By	system	
Created	2023/11/24 11:11:10 GMT+08:00	
Modified By		
* Attachment Type	Agency AK&SK Username & Password Other	
Credential		
endPoint https://{	{SMN_ENDPOINT}}/v2/{{project_id}}/	

Figure 13-32 Editing an asset connection

endPoint: Set this field to **https://**{{*SMN_ENDPOINT*}} v2 /{{*project_id*}} **notifications/topics**/*urn:smn:*{{*region_id*}}:{{*project_id*}}:SecMaster-Notification.

- SMN_ENDPOINT: Enter the domain name for invoking the SMN service. The value is in the format of endpoint:443. Obtain the endpoint information from the Regions and Endpoints. For example, if you choose CN North-Beijing4, enter "smn.cn-north-4.myhuaweicloud.com:443" in this field.
- project_id. Enter the ID of the project that the current workspace belongs to. To view the project ID, take the following steps:
 - a. Log in to the management console, hover the mouse over the username in the upper right corner, and select **My Credentials** from the drop-down list. The **API Credentials** page is displayed by default.
 - b. On the API Credentials page, view the project ID in the project list.

Figure 13-33 Project ID

My Credentials	API Credentials ③			
API Credentials	UM User Name	Account Name		
	WM User ID 2522a 354ee890 🗗	Account ID	0996e 0187c0 🗇	
	Projects		Enter a project name.	Q
	Project ID 😄	Project Name 💠	Region ¢	
	3c63c 2d72b77b	ap-coutheast-2	AP-Bangkok	

- urn:smn:{{region_id}}:{{project_id}}:SecMaster-Notification. Enter the URN of the SMN topic for sending email notifications. To view the URN, take the following steps:
 - a. In the upper left corner of the page, click and choose **Management** and Governance > Simple Message Notification.

- b. In the navigation pane on the left, choose **Topic Management** > **Topics**.
- c. In the topic list, view the topic URN of the topic created in **Creating and Subscribing to a Topic**.

Figure 13-34 Topic URN

Simple Message Notification	Topics 💮	Topics () 🕴 Fieldus 🔽									
Deshboard		n criteria at the same time, or the search results may be invalid.									
Topic Management	Q Search or filter by keyword.				C						
Topics	Name 10 💠	URN ¢	Enterprise Project 💠	Display Name 💠	Operation						
Subscriptons Nessage Templates	SecNater Notification 72:000 i53342	umann: 1442d.	oriuit	-	Publish Message Add Subscription Nore +						
	AUTO5669(boe30:32	L. un sm. K01412d.	debut		Publish Message Add Subscription Nove +						
	10 • Tabil Recents: 2 (1)										

Step 7 After the configuration, click **OK**.

----End

13.4.4 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Automatic notification of high-risk vulnerabilities** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Automatic notification of high-risk vulnerabilities** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Automatic notification of high-risk vulnerabilities** playbook.

Prerequisites

- You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.
- Asset connections have been configured. For details, see **Configuring an** Asset Connection.

Procedure

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

Figure 13-35 Workspace management page

SecMaster	Management ③				D Process
Security Overview Workspaces	$\begin{tabular}{c} \hline \label{eq:state} \hline $$ Total a name and layout for seach. \end{tabular}$				C
Purchased Resources Security Governance(beta)	O #08977 (Media Concert O #08977 (Media 2) Region (Project- More Not house.	 Incidents 0 Assets 0 	♥ Vulner 0 ⊜ Securi 0	O Alerts 0 instan 0	Selected Spaces C 🗟

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

Figure 13-36 Accessing the Playbooks tab

Resource Manager			Asset conner	tion Insta	nce Manager										
	•	Playbooks Workflows	Asset Colliner	LIUII IIISIA	ice Manager	neni									
Risk Prevention	*														
Threat Operations	+	Pen	ting review 0				Not enabled	10		Enabled 1					
Security Orchestration															
Objects															
Playbooks 💡										Status Al	* Name	• Enter a keywor	i. (C	Ľ
Layouts		Name	Detecless	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description		Operation		
Plugins		Add the IP indica.	Alert	Not enabled	vt	ø	system	2023/06/08 23:42:32 GMT+06:00	system	2023/06/08 23 42 32 GMT+06:00	-		Enable More -		

- **Step 5** On the **Playbooks** page, locate the row that contains the **Automatic notification of high-risk vulnerabilities** playbook and click **Enable** in the **Operation** column.
- **Step 6** In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.5 Automatic Notification of High-Risk Alerts

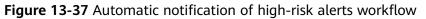
13.5.1 Overview

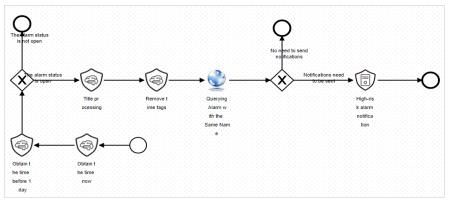
Scenario

SecMaster provides this playbook for automatically notifying you of new high-risk alerts after removing repeated ones.

How the Playbook Works

The **Automatic notification of high-risk alerts** playbook has been matched the **Automatic notification of high-risk alerts** workflow. This workflow uses Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.





Verification

Email sent when the playbook was triggered by high-risk alerts

Figure 13-38 Alert notification email

P	pmail_smnhw01 •••••• SecMaster High-risk alarm notification	
Affecting	risk-alarm(ID=58a9e≦38bf61fa9d5)]∶Alert_test, Please dealing it as soon. g resource: ype: Abnormal network behavior/Abnormal access frequency of IP address	

13.5.2 Creating and Subscribing to a Topic

Scenario

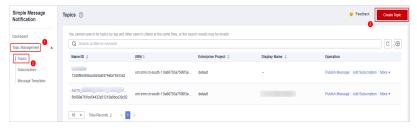
The **Automatic notification of high-risk alerts** workflow uses Simple Message Notification (SMN) to send notifications. You need to create and subscribe to a topic for receiving notifications.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, click and choose **Management and Governance** > **Simple Message Notification**.
- **Step 3** Create a topic.
 - 1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

Figure 13-39 Create Topic



- 2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.
 - **Topic Name**: **SecMaster-Notification** is recommended.
 - **Display Name**: SecMaster notification topic is recommended.
 - Retain the default values for other parameters.

Figure 13-40 Configuring a topic

Create Topic	×								
* Topic Name	SecMaster-Notification								
	The name cannot be changed after the topic is created.								
Display Name	SecMaster Notification Topic								
	If a display name is specified, the email sender is presented in the format "Display name <username@example.com>" when email messages are delivered.</username@example.com>								
* Enterprise Project	default C Create Enterprise Project								
	Enterprise Project Management Service (EPS) allows you to manage cloud resources and user groups by enterprise project.								
CTS Log									
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags C								
	To add a tag, enter a tag key and a tag value below.								
	Enter a tag key Add								
	Tags you can still add: 10								
	OK								

Step 4 Add a subscription.

- 1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
- 2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
 - Protocol: Select Email.
 - Endpoint: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-41 Add Subscription

Add Subscription							
Topic Name	SecMaster-Notification						
* Protocol	Email	•					
* Endpoint 🕐	Endpoints username@example.com	Description					
	Add Endpoint Batch Add Endpoints						

----End

13.5.3 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Automatic notification of high-risk alerts** workflow is enabled by default. You do not need to manually enable it. The

initial version (V1) of the **Automatic notification of high-risk alerts** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Automatic notification of high-risk alerts** playbook.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-42 Workspace management page

SecMaster	Management () (Process
Security Overview Workspaces Management Agencies	Credit With Space C If Enter a more and legened for search. Q
Purchased Resources Security Governance(beta)	Selected Space: C ()

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

Figure 13-43 Accessing the Playbooks tab

< / / Pitybods / Pitybods														
Security Situation	٠	Playbooks Workflows	Asset conner	eties Jacobase										
Resource Manager	٠		Asset colliner	cilon misiano	e Managerr	ien.								
Risk Prevention	٠													
Threat Operations	ř	Pendi	ing review 0			N	lot enabled	10		Enabled 1				
Security Orchestration	•													
Objects										Status Al	* Name	Enter a keyword.	QC	
Playbooks 2										Sidius	* Name	 Enter a keyword. 	u c	60
Layouts		Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description	c	peration	
Plugins Settinos	Ţ	Add the IP indica	Alert	Not enabled	v1	Ø	system	2023/06/08 23:42:32 GMT+06:00	system	2023/06/08 23:42:32 GMT+06:00	-	E	nable More 🔻	
orangs	•	Alert notification	Alert	Not enabled	vt	Ø	system	2023/06/08 23 42:32 GWT+08:00	system	2023/08/08 23 42 32 GWT+08:00	-	E	nable More 🔻	

- **Step 5** On the **Playbooks** page, locate the row that contains the **Automatic notification of high-risk alerts** playbook and click **Enable** in the **Operation** column.
- **Step 6** In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.6 Automatic Security Blocking of WAF Attacks

13.6.1 Overview

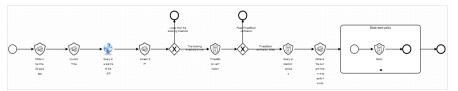
Scenario

SecMaster provides this built-in playbook to automatically blacklist source IP addresses reported in high-risk alerts in WAF.

How the Playbook Works

The Automatic security blocking of WAF attacks playbook has matched the Automatic security blocking of WAF attacks workflow.

Figure 13-44 Automatic security blocking of WAF attacks



Prerequisites

• You have enabled WAF access logs or WAF attack logs on the **Data** Integration page under **Settings** in the current workspace. For details, see Data Integration.

Figure 13-45 Enabling Access to WAF logs

< / Data Inte	C i i aa megalon								
	-	Cloud Service Access							
Risk Prevention									
Threat Operations	*	Ψ.							
Security Orchestration	•	Access Service Logs							
Collection		Cloud Services	Logs	Region Level	Workspace	Storage Location ③	Lifecycle	Automatically converts alarms	
Management Components		Web Application Firewall	WAF attack log (?)	Region		/ isap-cloudlogs-0a60703a750073a02tbac014	7 Days		
Data Integration		WAF access log (?)	Region		/ isap-cloudlogs-0a60703a7500f3a92bac014	7 Days	-		
Checks Directory		Object Storage Service 💿	Object Storage Service access log	Region		/isep-cloudlogs-0a60703a75000a82fbac014	180 Days		
Customization	IPS	IPS attack log	Region		/ isap-cloudlogs-0a90703a750003a92fbac014	180 Days	-		
		Identity and Access Management	IAM audit log	Region		/ isap-cloudlogs-0a90703a750003a92fbac014	180 Days	-	
			HSS alarm	Region	-	-1-1-	7 Days		
		Hast Security Service ⑦	HSS vulnerability scan result	Region		/ isap-cloudlogs-0a90703a750003a92fbac014	180 Days		

• The ThreatBook quota is sufficient.

Verification

If the IP address is blocked, the IP address should be included in the WAF blacklist. The procedure is as follows:

- 1. Log in to the WAF console, go to the **Policies** page, and click the name of the target protection policy.
- 2. On the protection policy details page, click **Blacklist and Whitelist** in the **Protection Details** area. You can see that the IP address is listed in the WAF blacklist.

Figure 13-46 Blacklist and Whitelist

Policies / policy_		 Feedback
policy_ 2 <	522 GMT+88 00	Add Domain Name Delete
Protection Status Domain Name		
Policy Details	Configures blacklists or whitelists to improve site security.	
Enter a keyword. Q	Add Rule Dence IP address or IP address ranges that can be added: 100	Rue name + Q C
 Basic Web Protection 	Rule Name Rule ID IP Address/Range/Gr Protective Action Known Attack Source Rule Status	Added Rule Description Operation
API Security	SedMaste_Discline1 ID707035e1fe435abo5 Intervention Disck No Intervention Disck	Nev 15, 2923 11:46:47 Disable Delete Modify
CC Allack Protection		
Precise Protection		
Blackbist and Winteest		
Knewn Allack Source		
Geolocation Access Control		

13.6.2 Configuring an Asset Connection

Scenario

Before using **Automatic security blocking of WAF attacks** workflow, you need to configure the API key of the ThreatBook plug-in used for the workflow. You can obtain it in the **threatbook authentication token** asset connection.

This topic describes how to configure an asset connection.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

Procedure

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

Figure 13-47 Workspace management page

SecMaster	Management () Process	
Security Overview Workspaces	Center Wannapee C If Center a name and legenerif for search. Q	
Purchased Resources Security Governance(beta)	Image: Construction Selected Space: C O Image: Construction Image: Construction Image: Construction O Value: O Arefs: 0 Image: Construction Image: Construling Image: Construling <	

Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 13-48 Asset connection tab

< / / Playbook Ma	inageme	int / Asset connection									
Security Situation	•	Playbooks Workflor	ws Asset connec	tion Instance Ma	inariement						
Resource Manager	•										
Risk Prevention	*										
Threat Operations	•	Add V Search by name								C	
Security Orchest	•									ų	
Object Management		Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation		
Playbook		Alert handling meth	SecMasterBiz	system	2023/06/24 14:35:52 GMT	-	-	Alert handling method set	Edit Delete		
Management		VPC authentication	ACL	system	2023/06/24 14:35:52 GMT	-	-	VPC authentication	Edit Delete		
Layout management		SMN notification to	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SMN notification token for operat	Edit Delete		
		SecMaster authenti	HTTP	system	2023/06/24 14:35:52 GMT	-	-	SecMaster authentication token	Edit Delete		
		CFW authentication	HTTP	system	2023/06/24 14:35:52 GMT	-	-	CFW authentication token	Edit Delete		

Step 5 On the **Asset connection** page, locate the row that contains the **threatbook authentication token** asset connection and click **Edit** in the **Operation** column.

Step 6 On the **Edit** pane sliding out from the right, configure the token.

- freeApiKey or payApiKey: Set either of them. The value can be obtained after you buy ThreatBook quota.
- **redisHost**: IP address of your Redis resources. If there are no IP addresses, leave this parameter blank.
- **redisPort**: Port of your Redis resources. If there are no such ports, leave this parameter blank.
- **redisPassword**: Passwords of your Redis resources. If there are no such passwords, leave this parameter blank.

Connection Nan	threatbook authenticati	on token	
Description	threatbook authenticati	on token	
r Plug In	ThreatBook	~	
Created By	system		
Created	Dec 14, 2023 10:02:46 G	MT+08:00	
Modified By	-		
redential			
eeApiKey	Enter a keyword.	Ø	
aidApiKey	Enter a keyword.	Ø	
disHost	Enter a keyword.		
disPort	Enter a keyword.		
disPassword	Enter a keyword.	Ø	

Figure 13-49 Edit credential information

Step 7 After the configuration, click **OK**.

----End

13.6.3 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Automatic security blocking of WAF attacks** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Automatic security blocking of WAF attacks** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Automatic security blocking of WAF attacks** playbook.

Prerequisites

Asset connections have been configured. For details, see **Configuring an Asset Connection**.

Procedure

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

Figure 13-50 Workspace management page

SecMaster	Management 💿				Process
Security Overview Workspeces Management Agencies	$\begin{tabular}{c} \hline \label{eq:rescaled} \hline $$ Total Wetgees $$ $$ $$ $$ Total a non- and knyword for search. $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$ $$$				C Q
Purchased Resources Security Governance(beta)	Control Reserver Control Reserver Proper- Nove Ver Annual	 incidents () Assets () 	♥ Vulner 0 ⊜ Securl 0	O Alerts 0 ⊗ Instan 0	Selected Spaces C i Indicat… 0 Playbo… 0

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

Figure 13-51 Accessing the Playbooks tab

< /P	laybooks / Playbooks											
Security Situation 🔹	Playbooks Workflows	Asset corne	ation Inches									
Resource Manager 🔹 🔻	Playbooks Wondows	Asset conne	ction insta	ance Manager	nent							
Risk Prevention 💌												
Threat Operations	Pendi	ing review 0			1	Not enabled	10		Enabled 1			
Security Orchestration												
Objects									Alutur .			
Playbooks 👩									Status All	* Name	 Enter a keyword. Q 	С 🕻 🛞
Layouts	Name	Detaclass	Playbo 7	7 Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operation	
Plugins	Add the IP indica	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GMT+08:00	system	2023/06/08 23:42:32 GMT+06:00	-	Enable More +	
Setlings 💌	Alert notification	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GWT+08:00	system	2823/06/08 23 42 32 GWT+06:00	-	Enable More 🕶	

- Step 5 On the Playbooks page, locate the row that contains the Automatic security blocking of WAF attacks playbook and click Enable in the Operation column.
- **Step 6** In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.7 HSS Isolation and Killing of Malware

13.7.1 Overview

Scenario

SecMaster provides this built-in playbook based on HSS to isolate and kill malware automatically.

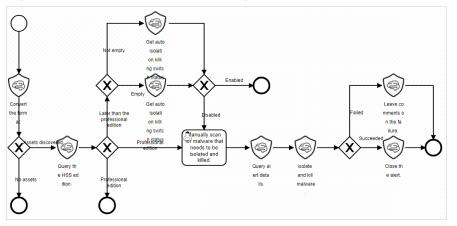
How the Playbook Works

The **HSS isolation and killing of malware** playbook has matched the **HSS isolation and killing of malware** workflow.

The **HSS isolation and killing of malware** workflow uses HSS to isolate and kill malware ransomware alerts.

If you are using the HSS professional edition or above to protect assets but have not enabled automatic isolation and killing of malware, manually review is required. If you agree to isolate or kill the infected file, HSS alerts will be generated. The alert is cleared when the malware has been isolated and killed. If the malware is not isolated, a comment on manual handling details will be left.

Figure 13-52 HSS isolation and killing of malware workflow



Prerequisites

You have enabled HSS access logs on **Data Integration** page under **Settings** in the current workspace. For details, see **Data Integration**.

Figure 13-53 Accessing HSS alerts

< / Data Integr	tion										
Security Situation		Coud Service Access									
Resource Manager 🔹 💌	-	Jaud Serrida Access									
Risk Prevention •											
Threat Operations 👻		*									
Security Orchestration		Access Service Logs									
Collection		Cloud Services	Loga	Region Level	Workspace	Storage Location	Lifecycle	Automatically converts alarms			
Management Components		Web Application Firewall	WAF attack log 💮	Region	-	-/-/-	7 Days				
Data Integration			WAF access log 🕥	Region		-1-1-	7 Days				
Checks		Object Storage Service ③	Object Storage Service access log	Region		/ isap-cloudlogs-0a90703a7500f3a92fbac014	180 Days				
Customization	4	IPS	IPS attack log	Region		/ isap-cloudlogs-0a90703a7500f3a92fbac014	180 Days				
		Identity and Access Management	IAM audit log	Region		/ isap-cloudlogs-0a00703a7500f3a92fbac014	180 Days	-			
			HSS alarm	Region		/isap-cloudlogs-0a60703a75005a92bac014	7 Days				
		Hast Security Service	HSS vulnerability scan result	Region		/insp-cloudlogs-0a90703a7500f3a92fbac014	100 Deys				
			HSS log	Region	-	-1-1-	7 Days				

Verification

• The malware has been killed and the alert is closed automatically.

Figure 13-54 Alerts automatically cleared

 Optimized [1:053]
 Maleure.202311 O Ingn
 Maleure.
 Disame
 Unneer
 2023120...
 2023120...
 Operation +

• If the malware is isolated and killed, a comment will be left indicating that the alert has been cleared.

Figure 13-55 Comment on succeeded isolation and killing of malware

curity Situation	V		Alert Overview	
Situation Overview Large Screen	° °		Comment H B TI / IJ G TE TP (*	
Reports Task Center ource Manager 🗢	Add Import Batch Close Batch Deinte Accounted Even			
Prevention •	C. Enter a keyword. By default, the search is performed by name or a combination of sear Alert Name	Alect Sex Alert Type Status Affected	Publish	
cidents	(Mateore) (HSS)	O High Matwaref Ossabled -	Comment Area S	0
erts Scaltors	Even Even	O Low Web atta Enabled test1 cn	8 C	
eligent Modeling	[vuin] [WM puspicious oper	O Low Web atta Enabled test1 cn	8 2022/12/95 20 31 41 824 GMT-08 00 8 Resolved Completed station of files	1
y Orchestration 👻	[vun] [VMJ suspicious oper	O Low Web atta Enabled test1.cm	• •	t
	[vuin] [WAS suspicious oper	O Low Web atta Enabled test1.cn		
	[vun] [vun] suspicious oper	O Low Web atta Enabled test1 cn	8	5
	Event Event	O Low Web atta Enabled test1 cn		
	[vun] [VIII suspicious oper	O Low Web atta Enabled test1 on		
	Event (two)	O Low Web atta Enabled test1.cn	5 🔻 Total Raconsi: 7 < 🚺 2 >	
	[vun] (WA)	O Low Web atta Enabled testion	OK Cancel Alarm D	Nam

• If the malware fails to be isolated or killed, a comment will be left indicating that manual handling is required.

Figure 13-56 Comment on failed isolation and killing of malwa	re
---	----

r / Alerts					Alert Overview	
ty Situation 💌	Urgent handling of Alerts 🕲	Expired atent @		Alert Sta	Comment	
revention • Operations • Idents	1	0			напиаавелениете	
s ators gent Modeling rity Analysis	Add Import Buick Close Q. Enter a keyvent. By detault, the search is perfor				Puttern Comment Area 2023-1305 30 35 32 751 GWT-96 00	
Orchestration +	Alert Name		Alert Type	Status Affected .	Automatic isolation of files for killing fails, piease manually handle the alerts.	
· · · ·	Children TITTE-D	O High	Malware!	Enabled -	and the second se	
•	(min) suspicio	O Law	Web attac	Enabled test1.co		
	[suin] suspicio	0 tav	viteb attac	Enabled lettion		
	(win) suspiso	0 Law	Web attac	Enabled tests.cn		
	[min] suspice	Oter	Web attac	Enabled leith.cn		
	(win) suspice	0 Low	Web attac	Enabled Section	the second s	
	[min]	O Law	Web attac	Enabled test1.cn	5 • Total Records: 19 < 1 2 3 4 >	
	[win]	0.04	Web attac	Enabled heatling		Alarm De

13.7.2 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **HSS isolation and killing of malware** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **HSS isolation and killing of malware** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **HSS isolation and killing of malware** playbook.

Procedure

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner of the page and choose Security & Compliance > SecMaster.
- **Step 3** In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-57 Workspace management page

SecMaster	Management ③	Process
Security Overview Workspaces Management Agencies	Could Workspoor IF later a same and layound for search.	Q
Purchased Resources Security Governance(beta)		Selected Space C O Witter 0 Alorts 0 ½ Indicat 0 Secont 0 IB Instan 0 IB Parybo 0

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

Figure 13-58 Accessing the Playbooks tab

<	/ Playbo	oks / Playbooks												
Security Situation Resource Manager		Playbooks 8	rkflows	Asset connec	tion Insta	ince Manager	ment							
Risk Prevention Threat Operations Security Orchestration	Ţ		Pendir	ng review 0				Not enabled	10		Enabled 1			
Objects Playbooks											Status	* Name	Enter a logword.	Q C 🕻 🛛
Layouts		Name Name		Detaclass	Playbo 7	7 Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operat	ion
Plugins	Ţ	Add the I	indica	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GWT+08:00	system	2023/06/06 23:42:32 GMT+06:00	-	Enable	More +
Semilis	Ť	Alert notif	cation	Alert	Not enabled	vt	Ø	system	2023/08/08 23 42:32 GMT+08:00	system	2023/08/08 23 42 32 GMT+08:00	-	Enable	More +

- **Step 5** On the **Playbooks** page, locate the row that contains the **HSS isolation and killing of malware** playbook and click **Enable** in the **Operation** column.
- **Step 6** In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.8 Real-time Notification of Critical Organization and Management Operations

13.8.1 Overview

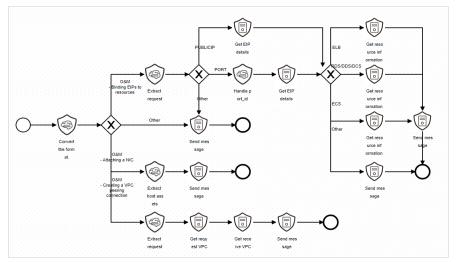
Scenario

SecMaster provides this playbook for real-time notification of key O&M operations. Based on O&M operations, SecMaster notifies you of key O&M operations by email in real time.

How the Playbook Works

The **Real-time notification of critical Organization and Management operations** playbook has matched the **Real-time notification of critical Organization and Management operations** workflow. This workflow uses Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.

Figure 13-59 Real-time notification of critical Organization and Management operations workflow



Prerequisites

• You have enabled CTS logs on the **Data Integration** page under **Settings** in the current workspace. For details, see **Data Integration**.

Figure	13-60	Access	to	CTS	logs
--------	-------	--------	----	-----	------

<								
Security Situation	•	Cloud Service Access						
Resource Manager	*							
Risk Prevention	•							
Threat Operations	*	· · ·						
Security Orchestration	*	Access Service Logs						
Collection		Cloud Services	Logs	Region Level	Workspace	Storage Location (2)	Lifecycle	Automatically converts alarms
Management		Web Application Firewall (?)	WAF attack log 🕐	Region		isep-claudiogs-6317673a-8e5c-41ee-9cd0-313	180 Days	
Data Integration			WAF access log ③	Region		/ isap-cloudlogs-6317673a-8e5c-41ee-9cd0-313	7 Days	-
Checks		IPS	IPS attack log	Region		/ isep-cloudlogs-6317673a-8e5c-41ee-9cd0-313	180 Days	-
Customization		Managed Threat Detection (MTD)	mtő-alarm	Region		/ isep-cloudlops-6317673a-8e5c-41ee-9cd0-313	7 Days	-
			HSS alarm	Region		/ isep-cloudlops-6317673a-8e5c-41ee-9cd0-313	180 Days	
		Host Security Service (2)	HSS vulnerability scan result	Region		/ issp-cloudlogs-6317673a-8e5o-41ee-9cd0-313	7 Days	
			NSS log	Region		/ isap-cloudlogs-6317673a-8e5c-41ee-9cd0-313	7 Days	-
		Cloud Trace Service (2)	CTS log	Region		/ isap-cloudlogs-6317673a-8e5c-41ee-9cd0-313	180 Days	-
			CFW access centrol log	Region		/ isap-cloudlogs-6317673a-8e5c-41ee-9cd0-313	180 Deys	-

• The corresponding O&M defense model has been enabled. For details, see **Enabling an Alert Model**.

Verification

When a key O&M operation is performed, this playbook is triggered. The playbook will send an email notification as configured. The following is an example.

Figure 13-61 Operation notifications

	2021/12/96 (₩⊡ 10:21 prmail_smmhw01 SecMaster real-time notification of critical Organization and Management operations	^
whether it is the	fraction of critical Organization and Management operations [IOB M]. reaction of critical Organization and Management operations [IOB M]. Reaction behavior of normal business personnel, if not, please take timely measures to rectify the situation according to the recommendations of the alarm disposal.	
Recommendation connection. 2. M	has created a VPC peering connection through 00Tiol:17:16:17:16:21:14:60:0 00Tiol:17:16:21:14:60:0 00Tiol:17:16:21:14:60:0 00Tiol:17:16:21:14:60:0 00Tiol:17:16:21:14:60:0 00Tiol:17:16:21:14:14:14:14:14:14:14:14:14:14:14:14:14	
[Affected Asset Name Type:p Reque Accep		

13.8.2 Enabling an Alert Model

Scenario

Before using **Real-time notification of critical Organization and Management operations** playbook, you need to enable some alert models, including the ones for O&M - Attaching NICs, O&M - Creating VPC peering connections, and O&M-Binding EIPs to resources.

This topic describes how to enable an alert model.

Procedure

Creating an alert model

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

Figure 13-62 Workspace management page

SecMaster	Management ③				🕞 Process
Sacurity Overview Workspaces	Creatly Workspace $\label{eq:creative} \overline{\Psi} \ \ \mbox{forther a name and layoutd for search}.$				C
Purchased Resources Security Governance(beta)	Constantial Constanti	incidents 0	♥ Vulner 0 Securl 0	 Alerts Instan 0 	Selected Spaces C 🛞

Step 4In the navigation pane on the left, choose Threat Operations > Intelligent
Modeling. On the displayed page, click the Model Templates tab.

Figure 13-63 Model Templates tab

< / / Intelligent	Modeling					
Security Situation 🔹						
Resource Manager 💌	Available Models Model Templates	0				
Risk Prevention 💌	Model Template Statistics	-	Severity			
Threat Operations	Available templates	Active templates				
Incidents	50	20	 Critical 1 High 	14 • Medium 28 • Low	0 • Informative 7	
Alerts						
Indicators	V Search by name.					Q®C
Intelligent Modeling	Severity 0	Name	Model Type	Updated o	Created 0	Operation
Security Analysis	Medium	Network - External malicious IP address scanning	Rule model	Jul 05, 2023 17:39:38 GMT+06:00	Jun 27, 2023 11:09:09 GMT+08:00	Details
Security Orchestration •	Medum	Application - Possible Java framework common c	- Diterrated	Jul 05, 2023 17:38:07 GMT+08:00	Jun 20, 2023 17:38:55 GMT+08:00	Details
Setings •		Approation - Possible Java transitions common c	o Rule model	au os, 2023 17.36.07 GM1+08.00	301 20, 2023 11:30:55 GM1+08:00	Linearen
	O Medium	Network - Suspicious DoS attacks	Rule model	Jul 05, 2023 17:37:37 GMT+06:00	Jun 20, 2023 19:23:13 GMT+08:00	Details

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

Figure 13-64 Template details

Q Search by name.					© C
Severity 😄	Name	Model Type	Updated o	Created	Operation
Informative	O&M - Binding EIPs to resources	Rule model	Jun 25, 2023 17:21:49 GMT+08:00	Jun 10, 2023 16:43:05 GMT+08:00	Details
Informative	Identity - Creating a federated user	Rule model	Jun 25, 2023 14:51:15 GMT+08:00	Jun 25, 2023 14:51:15 GMT+08:00	Detaits
Informative	Identity - Creating an IAM user	Rule model	Jun 25, 2023 14:34:34 GMT+08:00	Jun 03, 2023 18:01:27 GMT+08:00	Details

- **Step 6** On the details page, click **Create Model** in the lower right corner. The page for creating an alert model is displayed.
- **Step 7** On the **Create Alert Model** page, configure basic information.
 - **Pipeline Name**: Select an execution pipeline for the alert model.

Alert Template	Execution Pipeline
O&M - Attaching a NIC	sec-cts-audit
O&M - Creating a VPC peering connection	
O&M - Binding EIPs to resources	

- Retain default values of other parameters.
- **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. You are advised to retain the default value.
- **Step 10** After completing the basic settings, click **Next** in the lower right corner of the page.
- **Step 11** After confirming that the model is correct, click **OK** in the lower right corner of the page.
- **Step 12** Repeat **Step 5** to **Step 11** to create alert models with other templates.

Enabling an alert model

Step 13 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**.

<	ert Vodeling						
Security Situation 🛛 💌							
Resource Manager 🛛 💌	Available Models Model Templates						
Risk Prevention 💌	Model Statistics		Severity				
Threat Operations 🔍 🔺	Available Models	Active models					
Incidents	97 (()	93	 Critical 1 High 	25 • Medium 59	 Low 12 Inf 	ormative 0	
Alets							
Indicators	Create Model Enable Deable Delete	V Search by name.					Q @ C
Intelligent Modeling	Severity 0 Name1D	Status Debugging	Pipeline Name	Model Type Built in	Updated o	Created 0	Operation
Security Analysis Security Orchestration •	9731b122-0083-490-8424-71.	🔮 Enable 🔘 Disable	sec-nip-affack	Rule model No	Jun 03, 2023 16:50:53 GMT+	Jun 02, 2023 16:14:20 GMT+	Disable Edit Delete
Setings •	64415ca0-5c07-4ca7-8090-8d.	Contraction Disable	sec-rip-attack	Rule model No	Jun 02, 2023 17:33:52 GMT+	Jun 02, 2023 16:15:20 GMT+	Disable Edit Delete

- **Step 14** To enable models in batches, select all models you want to enable and click **Enable** in the upper left corner of the list.
- **Step 15** If the model status changes to **Enable**, the model is successfully enabled.

----End

13.8.3 Creating and Subscribing to a Topic

Scenario

The **Real-time notification of critical Organization and Management operations** workflow uses Simple Message Notification (SMN) to send notifications. You need to create and subscribe to a topic for receiving notifications.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** In the upper left corner of the page, click and choose **Management and Governance** > **Simple Message Notification**.
- **Step 3** Create a topic.
 - 1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

Figure 13-66 Create Topic

Simple Message Notification	Topics (2)				🙂 Feedback Create Topic
Dashboard Topic Management	You cannot search for topics by tag and o Q. Search or filter by keyword.	other search criteria at the same time, or the sea	rch results may be invalid.		C 0
Topics	Name/ID 💠	URN ≑	Enterprise Project 💠	Display Name 💠	Operation
Subscriptions Message Templates	72d8135d93ba436da4f475efa7553342	um.smn.cn-south-1:0a60703a7500f3a	default	-	Publish Message Add Subscription More +
	AUTO	um.smn.cn-south-1:0e00703e7500f3e	default		Publish Message Add Subscription More •
	10 🔻 Total Records: 2 <	1 >			

2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.

- **Topic Name**: **SecMaster-Notification** is recommended.
- Display Name: SecMaster notification topic is recommended.
- Retain the default values for other parameters.

Figure 13-67 Configuring a topic

Create Topic	×					
★ Topic Name	SecMaster-Notification					
	The name cannot be changed after the topic is created.					
Display Name	SecMaster Notification Topic					
	If a display name is specified, the email sender is presented in the format "Display name <username@example.com>" when email messages are delivered.</username@example.com>					
* Enterprise Project	default C Create Enterprise Project					
	Enterprise Project Management Service (EPS) allows you to manage cloud resources and user groups by enterprise project.					
CTS Log						
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags ${\bf C}$ To add a tag, enter a tag key and a tag value below.					
	Enter a tag key Add					
	Tags you can still add: 10					
	OK Cancel					

Step 4 Add a subscription.

- 1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
- 2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
 - Protocol: Select Email.
 - **Endpoint**: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-68 Add Subscription

dd Subscrip	tion		
Topic Name	SecMaster-Notification		
 Protocol 	Email	•	
k Endpoint	Endpoints username@example.com Add Endpoint Batch Add Endpoints	Description	

----End

13.8.4 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Real-time notification of critical Organization and Management operations** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Real-time notification of critical Organization and Management operations** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Real-time notification of critical Organization and Management operations** playbook.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing** to a **Topic**.

Procedure

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

Figure 13-69 Workspace management page

SecMaster	Management 🕥				Process
Security Overview Workspaces Management Agencies	$$\ensuremath{\mathbb{C}}\xspace$ Total Wangaoo $$\ensuremath{\mathbb{T}}\xspace$ for a non- and layered for seach.				C
Purchased Resources Security Governance(beta)	Grand accord G	 ⊡ Incidents 0 ○ Assets 0 	 ◊ Vulner 0 ⊜ Securl 0 	 Alerts 0 instan 0 	Selected Spaces C 🛞 indicat 0 Playbo 0

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

Figure 13-70 Accessing the Playbooks tab

K Play	books / Playbooks										
Security Situation 🔹											
Resource Manager 🔹 💌	Playbooks Workflows	Asset conne	ction insta	nce Manage	TIERE						
Risk Prevention 🔹											
Threat Operations	Pendi	ng review 0			l.	lot enabled	10		Enabled 1		
Security Orchestration											
Objects											
Playbooks									Status All	• Name • Enter a keyn	ort. Q C 🖸 🛛
Layouts	Name Name	Detaclass	Playbo 7	Current	Monitoring	Created By	Created	Updated By	Updated At	Description	Operation
Plugins	Add the IP indica.	Alert	Not enabled	vt	Ø	system	2023/06/08 23:42:32 GWT+00:00	system	2023/06/08 23:42:32 GMT+06:00	-	Enable More +
Settings 💌	Alert notification	Alert	Not enabled	vt	۵	system	2023/08/08 23 42:32 GWT+08:00	system	2023/06/08 23 42 32 GWT+08:00	-	Enable More +

Step 5 On the Playbooks page, locate the row that contains the Real-time notification of critical Organization and Management operations playbook and click Enable in the Operation column.

Step 6 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

14 Permissions Management

14.1 Creating a User and Granting Permissions

This topic describes how to use **IAM** to implement fine-grained permissions control for your SecMaster. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing SecMaster resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your SecMaster resources.

If your account does not require individual IAM users, skip over this section.

The following walks you through how to grant permissions. **Figure 14-1** shows the process.

Prerequisites

Learn about the permissions supported by SecMaster and choose policies or roles based on your requirements. For details, see **SecMaster Permissions**.

Table 14-1 lists all the system-defined roles and policies supported by SecMaster.

Policy Name	Description	Туре	Dependency
SecMaster FullAccess	All permissions of SecMaster.	Syste m- define d policy	None

Table 14-1 System-	defined permissions	s supported by SecMaster	
--------------------	---------------------	--------------------------	--

Policy Name	Description	Туре	Dependency
SecMaster ReadOnlyAcce ss	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	Syste m- define d policy	None

Permission Granting Process

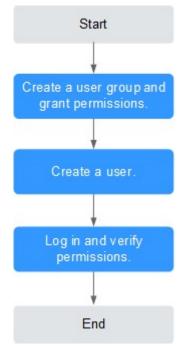


Figure 14-1 Process for granting permissions

1. Create a user group and assign permissions.

Create a user group on the IAM console, and assign the **SecMaster FullAccess** permission to the group.

2. Create a user and add the user to the user group.

Create a user on the IAM console and add the user to the group created in 1.

3. Log in to the management console as the created user and verify the permissions.

Log in to the SecMaster console as the created user, and verify that the user only has read permissions for SecMaster.

Choose any other service from **Service List**. If a message appears indicating that you do not have permissions to access the service, the **SecMaster FullAccess** policy has already taken effect.

14.2 SecMaster Custom Policies

Custom policies can be created to supplement the system-defined policies of SecMaster. For the actions that can be added to custom policies, see **SecMaster Permissions and Supported Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common SecMaster custom policies.

Example Custom Policies

• Example 1: Authorization for alert list search permission and permission execution analysis

```
Version": "1.1",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
           "secmaster:alert:list",
           "secmaster:search:createAnalysis"
        ]
     }
]
```

• Example 2: Preventing users from modifying alert configurations

A deny policy must be used together with other policies. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used to create a custom policy to disallow users who have the **SecMaster FullAccess** policy assigned to modify alert configurations. Assign both **SecMaster FullAccess** and the custom policies to the group to which the user belongs. Then the user can perform all operations except modifying alert configurations on SecMaster. The following is an example of a deny policy:

```
"Version": "1.1",
"Statement": [
{
"Effect": "Deny",
"Action": [
"secmaster:alert:updateType"
]
}
]
```

{

}

• Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
   "Version": "1.1",
   "Statement": [
     {
        "Effect": "Allow",
         "Action": [
           "secmaster:alert:get",
            "secmaster:alert:update"
        1
     },
         "Effect": "Allow",
         "Action": [
           "hss:vuls:set",
           "hss:vuls:list"
        1
     }
  ]
ļ
```

14.3 SecMaster Permissions and Supported Actions

This topic describes fine-grained permissions management for your SecMaster. If your account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using roles and policies. Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

SecMaster provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

15 Key Operations Recorded by CTS

15.1 SecMaster Operations Recorded by CTS

Cloud Trace Service (CTS) provides you with a history of SecMaster operations. After enabling CTS, you can view all generated traces to query, audit, and review performed SecMaster operations. For details, see *Cloud Trace Service User Guide*.

Table 15-1 shows the details about the SecMaster operations on CTS.

Operation	Resource Type	Trace Name
Reviewing a Playbook	playbook	approvePlaybook
Creating a Playbook Action	playbook	createPlaybookAction
Modifying a Playbook Action	playbook	updatePlaybookAction
Deleting a Playbook Action	playbook	deletePlaybookAction
Creating a Playbook	playbook	createPlaybook
Modifying a Playbook	playbook	updatePlaybook
Deleting a Playbook	playbook	deletePlaybook
Operating a Playbook Instance	playbook	operatePlaybookInstance
Exporting a Playbook Instance	playbook	exportPlaybookInstance
Exporting a Playbook	playbook	exportPlaybook
Importing a Playbook	playbook	importPlaybook

Table 15-1 SecMaster operations recorded by CTS

Operation	Resource Type	Trace Name
Adding a Playbook Triggering Rule	playbook	createPlaybookRule
Updating a Playbook Triggering Rule	playbook	updatePlaybookRule
Deleting a Playbook Triggering Rule	playbook	deletePlaybookRule
Creating a Playbook Version	playbook	createPlaybookVersion
Updating a Playbook Version	playbook	updatePlaybookVersion
Deleting a Playbook Version	playbook	deletePlaybookVersion
Cloning a Playbook Version	playbook	clonePlaybookVersion
Creating a Workflow	workflow	createWorkflow
Modifying a Workflow	workflow	updateWorkflow
Deleting a Workflow	workflow	deleteWorkflow
Creating a Workflow Version	workflow	createWorkflowVersion
Modifying a Workflow Version	workflow	updateWorkflowVersion
Reviewing a Workflow Version	workflow	approveWorkflowVersion
Deleting a Workflow Version	workflow	deleteWorkflowVersion
Exporting a Workflow	workflow	exportWorkflow
Importing a Workflow	workflow	importWorkflow
Creating an Asset Connection	asset	createAsset
Creating an Asset Connection	asset	updateAsset
Deleting an Asset Connection	asset	deleteAsset
Uploading an Attachment	component	uploadAttachement
Creating a Plug-in Template	component	createComponentTem- plate

Operation	Resource Type	Trace Name
Updating a Plug-in Template	component	updateComponentTem- plate
Deleting a Plug-in Template	component	deleteComponentTem- plate
Adding Comments	task	commentTask
Submitting a To-Do Task	task	commitTask
Creating a Workspace	workspace	createWorkspace
Deleting a Workspace	workspace	deleteWorkspace
Updating a Workspace	workspace	updateWorkspace
Recollecting Subservice Statistics	workspace	recollectServiceStatistics

15.2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- Viewing Real-Time Traces in the Trace List of the New Edition
- Viewing Real-Time Traces in the Trace List of the Old Edition

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

- 1. Log in to the management console.
- 2. Click in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
- 3. Choose **Trace List** in the navigation pane on the left.
- 4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
 - **Trace Name**: Enter a trace name.
 - **Trace ID**: Enter a trace ID.
 - Resource Name: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
 - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
 - **Trace Source**: Select a cloud service name from the drop-down list.
 - **Resource Type**: Select a resource type from the drop-down list.
 - **Operator**: Select one or more operators from the drop-down list.
 - Trace Status: Select normal, warning, or incident.
 - **normal**: The operation succeeded.
 - warning: The operation failed.
 - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
 - Time range: Select Last 1 hour, Last 1 day, or Last 1 week, or specify a custom time range.
- 5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
 - Enter any keyword in the search box and click Q to filter desired traces.
 - Click Export to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
 - Click $^{
 m C}$ to view the latest information about traces.
 - Click 🥺 to customize the information to be displayed in the trace list. If

Auto wrapping is enabled (), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

- 6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
- 7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

- 1. Log in to the management console.
- 2. Click in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
- 3. Choose **Trace List** in the navigation pane on the left.
- 4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
- 5. Set filters to search for your desired traces. The following filters are available:
 - Trace Type, Trace Source, Resource Type, and Search By: Select a filter from the drop-down list.
 - If you select **Resource ID** for **Search By**, specify a resource ID.
 - If you select **Trace name** for **Search By**, specify a trace name.
 - If you select **Resource name** for **Search By**, specify a resource name.
 - Operator: Select a user.
 - Trace Status: Select All trace statuses, Normal, Warning, or Incident.
 - Time range: You can query traces generated during any time range in the last seven days.
 - Click Export to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
- 6. Click Query.
- 7. On the **Trace List** page, you can also export and refresh the trace list.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
 - Click $^{\mathbb{C}}$ to view the latest information about traces.
- 8. Click \checkmark on the left of a trace to expand its details.

Trace Name		Resource Type	Trace Source	Resource ID (?)	Resource Name ⑦	Trace Status (?)	Operator (?)	Operation Time	Operation
createDocker	Config	dockerlogincmd	SWR		dockerlogincmd	📀 normal		Nov 16, 2023 10:54:04 GMT+08:00	View Trace
request									
trace_id									
code	200								
trace_name	createDockerConfig								
resource_type	dockerlogincmd								
trace_rating	normal								
api_version									
message	createDockerConfig. Method: POST Uri=/v2/manage/utilis/secret, Reason:								
source_ip									
domain_id									
trace_type	ApiCall								

9. Click **View Trace** in the **Operation** column. The trace details are displayed.

×

View Trace



- 10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
- 11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

A Change History

Released On	Description
2024-03-28	This issue is the tenth official release.
	 Updated Overview and Adding or Editing an Emergency Policy: Updated restrictions, and added the description of recommended emergency policy configurations.
	• Updated Collecting Data: Added descriptions about ECS sand VPC endpoints.
	 Updated Security Orchestration Overview and Viewing Monitored Playbook Instances: Updated the restrictions on playbooks and workflow instances.
	• Updated Viewing Baseline Inspection Results: Added the procedure for viewing the check result.
	 Updated the description of viewing data in Viewing Resource Information, Viewing Vulnerability Details, Viewing Incidents, Viewing Alerts, and Viewing Indicators.
	Added One-click Blocking or Unblocking.

Released On	Description
2024-02-29	 This issue is the ninth official release. Updated Editing a Workspace. Added content about interconnecting SecMaster with Tag Management Service (TMS).
	• Updated Creating an Agency. Added content about interconnecting SecMaster with Organizations.
	• Updated Viewing Alerts. Updated some descriptions as the alert details page on the console was optimized.
	• Updated Viewing Baseline Inspection Results. Added the description of the check result page.
	• Updated Handling Baseline Inspection Results. Added the operation guide for importing and exporting check results.
	• Updated Log Access Supported by SecMaster: Added description of accessing SecMaster baseline check results to the security analysis pipelines.
	• Updated Workspace Overview and Security Analysis Overview: Added restrictions on workspaces and security analysis.
	• Updated Built-in Playbooks and Workflows . Details about built-in playbooks, workflows, and asset connections were added.

Released On	Description
2023-12-11	This issue is the eighth official release.
	 Updated Buying SecMaster. Added descriptions of interconnection between SecMaster and TMS.
	 Updated Creating and Copying a Security Report and Viewing a Security Report. The description of the weekly reports were added.
	 Updated Overview, Situation Overview, Overall Situation Screen, Monitoring Statistics Screen, Asset Security Screen, Threat Situation Screen, and Vulnerable Assets Screen and added the statistical periods of metrics.
	• Updated contents in Viewing Completed Tasks.
	 Added the description of SecMaster agency permissions in section Authorizing SecMaster.
	Added Collecting Data.
	• Updated Built-in Playbooks and Workflows . Details about built-in playbooks, workflows, and asset connections were added.
	 Deleted sections "Purchasing an ECS", "Installing an Agent", "Adding a Node", "Configuring Components", "Adding Connections", "Configuring Parsers", and "Adding Collection Channels".
	 Moved content in formerly "Unblocking IP Address in Batches" to section Blocking or Canceling Blocking of an IP Address or IP Address Range.
	Optimized some descriptions.
2023-10-30	This issue is the seventh official release.
	• Updated Creating and Copying a Security Report. Description of configuration of sending report information were added.
	 Updated Viewing a Security Report. The description o the monthly report were added.
	 Added Built-in Playbooks and Workflows. Details about built-in playbooks, workflows, and asset connections were added.
	 Added Log Access Supported by SecMaster. Details about cloud service log access were added.
	Added Configuring Defense Policies.
	• Moved content in "Submitting a Workflow Version" to Managing Workflow Versions.
	 Updated the description in Buying the Standard Edition and Buying the Professional Edition.
	• Adjusted the document structure and optimized some descriptions.

Released On	Description
2023-09-25	 This issue is the sixth official release. Added Overview. Descriptions of asset sources and corresponding security services were provided.
	 Updated Log Fields. The description of WAF attack log fields were updated.
	 Updated Workspace Overview. Restrictions on workspaces were updated.
	Added Delivering Logs to LTS.
	Optimized some descriptions.

Released On	Description
2023-08-10	This issue is the fifth official release.
	• Updated Downloading a Security Report . Reports in multiple formats can be downloaded.
	Added remarks in Viewing To-Do Tasks.
	• Added Viewing Completed Tasks. Handled tasks can be viewed.
	 Added Configuring Resource Subscription. SecMaster supports subscriptions to information about other regions.
	 Added Policy Management. SecMaster supports centralized management of defense and emergency policies.
	 Updated Viewing Incidents. Users can view the affected consultation information.
	• Updated Closing or Deleting Incidents . Incidents can be closed and deleted in batches.
	• Updated Viewing Alerts. Users can view the affected consultation information.
	 Added operations for associating alerts with incidents i Converting an Alert to an Incident or Associating an Alert with an Incident.
	• Updated Closing or Deleting an Alert . Alerts can be closed and deleted in batches.
	• Added Handling Alerts based on Suggestions. Handling suggestions are provided for top alerts.
	 Added the description of MTD alarm fields in Log Fields.
	• Updated the content in Security Orchestration Proces The built-in playbook is activated by default. No manu- operation is required.
	 Added Viewing Custom Types. Types can be customized.
	 Updated the description in Adding an Asset Connection and Managing Asset Connections.
	 Added the supported installation systems in Data Collection Overview.
	 Added the supported installation systems in Buy an ECS.
	• Updated Managing Parsers. Parsers can be imported and exported.
	• Deleted "Modifying the Asset Information Synchronization Policy." The system automatically synchronizes asset information without using playbook

Released On	Description
2023-06-30	This issue is the fourth official release.
	 Added (Optional) Configuring and Enabling a Workflow and (Optional) Configuring and Enabling a Playbook.
	Optimized descriptions in Security Orchestration Overview and Security Orchestration Process.
	 Deleted sections "Adding a Playbook", "Adding a Workflow", "Adding a Layout", "Adding a Data Class", and "Adding a Data Field."
2023-05-25	This issue is the third official release.
	Added Data Delivery and Authorizing SecMaster.
	• Deleted sections "Asset Access Authorization" and "Baseline Inspection Access Authorization" as authorization is assigned in a centralized manner.
	• Updated the detailed data description in Overall Situation Screen, Monitoring Statistics Screen, Asset Security Screen, Threat Situation Screen, and Vulnerable Assets Screen.
	Optimized some descriptions.

Released On	Description
2023-04-25	This issue is the second official release.
	Added Workspace Agencies.
	 Added Viewing Purchased Resources to support unified management of purchased resources.
	• Added Vulnerable Assets Screen, Asset Security Screen, and Threat Situation Screen.
	• Added Downloading a Security Report.
	• Added Importing and Exporting Assets and Configuring Asset Management Policies to support asset import and asset synchronization policy management.
	 Added Fixing Vulnerabilities, Importing and Exporting Vulnerabilities, and Ignoring and Unignoring a Vulnerability.
	Added Plug-in Management.
	 Added Data Collection to support unified management of collected data on SecMaster.
	• Added Importing and Exporting Incidents, Importing and Exporting Alerts, and Importing and Exporting Intelligence Indicators.
	• Updated Buying SecMaster and added the intelligent analysis value-added package and version upgrade content.
	 Updated the parameter description in Creating a Workspace.
	• Updated Creating and Copying a Security Report : added the description that weekly and monthly reports can be created.
	• Updated Viewing a Security Report and added the description of security report templates.
	• Updated the description of asset category display in section Viewing Resource Information.
	• Updated Data Integration and added the description on newly accessed data sources.
2023-02-28	This issue is the first official release.