SecMaster

User Guide

Issue 14

Date 2025-02-06

Contents

1 Buying SecMaster

1.1 Buying SecMaster

Scenarios

SecMaster supports the yearly/monthly and pay-per-use billing modes. The basic and standard editions support only the yearly/monthly billing mode. The professional edition supports the yearly/monthly and pay-per-use billing modes. You can purchase a SecMaster edition that best fits your workloads.

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

Buying SecMaster

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 On the **Security Overview** page, click **Buy SecMaster** in the upper right corner.

Step 5 (Optional) Obtain purchase authorization.

Access authorization is required only when first time you buy the service. SecMaster needs your authorization to obtain the ECS asset details. On the **Access Authorization** slide-out panel displayed, select **Agree** and click **OK**.

Step 6 On the purchase page, configure parameters by referring to the following table.

Table 1-1 Parameters for purchasing SecMaster

Parameter	Description
Billing Mode	Select **Yearly/Monthly** or **Pay-per-use** billing mode based on your needs. ● Yearly/Monthly is a prepaid billing mode. You pay in advance for a subscription term. The longer you use the service, the more discounts you got. ● Pay-per-use billing is a postpaid mode in which you pay for what you use. You are billed by second based on the actual usage. Your bill is settled by the hour. With the pay-per-use billing mode, you can easily adapt to resource requirement changes, reducing the risk of over-provisioning of resources or lacking capacity. In this mode, there are no upfront commitments required.
Region	Select the region where your cloud resources are located.
Edition	SecMaster provides basic, standard, and professional editions for your choice. For details about their differences, see **Edition Differences**.
Quota	The maximum number of ECSs you want to protect. The quota must be greater than or equal to the total number of ECSs within your account. This value cannot be changed to a smaller one after your purchase is complete. **NOTE** ● The maximum quota is 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.
Large Screen Log Audit Security Analysis SOC	You can enable **Large Screen**, **Log Audit**, **Security Analysis**, and **SOC** function. If you want to purchase value-added package in yearly/monthly billing mode, select a required duration. For details about the value-added package and recommended configurations, see **Value-added Package Specifications**.
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	Select the required duration as required. You do not need to configure this parameter in pay-per-use mode. The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

Step 7 Confirm the product details and click **Next**.

Step 8 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 9 On the payment page, select a payment method and complete the payment.

----End

Value-added Package Specifications

Based on the standard and professional editions, SecMaster provides the following functions in the value-added package:

- **Large Screen**
  - Function description:

    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.

  - Purchase configuration description:

    Make a purchase based on your service needs.

- **Log Audit**
  - Function description:

    It collects varied types of log data and stores the collected data for security analysis. You can set the data collection volume and data retention volume for each day.

  - Purchase configuration description:

    In pay-per-use billing mode, you will be billed based on the actual collection and storage volume. You do not need to configure specifications.

    In yearly/monthly billing mode, you need to specify **New Log** per day based on your estimations on service requirements. SecMaster will automatically allocate package specifications based on the value you provide. For details about the specifications, see **Table 1-2**.

Table 1-2 Specifications of the security data collection and retention packages

Resource Package	Recommended Configuration for Yearly/Monthly Subscription	Package Specifications	Applicable Range
Security data collection	The volume of data you expect SecMaster to collect each day. Minimum value: 5 GB. You can estimate the volume by multiplying the number of ECSs you have by 120 MB. Maximum volume for each order: 500 GB. When you make a purchase, SecMaster auto-fills this parameter based on the new log volume you specify. You do not need to configure this parameter separately.	5 *1 GB	0 GB to 5 GB (included)
		5 *2 GB	5 GB to 10 GB (included)
		5 *3 GB	10 GB to 15 GB (included)
		...... The others follow the same rule. A maximum of 500 GB can be purchased through an order.	...... The others follow the same rule.

Resource Package	Recommended Configuration for Yearly/Monthly Subscription	Package Specifications	Applicable Range
Security data retention	The volume of data you expect SecMaster to store. The minimum volume is 100 GB. You can estimate the volume by multiplying new log volume per day by seven. The maximum volume for each order is 3,500 GB. When you make a purchase, SecMaster auto-fills this parameter based on the new log volume you specify. You do not need to configure this parameter separately.	100 *1 GB	0 GB to 100 GB (included)
		100 *2 GB	100 GB to 200 GB (included)
		100 *3 GB	200 GB to 300 GB (included)
		······ The others follow the same rule. A maximum of 3,500 GB can be purchased through an order.	······ The others follow the same rule.

☐ NOTE

- The quotas of security data retention and security data collection packages can be counted together. However, these packages cannot cover what you used before the purchase. Subscriptions to these packages cannot be cancelled.
- For yearly/monthly security data collection and retention packages, data volume in excess of the package quotas will be billed on a pay-per-use basis.
- Pay-per-use resources will not be disabled automatically even if yearly/ monthly security data retention and security data collection packages expire. They will always be enabled on a pay-per-use basis.

  For yearly/monthly security data collection package, data volume in excess of the package quota will be billed each day on a pay-per-use basis.

  For example, a user purchases a security data collection package with 5 GB/day/quota for one month. If the user uses 5 GB data collection before 22:00 on the purchase day, and then uses 2 GB data collection 22:00 00 and 24:00, the extra 2 GB will be billed on a pay-per-use basis. Starting from 00:00 on the next day, a 5 GB/day/quota is available to the user again.

- **Security Analysis**
  - Function description:

    Security analysis is the cloud native security information and event management solution SecMaster provides for you. The solution collects

logs, reports alerts, aggregates security data, performs association analysis, and more.

– Purchase configuration description:

Table 1-3 lists the free quota of security analysis. You can increase the quota at an extra cost if needed.

In pay-per-use billing mode, you will be billed based on the actual volume. You do not need to configure specifications.

In yearly/monthly billing mode, you need to set the data volume as required. For details, see **Table 1-4**.

Table 1-3 Specifications for free security analysis quota

Function		Standard Edition	Professional Edition
Security Analysis	Security data collection	120 MB/day/quota	120 MB/day/quota
	Security data retention	120 MB/day/quota	120 MB/day/quota
	Security data export	120 MB/day/quota	120 MB/day/quota
	Platform security data	40 MB/day/quota	40 MB/day/quota
	Security modeling analysis	×	120 MB/day/quota

Table 1-4 Recommended security analysis configurations

Value-added Package	Recommended Quantity for Yearly/Monthly Subscription
Security Analysis	You can estimate the security analysis data volume based on 120 MB/ECS/day.
	This estimate volume will be applied to security data collection, security data retention, security data export, platform security data, and security modeling analysis as well. If the quota for security analysis is used up, this function becomes unavailable on that day, but it turns to be available at 00:00 the next day.
	For example, if this parameter is set to 1 GB/day, each day there will be 1 GB of security data that can be collected, 1 GB of security data stored, 1 GB of security data exported, 1 GB of platform security data reported, and 1 GB of data for security modeling analysis.

- Security orchestration

  - Function description:

    Once SecMaster detects a threat, Security Orchestration (SOC) starts automated response orchestration and works with related cloud services to block and isolate threat sources. SOC provides quick and effective security event responses.

  - Purchase configuration description:

    Table 1-5 lists the free quota of security orchestration. You can increase the quota at an extra cost if needed.

    In pay-per-use billing mode, you will be billed based on the actual security orchestration operation times. You do not need to configure specifications.

    In yearly/monthly billing mode, you need to set the operation times as required. For details, see **Table 1-6**.

Table 1-5 Specifications for free security orchestration quota

Function	Standard Edition	Professional Edition
Security Orchestration	x	Operations: 7,000

Table 1-6 Recommended security orchestration configurations

Value-added Function	Recommended Quantity for Yearly/Monthly Subscription
Security Orchestration	SecMaster supports 7,000 operations per day for each server. Set this parameter as required.
	If the quota for security orchestration is used up, this function becomes unavailable on that day, but it turns to be available at 00:00 the next day.

Verification

After the payment is successful, you can view the SecMaster edition you have purchased 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 Quotas**.

- 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, go to the
Security Overview page, hover 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**.

1.2 Purchasing Value-Added Packages

Scenario

In addition to the standard and professional editions, SecMaster also provides
value-added features for you to choose. This topic describes how to purchase a
value-added package.

📖 **NOTE**

If you are stuck due to insufficient permission, refer to **Assigning Permissions**.

Value-added Package Specifications

Based on the standard and professional editions, SecMaster provides the following
functions in the value-added package:

● **Large Screen**

– Function description:

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.

– Purchase configuration description:

Make a purchase based on your service needs.

● **Log Audit**

– Function description:

It collects varied types of log data and stores the collected data for
security analysis. You can set the data collection volume and data
retention volume for each day.

– Purchase configuration description:

In pay-per-use billing mode, you will be billed based on the actual
collection and storage volume. You do not need to configure
specifications.

In yearly/monthly billing mode, you need to specify **New Log** per day
based on your estimations on service requirements. SecMaster will
automatically allocate package specifications based on the value you
provide. For details about the specifications, see **Table 1-7**.

Table 1-7 Specifications of the security data collection and retention packages

Package	Recommended Configuration for Yearly/Monthly Subscription	Package Specifications	Applicable Range
Security Data Collection	The volume of data you expect SecMaster to collect each day. Minimum value: 5 GB. You can estimate the volume by multiplying the number of ECSs you have by 120 MB. Maximum volume for each order: 500 GB. When you make a purchase, SecMaster auto-fills this parameter based on the new log volume you specify. You do not need to configure this parameter separately.	5 *1 GB	0 GB to 5 GB (included)
		5 *2 GB	5 GB to 10 GB (included)
		5 *3 GB	10 GB to 15 GB (included)
		... The others follow the same rule. A maximum of 500 GB can be purchased through an order.	... The others follow the same rule.

Package	Recommended Configuration for Yearly/Monthly Subscription	Package Specifications	Applicable Range
Security Data Retention	The volume of data you expect SecMaster to store. The minimum volume is 100 GB. You can estimate the volume by multiplying new log volume per day by seven. The maximum volume for each order is 3,500 GB. When you make a purchase, SecMaster auto-fills this parameter based on the new log volume you specify. You do not need to configure this parameter separately.	100 *1 GB	0 GB to 100 GB (included)
		100 *2 GB	100 GB to 200 GB (included)
		100 *3 GB	200 GB to 300 GB (included)
		... The others follow the same rule. A maximum of 3,500 GB can be purchased through an order.	... The others follow the same rule.

☐ **NOTE**

- The quotas of security data retention and security data collection packages can be counted together. However, these packages cannot cover what you used before the purchase. Subscriptions to these packages cannot be cancelled.
- For yearly/monthly security data collection and retention packages, data volume in excess of the package quotas will be billed on a pay-per-use basis.
- Pay-per-use resources will not be disabled automatically even if yearly/monthly security data retention and security data collection packages expire. They will always be enabled on a pay-per-use basis.

  For yearly/monthly security data collection package, data volume in excess of the package quota will be billed each day on a pay-per-use basis.

  For example, a user purchases a security data collection package with 5 GB/day/quota for one month. If the user uses 5 GB data collection before 22:00 on the purchase day, and then uses 2 GB data collection 22:00 00 and 24:00, the extra 2 GB will be billed on a pay-per-use basis. Starting from 00:00 on the next day, a 5 GB/day/quota is available to the user again.

- **Security Analysis**
  - Function description:

    Security analysis is the cloud native security information and event management solution SecMaster provides for you. The solution collects

logs, reports alerts, aggregates security data, performs association analysis, and more.

– Purchase configuration description:

Table 1-8 lists the free quota of security analysis. You can increase the quota at an extra cost if needed.

In pay-per-use billing mode, you will be billed based on the actual volume. You do not need to configure specifications.

In yearly/monthly billing mode, you need to set the data volume as required. For details, see **Table 1-9**.

Table 1-8 Specifications for free security analysis quota

Function		Standard Edition	Professional
Security Analysis	Security data collection	120 MB/day/quota	120 MB/day/quota
	Security data retention	120 MB/day/quota	120 MB/day/quota
	Security data export	120 MB/day/quota	120 MB/day/quota
	Platform security data	40 MB/day/quota	40 MB/day/quota
	Security Modeling Analysis	×	120 MB/day/quota

Table 1-9 Recommended security analysis configurations

Value-added Function	Recommended Quantity for Yearly/Monthly Subscription
Security Analysis	You can estimate the security analysis data volume based on 120 MB/ECS/day.
	This estimate volume will be applied to security data collection, security data retention, security data export, platform security data, and security modeling analysis as well. If the quota for security analysis is used up, this function becomes unavailable on that day, but it turns to be available at 00:00 the next day.
	For example, if this parameter is set to 1 GB/day, each day there will be 1 GB of security data that can be collected, 1 GB of security data stored, 1 GB of security data exported, 1 GB of platform security data reported, and 1 GB of data for security modeling analysis.

- SOC
  - Function description:

    Once SecMaster detects a threat, Security Orchestration (SOC) starts automated response orchestration and works with related cloud services to block and isolate threat sources. SOC provides quick and effective security event responses.

  - Purchase configuration description:

    Table 1-10 lists the free quota of security orchestration. You can increase the quota at an extra cost if needed.

    In pay-per-use billing mode, you will be billed based on the actual security orchestration operation times. You do not need to configure specifications.

    In yearly/monthly billing mode, you need to set the operation times as required. For details, see **Table 1-11**.

Table 1-10 Specifications for free security orchestration quota

Function	Standard Edition	Professional Edition
Security Orchestration	x	Operations: 7,000

Table 1-11 Recommended security orchestration configurations

Value-added Function	Recommended Quantity for Yearly/Monthly Subscription
SOC	SecMaster supports 7,000 operations per day for each server. Set this parameter as required.
	If the quota for security orchestration is used up, this function becomes unavailable on that day, but it turns to be available at 00:00 the next day.

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.

Buying a Value-Added Package

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Overview**, or select **Purchased Resources**. On the page displayed, click **Buy Value-added Pack** in the upper right corner.

Step 5 On the purchase page, configure required parameters.

Table 1-12 Parameters for purchasing a value-added package

Parameter	Description
Billing Mode	Select **Yearly/Monthly** or **Pay-per-use** billing mode based on your needs. ● Yearly/Monthly is a prepaid billing mode. You pay in advance for a subscription term. The longer you use the service, the more discounts you got. ● Pay-per-use billing is a postpaid mode in which you pay for what you use. You are billed by second based on the actual usage. Your bill is settled by the hour. With the pay-per-use billing mode, you can easily adapt to resource requirement changes, reducing the risk of over-provisioning of resources or lacking capacity. In this mode, there are no upfront commitments required.
Region	Select your region.
Configuration	The configuration of the current SecMaster edition.
Large Screen	Make a purchase based on your service needs.
Log Audit	Make a purchase based on your service needs. When purchasing a yearly/monthly package, you need to estimate the volume of new logs generated each day and specify **New Log**. SecMaster will automatically specify the security data collection and retention specifications. For details, see **Value-added Package Specifications**.
Security Analysis	Make a purchase based on your service needs. If you want to buy a yearly/monthly package, you are advised to estimate the data volume on a basis of 120 MB per day for each server. The data volume you set will be applied to security data collection, security data retention, security data export, platform security data, and security modeling analysis as well. For example, if this parameter is set to 1 GB/day, each day there will be 1 GB of security data that can be collected, 1 GB of security data stored, 1 GB of security data exported, 1 GB of platform security data reported, and 1 GB of data for security modeling analysis.
SOC	Make a purchase based on your service needs. If you want to buy a yearly/monthly package, set the number of operations as required.

Parameter	Description
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	Select the required duration as required. You do not need to configure this parameter in pay-per-use mode. 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

Follow-up Operations

- If the large screen function is about to expire or has expired, go to the **Purchased Resources**, locate the target resource, and 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 over the edition information in the upper right corner of the page, and click **Unsubscribe** or **Cancel** in the displayed pane. For details, see **Unsubscribing from SecMaster**.

1.3 Upgrading the Service Edition

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

Table 1-13 Edition upgrade

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.
Increase the quota	You can increase the quota. For details, see **Increasing Quotas**.

Scenario	Description
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 ● SecMaster does not support scale-downs. ● SecMaster provides basic, standard, and professional editions for your choice. For details about their differences, see **Edition Differences**. ● If you are stuck due to insufficient permission, refer to **Assigning Permissions**.	

Upgrading Basic to Standard or Professional

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Purchased Resources**. Locate the target region and click **Upgrade**.

Step 5 On the **Buy SecMaster** page, configure SecMaster parameters.

Table 1-14 Parameters for upgrading the basic edition

Parameter	Description
Current Configuration	The configuration of the current SecMaster edition.
Upgrade Method	**Version Upgrade** is selected by default.
Optional Version	Select **Standard** or **Professional**.
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 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

Upgrading Standard to Professional

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 4 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 5 On the **Buy SecMaster** page, configure SecMaster parameters.

Table 1-15 Parameters for upgrading the standard edition

Parameter	Description
Current Configuration	The configuration of the current SecMaster edition.
Upgrade Method	Select **Version Upgrade**. You can also select **Increase Quota** at the same time.
Optional Version	Select **Professional** to upgrade SecMaster to the professional edition.
Quota	The total ECS quota must be greater than or equal to the total number of ECSs within your account. This value cannot be changed to a smaller one after your purchase is complete. **NOTE** ● The maximum quota is 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.
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 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 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 Quotas**.

- 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, go to the **Security Overview** page, hover 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**.

1.4 Increasing Quotas

Scenario

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

📖 **NOTE**

If you are stuck due to insufficient permission, refer to **Assigning Permissions**.

Limitations and Constraints

- The quota is the total number of servers you authorize SecMaster to check. 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.

Increasing the Quota

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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 5 On the **Buy SecMaster** page, configure SecMaster parameters.

Table 1-16 Parameters for increasing ECS quota

Parameter	Description
Current Configuration	The configuration of the current SecMaster edition.
Upgrade Method	Click **Increase Quota**.
Quota	The total ECS quota must be greater than or equal to the total number of ECSs within your account. This value cannot be changed to a smaller one after your purchase is complete. **NOTE** ● The maximum quota is 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.
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 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

2 Authorizing SecMaster

Scenario

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

Your authorization is required first time you try to use SecMaster. The following table lists the permissions you need to assign to SecMaster.

Table 2-1 Agency permissions

Permission	Description	Assign To	When to Use
ECS FullAccess	All permissions for ECS	SecMaster_Agency	- Used to obtain the ECS asset information in the account when you purchase SecMaster for the first time. - Used to synchronize ECS asset information for asset management. - Used to execute ECS-related playbook workflows, such as one-click host de-isolation and one-click host isolation workflows.

Permission	Description	Assign To	When to Use
WAF FullAccess	Web Application Firewall (WAF) administrator	SecMaster_Agency	• Used to execute WAF-related playbook workflows, such as WAF blocking and WAF address group association policy configuration workflows. • Used to obtain website information in WAF for executing baseline inspections in playbook workflows.
SecMaster FullAccess	SecMaster administrator	SecMaster_Agency	Used to perform operations such as alert handling.
HSS FullAccess	Full permissions for HSS	SecMaster_Agency	• Used to obtain asset information in HSS for asset information synchronization in the asset management scenario. • Used to execute HSS-related playbook workflows, such as vulnerability management and host isolation workflows. • Used to obtain HSS status for executing baseline inspections in playbook workflows. • Used to execute the vulnerability fixing workflow in the host security vulnerability fixing scenario.
EPS ReadOnlyAccess	Read-only permissions for EPS.	SecMaster_Agency	• Used to obtain the list and details of enterprise projects for asset management. • Used to obtain the enterprise project ID and name for executing WAF-related playbook workflows, such as "WAF clear Non-domain Policy."

Permission	Description	Assign To	When to Use
Anti-DDoS ReadOnlyAccess	Read-only permissions for Anti-DDoS.	SecMaster_Agency	• Used to query asset information in Anti-DDoS for asset management. • Used to obtain Anti-DDoS information for executing baseline inspections in playbook workflows.
IAM ReadOnlyAccess	Read-only permissions for IAM.	SecMaster_Agency	Used to obtain IAM usernames for executing playbook workflows of batch blocking or unblocking IAM users.
WAF Administrator	WAF administrator, who has all permissions for WAF.	SecMaster_Agency	• Used to obtain website information in WAF for asset information synchronization in the asset management scenario. • Used to execute WAF-related playbook workflows, such as WAF blocking and WAF address group association policy configuration workflows. • Used to obtain website information in WAF for executing baseline inspections in playbook workflows.
SMN FullAccess	All permissions for SMN.	SecMaster_Agency	Used to execute playbook workflows related to notifications, for example, the "Automatic Notification of High-Risk Alerts" workflow.
RDS ReadOnlyAccess	Read-only permissions for RDS	SecMaster_Agency	• Used to obtain asset information in RDS for asset information synchronization in the asset management scenario. • Used to obtain the RDS instance list and details for executing baseline checks in playbook workflows.

Permission	Description	Assign To	When to Use
EIP ReadOnlyAccess	Read-only permissions for EIP	SecMaster_Agency	• Used to obtain the EIP list and details for asset management. • Used to obtain the EIP list and details for executing baseline checks in playbook workflows.
Tenant Guest	Read-only permissions for all cloud services except IAM	SecMaster_Agency	Used to query resource information of cloud services except IAM in the baseline check scenario.
NAT ReadOnlyAccess	Read-only permissions for NAT Gateway.	SecMaster_Agency	Used to obtain asset information in NAT Gateway for asset information synchronization in the asset management scenario.
VPC FullAccess	All permissions for VPC.	SecMaster_Agency	• Used to obtain asset information in VPC for asset information synchronization in the asset management scenario. • Used to execute VPC-related playbook workflows, such as security group blocking and security group blocking cancellation workflows. • Used to obtain security group information for executing baseline inspections in playbook workflows.
OBS OperateAccess	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, deleting objects, and obtaining an object ACL.	SecMaster_Agency	Used to query, upload, and download objects when the OBS plug-in is used.

Permission	Description	Assign To	When to Use
ELB ReadOnlyAccess	Read-only permissions for ELB.	SecMaster_Agency	• Used to synchronize asset information in ELB and provide details about affected assets. • Used to obtain asset information in ELB for executing baseline inspections in playbook workflows.
CFW FullAccess	All permissions for CFW.	SecMaster_Agency	• Used to obtain asset information in CFW for asset information synchronization in the asset management scenario. • Used to execute CFW-related playbook workflows, such as CFW blocking and one-click CFW unblocking workflows.

Prerequisites

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

Authorizing SecMaster

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 2-1 Workspaces > Management
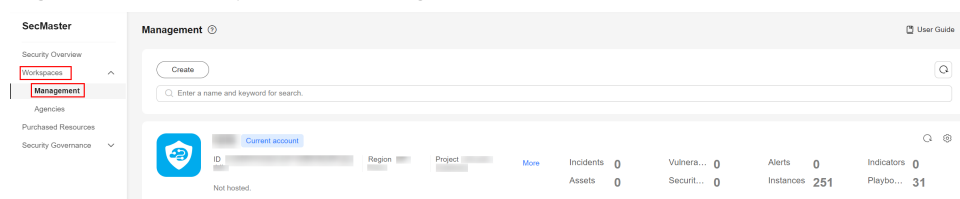
Step 5 (Optional) In the upper part of the workspace management page, click **Entrusted Service Authorization - Current Tenant**.

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

Step 6 On the page for assigning permissions, select all required permissions (which are selected by default), select **Agree to authorize**, and click **Confirm**.

----End

3 Viewing Security Overview

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

You can view the overall security assessment result by workspace, as well as view the assessment results of all workspaces.

- **Security Overview**: This page displays the overall security assessment results of all your workspaces in real time. You can follow the procedure provided below to check the results.

- **Security Situation** > **Situation Overview**: This page displays the security assessment results of the current workspace. For more details, see **Checking the Situation Overview**.

Viewing the Security Overview Page

Step 1 Log in to the management console.

Step 2 Click [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

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

Figure 3-1 Security Overview
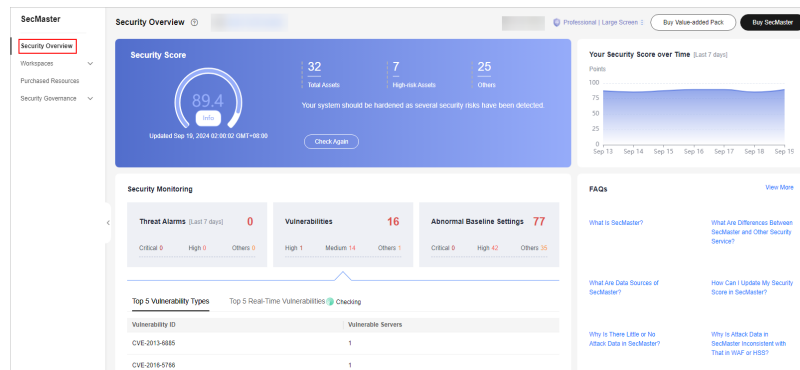
Step 5 On the **Security Overview** page, you can view the security overview of your assets and perform related operations. The **Security Overview** page consists of the following modules:

- **Security Score**
- **Security Monitoring**
- **Your Security Score over Time**

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

Table 3-1 Security Overview

| Parameter	Statistical Period	Update Frequency	Description
Security Score	Real-time	- 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 more details, see **Security Score**.
Threat Alarms	Last 7 days	Every 5 minutes	Total number of alerts in all SecMaster workspaces of your account.
Vulnerabilities	Last 7 days	Every 5 minutes	Total number of vulnerabilities in all SecMaster workspaces of your account.
Abnormal Baseline Settings	Real-time	Every 5 minutes	Total number of abnormal baseline settings in all SecMaster workspaces of your account.
Your Security Score over Time	Last 7 days	Every 5 minutes	Security scores in the last seven days.

----End

Security Score

The security score shows the overall health status of your workloads on the cloud based on the service edition you are using. You can quickly learn about unhandled risks and their threats to your assets.

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

- The score ranges from 0 to 100. A larger score indicates a lower risk and a more secure asset. For details about the security scores, see **Security Score**.

- Different color blocks in the security score ring chart indicate different severity levels. For example, yellow indicates that your security is medium.

- The security score is updated when you refresh status of the alert incident after risk handling. After you fix the risks, you can click **Check Again** so that SecMaster can check and score your system again.

  ◻ **NOTE**

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

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

Security Monitoring

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

Table 3-2 Security Monitoring parameters

Parameter	Description
Threat Alarms	This panel displays the unhandled threat alerts in all workspace of the current account for the **last 7 days**. You can quickly learn of the total number of unhandled threat alerts and the number of vulnerabilities at each severity level. The statistics are updated every 5 minutes. ● Risk severity levels: – **Critical**: There are intrusions to your workloads, and you should view alert details and handle the alert in a timely manner. – **High**: There are abnormal incidents on your workloads, and you should view alert details and handle the alert in a timely manner. – **Others**: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view alert details and take necessary actions. ● To quickly view details of top 5 threat alerts for the last 7 days, click the **Threat Alarms** panel. – You can view details of those threats, including the threat alert name, severity, asset name, and discovery time. – If no data is available here, no threat alerts are generated for the last 7 days.

Parameter	Description

Vulnerabilities	This panel displays the top five vulnerability types and the total number of unfixed vulnerabilities in your assets in all workspaces of your account for the **last 7 days**. You can quickly learn of the total number of unfixed vulnerabilities and the number of vulnerabilities at each severity level. The statistics are updated every 5 minutes.
	
	● 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 the five vulnerability types with the most affected servers.
	  – Vulnerability rankings are based on the number of hosts a vulnerability affects. The vulnerability ranked the first affects the most hosts.
	  – The data is displayed in **Top 5 Vulnerability Types** only when the hosts have Host Security Service (HSS) Agent version 2.0 installed. If no data is displayed or you want to view top 5 vulnerability types, upgrade Agent from 1.0 to 2.0.
	
	● Click **Top 5 Real-Time Vulnerabilities** tab. The system displays the top 5 vulnerability incidents for the **last 7 days**. You can quickly view vulnerability details.
	  – You can view details such as the vulnerability name, severity, asset name, and discovery time.
	  – If no data is available here, no vulnerabilities are detected on the current day.

Parameter	Description

Abnormal Baseline Settings	This panel displays the total number of compliance violations detected in all workspaces of your account. You can quickly learn of total number of violations and the number of violations at each severity level. The statistics are updated every 5 minutes.
	
	● 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 handle them in a timely manner.
	  – **Others**: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view details about results of compliance checks and take necessary actions.
	● To quickly view details of top 5 abnormal compliance risks discovered, click the **Abnormal Baseline Settings** panel.
	  – You can view details of the top compliance risks discovered in the latest check, such as check item name, severity, asset name, and discovery time.
	  – If no data is available, no violations are detected.

Your Security Score over Time

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

4 Workspaces

4.1 Workspace Overview

This topic describes the following details about workspaces:

- **What Is a Workspace?**
- **General Rules for Workspaces**

Actions you can do:

- **Creating a Workspace**: Workspaces are top-level operation platform in SecMaster. A workspace can be associated with general projects, regions, and enterprise projects to meet different security operations needs. Before using baseline inspection, alert management, security analysis, and security orchestration in SecMaster, you need to create at least one workspace first. You can use workspaces to group your resources by application scenario. This will make security operations more efficient.

- **Viewing a Workspace**: You can view the details about a workspace, including its name, type, and creation time.

- **Editing a Workspace**: You can modify the workspace basic settings, including its name and description.

- **Deleting a Workspace**: If you no longer need a workspace, you can delete it. After a workspace is deleted, SecMaster may be unable to detect security risks of assets managed in the workspace. So the risk of those assets may fail to be prevented. Deleted workspaces cannot be restored. Exercise caution when performing this operation.

- **Managing Workspace Tags**: 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.

- **Creating a Workspace Agency**: You can create a workspace agency to perform cross-account secure operations. In this way, you can centrally view asset risks, alerts, and incidents in workspaces of other users. You can create agencies to authorize other users to manage your workspaces in a project. In this way, asset risks, alerts, and incidents across workspaces can be centrally managed for security operations.

- **Managing Agencies**: 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. You can view, edit, modify, and delete an agency view, as well as delete agency views in batches.
  - **Workspaces Managed by Me**: On this tab, you can view workspaces managed in the agency view you create. You can check tasks managed by you and task parameters, and manage (accept, reject, release, and delete) tasks managed by you.
  - **My Workspaces Managed by Others**: On this tab, you can view which agency views are managing workspaces you create. You can view parameters related to the agency views, modify accepted agency tasks, withdraw accepted agency tasks, request for agencies again, release an agency, and delete agency tasks.

What Is a Workspace?

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

- Workspace management:

  A workspace can be associated with general projects and regions to support workspace operation modes in different scenarios.
- Workspace agencies:

  You can create an agency and use it to check asset risks, alerts, and incidents in many workspaces across accounts.

General Rules for Workspaces

- Paid SecMaster: A maximum of five workspaces can be created for an account in a region.
- Free SecMaster: Only one workspace can be created for an account in a 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 150 workspaces from different regions and accounts can be managed by a workspace agency view.
  - A maximum of 10 agencies can be created for an account.
- Currently, performing operations across different workspaces in multiple browser windows at the same time 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 baseline inspection, alert management, security analysis, and security orchestration in SecMaster, you need to create at least one workspace first. You can use workspaces to group your resources by application scenario. This will make security operations more efficient.

This section describes how to create a workspace.

Limitations and Constraints

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

Creating a Workspace

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-1 Workspaces > Management
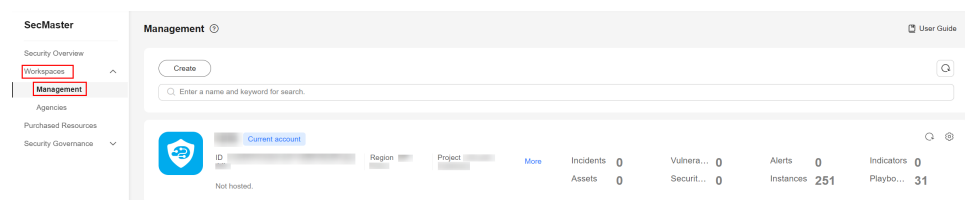
Step 5 On the **Management** page, click **Create**. The **Create Workspace** slide-out panel is displayed.

Step 6 Configure workspace parameters by referring to the following table.

Table 4-1 Parameters for creating a workspace

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.
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 7 Click **OK**.

----End

Operations You Can Do with a Workspace

You can perform security operations after adding a workspace. Functions you can use vary depending on the SecMaster edition in use. For details, see **Functions**.

● **Checking the Situation Overview**, **Checking Security Situation through Large Screens**, **Security Reports**, and **Task Center**: Check the security situation in a workspace, create security reports, handle to-do tasks, and check security situation on large screens.

● **Resource Manager**: Manage assets centrally.

● **Risk Prevention**: Prevent risks through baseline inspections, vulnerability management, emergency vulnerability notifications, and security policy management.

● **Threats**: Manage threats, including incidents, alerts, and indicators, use intelligent modeling, and perform security analysis.

● **Security Orchestration**: Implement security orchestration. Security orchestration combines security functions of different systems or components in a system involved in security operations in your 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. You can manage operations objects, playbooks, page layouts, and plug-ins.

● **Settings**: Configure log collection and access to aggregate logs into SecMaster.

4.3 Managing Workspaces

4.3.1 Viewing a Workspace

Scenario

This section describes how to view the information about a workspace, including its 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.

Viewing a Workspace

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-2 Workspaces > Management
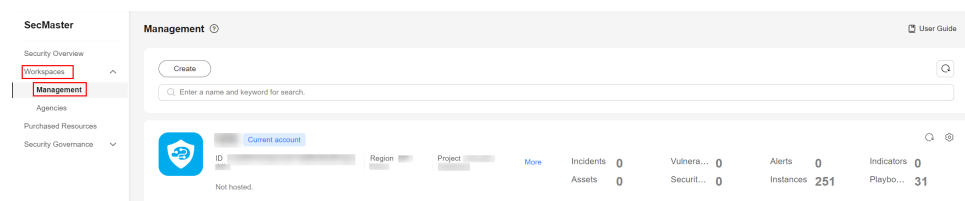
Step 5 On the **Management** page, view information about existing workspaces.

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

Figure 4-3 Workspace details
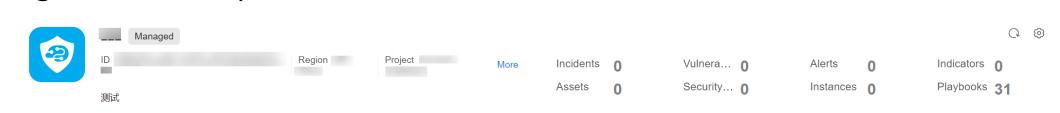
Table 4-2 Workspace parameters

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	Move the pointer over **More** to view the workspace details.
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 6 To view details about a workspace, click ⚙ on the right of the workspace. The workspace details page is displayed.

- On the workspace details page, you can view the workspace name, creation time, and project a workspace belongs to. You can also modify the workspace name and description.

- On the **Tag Management** tab, you can **edit tags**. For details, see **Managing Workspace Tags**.

----End

4.3.2 Editing a Workspace

Scenario

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

This section describes how to edit a workspace.

Editing a Workspace

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

**Step 4** In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-4 Workspaces > Management
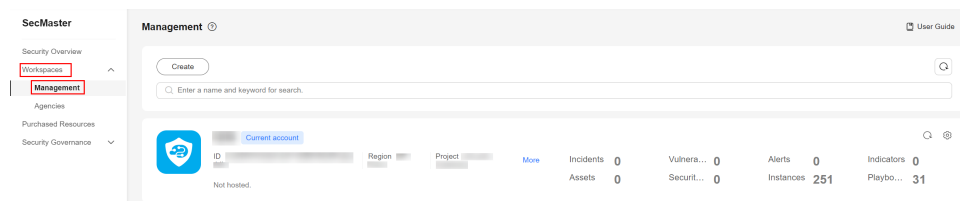
Step 5 Click ![icon] in the upper right corner of the target workspace.

Figure 4-5 Workspace details page
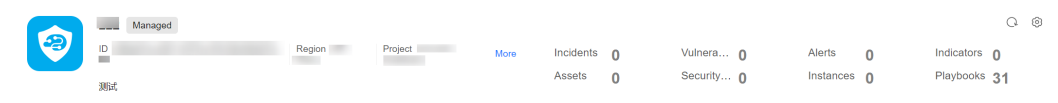
Step 6 On the workspace details page, click the edit icon ![icon] next to **Workspace Name** or **Description**.

Step 7 Edit the workspace name or description and click **OK**.

----End

4.3.3 Deleting a Workspace

Scenario

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

After a workspace is deleted, SecMaster may be unable to detect security risks of assets managed in the workspace. So the risk of those assets may fail to be prevented. 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 management console and select a region or project.

Step 3 Click [ ] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-6 Workspaces > Management
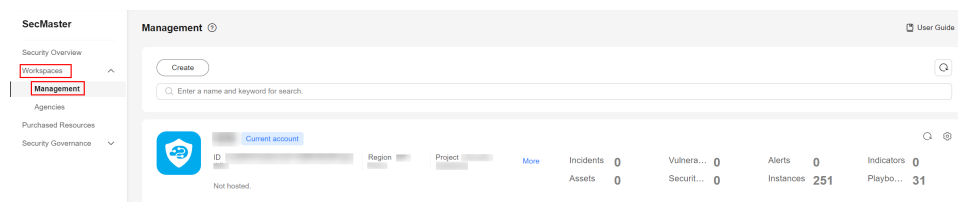
Step 5 Click [ ] in the upper right corner of the target workspace.

Figure 4-7 Workspace details page
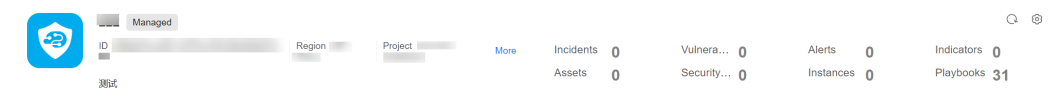
Step 6 On the workspace details page, click **Delete** in the lower right corner.

Step 7 In the **Delete Workspace** dialog box displayed, confirm the information and select **Permanently delete the workspace**. In the confirmation dialog box, enter **DELETE** and click **OK**.

> ⚠ **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

4.3.4 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.

This topic describes how to manage tags.

Limitations and Constraints

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

Managing Workspace Tags

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-8 Workspaces > Management
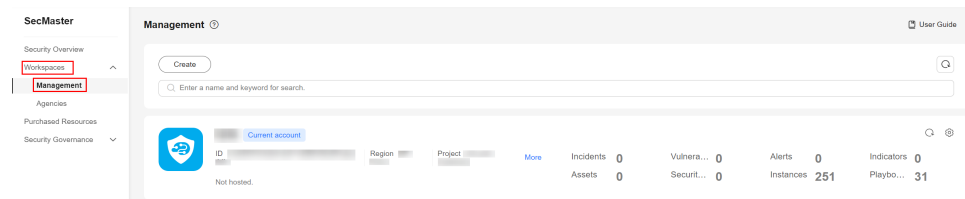
Step 5 Click ⚙ in the upper right corner of the target workspace.

Figure 4-9 Workspace details page
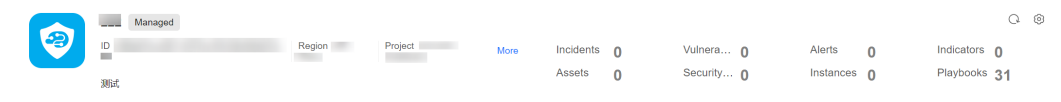
Step 6 On the workspace details page, click **Edit Tag**.

Figure 4-10 Edit Tag
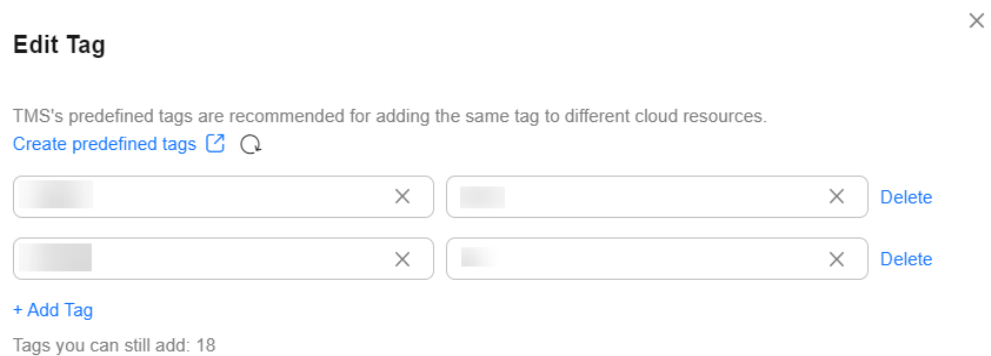
Step 7 On the page for editing a tag, you can perform the following operations on the tag.

Table 4-3 Managing tags

Operation	Description
Add Tag	1. On the tag management page, click **Add Tag**. 2. Configure **Tag key** and **Tag value**. 3. Click **OK**.
Delete Tag	1. On the tag management page, locate the row containing the target tag and click **Delete**. 2. Click **OK**.

----End

4.4 Workspace Agencies

4.4.1 Creating a Workspace Agency

Workspace Agency 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.

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.

Table 4-4 Workspace hosting process

Procedure	Description
Step 1: Create an Agency View	You need to create an agency view to manage the delegation that other users give you for workspace hosting.
Step 2: Create 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 and perform security operations for you in a unified manner.
Step 3: Authorize 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. 1. After you create an agency, authorize the user you specified in the agency to manage your workspaces. 2. Choose **Workspaces** > **Agencies** > **Workspaces Managed by Me** and accept workspaces that need to be managed by you centrally. The accepted workspaces will be attached to your workspaces.

Limitations and Constraints

- The specifications of the workspace agency views and the number of workspaces are as follows:
  - A maximum of one workspace agency view can be created for an account in a region.
  - A maximum of 150 workspaces from different regions and accounts can be managed by a workspace agency view.
  - A maximum of 10 agencies can be created for an account.
- If you select **Organization** for **Initiated By** while creating an agency, 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 to the agency.

## Step 1: Create an Agency View

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-11 Agencies
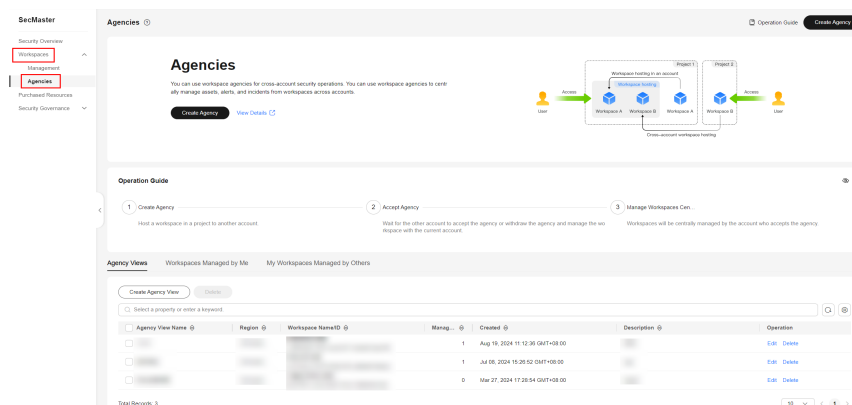
Step 5 On the **Agency Views** tab, click **Create Agency View**. The **Create Agency View** slide-out panel is displayed.

Figure 4-12 Creating an agency view
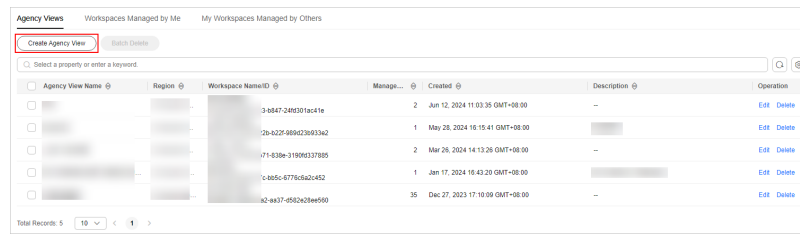
Step 6 Configure parameters required for creating the agency view.

Table 4-5 Parameters for creating an agency view

Parameter	Description
Agency View Name	Name of the agency view.
Workspace Name	The workspace you want to bind to the agency view.
(Optional) Description	Description of the agency view.

Step 7 Click **OK**.

The created agency view will be displayed on the **Agency Views** tab.

----End

Step 2: Create an Agency

Step 1 Log in to the management console.

Step 2 Click [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-13 Agencies
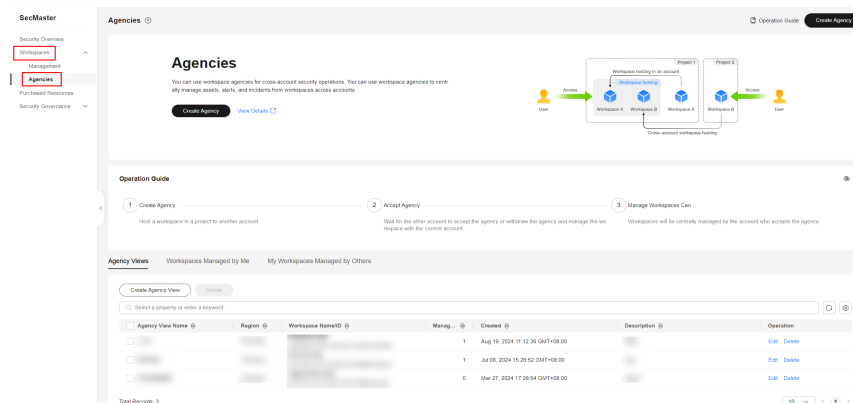
Step 5 Click **Create Agency** in the upper right corner of the page.

Step 6 On the **Create Agency** slide-out is displayed, configure agency parameters.

Table 4-6 Parameters for creating an agency

Parameter		Description
Initiated By		Agency creator.
Agency Created By	Workspace	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 4-14** Account Name
	Agency View	An existing agency view. If there are no agency views, click **Create Agency View** and create one. For details, see **Step 1: Create an Agency View**.
Agency Details	Agency Name	Name of the agency
	Agency Duration	How long the agency works
	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.

Parameter		Description
	Description	Description of the agency

Step 7 Click **Confirm**.

----End

Step 3: Authorize an Agency

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-15 Agencies
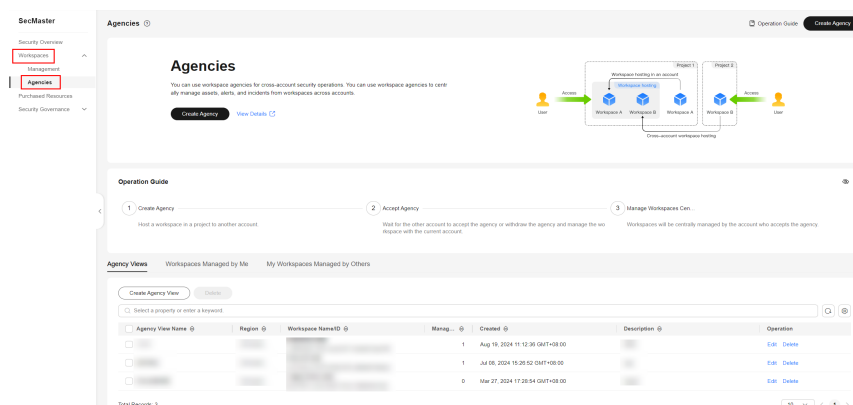
Step 5 On the **Agencies** page, click the **Workspaces Managed by Me** tab. In the row containing the workspace you want to manage, click **Accept** in the **Operation** column.

> **NOTE**
>
> If the system displays a message indicating that you are not authorized when you try to accept an agency, get authorization by referring to **Authorizing SecMaster** first.

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

----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.

Related Operations

- 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.

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

4.4.2 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. You can view, edit, modify, and delete an agency view, and delete agency views in batches.

- **Workspaces Managed by Me**: On this tab, you can view workspaces managed in the agency view you create. You can check tasks managed by you and task parameters, and manage (accept, reject, release, and delete) tasks managed by you.

- **My Workspaces Managed by Others**: On this tab, you can view which agency views are managing workspaces you create. You can view parameters related to the agency views, modify accepted agency tasks, withdraw accepted agency tasks, request for agencies again, release an agency, and delete agency tasks.

Agency Views

Step 1 Log in to the management console.

Step 2 Click ◉ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

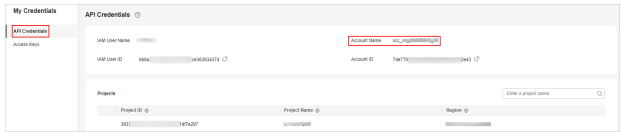**Step 4** In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-16 Agencies
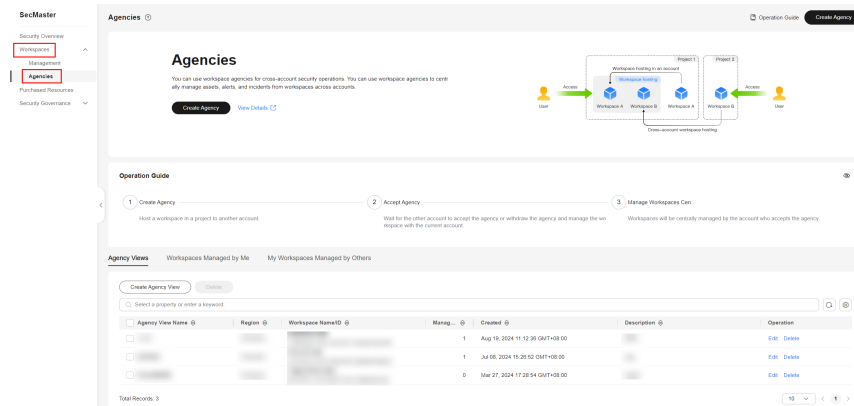
Step 5 On the **Agencies** page, click the **Agency Views** tab.

Step 6 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 **OK**.

**----End**

Workspaces Managed by Me

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-17 Agencies
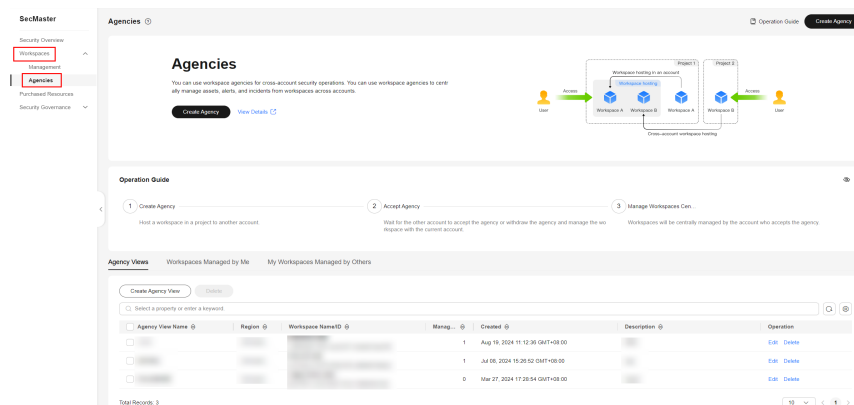
Step 5 On the **Agencies** page, click the **Workspaces Managed by Me** tab.

Step 6 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

Table 4-9 Managing workspaces managed by you

| Operation	Description
Accepting a workspace agency	1. 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. 2. In the displayed dialog box, click **Confirm**.
Rejecting a workspace agency	1. 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. 2. In the displayed dialog box, click **Confirm**.
Releasing a workspace agency	1. 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	1. 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

My Workspaces Managed by Others

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Agencies**.

Figure 4-18 Agencies
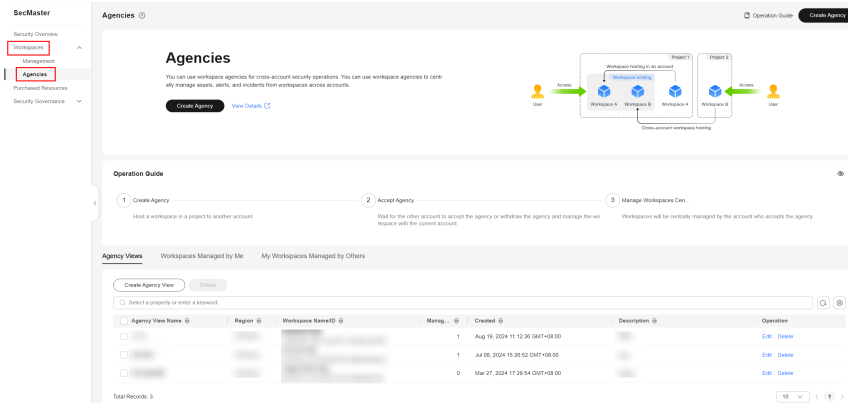
Step 5 On the **Agencies** page, click the **My Workspaces Managed by Others** tab.

Step 6 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 Managing your workspaces managed by others

| Operation	Description
Modifying an accepted workspace agency	1. Locate the row that contains the workspace agency, and click **Modify** in the **Operation** column. 2. In the displayed dialog box, modify the agency information. 3. Click **Confirm**.
Withdrawing an accepted workspace agency	1. 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. 1. 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	1. 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	1. 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.

Viewing Purchased Resources

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Purchased Resources**.

Step 5 View details on the purchased resource page.

Table 5-1 Parameters for purchased resources

Parameter	Description
Buy Value-added Pack	To get a value-added package, click **Buy Value-added Pack** and complete the purchase as prompted.
Buy SecMaster	To buy SecMaster, click **Buy SecMaster** and complete the purchase as prompted.
Total/Subscribed Regions	Regions where SecMaster has been enabled for the current account and the total number of regions where SecMaster is rolled out.
Upgradable	Number of resources that can be upgraded in all regions under the current account.
Versions About to Expire	The number of SecMaster editions and value-added packages that are about to expire in all regions under the current account.

Parameter	Description
Total Quota	The total quota purchased by the current account in all regions.
Purchased Resources	Details about SecMaster resources you purchased in each region. ● If there are many editions or regions, you can use filters to search for a specific resource by region, edition, or order number. ● You can upgrade, renew, and increase quotas for SecMaster in a specific region.

----End

6 Security Governance

6.1 Security Governance Overview

What Is Security Governance?

Security Governance in SecMaster can help you quickly assess how well your workloads comply with some security standards and practices. Based on Huawei 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 and displays compliance status in an intuitive way. You can download check reports to check details.

📖 **NOTE**

Before using security governance in SecMaster, you need to **submit a service ticket** to enable the service.

Application Scenarios

Security Governance in SecMaster can help you easily assess how well your cloud workloads comply with applicable security standards, regulations, and laws. You will quickly find the gap, rectify issues, and get related certification faster. SecMaster provides security governance templates and compliance policy scanning services. The standard clauses in security compliance packs have been converted into check items. If you subscribe to a compliance pack, SecMaster can automatically check your workload compliance with check items in the pack and generate a report for you.

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 code-based 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.

Process of Using SecMaster

Table 6-1 shows the process of using SecMaster security governance.

Figure 6-1 Process of using the security governance function

Table 6-1 Process description

Step	Description
Authorizing SecMaster to Access Cloud Service Resources	Before using security governance, you need to authorize SecMaster to access your cloud service resources. After that, you can check cloud assets on security compliance through policy scanning.
Subscribing to or Unsubscribing from a Compliance Pack	SecMaster provides different security compliance packs. You can subscribe to the one that best fits your needs.
Starting a Self-Assessment	You can execute check items in the compliance pack you subscribe to and evaluate your service compliance.
Viewing the result	After policy scanning or self-assessment, you can view the security governance status. ● **Viewing Security Compliance Overview**: View service compliance with laws, regulations, standards, and compliance pack, as well as policy scanning results. ● **Viewing Evaluation Results**: Check status and details of compliance with each compliance pack. ● **Viewing Policy Scanning Results**: Check the policy scanning results and details.
Downloading a Compliance Report	Security Governance provides security compliance reports. You can download the reports to learn of how well your services comply with mainstream security standards.

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 6-2** for you to comply with various privacy protection laws. You can refer to the guidelines and subscribe to compliance packs as you need.

Table 6-2 Security standards compliance packs

Pack	Description	Applicable Region	Category	Domain	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.	Global	Industry standards	Data security	1. Applicable to entities that handle payment cards. These entities include merchants, processing organizations, receipt organizations, card issuing organizations, and service providers. 2. 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. 3. 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.

Pack	Description	Applicable Region	Category	Domain	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.	Global	International standards	Information security	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	Applicable Region	Category	Domain	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.	Global	International standards	Privacy protection	1. 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. 2. 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 processors are privacy stakeholders who process the data based on these purposes and methods. 3. 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 Authorizing SecMaster to Access Cloud Service Resources

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.

Prerequisites

The account for using the security governance function must have the **Agent Operator**, **Tenant Administrator**, and **Security Administrator** permissions.

Authorizing SecMaster to Access Cloud Service Resources

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Step 5 On the **Subscriptions** page, click **Authorize** in the **Authorize Service** process. The service authorization dialog box is displayed.

Step 6 In the displayed dialog box, click **Agree to authorize**.

----End

6.4 Subscribing to or Unsubscribing from a Compliance Pack

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 walks you through how to subscribe to and unsubscribe from a compliance pack.

- **Subscribing to a Compliance Pack**: You can learn of compliance packs by referring to **Security Compliance Pack Description** and subscribe to the one you need.

- **Unsubscribing from a Compliance Pack**: If you need to cancel the subscription to a compliance pack, you can unsubscribe from it on the **Subscriptions** page.
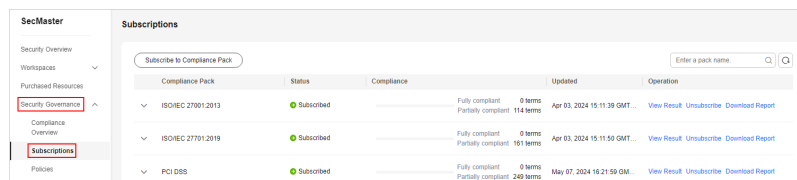
Prerequisites

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

Subscribing to a Compliance Pack

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-2 Subscriptions page

Step 5 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 6 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 7 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 **Starting a Self-Assessment**.

----End

Unsubscribing from a Compliance Pack

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Step 5 On the **Subscriptions** page, locate the row that contains the compliance pack you want to unsubscribe from, click **Unsubscribe** in the **Operation** column.

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

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

----End

6.5 Starting a 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 packs. For details, see **Subscribing to or Unsubscribing from a Compliance Pack**.

Starting a Self-Assessment

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-3 Subscriptions page
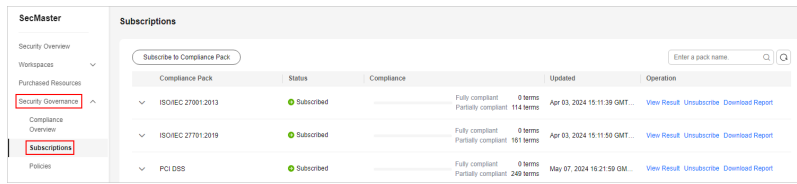
Step 5 Click ⌄ on the left of the compliance pack to be self-assessed to expand the compliance pack information. In the Tenant Self-Assessment area, click **Evaluate** in the **Operation** column. The evaluation page is displayed.

Figure 6-4 Evaluated by customers
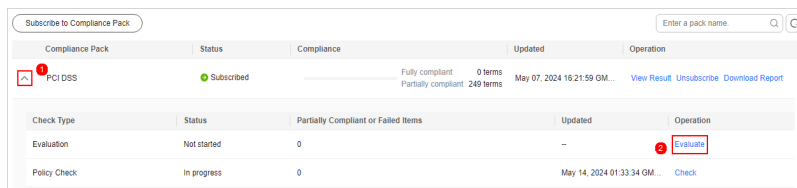
Step 6 On the **Evaluation** page, perform self-assessment on each check item.

Figure 6-5 Evaluation page
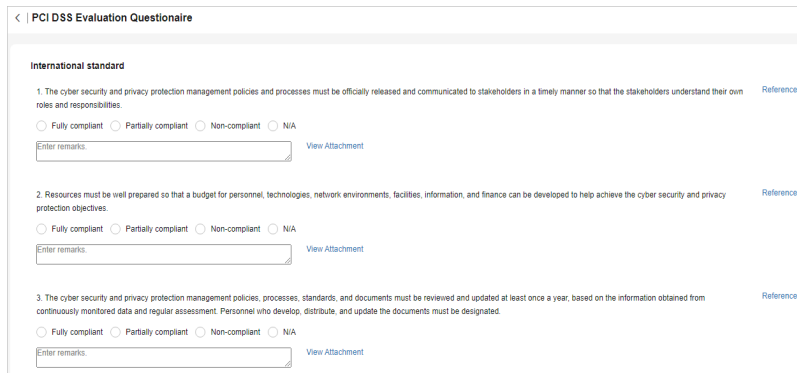
- To upload an attachment, click **View Attachment** > **Upload Attachment** and upload related credential information.
- During the evaluation, click **Reference** on the right of the evaluation item to view basic information, related terms, and historical records of the check item.

Step 7 After the evaluation is complete, click **Submit** in the lower right corner.

----End

6.6 Viewing 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 or Unsubscribing from a Compliance Pack**.

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 management console and select a region or project.

Step 3　Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4　In the navigation pane on the left, choose **Security Governance** > **Compliance Overview**. The **Compliance Overview** page is displayed.

Figure 6-6 Compliance overview page
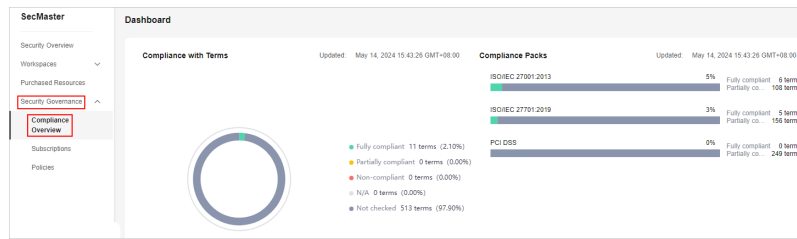
Step 5　On the **Compliance Overview** page, view the **Compliance with Terms**.

Figure 6-7 Compliance with Terms

----End

Viewing Policy Check Results

Step 1　Log in to the management console.

Step 2　Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3　Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4　In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Step 5 On the **Compliance Overview** page, view the **Policy Check**.

Figure 6-8 Policy check results
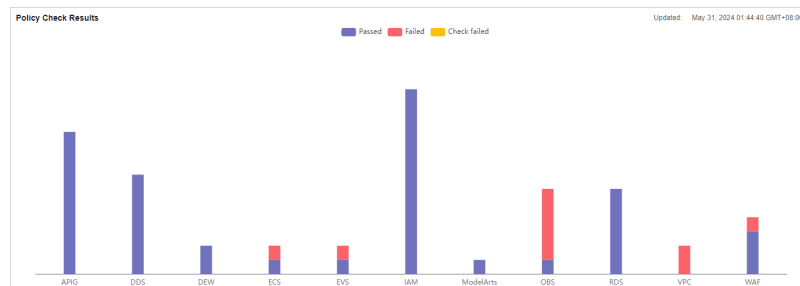
----**End**

6.7 Viewing Evaluation Results

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 or Unsubscribing from a Compliance Pack**.

Viewing Evaluation Results

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-9 Subscriptions page

Step 5 Click **View Result** in the **Operation** column. The **Evaluation Result** page is displayed.

Figure 6-10 View Result

Step 6 View the evaluation results.

Figure 6-11 Result page
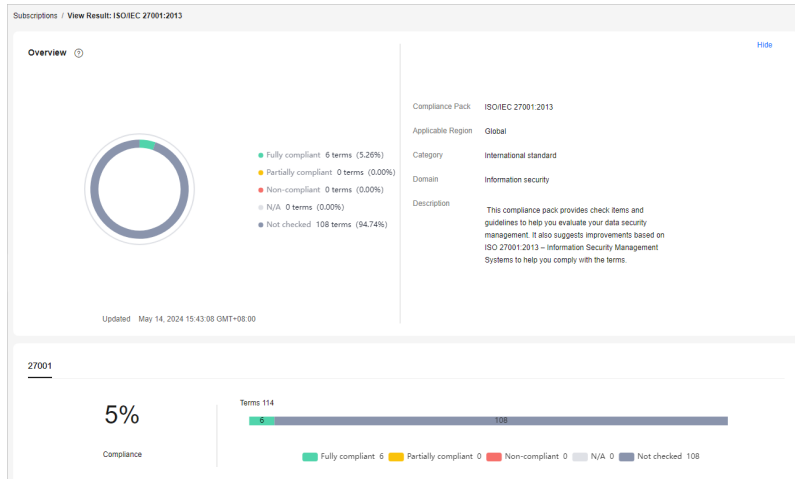
- View the overall compliance of the currently subscribed security compliance pack.

- 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 6-12 Selecting terms
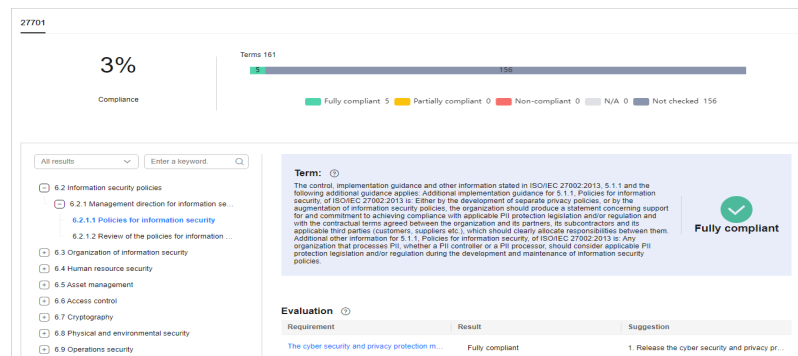
  b.   Click the name of a check item. On the displayed page, click **Edit** and enter the compliance status and evaluation remarks.

      If related credentials are available, click **Upload Files**.

Figure 6-13 Evaluated by customers

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

----End

6.8 Viewing Policy Scanning Results

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 or Unsubscribing from a Compliance Pack**.

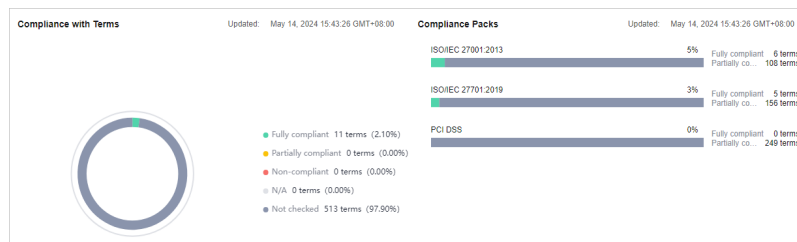## Viewing Policy Scanning Results

Step 1 Log in to the management console.

Step 2 Click 🌐 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Governance** > **Policies**. The **Policy Check** page is displayed.

Figure 6-14 Policy Check page
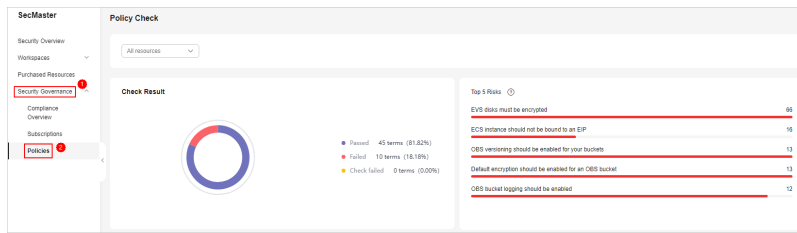
Step 5 View policy check result.

Figure 6-15 Policy check
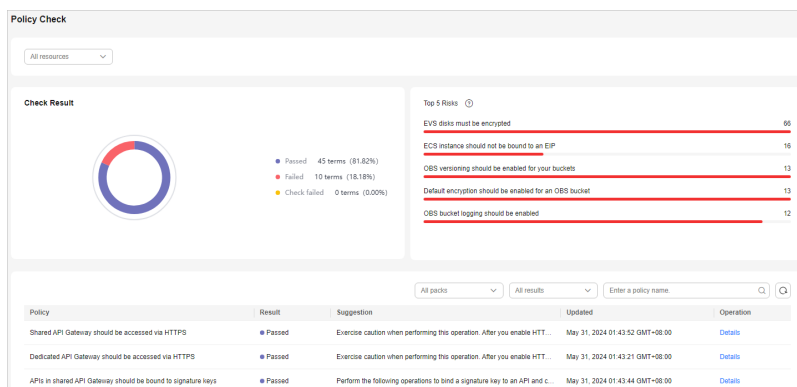
- By default, the check status of all resource policies displayed.
  - Check result: overall pass rate, passed policies, failed policies, and check failures.
  - Top 5 risks: Top 5 policies with the most failures.
- To view the check result of all policies of a resource, select the resource from the filter box in the upper part.

Figure 6-16 Selecting a resource
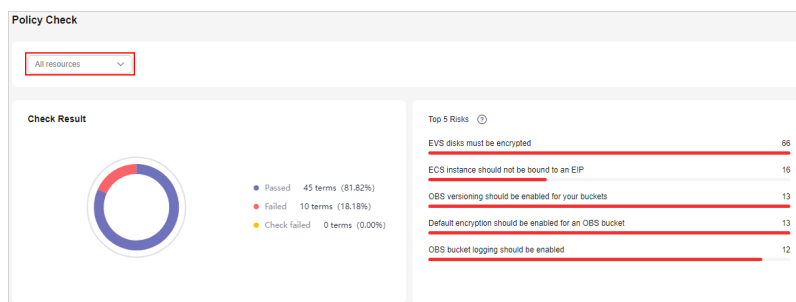
- To view the scanning status of all resources in a policy, select the corresponding compliance pack in the upper part of the table.

  You can also filter the results by result type or policy name.

Figure 6-17 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.

Step 6 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.

Figure 6-18 Details of a check

📖 **NOTE**

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

----End

6.9 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 or Unsubscribing from a Compliance Pack**.

Downloading a Compliance Report

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Step 5 On the **Subscriptions** page, click **Download Report** in the **Operation** column.

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

----End

7 Security Situation

7.1 Checking the Situation Overview

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

You can view the overall security assessment result by workspace, as well as view the assessment results of all workspaces.

- **Security Overview**: This page displays the overall security assessment results of all your workspaces in real time. You can follow the procedure provided in **Viewing Security Overview** to do this.

- **Situation Overview**: The **Security Situation** > **Situation Overview** page in each workspace displays the security assessment result of the logged-in workspace. You can follow the procedure below to view the assessment result of a specific workspace.

Checking the Situation Overview

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
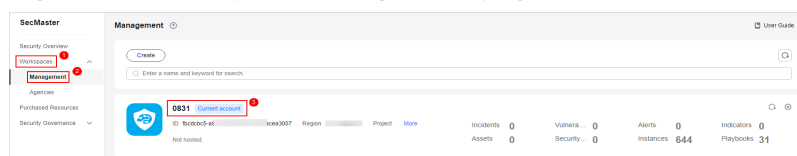
Step 5 In the navigation pane on the left, choose **Security Situation** > **Situation Overview**.

Figure 7-2 Situation Overview
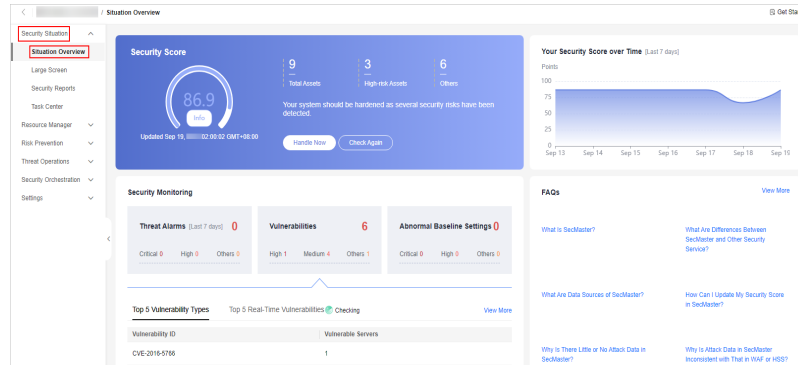
Step 6 On the **Security Overview** page, you can view the security overview of your assets and perform related operations. The **Situation Overview** page consists of the following modules:

- **Security Score**

- **Security Monitoring**

- **Your Security Score over Time**

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

Table 7-1 Situation Overview

Parameter	Reference Period	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 severity levels and numbers of unhandled configuration issues, vulnerabilities, and threats. For more details, see **Security Score**.
Threat Alarms	Last 7 days	Every 5 minutes	Total number of alerts on the **Threats** > **Alerts** page in a workspace.
Vulnerabilities	Last 7 days	Every 5 minutes	Total number of vulnerabilities on the **Risk Prevention** > **Vulnerabilities** in a workspace.
Abnormal Baseline Settings	Real-time	Every 5 minutes	Total number of issues on the **Risk Prevention** > **Baseline Inspection** page in a workspace.

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 service edition you are using. You can quickly learn about unhandled risks and their threats to your assets.

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

- The score ranges from 0 to 100. A larger score indicates a lower risk and a more secure asset. For details about the security scores, 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.

- Click **Handle Now**. The **Risks** pane is displayed on the right. You can handle risks by referring to the corresponding guidance.

  - The **Risks** slide-out panel lists all threats that you should handle in a timely manner. These threats are included in the **Threat Alarms**, **Vulnerabilities**, and **Abnormal Baseline Settings** areas.

  - The **Risks** pane displays the latest check results of the last scan. The **Alerts**, **Vulnerabilities**, and **Abnormal Baseline Settings** pages show check results of all previous scans. So, you will find the threat number on the **Risks** pane is less than that on those pages. You can click **Handle** for an alert on the **Risks** pane to go to the corresponding page quickly.

  - **Handling detected security risks:**

    i. In the **Security Score** area, click **Handle Now**.

    ii. On the **Risks** slide-out panel displayed, click **Handle**.

    iii. On the page displayed, handle risk alerts, vulnerabilities, or baseline inspection items.

- The security score is updated when you refresh status of the alert incident after risk handling. After you fix the risks, you can click **Check Again** so that SecMaster can check and score your system again.

  ◻ NOTE

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

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

Security Monitoring

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

Table 7-2 Security Monitoring parameters

Parameter	Description

Threat Alarms	This panel displays the unhandled threat alerts in a workspace for the last 7 days. You can quickly learn of the total number of unhandled threat alerts and the number of vulnerabilities at each severity level. The statistics are updated every 5 minutes.
	● Risk severity levels:
	  – **Critical**: There are intrusions to your workloads, and you should view alert details and handle the alert in a timely manner.
	  – **High**: There are abnormal incidents on your workloads, and you should view alert details and handle the alert in a timely manner.
	  – **Others**: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view alert details and take necessary actions.
	● To quickly view details of top 5 threat alerts for the last 7 days, click the **Threat Alarms** panel.
	  – You can view details of those threats, including the threat alert name, severity, asset name, and discovery time.
	  – If no data is available here, no threat alerts are generated for the last 7 days.
	  – You can click **View More** to go to the **Alerts** page and view more alerts. You can also customize filter criteria to query alert information. For details about how to view threat alerts, see **Viewing Alert Details**.

Parameter	Description

Vulnerabilities	This panel displays the top five vulnerability types and the total number of unfixed vulnerabilities in your assets in a workspace for the last 7 days. You can quickly learn of the total number of unfixed vulnerabilities and the number of vulnerabilities at each severity level. The statistics are updated every 5 minutes.
	
	● 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 the five vulnerability types with the most affected servers.
	  – Vulnerability rankings are based on the number of hosts a vulnerability affects. The vulnerability ranked the first affects the most hosts.
	  – The data is displayed in **Top 5 Vulnerability Types** only when the hosts have Host Security Service (HSS) Agent version 2.0 installed. If no data is displayed or you want to view top 5 vulnerability types, upgrade Agent from 1.0 to 2.0.
	● Click **Top 5 Real-Time Vulnerabilities** tab. The system displays the top 5 vulnerability incidents for the last 7 days. You can quickly view vulnerability details.
	  – You can view details such as the vulnerability name, severity, asset name, and discovery time.
	  – If no data is available here, no vulnerabilities are detected on the current day.
	  – You can click **View More** to go to the **Vulnerabilities** page and view more vulnerabilities. You can also customize filter criteria to query vulnerability information. For details, see **Viewing Vulnerability Details**.

Parameter	Description

Abnormal Baseline Settings	This panel displays the total number of compliance violations detected in a workspace. You can quickly learn of total number of violations and the number of violations at each severity level. The statistics are updated every 5 minutes.
	
	● 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, 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.
	  – 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 Check Results**.

Your Security Score over Time

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

7.2 Checking Security Situation through Large Screens

7.2.1 Large Screen Overview

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 the following large screens:

● **Overall Situation Screen**: This screen helps display attack history, identify attacks, and predict attack trends. It can provide you with powerful pre-event,

in-event, and post-event security management capabilities, making it easier to understand your cloud security via one screen.

- **Monitoring Statistics Screen**: You can view the overview of unhandled alerts, incidents, vulnerabilities, and unsafe baselines on this screen.

- **Asset Security Screen**: With this screen, you can quickly learn of the asset protection status, including the total number of assets, number of attacked assets, and number of unprotected assets.

- **Threat Situation Screen**: You can view threats to and attacks at your networks, applications, and servers via this screen.

- **Vulnerable Assets Screen**: You can check vulnerable assets, vulnerabilities, unsafe baseline settings, as well unprotected assets via this screen.

7.2.2 Overall Situation Screen

Scenarios

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

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

Prerequisites

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

Viewing the Overall Situation Screen

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-3 Workspace management page
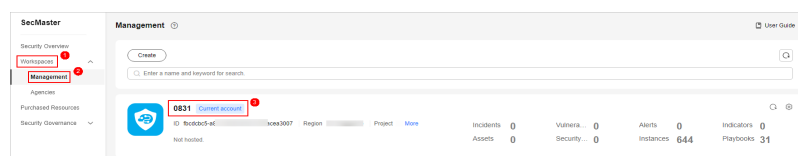
Step 5 In the navigation pane on the left, choose **Security Situation** > **Large Screen**.

Figure 7-4 Large Screen
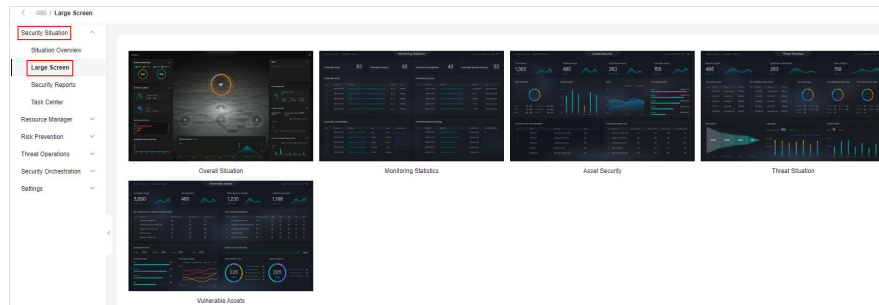
Step 6 Click **Play** in the lower right corner of the overall situation screen to access the page.

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

----End

Security Score

The security score of the current assets is displayed.

Table 7-3 Security Score

Parameter	Reference Period	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 7-5 Security Score
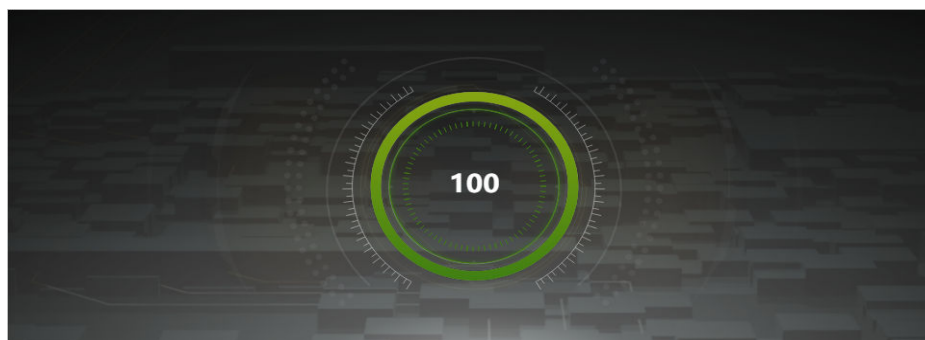
Alert Statistics

The alert statistics of interconnected services are displayed, as shown in **Figure 7-6**.

The alert data comes from the **Threats** > **Alerts** data in the current workspace. You can view more details on this page.

Table 7-4 Alert statistics

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

Figure 7-6 Alert Statistics
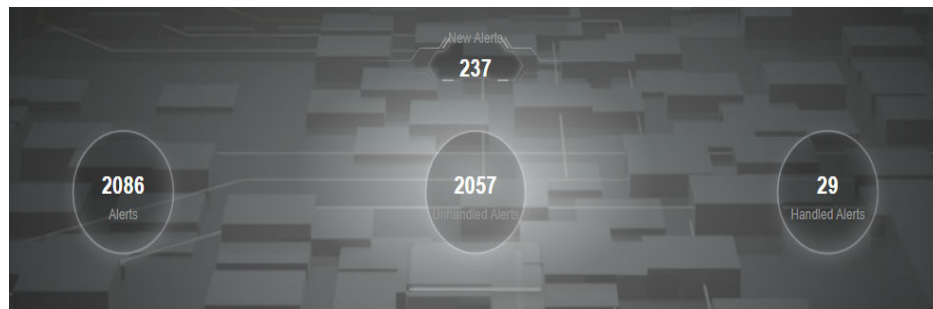
Asset Protection

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

Table 7-5 Asset protection rate

Parameter	Reference Period	Update Frequency	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

Figure 7-7 Asset protection rate
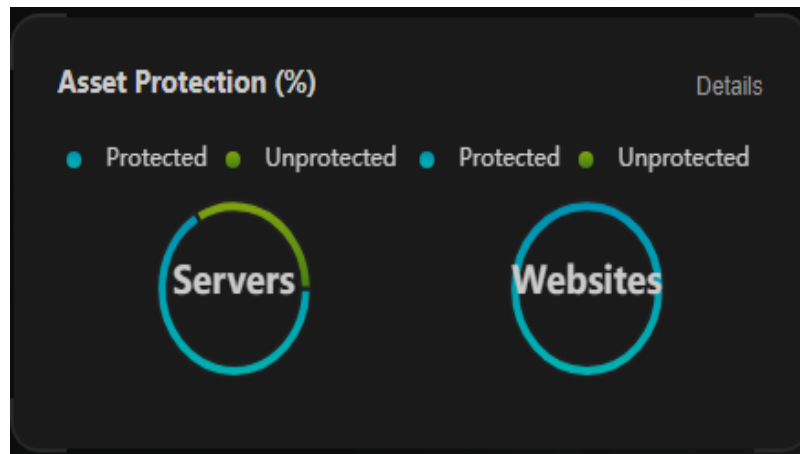
Baseline Inspection

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 7-8**.

● The baseline data comes from the **Risk Prevention** > **Baseline Inspection** page in the current workspace. You can view more details on this page.

● The vulnerability data comes from the **Risk Prevention** > **Vulnerabilities** page in the current workspace. You can view more details on this page.

Table 7-6 Baseline inspection

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

Figure 7-8 Baseline Inspection
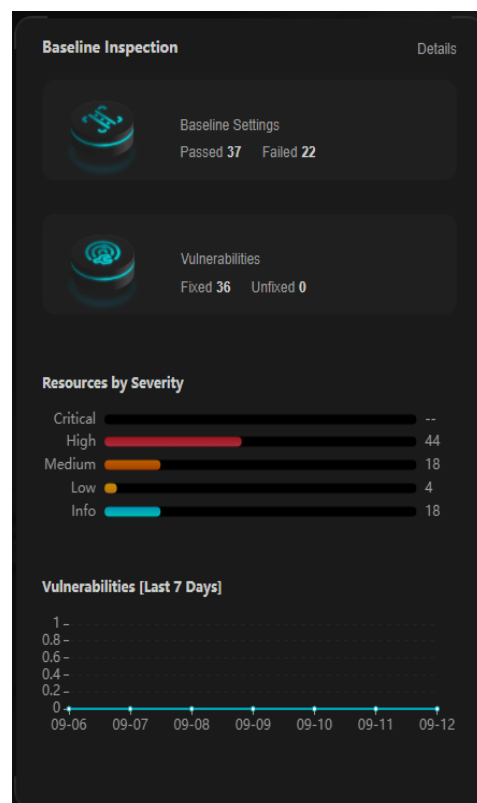
Recent Threats

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

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

Table 7-7 Recent threats

Parameter	Reference Period	Update Frequency	Description
Attacks	Last 7 days	5 minutes	Number of daily alerts over the last seven days. The alert data comes from the **Threats** > **Alerts** data in the current workspace. You can view more details on this page.
Logs	Last 7 days	5 minutes	Number of security logs reported every day in the last seven days.

Figure 7-9 Recent threats
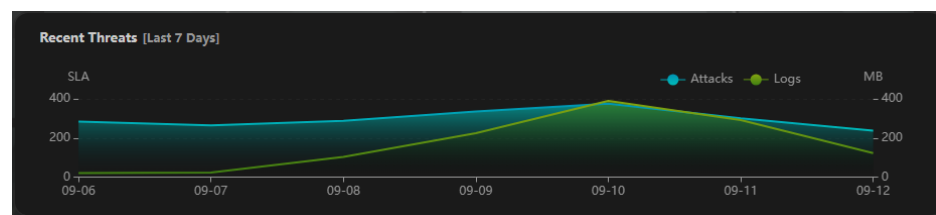
To-Dos

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

Table 7-8 To-dos

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

Figure 7-10 To-Dos
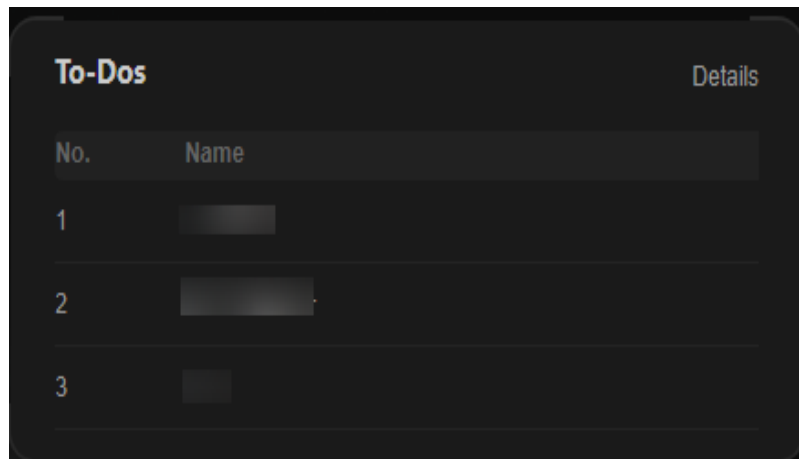
Resolved Issues

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

The alert data comes from the **Threats** > **Alerts** data in the current workspace. You can view more details on this page.

Table 7-9 Resolved issues

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

Parameter		Reference Period	Update Frequency	Description
SLA and MTTR [Last 7 Days]	SLA Statistics	Last 7 days	5 minutes	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.
Handled Alerts [Last 7 Days]		Last 7 days	5 minutes	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 7-11 Resolved issues
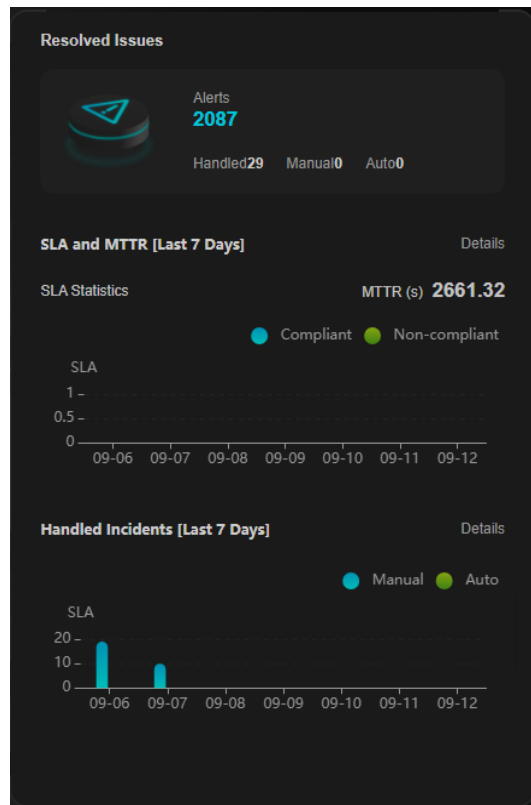
7.2.3 Monitoring Statistics Screen

Scenarios

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

By default, SecMaster provides a **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**.

Viewing Monitoring Statistics Screen

Step 1 Log in to the management console.

Step 2 Click [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-12 Workspace management page
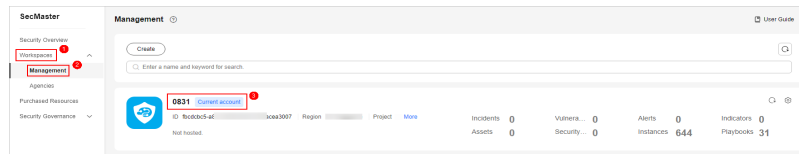
Step 5 In the navigation pane on the left, choose **Security Situation** > **Large Screen**.

Figure 7-13 Large Screen
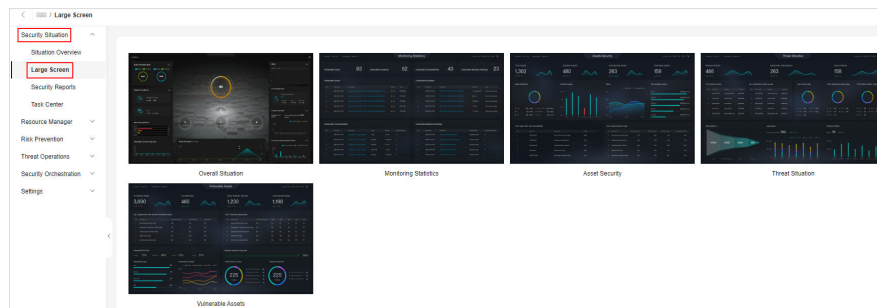
Step 6 Click **Play** in the lower right corner of the monitoring statistics screen to open the page.

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

----End

Monitoring Statistics Overview

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

Table 7-10 Security Response Overview

Parameter	Statistical Period	Update Frequency	Description
Unhandled Alerts	Last 7 days	5 minutes	Number of alerts to be handled in the last seven days. The alert data comes from the **Threats** > **Alerts** data in the current workspace. You can view more details on this page.

Parameter	Statistical Period	Update Frequency	Description
Unhandled Incidents	Last 7 days	5 minutes	Number of open or blocked incidents in the last seven days. The incident data comes from the **Threats** > **Incidents** data in the current workspace. You can view more details on this page.
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.
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 7-14 Monitoring Statistics Overview

| Unhandled Alarms | 1508 | Unhandled Events | 3 | Unhandled Vulnerabilities | 5 | Unhandled Baseline Settings | 21 |
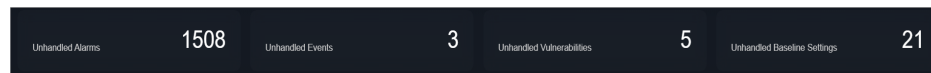
Unhandled Alerts

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 7-11 Unhandled Alerts

Parameter	Statistical Period	Update Frequency	Description
Unhandled Alerts	Last 7 days	5 minutes	Number of alerts that have not been handled for the last seven days. The alert data comes from the **Threats** > **Alerts** data in the current workspace. You can view more details on this page.

Figure 7-15 Unhandled Alerts

Unhandled Incidents

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

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

Table 7-12 Unhandled Incidents

Parameter	Statistical Period	Update Frequency	Description
Unhandled Incidents	Last 7 days	5 minutes	Number of incidents that have not been closed in the last seven days. The incident data comes from the **Threats** > **Incidents** data in the current workspace. You can view more details on this page.

Figure 7-16 Unhandled Incidents

Unhandled Vulnerabilities

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

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

Table 7-13 Unhandled Vulnerabilities

Parameter	Statistical Period	Update Frequency	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.

Figure 7-17 Unhandled Vulnerabilities

Unhandled Baseline Settings

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

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

Table 7-14 Unhandled Baseline Settings

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

Figure 7-18 Unhandled Baseline Settings

7.2.4 Asset Security Screen

Scenarios

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

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

Prerequisites

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

Viewing the Asset Security Screen

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-19 Workspace management page
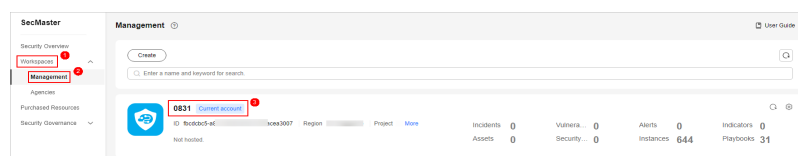
Step 5 In the navigation pane on the left, choose **Security Situation** > **Large Screen**.

Figure 7-20 Large Screen
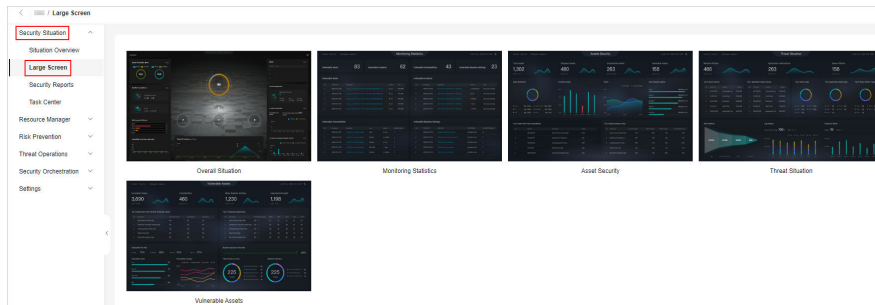
Step 6 Click **Play** in the lower right corner of the asset security image to access the screen.

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

----End

Asset Security Screen Overview

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

Table 7-15 Asset Security Screen

Parameter	Statistical Period	Update Frequency	Description
Assets	Real-time	Hourly	Total number of assets managed in **Resource Manager**.
Attacked Assets	Last 7 days	Hourly	Number of assets affected by alerts aggregated in **Threats** > **Alerts** in the current workspace.

Parameter	Statistical Period	Update Frequency	Description
Unprotected Assets	Real-time	Hourly	Number of assets that are not protected by any security service; for example, ECSs that are not protected by HSS and EIPs that are not protected by DDoS. You will learn of how many assets with **Protection Status** marked as **Unprotected** in **Resource Manager**. In **Resource Manager**, the protection status for assets is as follows: ● **Protected**: The security product required for an asset is enabled for the asset. ● **Unprotected**: The security product required for an asset has not been purchased or enabled for the asset. If you want to protect target assets, purchase corresponding security products and enable protection. For example, if you want to protect ECSs, purchase HSS and enable HSS for each ECS. ● **--**: The required security product is not supported in the current region.
Assets with Vulnerabilities or Unsafe Settings	Real-time	Hourly	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 the **Risk Prevention** > **Vulnerabilities** page, and the baseline inspection data comes from the **Risk Prevention** > **Baseline Inspection** > **Resources to Check** page.

Figure 7-21 Asset Security Screen
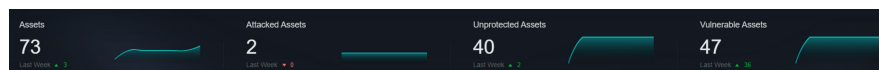
Asset Distribution

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

Table 7-16 Asset Distribution

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

Figure 7-22 Asset Distribution

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 7-17 Top 5 Assets with the Most Vulnerabilities and Top 5 Departments with the Highest Protection Rate

Parameter	Statistical Period	Update Frequency	Description
Top 5 Assets with the Most Vulnerabilities	Real-time	Hourly	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.
Top 5 Departments with the Highest Protection Rate	Real-time	Hourly	This graph lists 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 7-23 Top 5 Assets with the Most Vulnerabilities and Top 5 Departments with the Highest Protection Rate
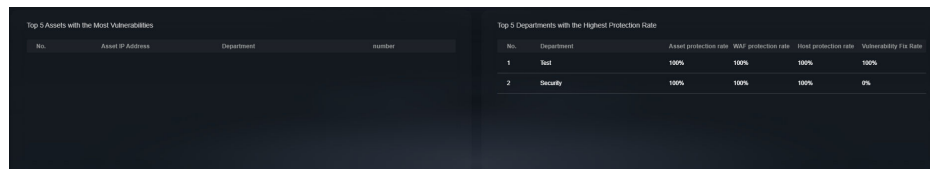
7.2.5 Threat Situation Screen

Scenarios

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

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

Prerequisites

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

Viewing the Threat Situation Screen

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-24 Workspace management page
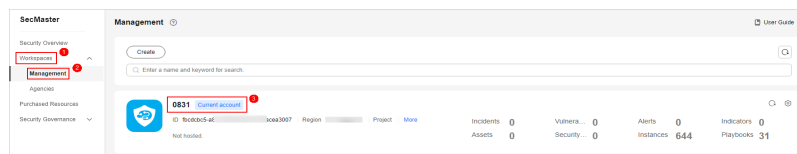
Step 5 In the navigation pane on the left, choose **Security Situation** > **Large Screen**.

Figure 7-25 Large Screen
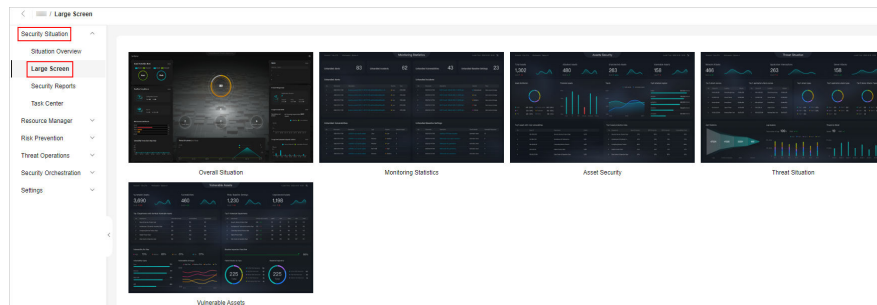
Step 6 Click **Play** in the lower right corner of the **Threat Situation** image to access the screen.

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

----End

Threat Situation screen

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

Table 7-18 Threat Situation screen

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

Figure 7-26 Threat Situation screen
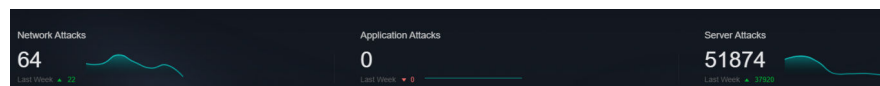
Attack Source Distribution

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

Table 7-19 Attack source distribution

Parameter	Statistical Period	Update Frequency	Description
Top 5 Source IP Addresses by Network Alerts	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	Statistical Period	Update Frequency	Description
Top 5 Source IP Addresses by Application Alerts	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 7-27 Attack source distribution
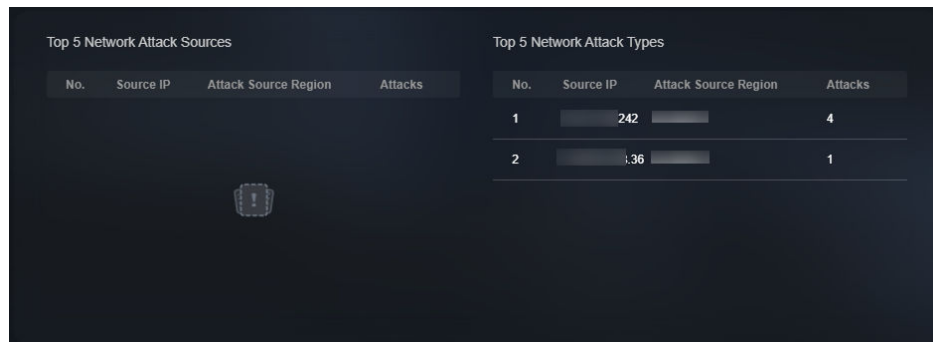
Attacks by Type

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

Table 7-20 Attacks by Type

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

Parameter	Statistical Period	Update Frequency	Description
Top 5 Server Attack Types	Last 7 days	Hourly	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 **Threats** > **Alerts** page in SecMaster.

Figure 7-28 Attack type distribution
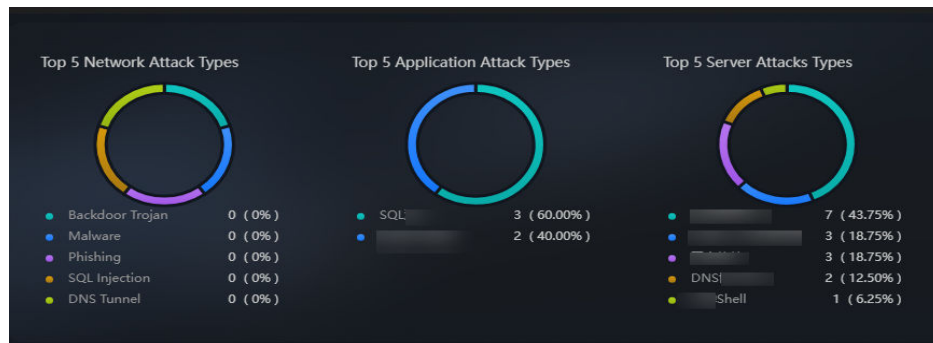
Threat Situation Statistics

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

Table 7-21 Threat Situation Statistics

Parameter		Statistical Period	Update Frequency	Description
Alert Statistics	Logs	Last 7 days	Hourly	Total number of network, application, and server access logs for the last seven days.
	Threats			Total number of threats identified for protected networks, applications, and servers for the last seven days.
	Alerts			This number reflects alerts generated for the last seven days based on attack logs. The data comes from the **Threats** > **Alerts** page.

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

Figure 7-29 Threat situation statistics

7.2.6 Vulnerable Assets Screen

Scenarios

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

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

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

Prerequisites

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

Viewing the Vulnerable Assets Screen

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-30 Workspace management page
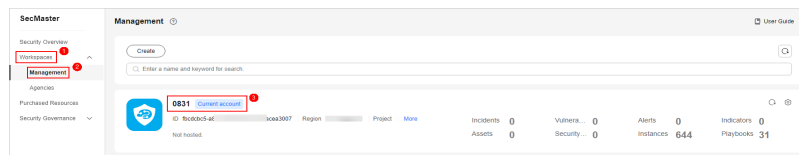
Step 5 In the navigation pane on the left, choose **Security Situation** > **Large Screen**.

Figure 7-31 Large Screen
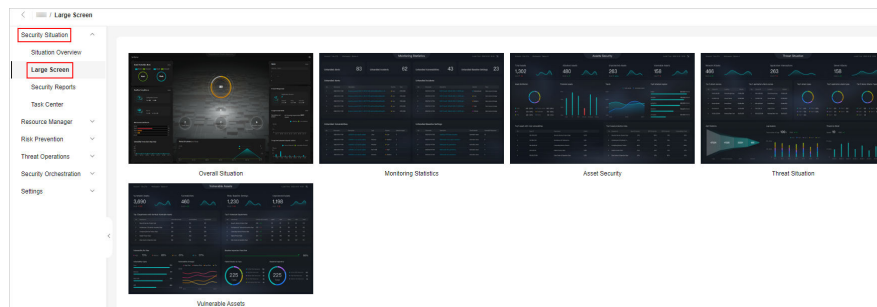
Step 6 Click **Play** in the lower right corner of the vulnerable assets image to access the screen.

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

----End

Vulnerable Assets Overview

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

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

Table 7-22 Vulnerable Assets Overview

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

Figure 7-32 Vulnerable Assets Screen
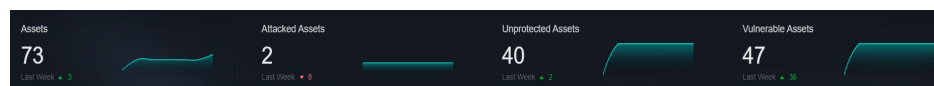
Top 5 Departments with the Most Vulnerabilities

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.

Table 7-23 Vulnerable departments

Parameter	Statistical Period	Update Frequency	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.

Figure 7-33 Top 5 Vulnerable Departments
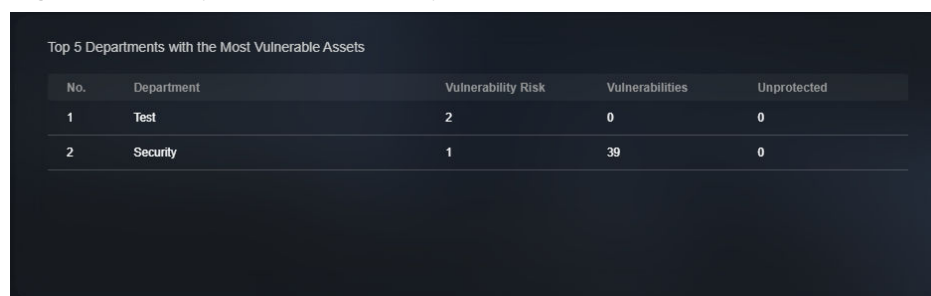
Top 5 Department with the Most Unprotected Assets

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

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

Table 7-24 Department with the most unprotected assets

Parameter	Statistical Period	Update Frequency	Description
Top 5 Department with the Most Unprotected Assets	Real-time	Hourly	The five departments with the most unprotected assets.

Figure 7-34 Top 5 Department with the Most Unprotected Assets

Vulnerability Fix Rate

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

Table 7-25 Vulnerability fix rate

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

Figure 7-35 Vulnerability fixing rate

Baseline Inspection Pass Rate

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

Table 7-26 Baseline Inspection Pass Rate

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

Figure 7-36 Baseline Inspection Pass Rate
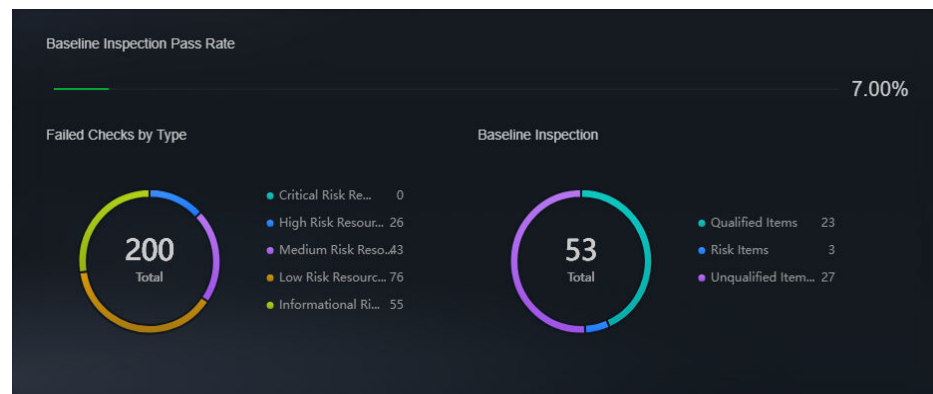
7.3 Security Reports

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 workspace of an 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-37 Workspace management page
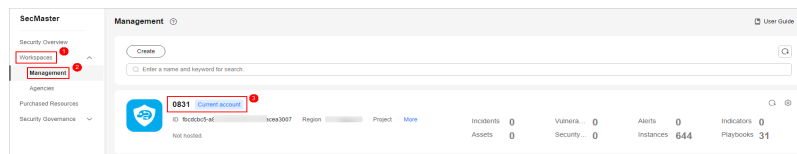
Step 5 In the navigation pane on the left, choose **Security Situation** > **Security Reports**.

Figure 7-38 Security Reports
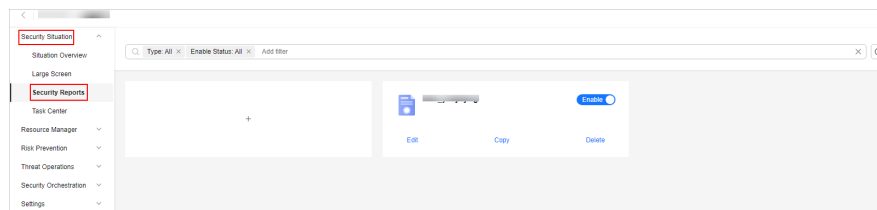
Step 6 On the **Reports** page, click ✛ to go to the basic configuration page.

Step 7 Configure basic information of the report.

Table 7-27 Report parameters

Parameter	Description
Report Name	Name of the report you want to create.

Parameter	Description
Schedule	Select a report type. ● **Daily**: SecMaster collects security information from 00:00:00 to 23:59:59 of the previous day by default. ● **Weekly**: SecMaster collects statistics on security information from 00:00:00 on Monday to 23:59:59 on Sunday of the previous week. ● **Monthly**: SecMaster collects statistics on security information from 00:00:00 on the first day to 23:59:59 on the last day of the previous month. ● **Custom**: Customize a time range.
Data Scope	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 send 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 00:00:00 last Monday to 23:59:59 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 an interval to let SecMaster send reports.
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.
Report Format	Format of the security report. The options are HTML, JPG, WORD, and PDF.
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 semicolons (;). 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 semicolons (;). Example: test03@example.com;test04@example.com
(Optional) Remarks	Remarks for the security report.

Step 8 Click **Next: Report Choose** in the upper right corner.

Step 9 On the **Report Selection** page, select a report from the left. After selecting, you can preview the report layout in the right pane.

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

- To download a report, click ⬇ in the upper left corner of the report preview page. In the dialog box displayed, select a report format and click **OK**.

  The system then automatically downloads the report for you.

- To view a report in full screen, click 🖥 in the upper left corner of the report preview page.

Step 10 Click **Complete** in the lower right corner. On the displayed **Security Reports** page, view the created report.

----End

Copying a Report

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-39 Workspace management page
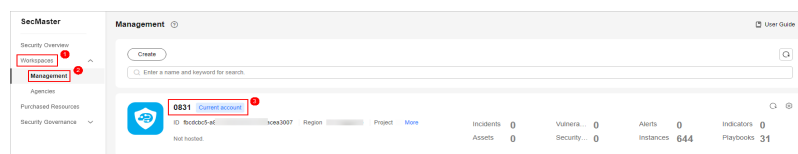
Step 5 In the navigation pane on the left, choose **Security Situation** > **Security Reports**.

Figure 7-40 Security Reports
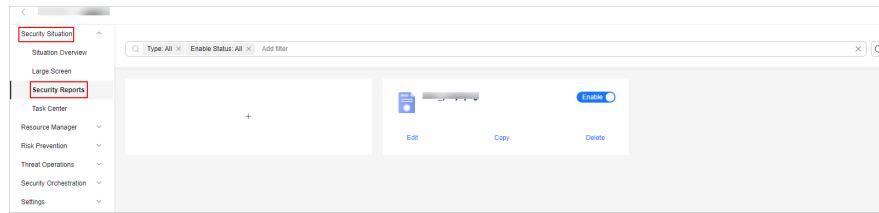
Step 6 Select a report template and click **Copy**.

Step 7 Edit basic information of the report.

Step 8 Click **Next: Report Choose**. The report configuration page is displayed.

- To download a report, click ⬇ in the upper left corner of the report preview page. In the dialog box displayed, select a report format and click **OK**.

  The system then automatically downloads the report for you.

- To view a report in full screen, click 🖥 in the upper left corner of the report preview page.

Step 9 Click **Complete** in the lower right corner. On the displayed **Security 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.

Viewing a Security Report

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
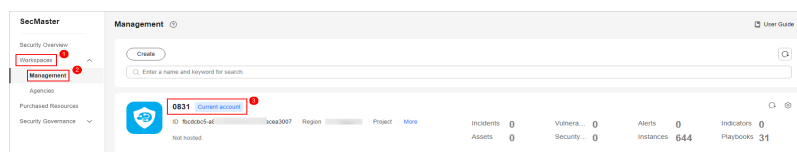
Step 5 In the navigation pane on the left, choose **Security Situation** > **Security Reports**.

Figure 7-42 Security Reports
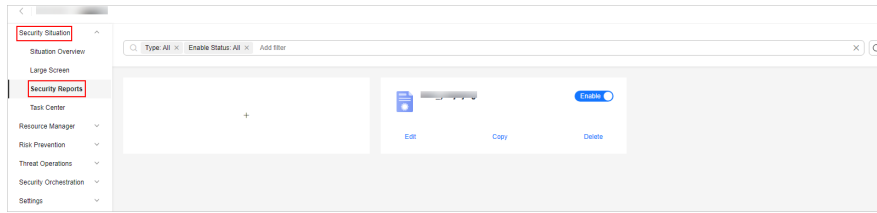
Step 6 Click the module where the target report is located. The report details page is displayed.

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

----End

Content in the Daily Report Template

Table 7-28 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.
Baseline Inspection	Displays the statistics of the latest baseline check, including the following information: ● The number of baseline check items ● Number of failed compliance 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

Parameter	Description
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 ● MTTR ● Number of confirmed high-risk intrusion incidents
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 by asset type

Parameter	Description
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/Server attacks over time ● WAF inspection findings ● Top 5 network alert types ● Top 5 application alert type statistics ● Top 5 server alert type statistics ● Top 5 source IP addresses by application alerts ● Top 5 destination IP addresses by application alerts ● Top 5 source IP addresses by network alerts ● Top 5 destination IP addresses by server alerts ● 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 volume 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 7-29 Content in the **Weekly** Report Template

Parameter	Description
Data Scope	SecMaster collects security information from 00:00:00 on Monday to 23:59:59 on Sunday of the previous week.
Security 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
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 ● 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 rate by asset type (%)

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/Server attacks over time • WAF inspection findings • Top 5 network alert types • Top 5 application alert types • Top 5 server alert types • Top 5 source IP addresses by application alerts • Top 5 destination IP addresses by application alerts • Top 5 source IP addresses by network alerts • Top 5 destination IP addresses by server alerts • 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

Table 7-30 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 items ● Number of compliance check items in the latest baseline check
Security Vulnerabilities	Displays the vulnerability statistics of the accessed cloud services on the last data of the previous month, including the following information: ● 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

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 • 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 rate by asset type (%)

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/Server attacks over time ● WAF inspection findings ● Top 5 network alert types ● Top 5 application alert types ● Top 5 server alert types ● Top 5 source IP addresses by application alerts ● Top 5 destination IP addresses by application alerts ● Top 5 source IP addresses by network alerts ● Top 5 destination IP addresses by server alerts ● 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.

Downloading a Security Report

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-43 Workspace management page
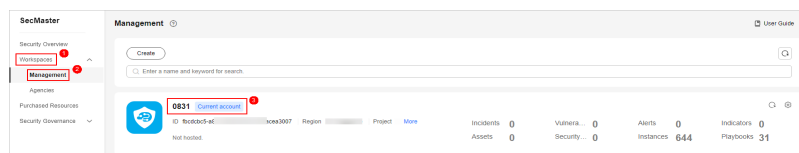
Step 5 In the navigation pane on the left, choose **Security Situation** > **Security Reports**.

Figure 7-44 Security Reports
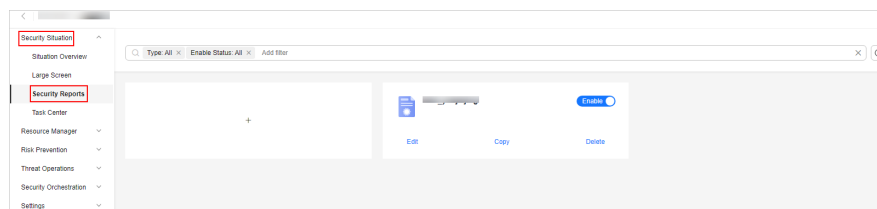
Step 6 Locate a report template and click **Edit**.

You can also download the report. For details, see **Creating and Copying a Security Report**.

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

Step 8 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 9 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.

Managing Security Reports

Step 1 Log in to the management console.

Step 2 Click 🌐 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-45 Workspace management page
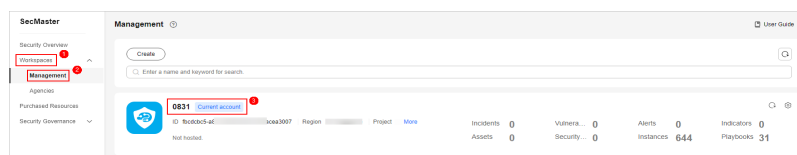
Step 5 In the navigation pane on the left, choose **Security Situation** > **Security Reports**.

Figure 7-46 Security Reports
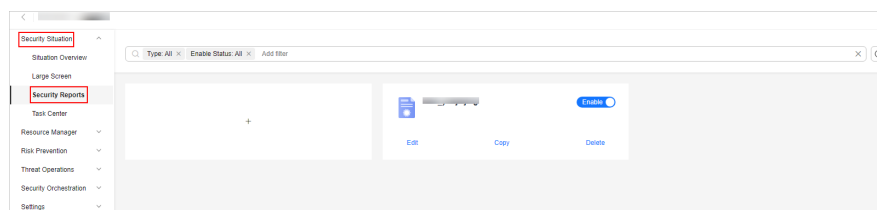
Step 6 Manage security reports.

Table 7-31 Managing security reports

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 **Finish** in the upper right corner.
Deleting a Security Report	1. On the **Reports** page, locate the desired report and click **Delete**. 2. Click **OK**.

----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.

Viewing To-Do Tasks

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-47 Workspace management page
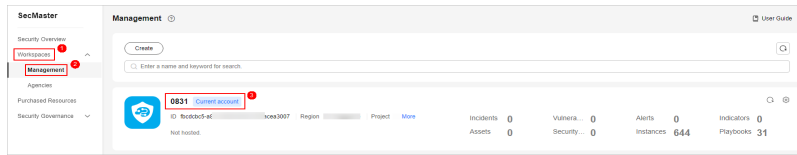
Step 5 In the navigation pane on the left, choose **Security Situation** > **Task Center**.

Figure 7-48 To-Dos
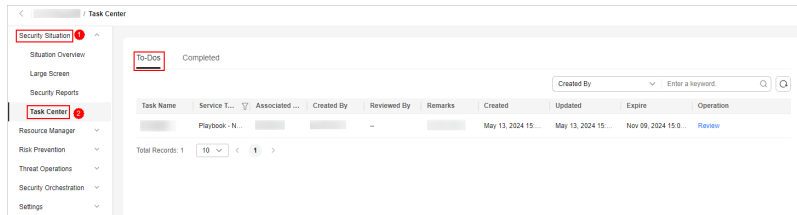
Step 6 On the **To-Dos** tab page displayed, view details about the to-do tasks.

Table 7-32 To-do task parameters

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.

----End

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.

Handling a To-Do Task

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
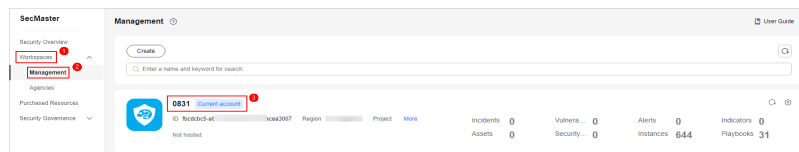
Step 5 In the navigation pane on the left, choose **Security Situation** > **Task Center**.

Figure 7-50 To-Dos
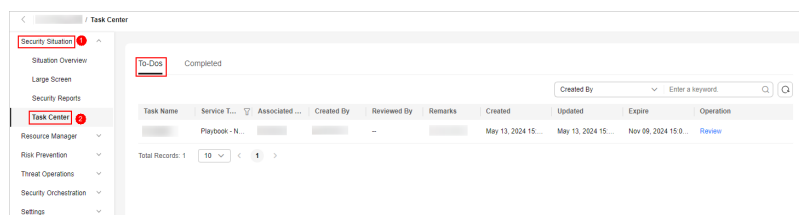
Step 6 In the row containing the target to-do task, click **Approve** in the **Operation** column.

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.

Viewing Completed Tasks

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
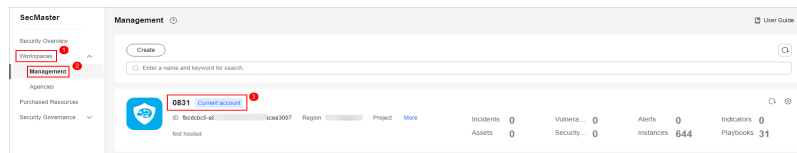
Step 5 In the navigation pane on the left, choose **Security Situation** > **Task Center**. On the displayed page, click the **Completed** tab.

Figure 7-52 Completed
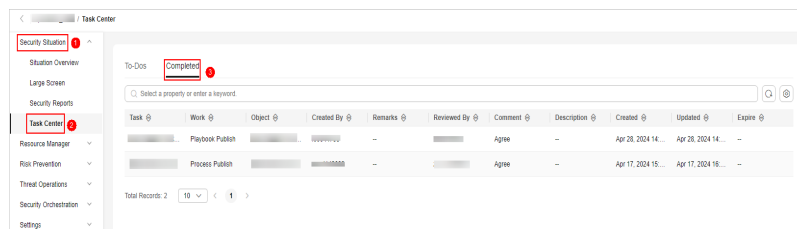
Step 6 View details about handled tasks in the task list.

Table 7-33 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.

- Cloud assets: assets on this cloud, for example, Elastic Cloud Server (ECS), Web Application Firewall (WAF), Relational Database Service (RDS), Elastic IP (EIP), and Virtual Private Cloud (VPC).

- Off-cloud assets: assets not on this cloud, for example, on-premises servers, IDC servers, or servers on third-party cloud platforms.

With SecMaster, you can:

- Manage cloud assets: **Set asset subscription**, **view asset information**, **import or export assets**, and **edit or delete assets**.

- Manage off-cloud assets: **View asset information**, **import or export assets**, and **edit or delete assets**.

To manage off-cloud assets, you need to import asset information into SecMaster first. This is the only difference from management of cloud assets.

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

Asset Source and Corresponding Security Products

Table 8-1 Asset source and corresponding security products

Asset Type	Asset Name	Source	Security Product
Cloud asset	Servers	Elastic Cloud Server (ECS)	Host Security Service (HSS)

Asset Type	Asset Name	Source	Security Product
Cloud asset	Website	Web Application Firewall (WAF)	Web Application Firewall (WAF)
Cloud asset	Database	Relational Database Service (RDS)	Database Security Service (DBSS)
Cloud asset	VPC	Virtual Private Cloud (VPC)	Cloud Firewall (CFW)
Cloud asset	EIP	Elastic IP (EIP)	CNAD Basic (Anti-DDoS)
Off-cloud asset	Device	Off-cloud assets include on-premises servers, IDC servers, servers on third-party cloud platforms. In a word, off-cloud assets include assets that are not on Huawei Cloud.	--

> **NOTE**
>
> After the asset information is synchronized to SecMaster, the protection status of assets will be displayed on the SecMaster console. The protection status is as follows:
>
> ● If **Protection Status** for an asset is **Protected**, the corresponding security product has been enabled for the asset.
>
> ● If **Protection Status** for an asset is **Unprotected**, the corresponding security product has not been purchased or enabled for the asset. If you want to protect target assets, purchase corresponding security products and enable protection. For example, if you want to protect ECSs, purchase HSS and enable HSS for each ECS.
> For details about security products, see **HSS Operation Guide**, **WAF Operation Guide**, **DBSS Operation Guide**, **CFW Operation Guide**, and **Anti-DDoS Operation Guide**.
>
> ● If **protection status** for an asset is **--**, the corresponding security product is not supported in the current region.

Limitations and Constraints

After asset subscription, you can click **System Synchronize Assets** on the **Resource Manager** page to synchronize asset information again. The basic edition allows you to synchronize assets one time per day, and the standard or professional edition allows you to synchronize assets 20 times per day. If you exceed this threshold, the system displays error message "**Insufficient resource synchronization quota.**" In this case, synchronize assets again the next day.

8.2 Configuring the Asset 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. Then, resource information will be automatically synchronized every night.

This section describes how to make a subscription to resources.

📖 **NOTE**

- SecMaster automatically synchronizes all asset data within a region to the first workspace in the region. For non-first workspaces, you need to configure log access manually.
- Only cloud resources can be subscribed to and synchronized to SecMaster. Subscribing to resource information to multiple workspaces in a region is not recommended.

Configuring the Asset Subscription

Step 1 Log in to the management console.

**Step 2** Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
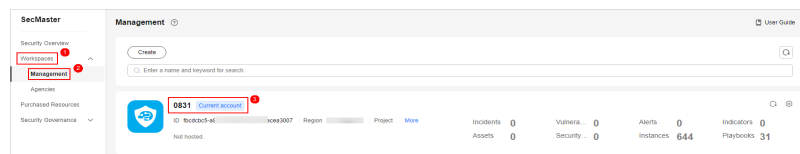
Step 5 In the navigation pane on the left, choose **Resource Manager** > **Resource Manager**.

Figure 8-2 Resource Manager
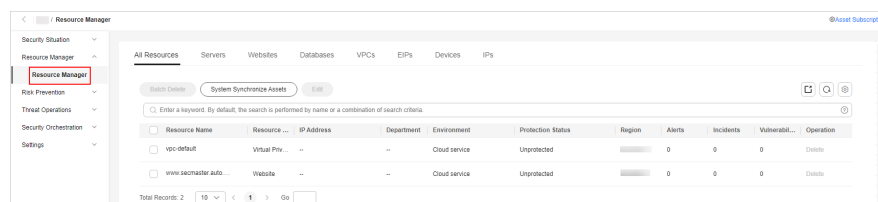
Step 6 On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.

Step 7 On the **Asset Subscription** page sliding out from the right, locate the row that contains the region where the target resource is located, and enable subscription.

Step 8 Click **OK**.

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

After asset subscription, you can click **System Synchronize Assets** on the **Resource Manager** page to synchronize asset information again. The basic edition allows you to synchronize assets one time per day, and the standard or professional edition allows you to synchronize assets 20 times per day. If you exceed this threshold, the system displays error message "**Insufficient resource synchronization quota.**" In this case, synchronize assets again the next day.

----End

8.3 Viewing Asset Information

Scenario

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

Prerequisites

- You have completed asset subscriptions. For details, see **Configuring the Asset Subscription**.
- You have purchased the SecMaster standard or professional edition.

Viewing Resource Information

**Step 1** Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
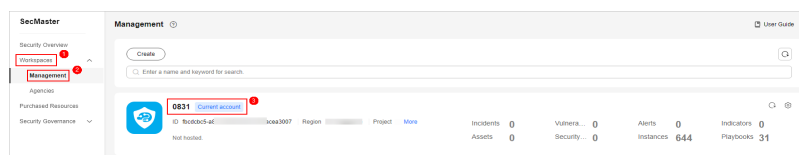
Step 5 In the navigation pane on the left, choose **Resource Manager** > **Resource Manager**.

Figure 8-4 Resource Manager
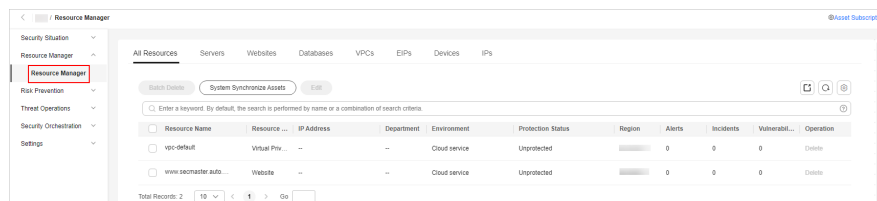
Step 6 (Optional) Complete the asset subscription first. If you have done this once, skip this step.

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

📖 NOTE

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

1. On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.

2. 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.

3. Click **OK**.

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

   After asset subscription, you can click **System Synchronize Assets** on the **Resource Manager** page to synchronize asset information again. The basic edition allows you to synchronize assets one time per day, and the standard or professional edition allows you to synchronize assets 20 times per day. If you exceed this threshold, the system displays error message "**Insufficient resource synchronization quota.**" In this case, synchronize assets again the next day.

Step 7 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.

- You can view the total number of assets below the asset list. You can view a maximum of 10,000 asset records page by page. To view more than 10,000 asset records, optimize the filter criteria.

- To view more details about an asset, check its asset type. Then, go to the corresponding resource tab and click the resource name of the asset to go to its details page.

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

  – On the asset details page, you can view the environment, asset, and network details related to the asset.

  – Edit the owner, service system, and department of the resource. You can also bind the resources to or unbind the resources from an owner, service system, or department.

Table 8-2 Asset source and corresponding security products

Asset Type	Asset Name	Source	Security Product
Cloud asset	Servers	Elastic Cloud Server (ECS)	Host Security Service (HSS)
Cloud asset	Website	Web Application Firewall (WAF)	Web Application Firewall (WAF)
Cloud asset	Database	Relational Database Service (RDS)	Database Security Service (DBSS)
Cloud asset	VPC	Virtual Private Cloud (VPC)	Cloud Firewall (CFW)
Cloud asset	EIP	Elastic IP (EIP)	CNAD Basic (Anti-DDoS)
Off-cloud asset	Device	Off-cloud assets include on-premises servers, IDC servers, servers on third-party cloud platforms. In a word, off-cloud assets include assets that are not on Huawei Cloud.	--

NOTE

After the asset information is synchronized to SecMaster, the protection status of assets will be displayed on the SecMaster console. The protection status is as follows:

- If **Protection Status** for an asset is **Protected**, the corresponding security product has been enabled for the asset.

- If **Protection Status** for an asset is **Unprotected**, the corresponding security product has not been purchased or enabled for the asset. If you want to protect target assets, purchase corresponding security products and enable protection. For example, if you want to protect ECSs, purchase HSS and enable HSS for each ECS.
  For details about security products, see **HSS Operation Guide**, **WAF Operation Guide**, **DBSS Operation Guide**, **CFW Operation Guide**, and **Anti-DDoS Operation Guide**.

- If **protection status** for an asset is **--**, the corresponding security product is not supported in the current region.

----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 files in .xlsx can be imported. Each time you can import one file no larger than 5 MB and with a maximum of 100 records.
- A maximum of 9,999 resource records can be exported.

Importing Assets

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
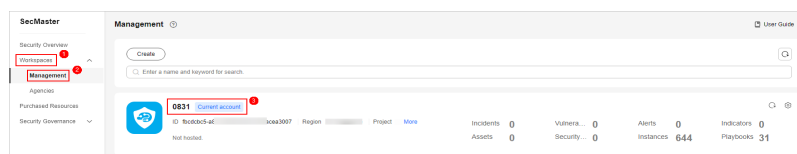
Step 5 In the navigation pane on the left, choose **Resource Manager** > **Resource Manager**.

Figure 8-6 Resource Manager
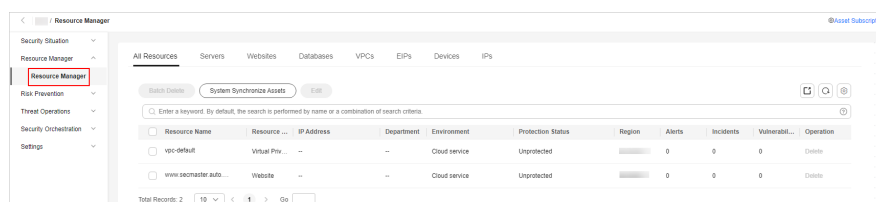
Step 6 On the **Resource Manager** page, click a tab corresponding to the type of the resources you want to import. For example, if you want to import servers, click the **Servers** tab.

Step 7 In the upper left corner of the asset list, click **Import**.

Step 8 In the **Import** dialog box, click **Download Template**. Then, fill information about the resource to be imported in the template.

Step 9 After the template is completed, click **Select File** in the **Import** dialog box and select the Excel file you want to import.

**Step 10** Click **OK**.

----End

Exporting Assets

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
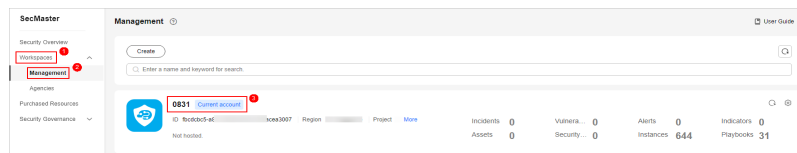
Step 5 In the navigation pane on the left, choose **Resource Manager** > **Resource Manager**.

Figure 8-8 Resource Manager
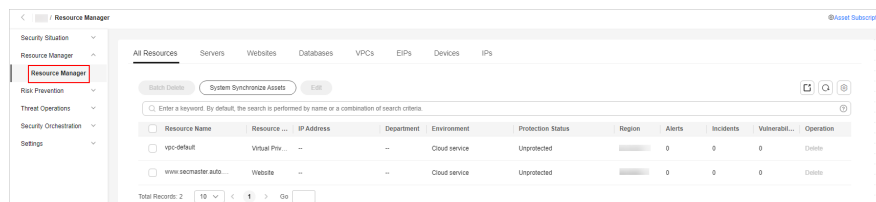
Step 6 On the asset management page, click the corresponding asset tab. For example, if you want to export servers, click the **Servers** tab.

Step 7 On the asset page, select the assets to be exported and click in the upper right corner of the list.

Step 8 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 9 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

8.5 Editing or Deleting an Asset

Scenario

On the **Resource Manager** page, you can edit the department, service system, and owner of a resource. You can also delete assets you imported into SecMaster. You can delete them one by one or in batches.

This topic describes how to edit or delete assets from SecMaster.

Prerequisites

You have purchased the SecMaster standard or professional edition.

Limitations and Constraints

Only assets imported outside the cloud can be deleted.

Editing or Deleting an Asset

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
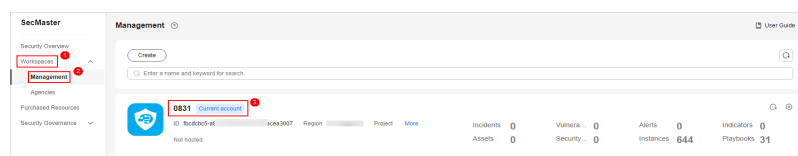
Step 5 In the navigation pane on the left, choose **Resource Manager** > **Resource Manager**.

Figure 8-10 Resource Manager
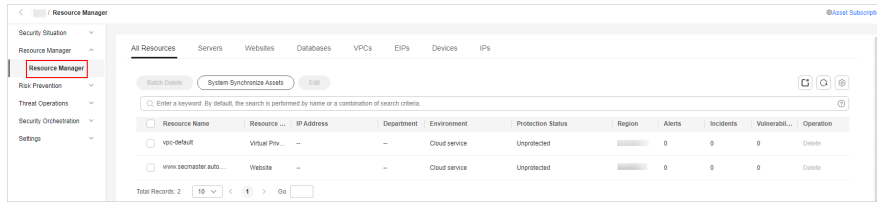
Step 6 Edit or delete the resource.

Table 8-4 Parameters for resource edit or deletion

Operation	Procedure
Batch Edit	1. 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. 2. In the displayed box, you can edit the department, service system, and owner of the resource. 3. Click **OK**.
Batch Delete	1. On the **Resource Manager** page, click the corresponding resource type tab. For example, if you want to delete servers, click the **Servers** tab. 2. On the displayed page, select the resources you want to delete and click **Batch Delete** above the list. The system will delete all selected resources.

----End

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.

SecMaster can check key cloud service configurations for your workloads on the cloud based on preconfigured compliance packs, **Cloud Security Compliance Check 1.0**, **DJCP 2.0 Level 3 Requirements**, **Network Security**, and **Huawei Cloud Security Configuration**. In addition, you can add custom check items and compliance packs to make custom checks to meet your own needs.

Limitations and Constraints

The SecMaster basic and standard editions do not support custom check items or compliance packs.

Baseline Check Methods

- Automated baseline checks

  By default, SecMaster performs a check every three days. From 00:00 to 06:00, SecMaster checks all assets in the current region under your account based on compliance pack **Cloud Security Compliance Check 1.0**. The default check plan can be enabled or disabled only. No changes on its compliance packs or execution time can be made.

- Scheduled custom baseline checks

  You can customize the automatic check period, time, and scope. You can also customize the check items that can be automated in **Cloud Security Compliance Check 1.0**, **Network Security**, and **Huawei Cloud Security Configuration**. For details about how to perform a baseline inspection, see **Performing a Scheduled Baseline Check**.

- Immediate baseline checks

You can start all security standards or a specific check plan to detect violations in real time. You can set auto check items in **Cloud Security Compliance Check 1.0**, **Network Security**, and **Huawei Cloud Security Configuration** packs. For check items that support only manual check, the system generates check items whose check results are **To be checked**. You need to perform a manual check offline and then report the check results to the SecMaster console. For details about immediate baseline checks, see **Starting an Immediate Baseline Check**.

You can start all security standards or a specific check plan to detect violations in real time. You can set the auto check items in the compliance packs. For check items that support only manual check, the system generates check items whose check results are **To be checked**. You need to perform a manual check offline and then report the check results to the SecMaster console. For details about immediate baseline checks, see **Starting an Immediate Baseline Check**.

– You can start all compliance packs in use to detect violations against automatic check items.

– You can start a check plan to detect violations against check items in the compliance pack configured in the check plan.

– You can select one or more check items and start them at once.

● 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.

All check items in **DJCP 2.0 Level 3 Requirements** are manual. Some check items in **Cloud Security Compliance Check 1.0**, **Huawei Cloud Security Configuration**, and **Network Security** are manual.

For details about manual checks, see **Performing a Manual Baseline Check**.

Process

The process of baseline inspection is as follows.

Table 9-1 Process

No.	Operation	Description
1	**Conducting a Scheduled Baseline Inspection**	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 plans: SecMaster performs baseline inspections based on the compliance packs and time you specify in the custom check plans.

No.	Operation	Description
2	**Starting an Immediate Baseline Check**	The baseline inspection supports periodic and immediate checks. ● Periodic check: The system automatically executes the default check plan or the check plans you configure. ● Immediate check: You can add or modify a custom check plan and start the check plan immediately. In this way, you can check whether the servers have certain unsafe configurations in real time.
3	**Viewing Baseline Inspection Results**	You can view the baseline inspection results after each manual check or automated check. You can quickly learn affected assets and details about the baseline inspection items.
4	**Handling Baseline Inspection Results**	You can handle risky items based on the rectification suggestions.

9.1.2 Starting an Immediate Baseline Check

Scenarios

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

● Periodic check: SecMaster periodically executes the default check plan or the check plans you configure.

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

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

● **Immediate Check on All Compliance Packs**: Check the compliance of all automatic check items in in-use compliance packs.

● **Starting a Check Based on a Check Plan**: Check the compliance of the check items in the compliance pack configured in a selected check plan.

● **Immediate Checks on Certain Check Items**: check the selected check items.

Limitations and Constraints

● An immediate check task can be executed only once within 10 minutes.

● A periodic check can be manually started only once within 10 minutes.

Immediate Check on All Compliance Packs

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

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
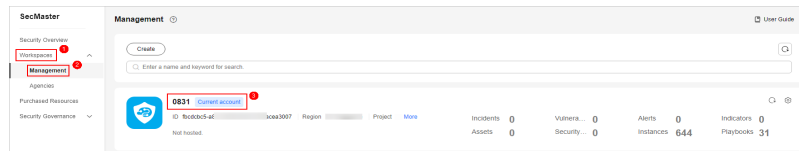
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-2 Accessing the check result page

Step 6 On the **Check Result** tab, click **Check Now**. In the dialog box displayed, click **OK**.

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

----End

Starting a Check Based on a Check Plan

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

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![menu icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
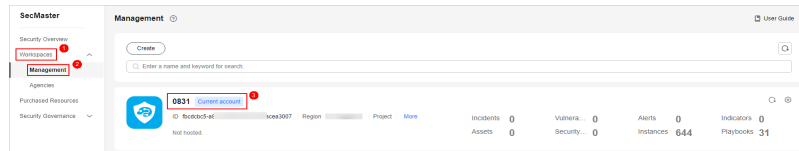
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Plan** tab.

Figure 9-4 Check Plan tab
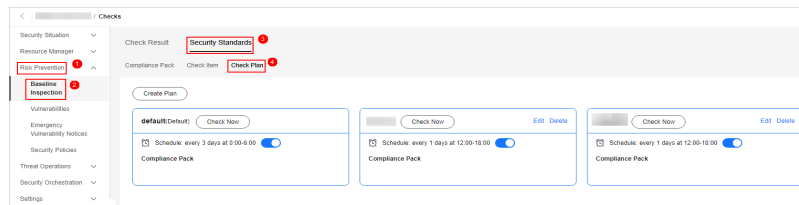
Step 6 In a check plan box, click **Check Now**.

SecMaster immediately executes the selected baseline check plan.

----End

Immediate Checks on Certain Check Items

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

Step 1 Log in to the management console.

Step 2 Click ![location icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![menu icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

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

Figure 9-6 Accessing the check result page
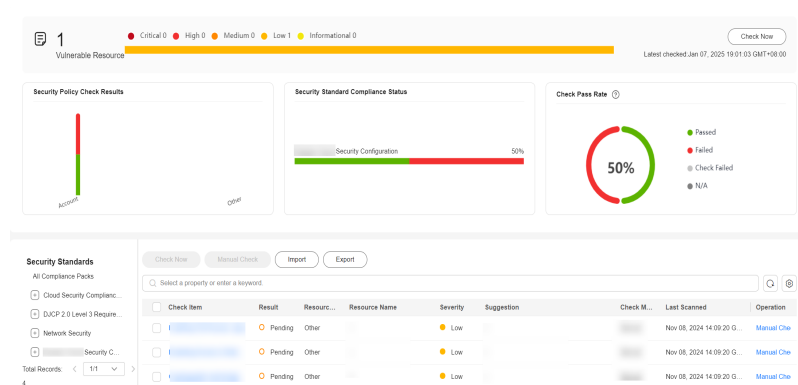
Step 6 Check one or more check items immediately.

- Check on a single check item

    a. In the check item list in the lower part of the **Check Result** tab, locate the target automatic check item and click **Check Now** in the **Operation** column.

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

       Refresh the page and check the details next to **Last checked** and ensure that the latest scan result is displayed.

- Checks on some check items

    a. In the check item list in the lower part of the check result tab, select multiple auto check items and click **Check Now** in the upper left corner above the check item list.

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

       Refresh the page and check the details next to **Last checked** and ensure that the latest scan result is displayed.

----End

9.1.3 Performing a Scheduled Baseline Check

Scenarios

SecMaster can check whether your assets have risks based on baseline check plans. By default, every three days SecMaster automatically performs a baseline check on all assets in the current region under your account from 00:00 to 06:00 in accordance with compliance pack **Cloud Security Compliance Check 1.0**. This function is enabled by default. So there are no manual actions required.

You can customize the automatic inspection period, time, and scope to create custom check plans.

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

Limitations and Constraints

- A compliance pack can be added to only one check plan.
- SecMaster cannot execute check plans that include manual check items. So do not add compliance packs that include manual check items to a check plan. There are manual check items in **DJCP 2.0 Level 3 Requirements**.
- The default check plan can be enabled or disabled only. No changes on its compliance packs or execution time can be made.

Procedure

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
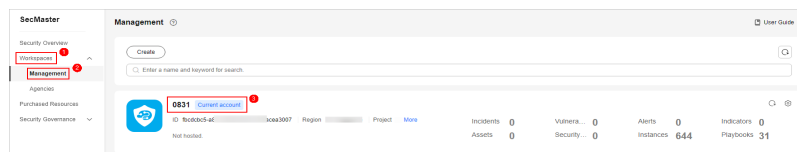
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Plan** tab.

Figure 9-8 Check Plan tab
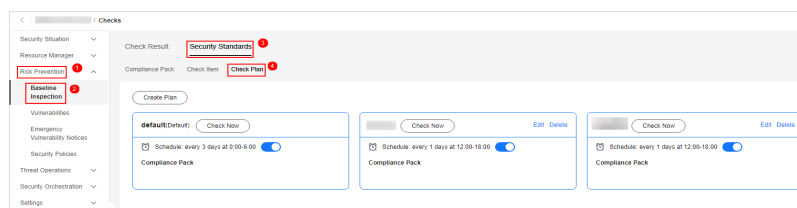
Step 6 On the **Check Plan** tab, click **Create Plan**. The pane for creating a plan is displayed on the right.

Step 7 Configure the check plan.

Table 9-2 Parameters for creating a check plan

Parameter		Description
Basic Information	Name	Custom plan name.

Parameter		Description
	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
Select Compliance Pack		Select the compliance pack you want to use.

Step 8 Click **OK**.

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

----End

Related Operations

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

● Viewing a check plan

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

    b. On the **Check Plan** page, view what check plans you already have.

● Editing a custom check plan

    Only custom check plans can be edited.

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

    b. In the upper right corner of the check plan box, click **Edit**. The pane for editing the check plan is displayed on the right.

    c. Edit settings and click **OK**.

● Deleting a custom check plan

    Only custom check plans can be deleted.

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

    b. In the upper right corner of the check plan box, click **Delete**.

    c. In the displayed dialog box, click **OK**.

● Disabling or enabling a check plan

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

b. Toggle on or off the status button in the box where the target plan is located.

9.1.4 Performing a Manual Baseline Check

Scenarios

There are some manual check items included in baseline inspection. You need to perform these checks manually. 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. The following compliance packs contain manual check items:

- All check items in **DJCP 2.0 Level 3 Requirements**
- **Manual** check items in **Cloud Security Compliance Check 1.0**
- **Manual** check items in **Network Security**
- Manual check items in **Huawei Cloud Security Configuration**

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

Prerequisites

- You have completed the check offline.

Limitations and Constraints

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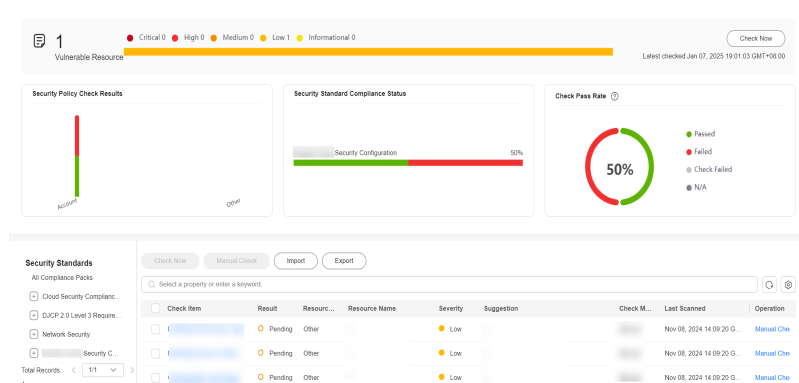
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
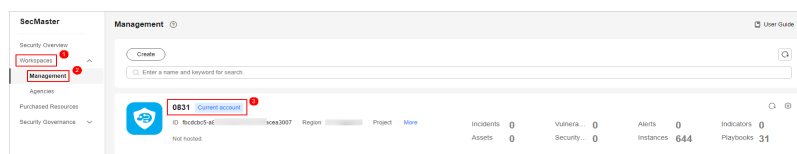
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-10 Accessing the check result page
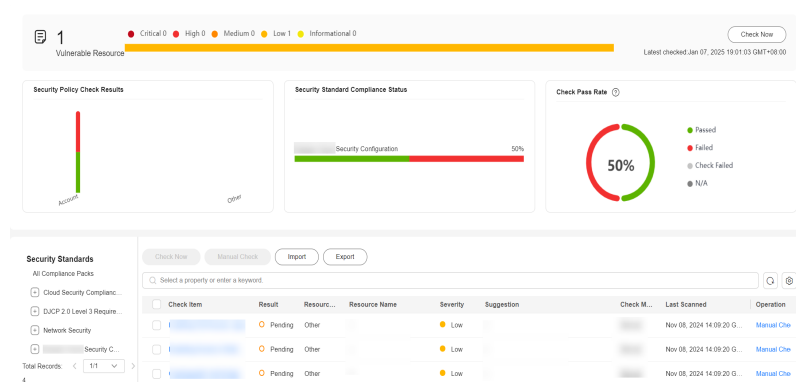
Step 6 In the **Operation** column of the target manual check item, click **Manual Check**.

Figure 9-11 Manual Check
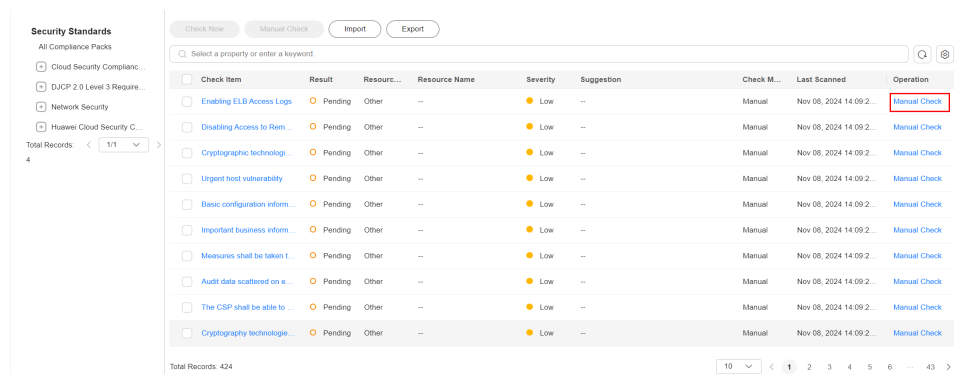

Step 7 In the displayed dialog box, report the result and click **OK**.

☐☐ **NOTE**

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

----End

9.1.5 Viewing Baseline Check Results

Scenarios

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

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

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

Prerequisites

- Cloud service baseline scanning has been performed.

Viewing Baseline Check Results

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
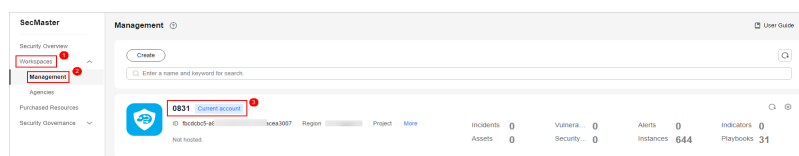
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-12 Workspace management page
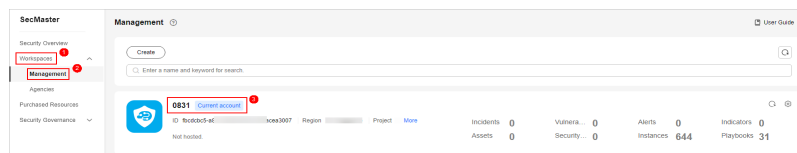
Step 5 (Optional) In the navigation pane on the left, choose **Settings** > **Data Integration**. On the displayed page, locate the row where **SecMaster** is located, enable the log access to compliance baseline logs in the **Logs** column.

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

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

Figure 9-13 Compliance baseline log

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

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

Step 6 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-14 Accessing the check result page
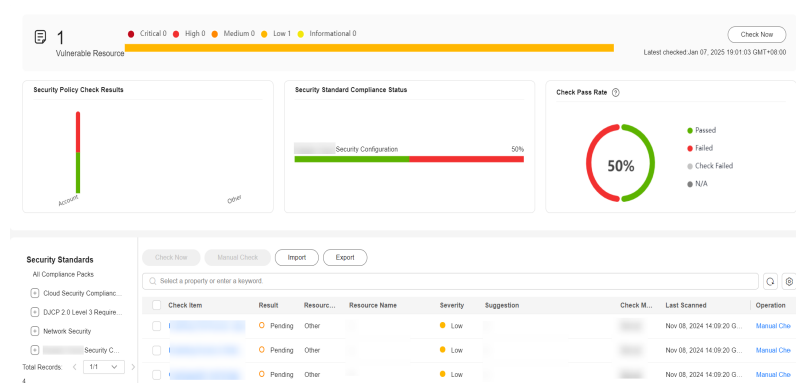
Step 7 On the **Check Result** tab, view the check results of check items. For details about the parameters, see **Table 9-3**.

Figure 9-15 Viewing check results
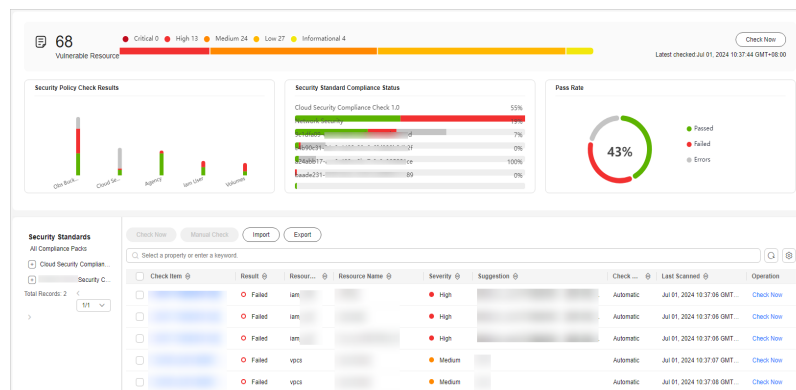
Table 9-3 Check result parameters

Parameter	Description
Risks By Severity	Risks found in the last baseline check are listed by severity as well as the corresponding resource quantity. **Severity**: **Critical**, **High**, **Medium**, **Low**, and **Informational**.
Security Policy Check Results	This graph shows how many failed and passed check items your cloud services have in the last baseline check.
Security Standard Compliance Status	This part shows how well your workloads comply with each security standard. You will see a percentage of passed check items in total check items for each standard.

Parameter	Description
Check Pass Rate	Rate of the passed check items in the latest baseline check. Check pass rate = Passed check items/(Passed check items + failed check items + check item errors) x 100%. Note that check items not performed are not counted.
Security Standards and the check result list	All security standards and check results are displayed. ● To view the check results of a specific compliance pack, click the security standard on the left. The check result details will be displayed on the right. ● To display certain columns only, click the setting button in the upper right corner of the check result list and complete the settings (for example, whether to wrap lines and whether to fix the operation column). ● To view details about a check item, click the name of the check item to go to its details page. On the check item details page, view details about description, check process, check result, and checked resources.

----End

9.1.6 Handling Check Results

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

● **Handling Unsafe Settings**: Rectify the risky check items based on the check result.

● **Check Result Feedback**: For manual check items you performed offline, report the check result to SecMaster. The pass rate is calculated based on results from both manual and automatic checks.

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

● **Importing Check Results**: Export the online check result to a local PC.

● **Exporting Check Results**: Import offline check results to the SecMaster baseline inspection page.

Limitations and Constraints

When you import check results, note the following restrictions:

● Only .xlsx files can be imported.

● Each time only one file can be imported. Maximum file size: 500 KB and 500 records.

● Duplicate data will be removed and will not be imported repeatedly.

Prerequisites

● The cloud service baseline has been scanned.

Handling Unsafe Settings

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

**Step 3** Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
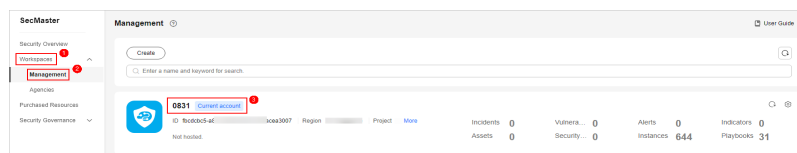
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-17 Accessing the check result page

Step 6 In the check result list in the lower part of the check result page, click the name of the target check item to go to its details page.

Step 7 View the description of the check item and rectify the fault based on the suggestions in the **Recommendation** column

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

----End

Check Result Feedback

For manual check items you performed offline, report check results to SecMaster. The pass rate is calculated based on results from both manual and automatic checks.

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-18 Workspace management page
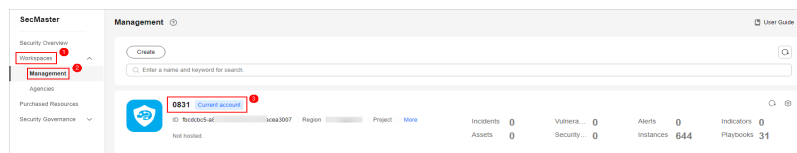
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-19 Accessing the check result page
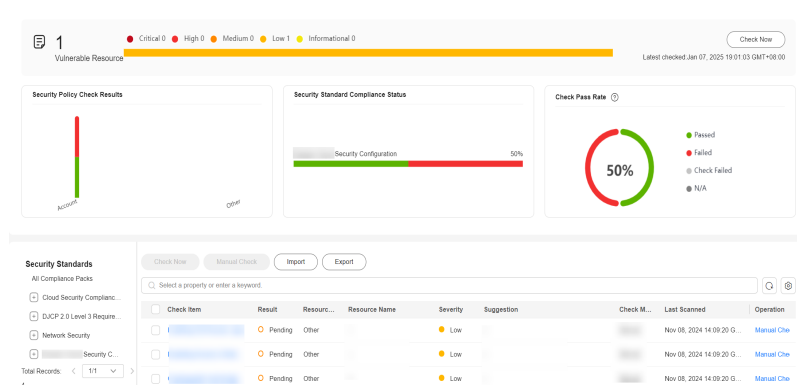
Step 6 In the check result list in the lower part of the **Check Result** tab, click **Manual Check** in the **Operation** column of the target check item.

Step 7 In the displayed dialog box, select a result and click **OK**.

📖 **NOTE**

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

----End

Ignoring a Check Item

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

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

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

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

**Figure 9-20** Workspace management page
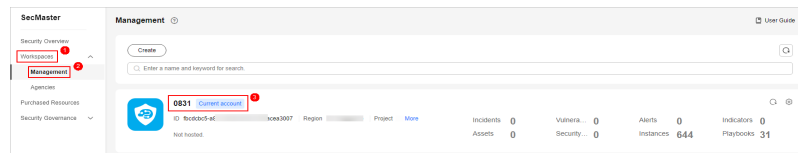
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.

Figure 9-21 Accessing the Compliance Pack tab
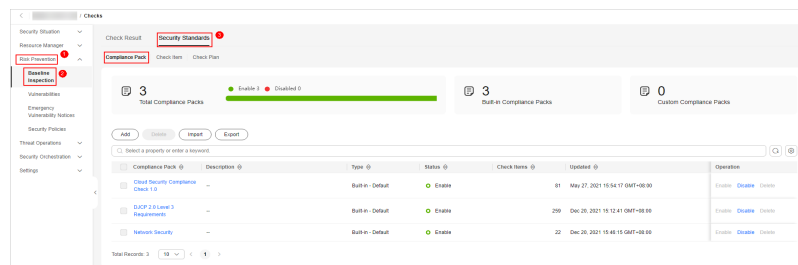
Step 6 Click the name of the target compliance pack to go to its details page.

Step 7 Search for the target check item in the compliance pack list and click **Ignore** in the **Operation** column.

Step 8 In the displayed dialog box, click **OK**.

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

----End

Importing Check Results

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

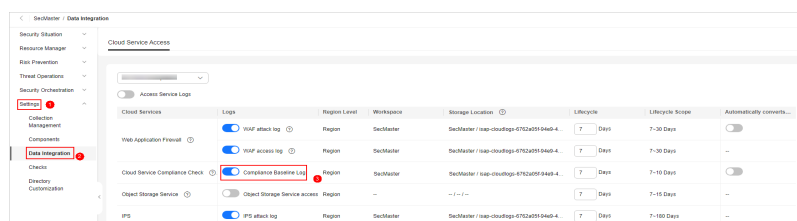**Figure 9-22** Workspace management page
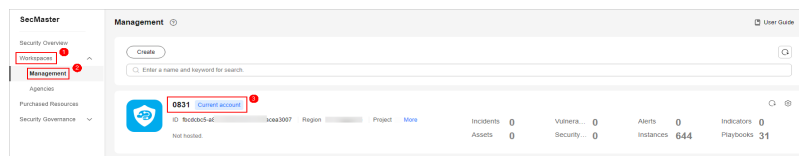
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-23 Accessing the check result page

Step 6 In the upper left corner above the check result list, click **Import**.

Step 7 In the dialog box displayed, click **Download Template** and complete the template.

Step 8 In the displayed dialog box, click **Add File** and upload the completed template file.

☐ NOTE

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

Step 9 Click **Import**.

----End

Exporting Check Results

Step 1 Log in to the management console.

Step 2   Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3   Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4   In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

**Figure 9-24** Workspace management page
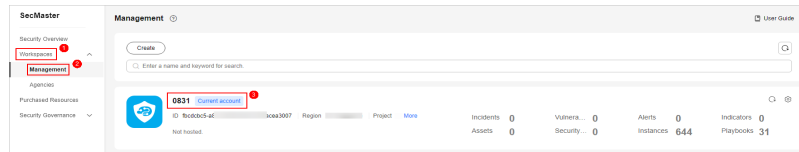
Step 5   In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-25 Accessing the check result page
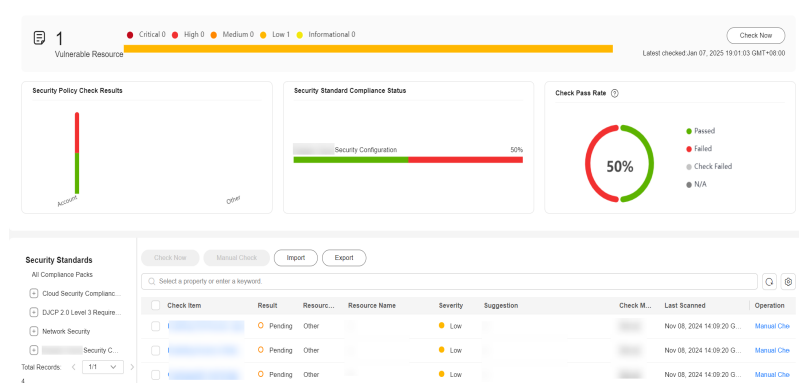
Step 6   Select target check items from the result list and click **Export** in the upper left corner above the check result list.

Step 7   In the displayed dialog box, select the format and data columns you want.

Step 8   Click **OK**.

----End

9.1.7 Managing Compliance Packs

This topic describes how to manage compliance packs. You can **view a compliance pack**, **add a custom compliance pack**, **import a compliance pack**, and **export a compliance pack**.

Limitations and Constraints

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

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

Viewing Compliance Packs

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-26 Workspace management page
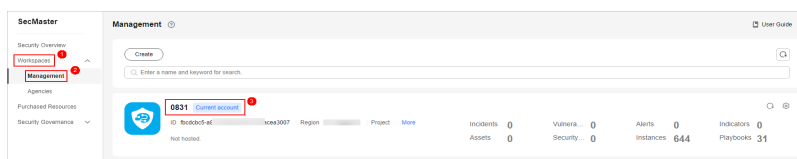
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.

Figure 9-27 Accessing the Compliance Pack tab
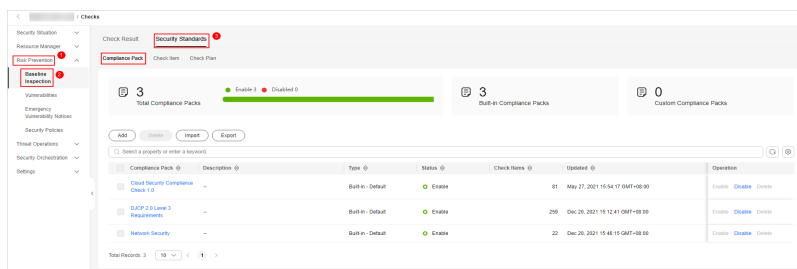
Step 6 View details about compliance packs. For details about the parameters, see **Table 9-4**.

Figure 9-28 Viewing compliance packs

Table 9-4 Parameters for compliance packs

Parameter	Description
Total Compliance Packs	Total number of existing compliance packs are organized, as well as the number of compliance packs by their statuses. The compliance pack status can be **Enabled** or **Disabled**.
Built-in Compliance Packs	The number of compliance packs preconfigured in SecMaster.
Custom Compliance Packs	The number of compliance packs you create.
Compliance packs and their details	All compliance packs and their basic information. ● In the compliance pack list, you can view the type, status, and number of check items of a compliance pack. You can also enable, disable, and delete a compliance pack. ● To display certain columns only, click the setting button in the upper right corner of the compliance pack list and complete the settings (for example, whether to wrap lines and whether to fix the operation column). ● To view details about a compliance pack, click its name to go to its details page. On the compliance pack details page, you can view its version, description, and check items.

----End

Creating a Custom Compliance Pack

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
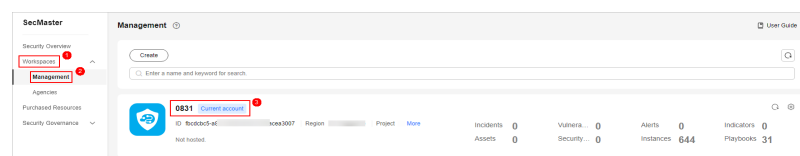
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.

Figure 9-30 Accessing the Compliance Pack tab
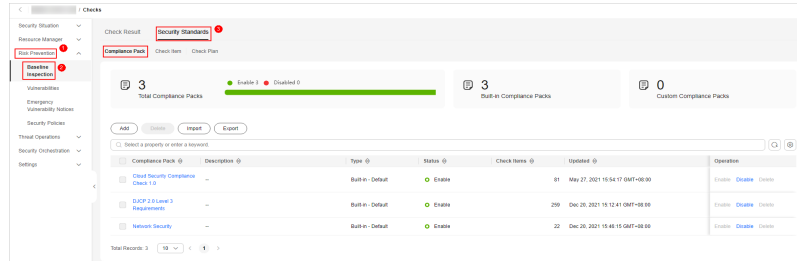
Step 6 In the upper left corner above the compliance list, click **Add**

Step 7 On the displayed page, configure basic information about the compliance pack.

Table 9-5 Basic information

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

Step 8 Click **Next** to go to the configuration page.

Step 9 On the displayed page, complete other parameters of the compliance pack.

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

Figure 9-31 Compliance pack configuration
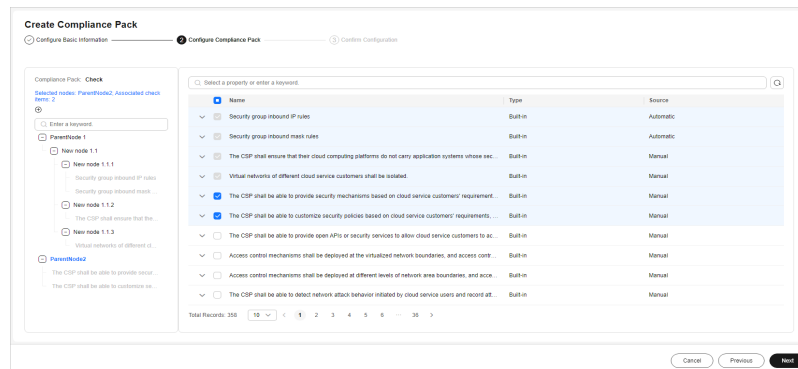
Step 10　Click **Next** to enter the confirmation page.

Step 11　Confirm the settings and click **OK**.

After the compliance pack is added, you can enable, disable, edit, and delete it.
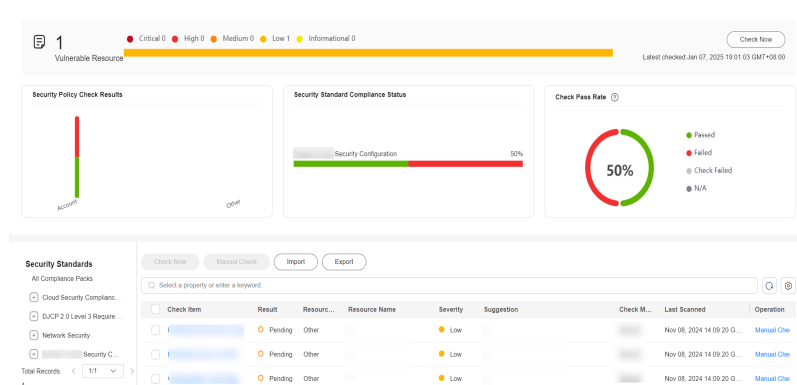
----End

## Importing a Compliance Pack

Step 1　Log in to the management console.

Step 2　Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3　Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4　In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-32 Workspace management page
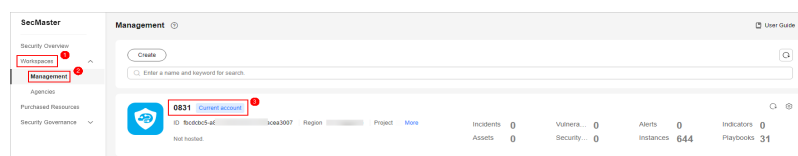
Step 5　In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.

Figure 9-33 Accessing the Compliance Pack tab
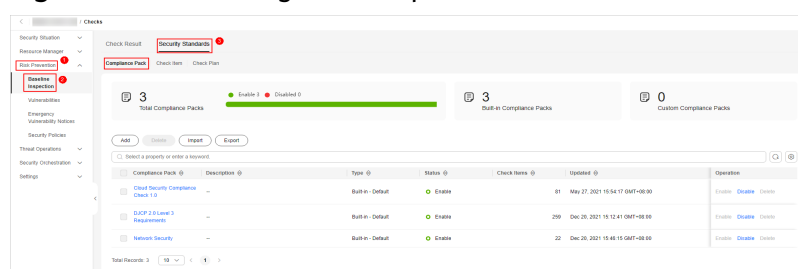
Step 6 In the upper left corner above the compliance pack list, click **Import**.

Step 7 In the dialog box displayed, click **Download Template** and complete the template.

Step 8 In the displayed dialog box, click **Add File** and upload the completed template file.

> ☐ NOTE
>
> ● Only .xlsx files can be imported.
> ● Only one file can be imported at a time. Maximum file size: 100 records.

Step 9 Click **OK**.

**----End**

Exporting a Compliance Pack

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-34 Workspace management page
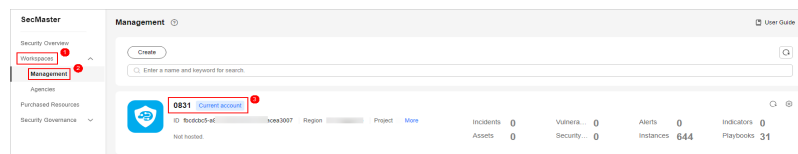
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.

Figure 9-35 Accessing the Compliance Pack tab
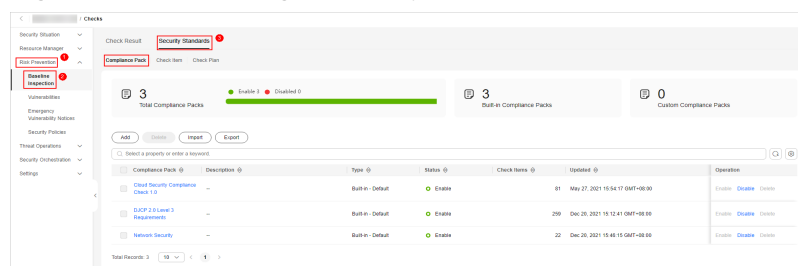
Step 6 Select the target compliance pack and click **Export** in the upper left corner of the compliance pack list.

Step 7 In the displayed dialog box, select the format and data columns you want.

Step 8 Click **Export**.

----End

9.1.8 Managing Check Items

This topic describes how to manage check items, including **Viewing Check Items**, **Creating a Custom Check Item**, **Importing Check Items**, and **Exporting Check Items**.

Limitations and Constraints

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

- When you import check items, note the following restrictions:
  - Only .xlsx files can be imported.
  - Only one file can be imported at a time. Maximum file size: 100 records.
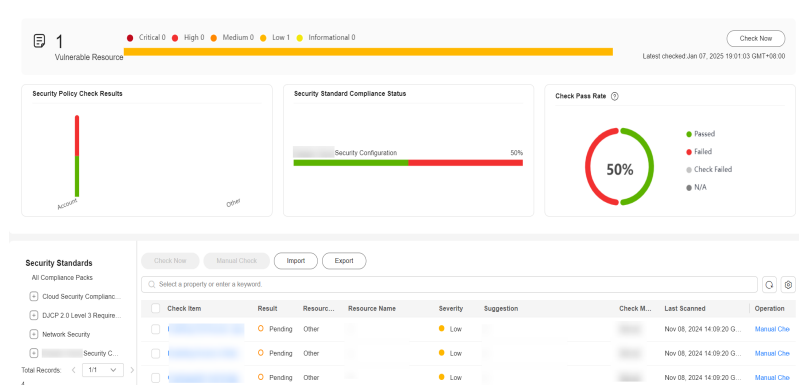
Viewing Check Items

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-36 Workspace management page
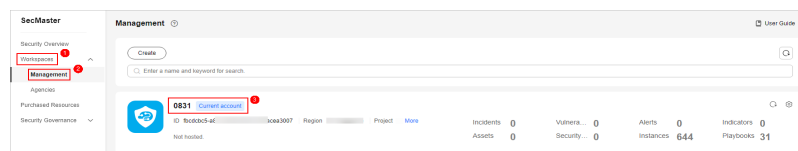
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.

Figure 9-37 Accessing the Check Item tab

Step 6 On the **Check Item** tab, view the information about existing check items. For details about the parameters, see **Table 9-6**.

Figure 9-38 Check items

Table 9-6 Parameters for check items

| Parameter	Description
Check Items	Total number of check items in the current workspace.
Built-in Check Items	The number of check items preconfigured in SecMaster.
Custom Check Items	The number of check items you create.
Check items and details	All check items and their basic information. ● In the check item list, you can view the description, type, and number of compliance packs used for a check item. You can also edit or delete custom check items. ● To display certain columns only, click the setting button in the upper right corner of the check item list and complete the settings (for example, whether to wrap lines and whether to fix the operation column). ● To view details about a check item, click its name. The details page is displayed on the right. On the check item details page, you can view the description and compliance pack used for the check item.

----End

Creating a Custom Check Item

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ![menu icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
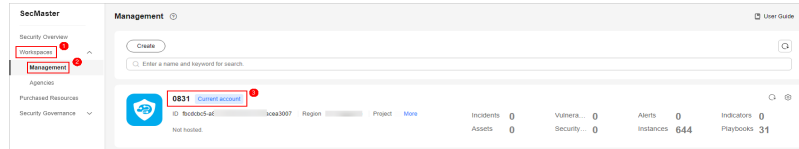
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.

Figure 9-40 Accessing the Check Item tab
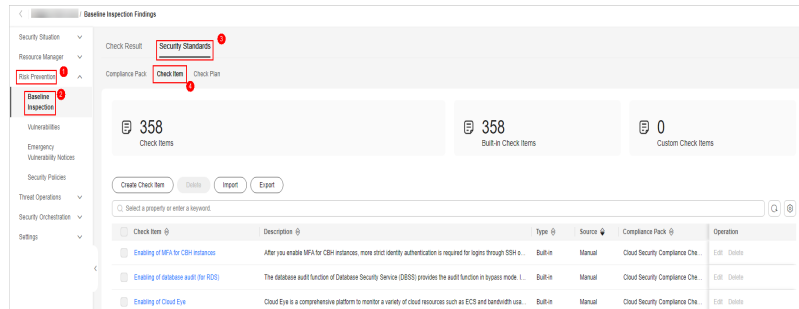
Step 6 Click **Create Check Item** in the upper left corner of the check item list.

Step 7 On the **Create Check Item** page, set check item parameters.

Table 9-7 Parameters for creating check items

Parameter	Description
Check Item	Name you specify for the check item.
Description	Description you provide for the check item.
Severity	Select the severity of the check item.
Action	Select an action for the check item. ● **Executed by workflows**: The check item is automatically executed through a workflow you specify, and the check result is reported by the workflow as well. ● **Executed manually**: You will manually complete the check item offline.

Parameter	Description
Select Workflow	If **Action** for a check item is set to **Executed by workflows**, you need to select a workflow for the check item. If no appropriate workflows are available, click **Create Workflow** and create one on the workflow page.
Manual Check Items	If **Action** for a check item is set to **Executed manually**, SecMaster sets the check result options by default.
Cloud Service	Enter the information about the cloud service associated with the check item.

Step 8 Click **OK**.

📖 **NOTE**

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

You can edit or delete custom check items you add as required.

**----End**

Importing Check Items

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

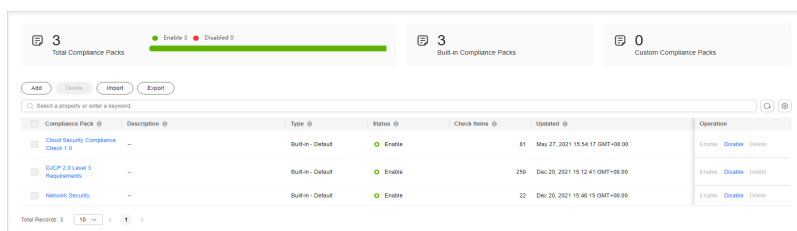**Figure 9-41** Workspace management page
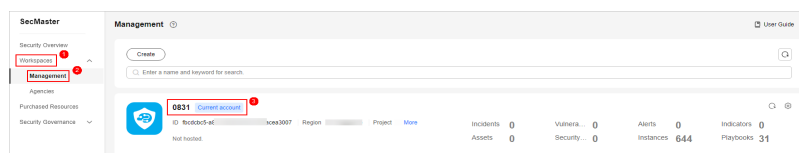
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.

Figure 9-42 Accessing the Check Item tab
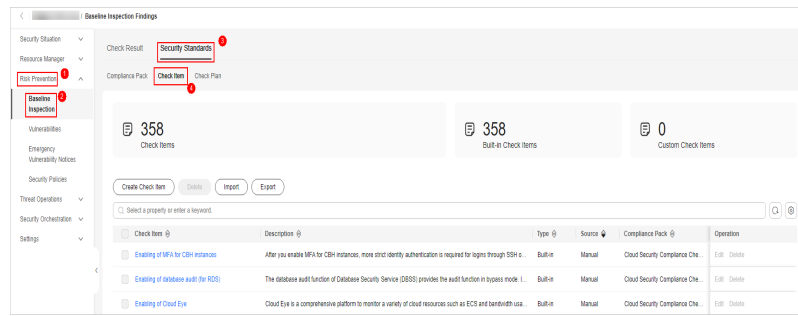
Step 6 In the upper left corner above the check item list, click **Import**.

Step 7 In the dialog box displayed, click **Download Template** and complete the template.

Step 8 In the displayed dialog box, click **Add File** and upload the completed template file.

📖 NOTE

● Only .xlsx files can be imported.

● Only one file can be imported at a time. Maximum file size: 100 records.

Step 9 Click **Import**.

----End

Exporting Check Items

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.

Figure 9-44 Accessing the Check Item tab
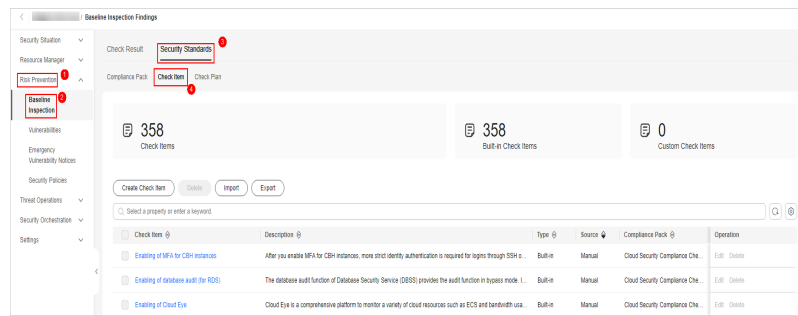
Step 6 Select check items you want to export from the check item list and click **Export** in the upper left corner above the list.

Step 7 In the displayed dialog box, select the format and data columns you want.

Step 8 Click **Export**.

----End

9.2 Vulnerability Management

9.2.1 Overview

Background

SecMaster can integrate the vulnerability scan results from Host Security Service (HSS) and display them centrally, so that 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**.

- **Viewing Vulnerability Details**: describes how to view vulnerability details.

- **Fixing Vulnerabilities**: If HSS detects a vulnerability on a server, you need to handle the vulnerability in a timely manner based on its severity and your business conditions to prevent further vulnerability exploits. If a vulnerability may harm your services, fix it as soon as possible. For Linux and Windows vulnerabilities, you can go to the HSS console and fix them in one-click. Web-CMS, emergency, and application vulnerabilities cannot be automatically fixed. You can handle them by referring to suggestions provided on the vulnerability details page.

- **Ignoring and Unignoring a Vulnerability**: Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but 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.

- **Importing and Exporting Vulnerabilities**: describes how to import or export vulnerabilities.

ECS Vulnerabilities

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

The following host vulnerabilities can be detected:

Table 9-8 ECS vulnerability check items

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

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

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

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

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

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

9.2.2 Viewing Vulnerability Details

Scenario

This topic describes how to view vulnerabilities details.

Prerequisites

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

- You have installed HSS agent. For details, see the **Installing an Agent**.

- HSS logs have been connected to SecMaster and the function of automatically converting logs into alerts has been enabled. For details, see **Data Integration**. If access to HSS vulnerability scan results has been enabled during data integration but the automatic alert conversion is disabled, the vulnerability scan results will not be displayed on the **Vulnerabilities** page in SecMaster.

Viewing Vulnerability Details

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
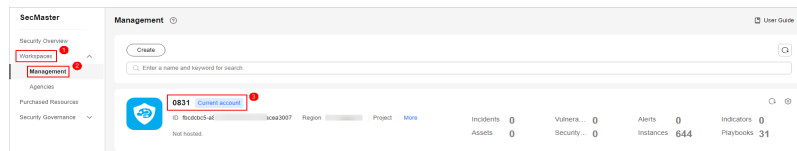
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Vulnerabilities**.

Figure 9-46 Accessing the vulnerability management page
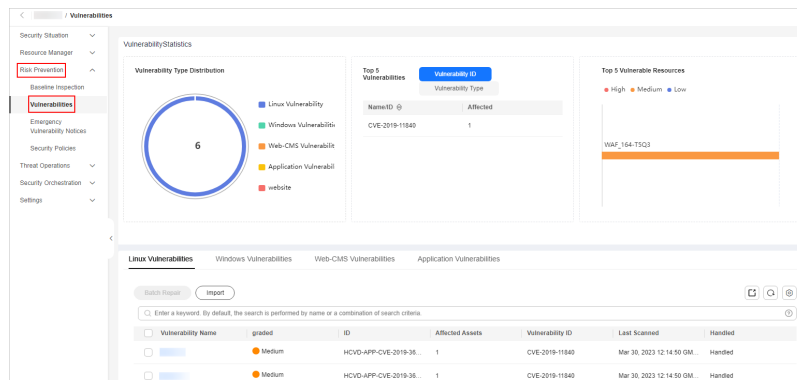
Step 6 View vulnerability information on the **Vulnerabilities** page.

Table 9-9 Viewing vulnerability information

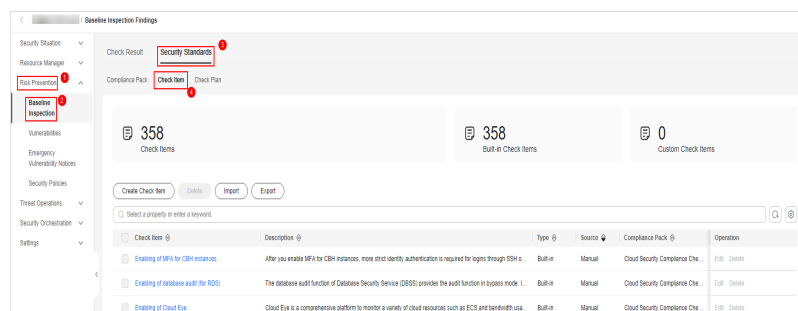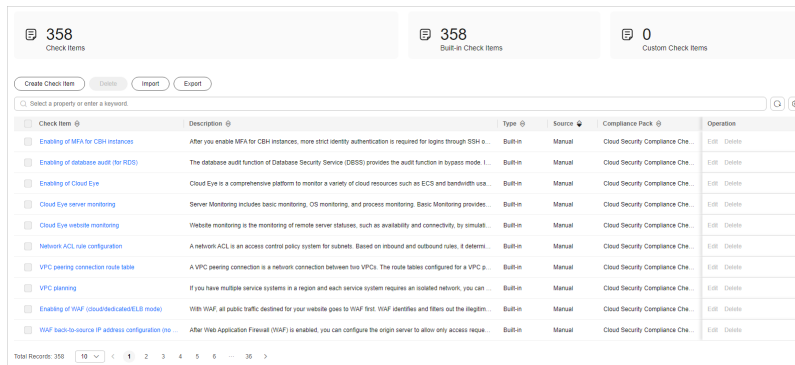| Parameter	Description
Vulnerability Type Distribution	This graph displays the total number of vulnerabilities and the distribution of vulnerabilities by type.
Top 5 Vulnerabilities	• The **Top 5 Vulnerabilities** area lists the five vulnerabilities with the most affected assets. The more affected assets, 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.
Top 5 Vulnerable Resources	This graph displays the five resources with the most vulnerabilities.
Vulnerability List	• In the vulnerability list, click the tab of a vulnerability type (for example, **Linux Vulnerabilities**) to go to the corresponding page. For details about the vulnerability parameters, see **Table 9-10**. • 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 9-10 Vulnerability parameters

Parameter	Description
Vulnerability Name	Name of the scanned vulnerability. Click a vulnerability name to view vulnerability description and vulnerability library information.
Severity	Severity level of the vulnerability.
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

Parameter	Description
Handled	This column specifies whether the vulnerability has been handled.

NOTE

> SecMaster aggregates the vulnerability scan results from HSS and displays vulnerabilities on the **Vulnerabilities** page in SecMaster. HSS supports automatic, scheduled, and manual scans.
>
> - Automatic scan
>
>   By default, the system automatically scans for Linux, Windows, and Web-CMS vulnerabilities every day and scans for application vulnerabilities every Monday. The time of an automatic application vulnerability scan changes with the middleware asset scan time. If a manual or scheduled vulnerability scan has been performed on a day, HSS will not automatically scan for vulnerabilities on that day.
>
> - Scheduled scan
>
>   By default, a full server vulnerability scan is performed once a week. To protect workloads, you are advised to set a proper scan period and scan server scope to periodically scan server vulnerabilities.
>
> - Manual scan
>
>   If you want to view the vulnerability fixing status or vulnerabilities of a server in real time, manual scans are recommended.
>
> For newly purchased ECSs, if scheduled vulnerability scan and manual scan are not configured in HSS, HSS automatically scans for Linux, Windows, and Web-CMS vulnerabilities in the early morning every day. So, you can view vulnerabilities for newly purchased ECSs on the **Vulnerabilities** page in SecMaster the next day. Before collecting HSS logs, make sure you have enabled HSS protection for ECSs during the purchase, installed HSS agent, and enabled access to HSS logs and the function of converting logs to alerts in SecMaster.
>
> For more details, see **Vulnerability Scan**.

----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.

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

Constraints and Limitations

- For details about vulnerability management in Host Security Service (HSS), see **Types of Vulnerabilities That Can Be Scanned and Fixed**.

- CentOS 7, CentOS 8, Debian 9 and 10, Windows 2012 R2, and Ubuntu 14.04 and earlier have reached EOL and cannot be fixed because no official patches are available. You are advised to change to the OSs in active support.

- Ubuntu 16.04 to Ubuntu 22.04 do not support free patch updates. You need to subscribe to Ubuntu Pro to install upgrade packages. If Ubuntu Pro is not configured, vulnerabilities will fail to be fixed.

- Fixing kernel vulnerabilities may cause servers to be unavailable. Therefore, HSS does not automatically fix the server kernel vulnerabilities of CCE, MRS, or BMS. When batch fixing vulnerabilities, HSS filters out these types of vulnerabilities.

- To handle vulnerabilities on a server, ensure the server is in the **Running** state, its agent status is **Online**, and its protection status is **Protected**.

Precautions

- Vulnerability fixing operations cannot be rolled back. If a vulnerability fails to be fixed, services will probably be interrupted, and incompatibility issues will probably occur in middleware or upper layer applications. To prevent unexpected consequences, you are advised to use CBR to back up ECSs. 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.

  – Linux OS: If your servers cannot access the Internet, or the external image sources cannot provide stable services, you can use the image source provided by Huawei Cloud to fix vulnerabilities. Before fixing vulnerabilities online, configure the Huawei Cloud image sources that match your server OSs. For details, see **Image Source Management**.

  – Windows OS: If your servers cannot access the Internet, ensure you have set up a patch server.

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 management console and select a region or project.

Step 3 Click ▤ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
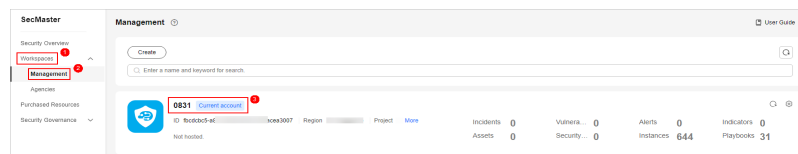
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-47 Workspace management page
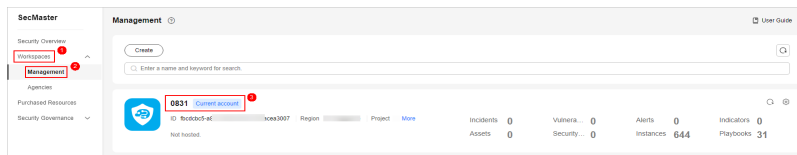
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Vulnerabilities**.

Figure 9-48 Accessing the vulnerability management page
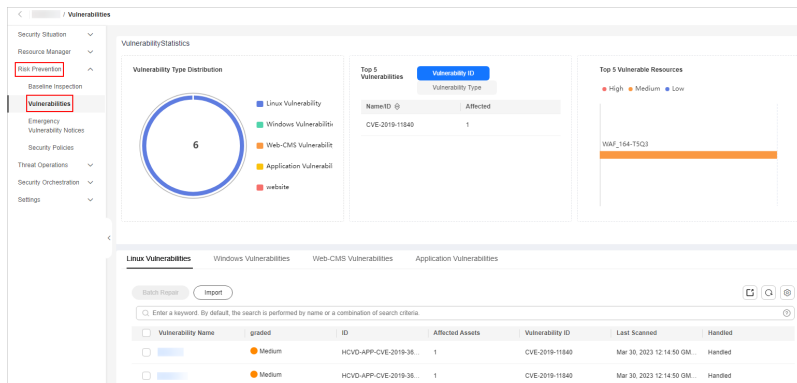
Step 6 On the displayed page, click **Linux Vulnerabilities** or **Windows Vulnerabilities**.

Step 7 In the vulnerability list, click the name of the target vulnerability. The vulnerability details page is displayed.

Step 8 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 9 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 9-11**.

📖 **NOTE**

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

Table 9-11 Vulnerability fix commands

OS	Fix Command
CentOS/Fedora/EulerOS/Red Hat/Oracle	**yum update** *Software name*
Debian/Ubuntu	**apt-get update && apt-get install** *Software name --only-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**.

 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.

Table 9-12 Verification

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: **emerge --search** *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.

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 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.

Ignoring and Unignoring a Vulnerability

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
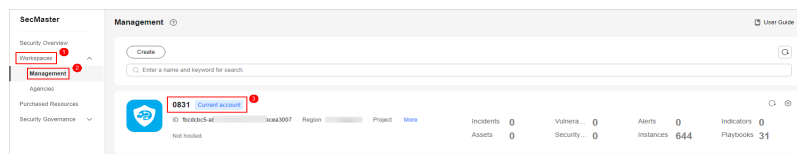
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Vulnerabilities**.

Figure 9-50 Accessing the vulnerability management page
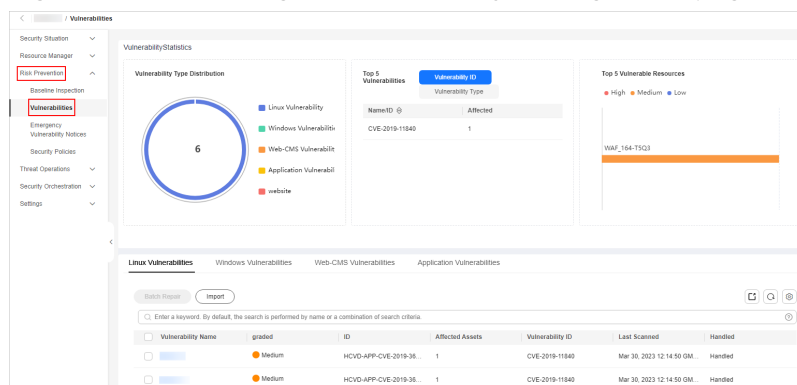
Step 6 On the **Vulnerabilities** page, click any vulnerability type tab. In the vulnerability list, click the name of the target vulnerability. The vulnerability details page is displayed on the right.

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

Step 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

9.2.5 Importing and Exporting Vulnerabilities

Scenario

This section describes how to import and export vulnerabilities.

Constraints

- Only files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.
- 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 management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

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

Figure 9-52 Accessing the vulnerability management page
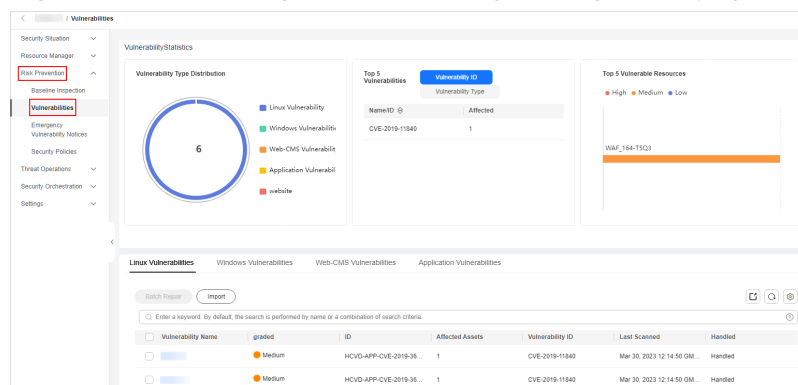
Step 6 On the displayed page, select a tab to go to the corresponding vulnerability management page.

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

Step 7 Click **Import** above the vulnerability list. The **Import** dialog box is displayed.

☐ NOTE

Only files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.

Step 8 In the **Import** dialog box, click **Download Template** to download a template, and fill in the downloaded template according to the requirements.

Step 9 After the vulnerability file is ready, click **Select File** in the **Import** dialog box, and select the Excel file you want to import.

Step 10 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-53 Workspace management page
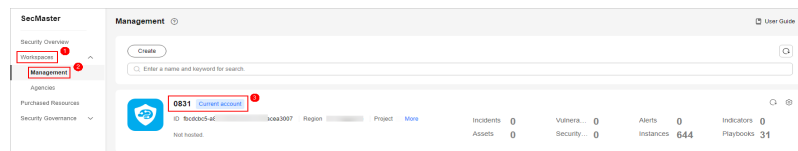
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Vulnerabilities**.

Figure 9-54 Accessing the vulnerability management page
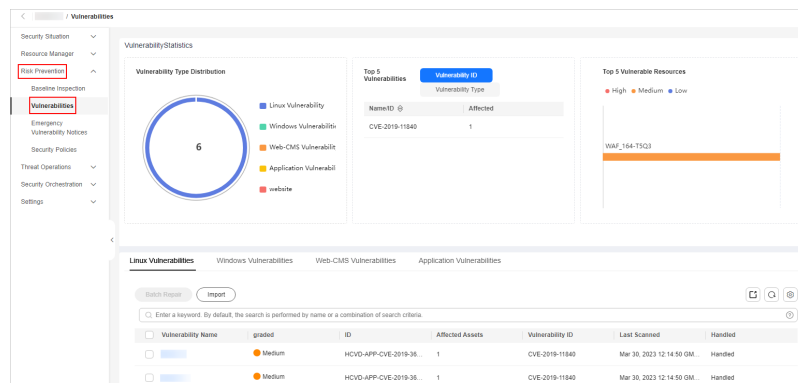
Step 6 On the **Vulnerabilities** page, click the target vulnerability tab.

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

Step 7 Click ⬈ in the upper right corner above the vulnerability list. The **Export** dialog box is displayed.

📖 **NOTE**

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

Step 8 In the **Export** dialog box, set vulnerability parameters.

Table 9-13 Exporting vulnerabilities

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

Step 9 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

9.3 Viewing and 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-55 Workspace management page
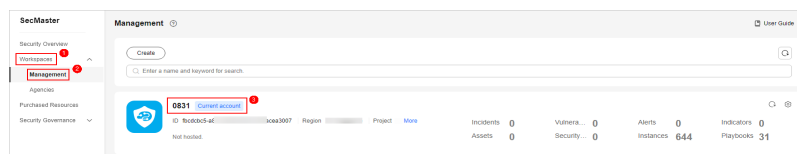
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Emergency Vulnerability Notices**.

Figure 9-56 Accessing the emergency vulnerability notices page
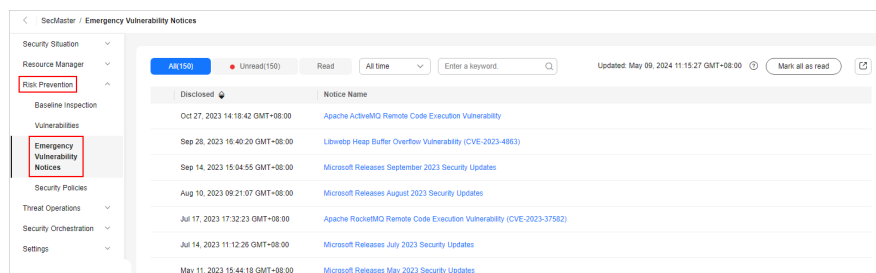
Step 6 View the update time of emergency vulnerability notices.

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

Step 7 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 8 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 9 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. You can view all policies centrally, manage policies for seven defense lines manually, and query manual and automatic block records quickly.

- **Viewing and Configuring Defense Policies**: describes how to view and configure defense policies. There are seven defense lines: physical, identity, server, maintenance, data, application, and network defense lines.

- **Adding an Emergency Policy**: An emergency policy is used to quickly prevent attacks. You can select a block type based on the alert source to block attackers.

- **Managing Emergency Policies**: describes **Viewing Emergency Policies**, **Editing an Emergency Policy**, and **Deleting an Emergency Policy**.

- **Batch Blocking and Canceling Batch Blocking of an IP Address or IP Address Range**: describes how to block access from blacklisted IP addresses, IAM users, or IP address ranges. You can add an IP address, IAM user, or IP address range as blocked object for an emergency policy in several operation connections. If there is no need to block an IP address, IAM user, or IP address range for operation connections, you can cancel the blocking from all operation connections.

Limitations and Constraints

- Currently, the emergency policies include only the blacklist policies of CFW, WAF, VPC security groups and 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. Limits on blocked objects at a time are as follows:

  - When a policy needs to be delivered to CFW, each time a maximum of 50 IP addresses can be added as blocked objects for each account.

- – When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account.

- – When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account.

- – When a policy needs to be delivered to IAM, each time a maximum of 50 IAM users can be added as blocked objects for each account.

- If an IP address or IP address range or an IAM user is added to the blacklist, CFW, WAF, VPC, and IAM will block requests from that IP address or user without checking whether the requests are malicious.

9.4.2 Viewing and Configuring Defense Policies

Scenario

This section describes how to view and configure defense policies.

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

Viewing Defense Policies

Step 1 Log in to the management console.

Step 2 Click ⬙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-57 Workspace management page
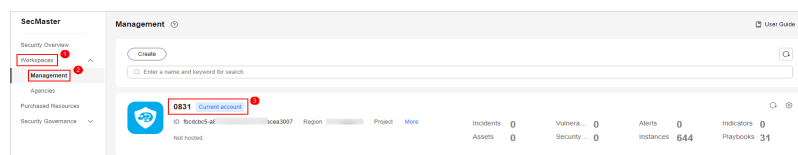
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Policy Management**.

Figure 9-58 Defense Layer Policies
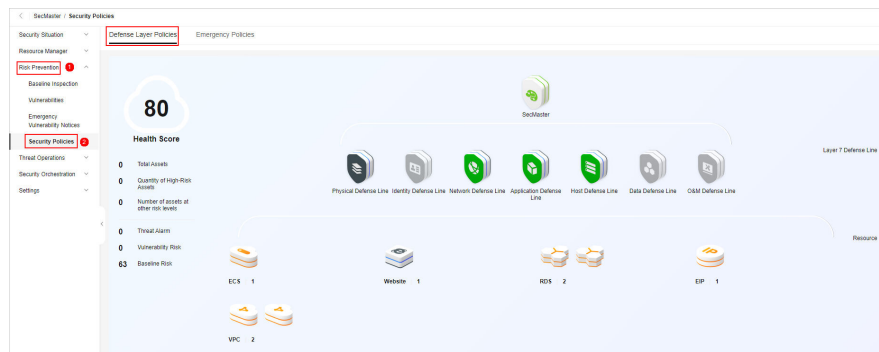
Step 6 View defense policy statistics.

- **Health Score**: indicates the current health status of resources.

  The score ranges from 0 to 100. A larger score indicates a lower risk and higher asset security. For details about the security scores, see **Security Overview and Situation Overview**.

- **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

Configuring Defense Policies

Step 1 Log in to the management console.

Step 2 Click [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-59 Workspace management page
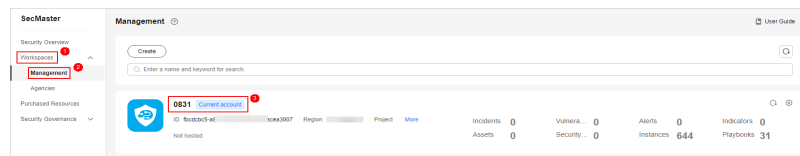
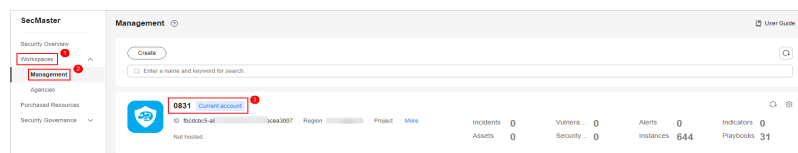**Step 5** In the navigation pane on the left, choose **Risk Prevention** > **Policy Management**.

Figure 9-60 Defense Layer Policies
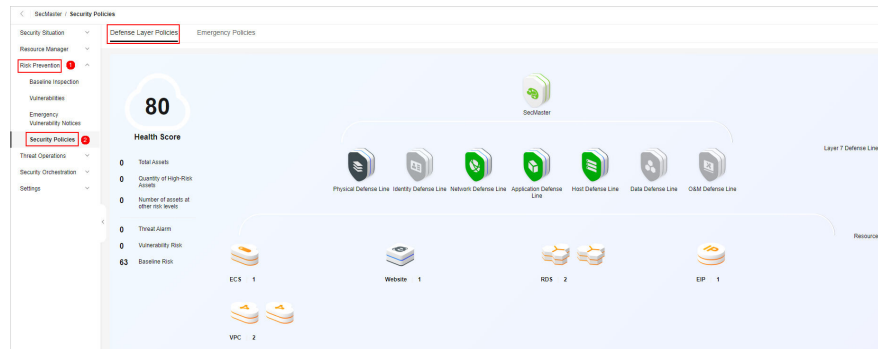
Step 6 Click the name of the defense line the security service belongs to. The cloud service information corresponding to the defense line slides out from the right.

Step 7 On the 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 8 On the policy configuration page, configure policies of the corresponding cloud service.

- Anti-DDoS policy configuration:
  - **Configuring a Protection Policy**
  - **Configuring a Protection 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

9.4.3 Adding an Emergency Policy

Scenario

An emergency policy is used to quickly block attacks. You can select a block type based on the alert source to block attackers. **Table 9-14** lists recommended settings. You can also block a single attack source based on the comprehensive investigation of multiple alerts.

Table 9-14 Recommended blocking policies

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.

This topic describes how to add an emergency policy.

Limitations and Constraints

- A maximum of 300 emergency policies that support block aging can be added for a single workspace you have. A maximum of 1,300 emergency policies can be added for a single workspace you have. Limits on blocked objects at a time are as follows:
  - When a policy needs to be delivered to CFW, each time a maximum of 50 IP addresses can be added as blocked objects for each account.
  - When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account.
  - When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account.
  - When a policy needs to be delivered to IAM, each time a maximum of 50 IAM users can be added as blocked objects for each account.
- If an IP address or IP address range or an IAM user is added to the blacklist, CFW, WAF, VPC, and IAM will block requests from that IP address or user 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.

Adding an Emergency Policy

Step 1 (Optional) Create a SecMaster agency.

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

1. Log in to the management console.

2. Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

3. Add a custom policy.

   a. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.

   b. 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"
            ]
        }
    ]
}
```

   c. Click **OK**.

4. Create an agency.

   a. 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.

   b. On the **Permissions** tab page, click **Authorize**.

   c. On the **Select Policy/Role** page, search for and select the policy added in **Step 1.3** and click **Next**.

   d. Set the authorization scope. Select **All resources** for **Scope**. After the setting is complete, click **OK**.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-61 Workspace management page
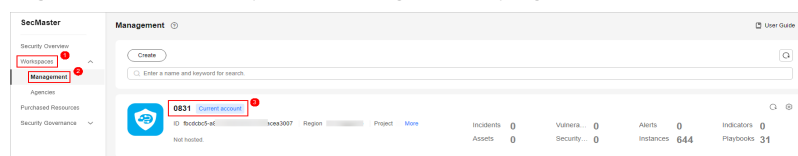
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Security Policies**. Then, click the **Emergency Policies** tab to go to the emergency policy page.

Figure 9-62 Emergency Policies
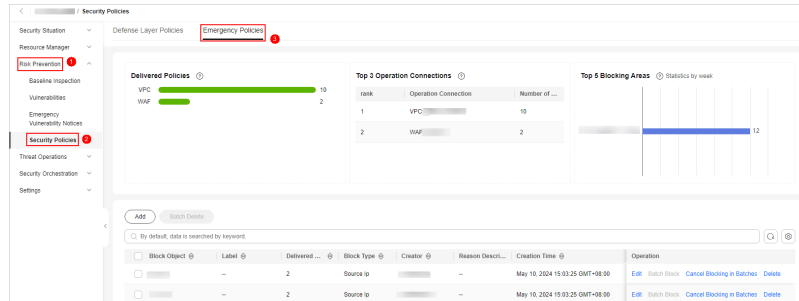
Step 6 On the **Emergency Policies** page, click **Add**. The page for adding policies slides out from the right of the page.

Step 7 On the **Add** page, configure policy information.

Table 9-15 Emergency policy parameters

Parameter	Description
Blocked Object Type	Type of the object you want to block. 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 (,). - If you select **IAM** for **Blocked Object Type**, enter IAM user names. - There are some restrictions on delivery of blocked objects: - When a policy needs to be delivered to CFW, each time a maximum of 50 IP addresses can be added as blocked objects for each account. - When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account. - When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account. - When a policy needs to be delivered to IAM, each time a maximum of 50 IAM users can be added as blocked objects for each account.
Label	Label of a custom emergency policy.

Parameter	Description
Operation Connection	Asset connections that are used to operate blocking workflows of security services in the seven layers of defense. Select the operation connection for the policy.
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/range or the IAM user will not be blocked. ● If you select **No**, the policy is always valid and blocks the specified IP address/range or the IAM user.
Policy Description	Description of the custom policy.

Step 8 Click **OK**. In the dialog box displayed, confirm the information and click **OK**.

----End

9.4.4 Managing Emergency Policies

Scenario

This topic describes how to manage emergency policies, including **Viewing Emergency Policies**, **Editing an Emergency Policy**, and **Deleting an Emergency Policy**.

Viewing Emergency Policies

Step 1 Log in to the management console.

Step 2 Click 🔲 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-63 Workspace management page
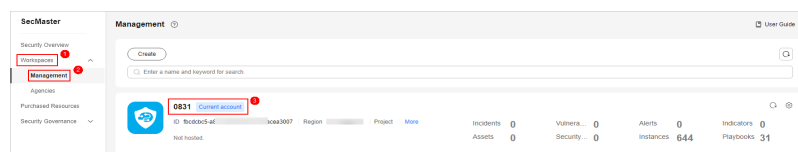
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Security Policies**. Then, click the **Emergency Policies** tab to go to the emergency policy page.

Figure 9-64 Emergency Policies
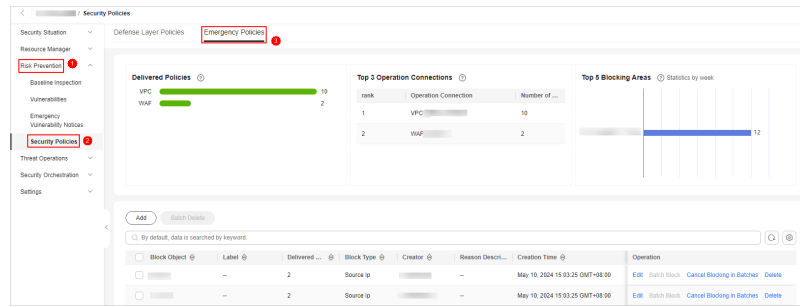
Step 6 On the **Emergency Policies** page, view emergency policy details.

Table 9-16 Parameters of emergency policies

Parameter	Description
Delivered Policies	Shows how many policies that have been applied over the last week.
Top 3 Operation Connections	The 3 operation connections that have blocked the most IP addresses over the last week.
Top 5 Blocking Areas	The 5 regions blocked the most times over the last week.
Emergency policy list	● In the emergency policy list, you can view the blocked objects, blocking type, and number of delivered policies. In the list, you can edit, block, cancel blocking, and delete a policy. ● 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

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 management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-65 Workspace management page
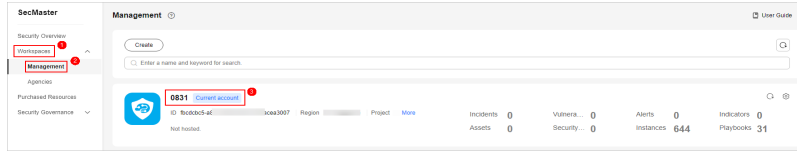
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Security Policies**. Then, click the **Emergency Policies** tab to go to the emergency policy page.

Figure 9-66 Emergency Policies
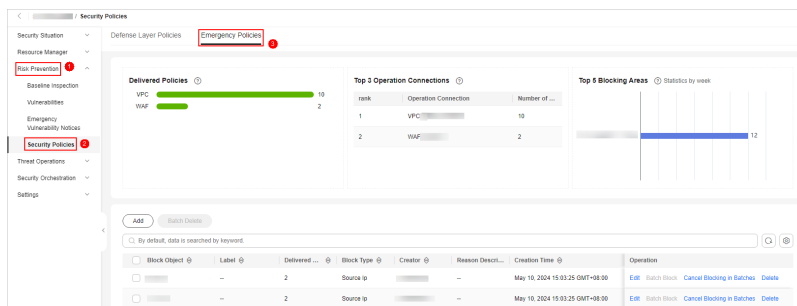
Step 6 On the emergency policy management page, locate the row that contains the policy you want to edit and click **Edit** in the **Operation** column.

Step 7 On the edit policy page, modify the policy information.

Table 9-17 Parameters for editing an emergency policy

Parameter	Description
Blocked Object Type	After an emergency policy is added, this parameter cannot be modified.
Block Object	After an emergency policy is added, this parameter cannot be modified.
Label	Label of the custom emergency policy.
Operation Connection	Select the operation connections for the policy.
Block Aging	The time the block action expires. • If you select **Yes**, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address/range or the IAM user will not be blocked. • If you select **No**, the policy is always valid and blocks the specified IP address/range or the IAM user.
Policy Description	Description of the custom policy.

Step 8 Click **OK**.

----End

Deleting an Emergency Policy

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-67 Workspace management page
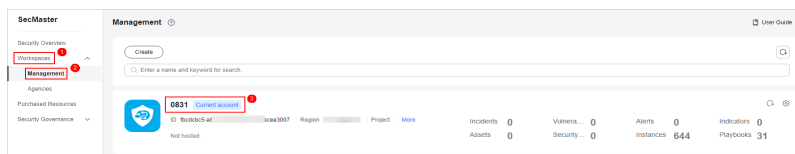
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Security Policies**. Then, click the **Emergency Policies** tab to go to the emergency policy page.

Figure 9-68 Emergency Policies
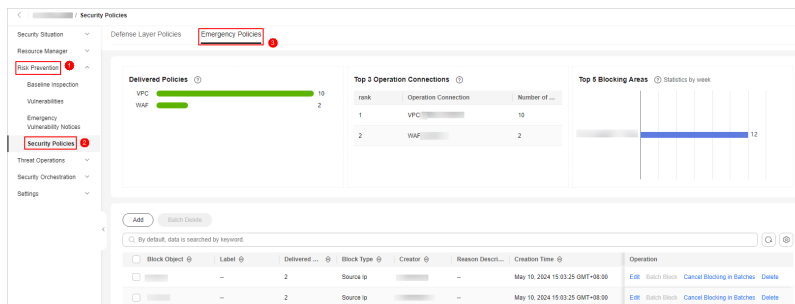
Step 6 On the **Emergency Policies** tab, locate the row that contains the policy you want to delete and click **Delete** in the **Operation** column.

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

Step 7 In the displayed confirmation dialog box, click **Confirm**.

----End

9.4.5 Batch Blocking and Canceling Batch Blocking of an IP Address or IP Address Range

Scenario

You can batch block access from blacklisted IP addresses, IAM users, or IP address ranges.

You can add an IP address, IAM user, or IP address range as blocked object for an emergency policy in several operation connections. If there is no need to block an IP address, IAM user, or IP address range for operation connections, you can cancel the blocking from all operation connections.

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, and 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 ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-69 Workspace management page
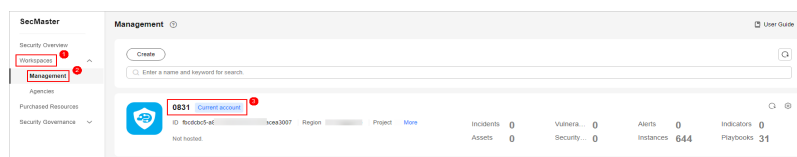
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Security Policies**. Then, click the **Emergency Policies** tab to go to the emergency policy page.

Figure 9-70 Emergency Policies

Step 6 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 7 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 management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-71 Workspace management page
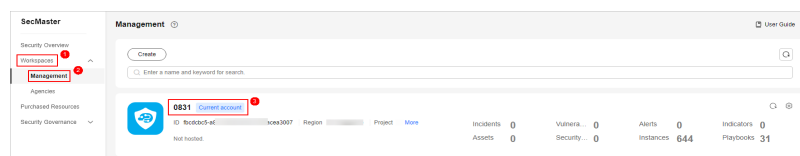
Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Security Policies**. Then, click the **Emergency Policies** tab to go to the emergency policy page.

Figure 9-72 Emergency Policies
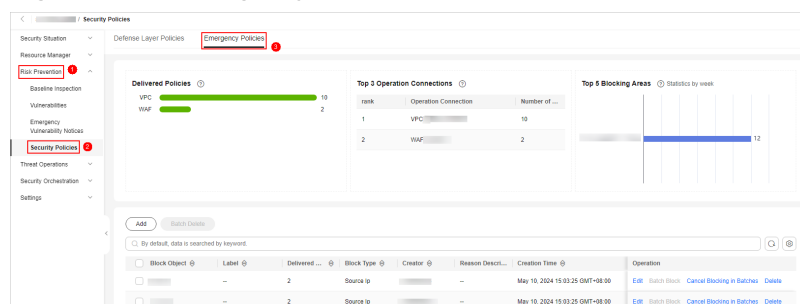
Step 6 On the emergency policy page, locate the row that contains the target policy, click **Cancel Blocking in Batches** in the **Operation** column.

Step 7 In the dialog box displayed, enter the reason for canceling the blocking and click **OK**.

----End

10 Threats

10.1 Incident Management

10.1.1 Viewing Incidents

Scenario

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

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

On the **Incidents** page in SecMaster, you can check the incident list for the last 360 days. The list contains the incident name, type, severity, and occurrence time of each incident. 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.

Viewing Incidents

Step 1 Log in to the management console.

Step 2 Click ⦿ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Threats** > **Incidents**.

Figure 10-2 Incidents
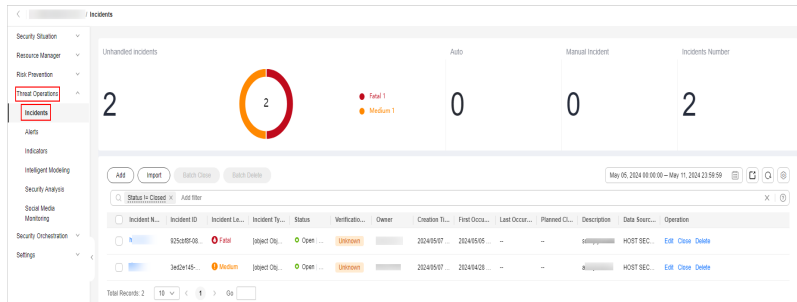
Step 6 On the **Incidents** page, view incident details.

Figure 10-3 Viewing an Incident
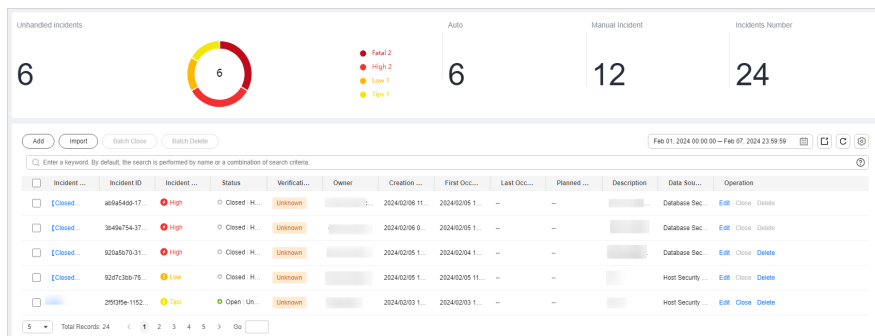
Table 10-1 Viewing an Incident

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.

Parameter	Description
Incidents Number (Incidents)	This area displays how many incidents that are reported within the specified time range in the current workspace.
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 and Editing an Incident

Scenario

This section describes how to add or edit an incident.

Adding an Incident

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Threats** > **Incidents**.

Figure 10-5 Incidents
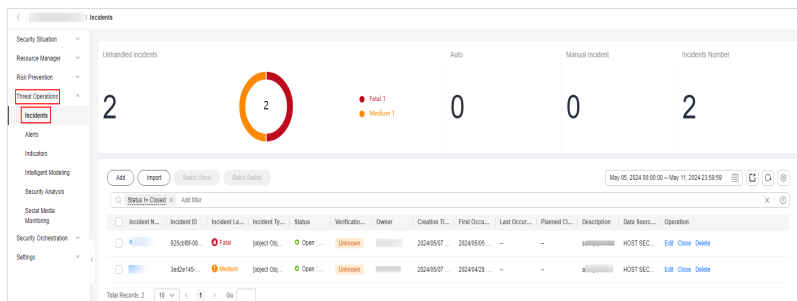
Step 6 On the **Incidents** page, click **Add**. On the displayed **Add** page, set parameters as described in **Table 10-2**.

Table 10-2 Parameters for adding an incident

Parameter		Description
Basic Information	Incident Name	Custom incident name. The value must contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 2,550 characters
	Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Severity	Select a severity level.
	Status	Select an incident status.
	(Optional) Owner	Primary owner of the incident.

Parameter		Description
	Data Source Product Name	Select the name of the data source product.
	Data Source Type	Select the type of the data source. For example, if the data source is a cloud service, select the cloud service.
Timeline	First Occurrence Time	Time when the incident occurred first time.
	(Optional) Last Occurrence Time	Time when the incident occurred last time.
	(Optional) Planned Closure Time	Time to close the incident.
Other	(Optional) Verification Status	Verification status of the incident to identify the accuracy of the incident.
	(Optional) Stage	Incident phase. ● **Preparation**: Prepare resources to process incidents. ● **Detection and analysis**: Detect and analyze the cause of an incident. ● **Containment, extradition, and recovery**: Handle an incident. ● **Post Incident Activity**: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging
	(Optional) Labels	Label of the incident.
	Description	Incident description. The value can contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 10,240 characters.

Step 7 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 management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
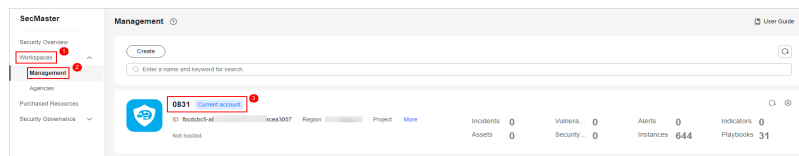
Step 5 In the navigation pane on the left, choose **Threats** > **Incidents**.

Figure 10-7 Incidents
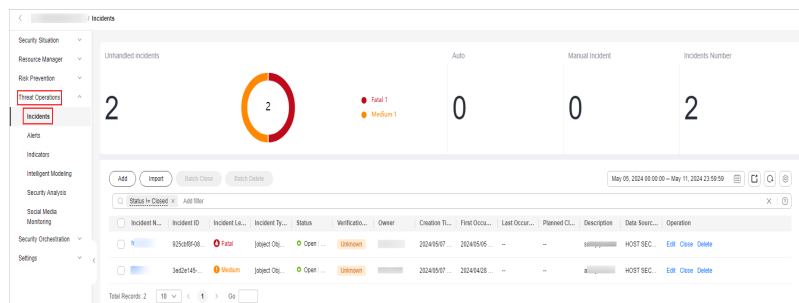
Step 6 In the incident list, locate the row that contains the target incident and click **Edit** in the **Operation** column.

Step 7 On the **Edit** page that is displayed, edit incident parameters.

Table 10-3 Parameters for editing an incident

Parameter		Description
Basic Information	Incident Name	Custom incident name. The value must contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 2,550 characters
	Incident Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Level	Select a severity level.

Parameter		Description
	Status	Select an incident status.
	(Optional) Owner	Primary owner of the incident.
	Data Source Name	Name of the data source, which **cannot be changed**
	Data Source Type	Type of the data source, which **cannot be changed**
Timeline	First Occurrence Time	Time when the incident occurred first time.
	(Optional) Last Occurrence Time	Time when the incident occurred last time.
	(Optional) Planned Closure Time	Time to close the incident.
Other	(Optional) Verification Status	Verification status of the incident to identify the accuracy of the incident.
	(Optional) Phase	Incident phase. ● **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 10,240 characters.

Step 8 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 files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.
- 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 management console and select a region or project.

**Step 3** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
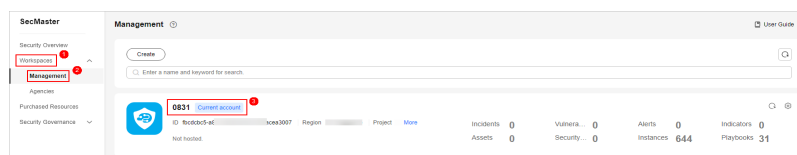
Step 5 In the navigation pane on the left, choose **Threats** > **Incidents**.

Figure 10-9 Incidents
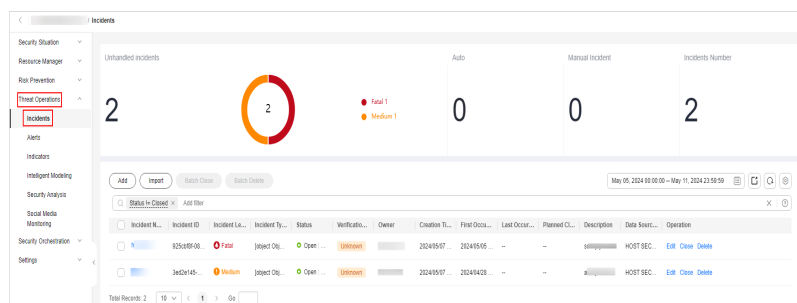
Step 6 On the **Incidents** page, click **Import** in the upper left corner above the incident list.

> **NOTE**
>
> Only files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.

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

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

Step 9 Click **OK**.

----End
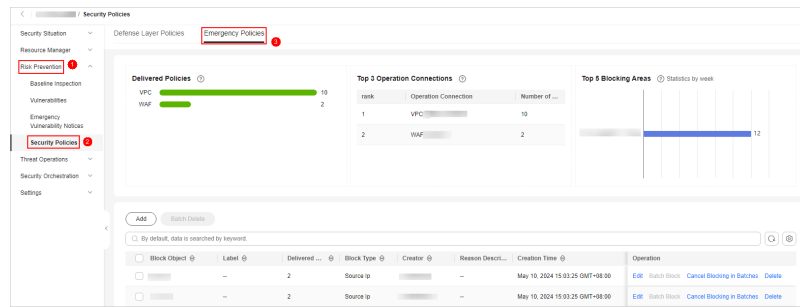
Exporting Incidents

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
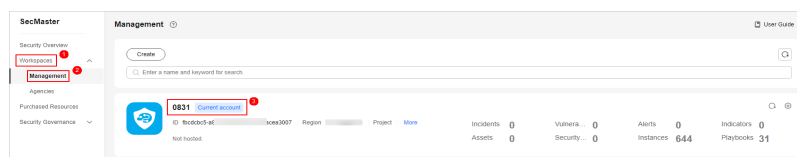
Step 5 In the navigation pane on the left, choose **Threats** > **Incidents**.

Figure 10-11 Incidents
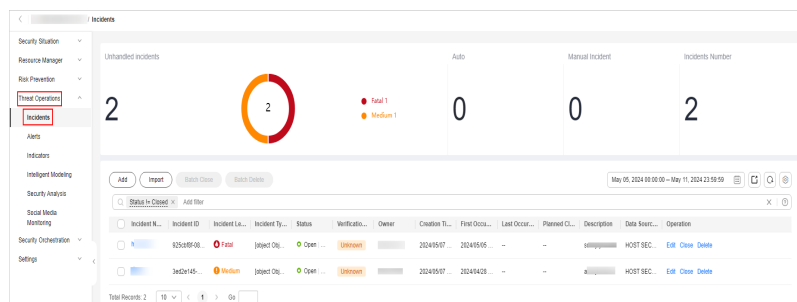
Step 6 On the **Incidents** page, select the incidents to be exported and click ⬈ in the upper right corner of the list. The **Export** dialog box is displayed.

📖 NOTE

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

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

Table 10-4 Exporting incidents

Parameter	Description
Format	By default, the incident 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

10.1.4 Closing and Deleting an Incident

Scenario

This topic describes how to close and delete an incident.

## Closing and Deleting an Incident

Step 1   Log in to the management console.

Step 2   Click [icon] in the upper left corner of the management console and select a region or project.

Step 3   Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4   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
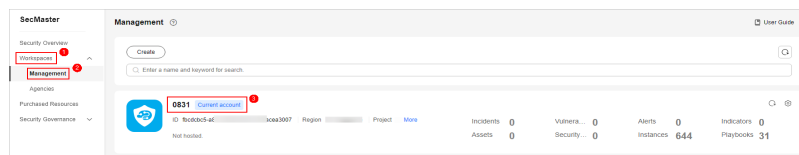
Step 5   In the navigation pane on the left, choose **Threats** > **Incidents**.

Figure 10-13 Incidents
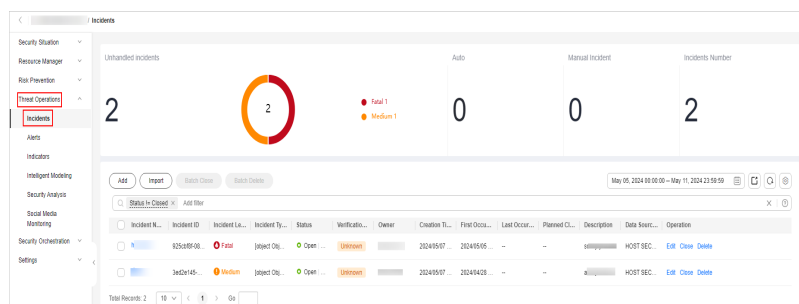
Step 6   On the **Incidents** page, close or delete an incident.

Table 10-5 Managing incidents

Operation	Description
Closing an Incident	1. Locate the row that contains the target incident and click **Close** in the **Operation** column. To close multiple incidents, select them in the incident list and click **Close** above the list. 2. In the confirmation dialog box, select **Reason for**, enter **Close Comment**, and click **OK**.
Deleting an Incident	1. On the **Incident** page, locate the row that contains the target incident and click **Delete** in the **Operation** column. To delete multiple incidents, select the target incidents in the incident list and click **Delete** above the list. 2. In the dialog box that is displayed, click **OK**. **NOTE** Deleted incidents cannot be restored. Exercise caution when deleting an incident.

----End

10.2 Alert Management

10.2.1 Overview

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

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

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

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

On SecMaster **Alerts** page, you can:

- **Check alert details**. You can check alerts generated over the last 360 days as well as their details, including the alert name, type, severity, and time it was generated. You can customize filters to quickly search for a specific alert by its name, risk severity, occurrence time, and other attributes.

- **Convert an alert into an incident or associate an alert with incidents**. During the alert analysis, if SecMaster detects attacks or serious threats, it

converts such alerts into incidents or associates such alerts with certain incidents.

- **Start or stop one-click blocking** by using an emergency policy. You can quickly contain a certain type of attacks based on attack sources identified in an alert.

- **Disable or delete an alert**. Deleted alerts cannot be restored. Exercise caution when performing this operation.

- **Add an alert or edit parameters for an alert**.

- **Import or export alerts**.

10.2.2 Viewing Alert Details

Scenario

On the **Alerts** page in SecMaster, you can check the alert list for the last 360 days. The list contains alert names, types, severity levels, and occurrence time. By customizing filtering conditions, such as the alert name, risk severity, and time, you can quickly query information about the specific alerts.

This section describes how to view alert information.

Prerequisites

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

Viewing Alert Details

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
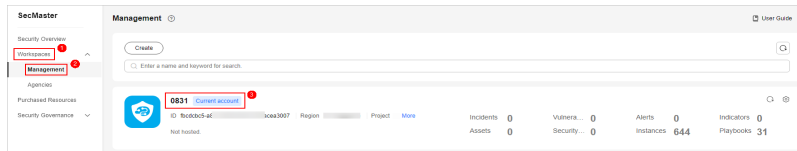
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-14 Workspace management page
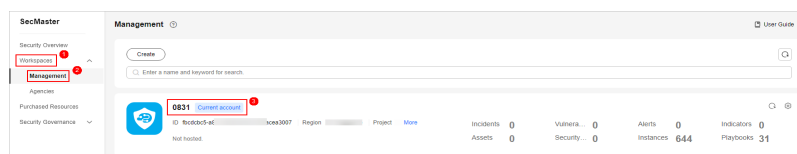
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-15 Alerts
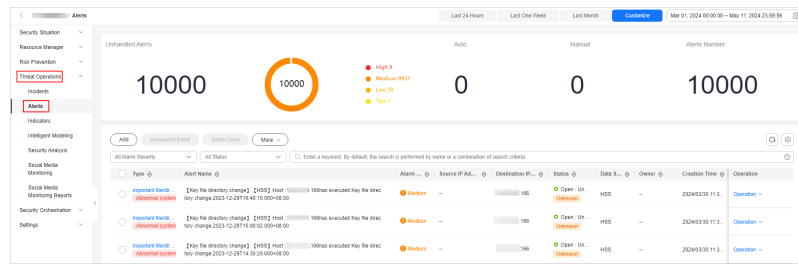
Step 6 View alert information.

Figure 10-16 Viewing Alerts
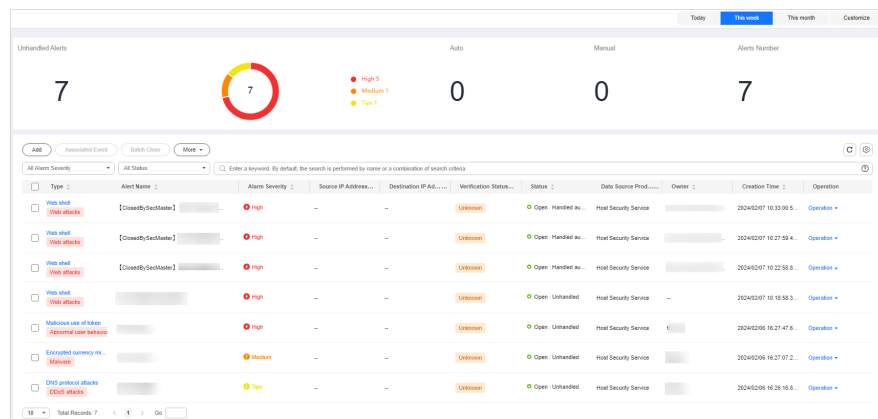
Table 10-6 Viewing Alerts

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 Alerts	This area displays how many alerts that are not handled within the specified time range in the current workspace. The unhandled alerts are displayed by severity.
Alerts Handled Automatically (**Auto**)	This area displays how many alerts that are handled automatically by playbooks within the specified time range in the current workspace.
Alerts Handled Manually (**Manual**)	This area displays how many alerts that are handled manually within the specified time range in the current workspace.
Alerts	This area displays how many alerts that are reported within the specified time range in the current workspace.

Parameter	Description
Alarm list	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 into 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

10.2.3 Suggestions on Handling Common Alerts

During data integration, SecMaster can automatically convert cloud service logs into 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**: HSS

  High-Risk command

- **Alert Field**

To view corresponding high-risk command 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.

   The high-risk command execution corresponds to **msg.appendInfo.event_type=3015**.

- **Investigation Guideline and Handling Suggestion**

  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 for pipeline **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 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 probing, and PoC execution.

     - If it is confirmed that the fault is triggered by attacks, contact the resource owner immediately.

- **High-Risk Commands**

  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 for pipeline **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 for pipeline **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 for pipeline **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 for pipeline **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 for pipeline **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.

10.2.4 Converting an Alert into an Incident or Associating an Alert with an Incident

Scenario

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

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

Relationships Between Alerts and Incidents

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

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

Table 10-7 Meanings and differences between alerts and incidents

Type	Description
Definition	- Alerts An alert is a notification of abnormal signals in O&M. It is usually automatically generated by a monitoring system or security device when detecting an exception in the system or networks. For example, when the CPU usage of a server exceeds 90%, the system may generate an alert. These exceptions may include system faults, security threats, or performance bottlenecks. Generally, an alert can clearly indicate the location, type, and impact of an exception. In addition, alerts can be classified by severity, such as critical, major, and minor, so that O&M personnel can determine which alerts need to be handled first based on their severity. The purpose of an alert is to notify related personnel in a timely manner so that they can make a quick response and take measures to fix the problem. - Incidents An incident is a broad concept, and may include, but is not limited to, an alert. An incident can be a part of the normal operation of the system, an exception, or an error. In the O&M and security fields, an incident usually refers to a problem or fault that has occurred and needs to be focused on, investigated, and handled. An incident may be triggered by one or more alerts or other factors, such as user operations and system logs. An incident is usually used to record and report historical activities in a system for analysis and audits.

Type	Description
Handling process	● Alerts The alert handling process includes receiving, confirming, analyzing, responding to, and closing alerts. When the monitoring system generates an alert, O&M personnel need to confirm that the alert is a positive one. Then, they need to analyze the alert causes and impact scope, take measures to rectify the fault, and close the alert. ● Incidents The event handling process is more complex and comprehensive. In addition to each phase in the alert handling process, incident handling also involves incident investigation, impact assessment, risk analysis, emergency plan formulation, emergency response execution, and post-event summary. The objective of incident handling is to completely solve problems, prevent similar incidents in the future, and reduce the impact of incidents on services.
Importance and urgency	● Alerts Generally, alerts need to be evaluated and responded immediately. The severity and importance of each alert vary depending on the alert type, severity, and impact scope. Some alerts may be simple reminders or warnings, while others may indicate that the system has been severely attacked or faces major fault risks. ● Incidents In some cases, incidents may need to be recorded, analyzed, and handled, but do not require immediate responses. An incident is usually of higher importance and urgency than an alert. Because an incident has occurred and has had an actual impact, immediate measures need to be taken to control the risk and solve the problem. If an incident is not handled in a timely manner, it may cause significant economic loss or reputation damage to the organization.

● **Causes for converting alerts into incidents or associating alerts with incidents**

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

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

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

Table 10-8 Causes for converting alerts into incidents or associating alerts with incidents

Type	Description
Alert-to-Incident reasons	When the severity of an alert reaches a certain level, an alert appears continuously, or the impact scope is wide, the alert may not only be a signal that requires attention. It also indicates that a continuous problem exists in the system or network. In this case, the alert has evolved into an incident that needs to be handled immediately. So, we need to convert such alerts into incidents to further investigate the root causes and take necessary measures. Generally, an alert will be converted to an incident out of the following causes: ● Information aggregation and classification An alert is usually an instant response to a violation against a specific condition or threshold. The number of alerts is increasing over time. If they are handled independently, it would cause chaos and waste time and human resources. Aggregating these alerts into incidents helps related personnel classify alerts by alert type, source, and impact so that they can handle them more effectively. ● Simplified working processes During the process to convert alerts into incidents, alerts are filtered, deduplicated, and aggregated. So that multiple similar alerts that may be triggered are integrated into a more representative incident. In this way, the workload of handling alerts is reduced; the handling process is clearer; and the tracing and recording become easier. ● **Higher problem-solving efficiency** As an incident has much more context details than an alert, related personnel can easily identify the root cause. This helps quickly locate issues and take effective measures. ● Historical data review and trend analysis An incident usually records the entire process of how an issue occurred, evolved, and is resolved. So converting alerts into incidents provides helpful historical data for prevention of similar issues and system optimization. By analyzing the trend of an incident, O&M personnel can discover potential weak points in the system and take measures in advance. ● Cross-department collaboration enhanced In a large organization, different departments may need to participate in the handling of problems. After an alert is converted into an incident, related information can be shared among departments more easily, which promotes cross-department

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

Type	Description
Causes for associating alerts with incidents	As an important part of monitoring and fault management, associating alerts with incidents involve combining multiple independent but possibly correlated incidents or alerts to better understand the root cause and scope of a problem, facilitating troubleshooting and response. Generally, an alert will be associated with an incident out of the following causes: • Dependencies In a complex system, there are complex dependencies between components. When a component becomes faulty, other components that depend on the component may be affected, causing a series of alerts. For example, in the microservice architecture, the crash of a service may cause problems in other services that use the service. • Resource sharing When multiple systems or services share the same resource (such as a server, database, or network device), the problem of the resource may cause multiple systems or services to generate alerts at the same time. For example, a performance deterioration of a shared database server may trigger performance alerts for multiple applications that depend on the database. • Chain reactions In some cases, an initial failure may trigger a series of chain reactions, affecting more components or systems. This chain reaction may be caused by improper system design, incomplete error handling mechanism, or resource limitations (such as performance deterioration caused by memory leakage). • Configuration errors Incorrect or inconsistent configurations may cause system behavior exceptions, triggering multiple seemingly irrelevant alerts. For example, incorrect routing configurations may cause traffic to be incorrectly routed to unstable servers, causing multiple performance-related alerts. • Software defects Software defects, such as bugs, may cause programs to be abnormal in specific conditions and trigger alerts. If these defects affect multiple components or systems, multiple associated alerts may be generated. • External factors External factors, such as natural disasters (such as earthquakes and floods), network attacks, and

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

Converting an Alert into an Incident

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
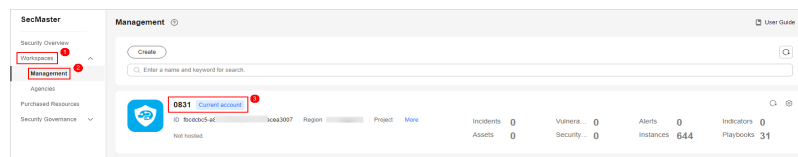
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-18 Alerts
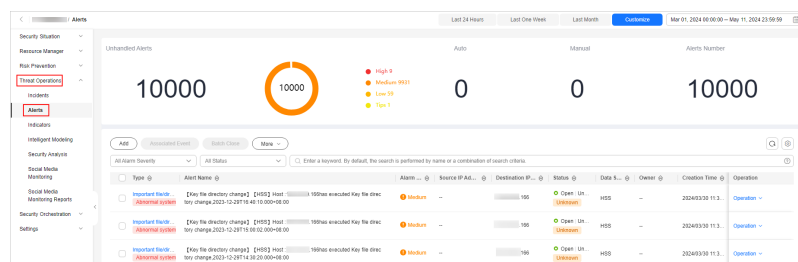
Step 6 In the alert list, locate the row that contains the target alert, click **Convert to Incident** in the **Operation** column. The **Convert to Incident** page is displayed on the right.

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

Step 7 On the **Convert to Incident** page, specify **Incident Name** and **Type**.

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

Step 8 Click **OK**.

----End

Associating an Alert with an Incident

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
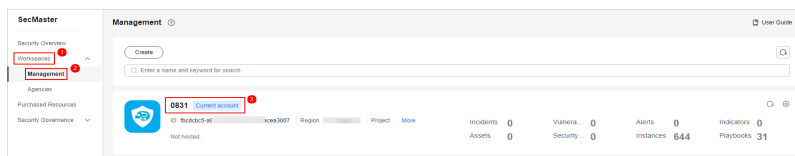
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-20 Alerts

Step 6 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 7 In the dialog box displayed, select the target incidents and click **OK**.

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

----End

10.2.5 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 10-9** lists recommended settings. You can also block a single attack source based on the comprehensive investigation of multiple alerts.

Table 10-9 Recommended blocking policies

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.

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 management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
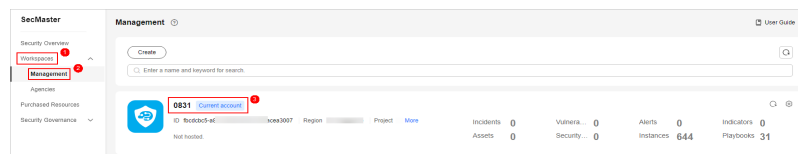
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-22 Alerts
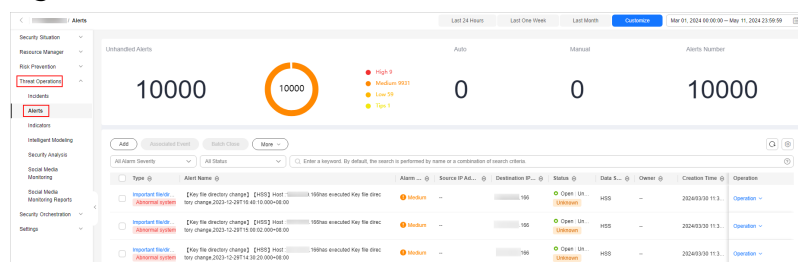
Step 6 In the alert list, locate the row that contains the target alert and choose **Operation** > **One-Click Block** in the **Operation** column. The **One-Click Block** panel is displayed on the right.

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 7 On the displayed page, configure the blocking policy.

Table 10-10 One-click blocking

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 (,).
	• If you select **IAM** for **Blocked Object Type**, enter IAM user names.
	• There are some restrictions on delivery of blocked objects:
	  – When a policy needs to be delivered to CFW, each time a maximum of 50 IP addresses can be added as blocked objects for each account.
	  – When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account.
	  – When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account.
	  – When a policy needs to be delivered to IAM, each time a maximum of 50 IAM users can be added as blocked objects for each account.

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.
Policy Description	Description of the custom policy.

Step 8 Click **OK**. In the dialog box displayed, confirm the information and click **OK**.

----End

One-click Unblocking

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
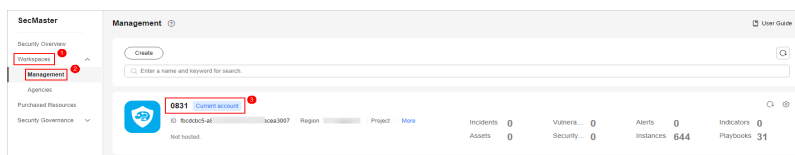
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-24 Alerts

Step 6 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 7 In the displayed dialog box, enter the reason and click **OK**.

----End

10.2.6 Closing and Deleting an Alert

Scenario

This topic describes how to close and delete an alert.

Closing and Deleting an Alert

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
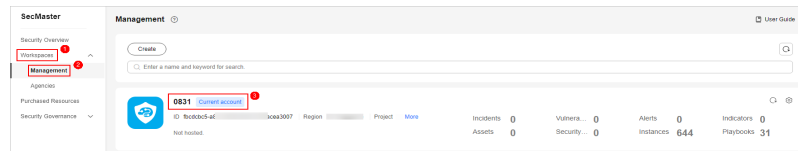
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-26 Alerts
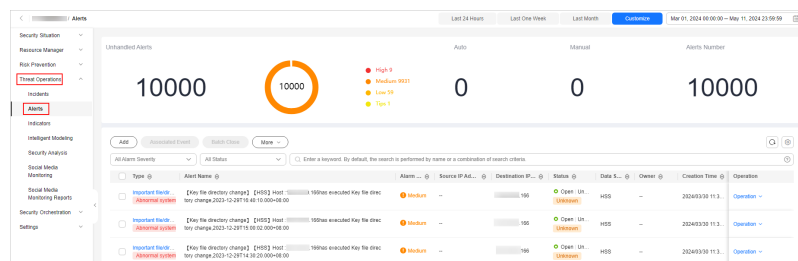
Step 6 On the **Alerts** page, close or delete an alert.

Table 10-11 Managing alerts

Operation	Description
Closing an alert	1. Locate the row that contains the target alert, click **Close** in the **Operation** column. A dialog box is displayed for you to confirm the close operation. To close multiple alerts, select the alerts in the alert list and click **Batch Close** above the list. 2. In the confirmation dialog box, select **Reason for**, enter **Close Comment**, and click **OK**.
Deleting an alert	1. Locate the row that contains the target alert, click **More** in the **Operation** column, and select **Delete**. The deletion confirmation dialog box is displayed. To delete multiple alerts, select the alerts in the alert list and click **More** > **Batch Delete** above the list. 2. In the displayed dialog box, click **OK**. **NOTE** Deleted alerts cannot be restored. Exercise caution when deleting an alert.

----End

10.2.7 Adding and Editing an Alert

Scenario

This section describes how to add or edit an alert.

Adding an Alert

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
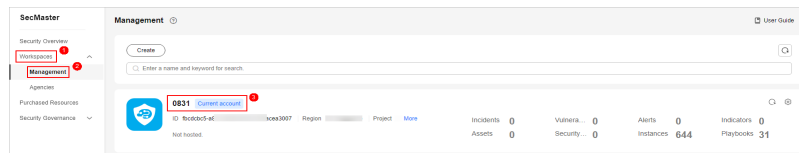
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-28 Alerts
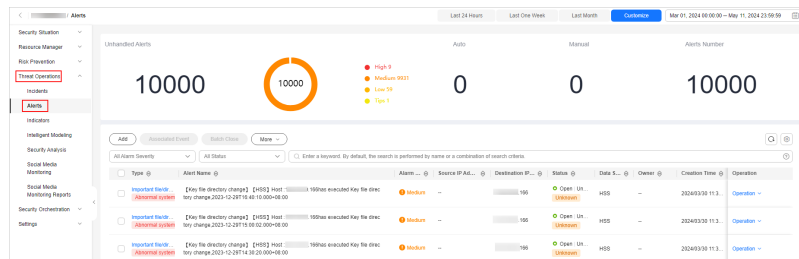
Step 6 On the **Alerts** page, click **Add**. On the **Add** page displayed on the right, set parameters as described in **Table 10-12**.

Table 10-12 Alert parameters

Parameter		Description
Basic information	Alert Name	User-defined alert name. The value must contain: • Only uppercase letters, lowercase letters, digits, and the special characters: -_ () • A maximum of 2,550 characters
	Alert Type	Alert type

| Parameter		Description
	Alert Severity	Alert severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**.
	Status	Alert status. The options are **Open**, **Blocked**, and **Closed**.
	(Optional) Owner	Primary owner of the alert.
	Data Source Product Name	Data source name
	Data Source Type	Type of the data source. The options are **Cloud Service**, **Third-party**, and **Private**.
Timeline	First Occurrence Time	Time when an alert is generated for the first time.
	(Optional) Last Occurrence Time	Last time when an alert was generated
	(Optional) Planned Closure Time	Time when the alert plan is disabled.
Other	(Optional) Verification Status	Verification status of the alert to identify the accuracy of the alert. The options are **Unknown**, **Positive**, and **False positive**.
	(Optional) stage	Alert phase. ● **Preparation**: Prepare resources to process alert. ● **Detection and analysis**: Detect and analyze the cause of an alert. ● **Containment, extradition, and recovery**: Handle an alert. ● **Post Incident Activity**: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging.
	(Optional) Labels	Alert labels.
	Description	Alert description. The value can contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 10,240 characters.

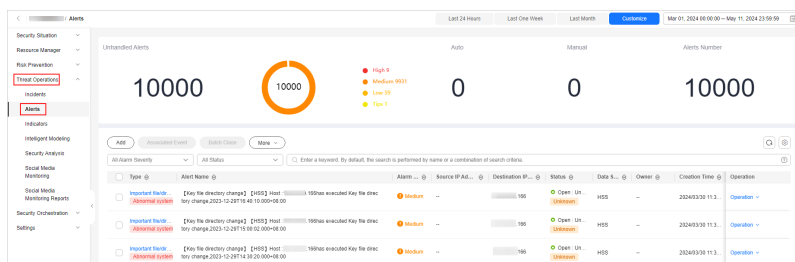**Step 7** Click **OK**.

----End

Editing an Alert

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
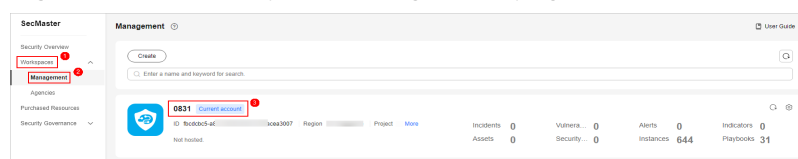
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-30 Alerts
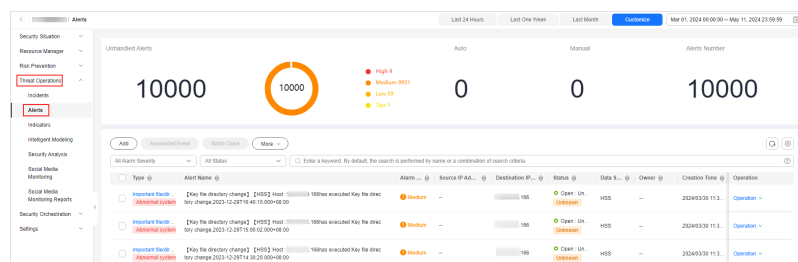
Step 6 In the alert list, locate the row that contains the target alert and click **More** > **Edit** in the **Operation** column.

Step 7 On the **Edit** slide-out that is displayed, modify alert parameters. For details about the parameters, see **Table 10-13**.

Table 10-13 Alert parameters

Parameter		Description
Basic Information	Alert Name	User-defined alert name. The value must contain: • Only uppercase letters, lowercase letters, digits, and the special characters: -_ () • A maximum of 2,550 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**.

Parameter		Description
	(Optional) Owner	Primary owner of the alert.
	Data Source Product Name	Name of the data source, which **cannot be changed**
	Data Source Type	Type of the data source, which **cannot be changed**
Timeline	First Occurrence Time	Time when an alert is generated for the first time.
	Last Occurrence Time	Last time when an alert was generated
	Planned Closure Time	Time when the alert plan is disabled.
Other	Labels	Alert labels.
	Debugging data	Whether to enable simulated debugging. This parameter **cannot be modified** once configured.
	Verification Status	Verification status of the alert to identify the accuracy of the alert. The options are **Unknown**, **Positive**, and **False positive**.
	Stage	Alert phase. ● **Preparation**: Prepare resources to process alert. ● **Detection and analysis**: Detect and analyze the cause of an alert. ● **Contain, extradition, and recovery**: Handle an alert. ● **Post Incident Activity**: Follow-up activities.
	Description	Alert description. The value can contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 10,240 characters.

Step 8 Click **OK**.

----End

10.2.8 Importing and Exporting Alerts

Scenario

This section describes how to import and export alerts.

Limitations and Constraints

- Only files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.
- A maximum of 9,999 alert records can be exported.

Importing Alerts

Step 1 Log in to the management console.

Step 2 Click [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
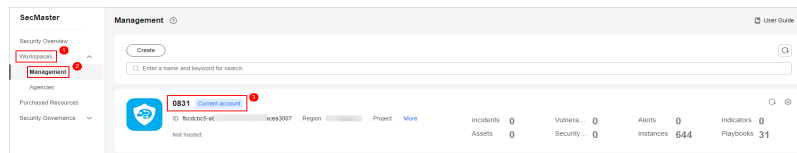
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-32 Alerts

Step 6 On the **Alerts** page, click **More** > **Import** in the upper left corner of the list.

📖 **NOTE**

Only files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.

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

Step 8 After the alert 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 Alerts

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
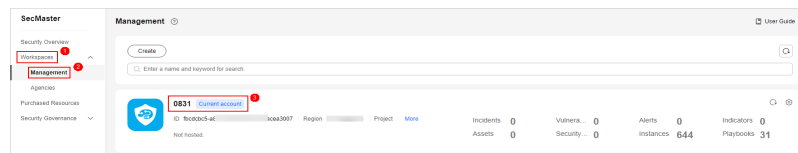
Step 5 In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 10-34 Alerts
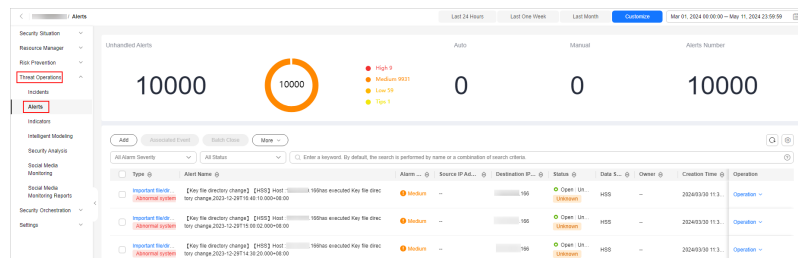
Step 6 In the alert list, select the alerts you want to export and click **More** > **Export** in the upper right corner of the list.

> **NOTE**
>
> A maximum of 9,999 alert records can be exported.

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

Table 10-14 Exporting alerts

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

Step 8   Click **OK**.

The system automatically downloads the Excel to your local PC.

----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.
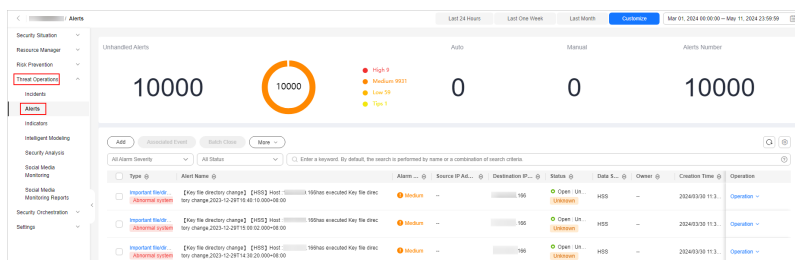
Adding an Indicator

Step 1   Log in to the management console.

Step 2   Click [icon] in the upper left corner of the management console and select a region or project.

Step 3   Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4   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
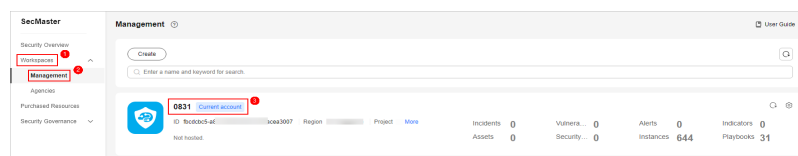
Step 5   In the navigation pane on the left, choose **Threats** > **Indicators**.

Figure 10-36 Indicators
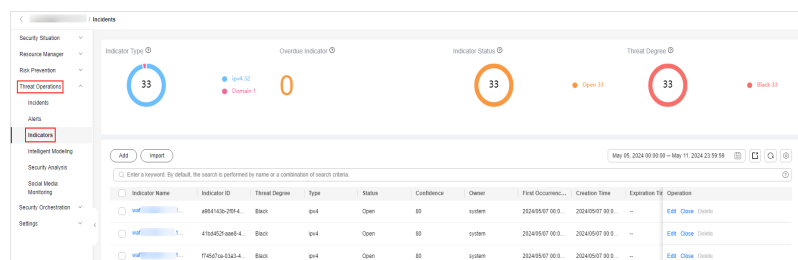
Step 6   On the **Indicators** page, click **Add**. On the **Add** page, set parameters.

Table 10-15 Indicator parameters

Parameter	Description
Indicator Name	Name of a user-defined threat indicator. The value can contain: Only uppercase letters, lowercase letters, digits, and the special characters: -_ ()
Type	Indicator type.
Threat Degree	Select a threat degree level. ● **Black**: dangerous ● **Gray**: minor ● **White**: secure
Data Source Product Name	Data source product name
Data Source Type	Type of the data source. The options are **Cloud Service**, **Third-party**, and **Private**.
Status	Indicator status. Possible values are **Open**, **Closed**, and **Revoked**.
(Optional) Confidence	Reliability of the selected indicator. The value ranges from 80 to 100.
(Optional) Owner	Primary owner of the indicator.
(Optional) Labels	Label of a user-defined counter.
First Occurrence Time	First occurrence time of the indicator.
Last Occurrence Time	Latest occurrence time of the indicator.
(Optional) Expiration Time	Expiration time of the indicator.
Invalid or not	Whether to invalidate the indicator. The default value is **No**.
Granularity	Granularity of the indicator. The options are **First time observed**, **In-house data**, **To be purchased**, and **Queried from external networks**.
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 7 Click **OK**.

----End

## Editing an Indicator

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

**Step 3** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Threats** > **Indicators**.

Figure 10-38 Indicators
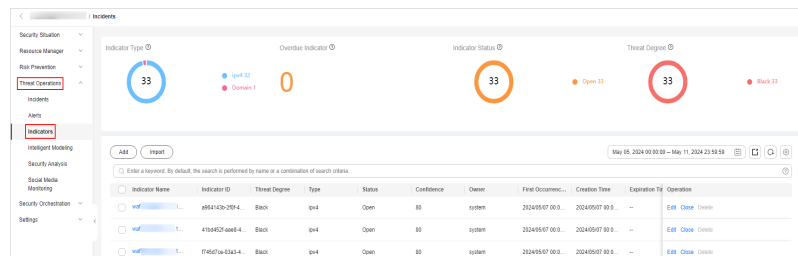
Step 6 On the **Indicators** page, locate the target indicator and click **Edit** in the **Operation** column.

Step 7 On the **Edit** page that is displayed, edit indicator parameters.

Table 10-16 Indicator parameters

Parameter	Description
Indicator Name	Name of a user-defined threat indicator. The value can contain: Only uppercase letters, lowercase letters, digits, and the special characters: -_ ()
Type	Indicator type.

Parameter	Description
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**, **In-house data**, **To be purchased**, and **Queried from external networks**.
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 8 Click **OK**.

----End

10.3.2 Closing and Deleting an Indicator

Scenario

This topic describes how to disable or delete an indicator.

Closing and Deleting an Indicator

Step 1 Log in to the management console.

Step 2 Click [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
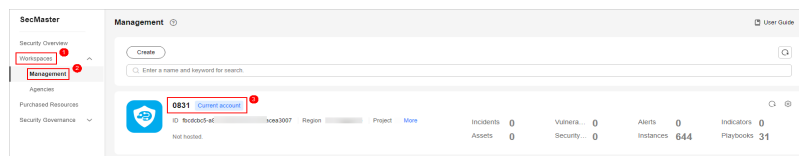
Step 5 In the navigation pane on the left, choose **Threats** > **Indicators**.

Figure 10-40 Indicators
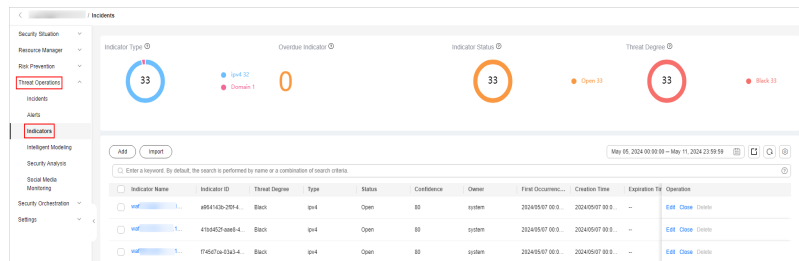
Step 6 On the **Indicators** page, close or delete an indicator.

Table 10-17 Indicator parameters

Operation	Description
Close	1. On the **Indicator** page, locate the row that contains the target indicator, click **Close** in the **Operation** column. The **Close** dialog box is displayed. 2. In the dialog box that is displayed, select the close reason and enter comments. 3. Click **OK**.
Delete	1. 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.

----End

10.3.3 Importing and Exporting Indicators

Scenario

This section describes how to import and export indicators.

Constraints

- Only files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.

- 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
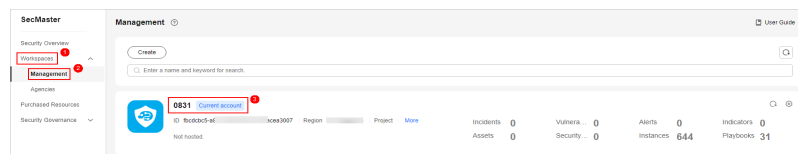
Step 5 In the navigation pane on the left, choose **Threats** > **Indicators**.

Figure 10-42 Indicators

Step 6 On the **Indicator** page, click **Import** in the upper left corner above the indicator list.

NOTE

> Only files in .xlsx can be imported. Each time you can import a file no larger than 5 MB with a maximum of 100 records.

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

Step 8 After the indicator 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 Indicators

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
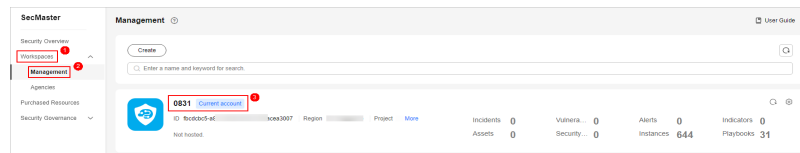
Step 5 In the navigation pane on the left, choose **Threats** > **Indicators**.

Figure 10-44 Indicators
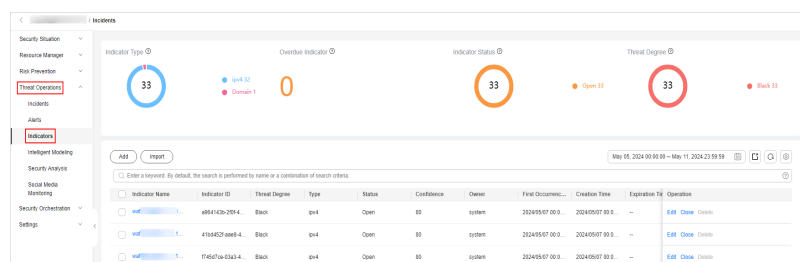
Step 6 On the **Indicators** page, select the indicators you want to export and click in the upper right corner of the list. The **Export** dialog box is displayed.

NOTE

> A maximum of 9,999 indicator records can be exported.

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

Table 10-18 Exporting indicators

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

Step 8 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.
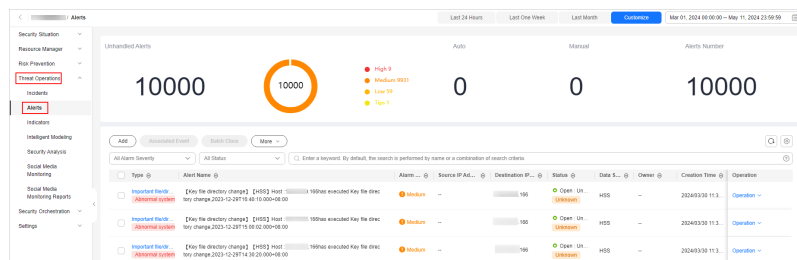
Viewing Indicators

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
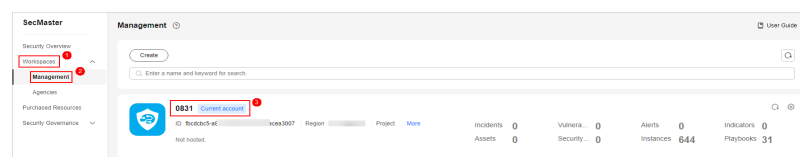
Step 5 In the navigation pane on the left, choose **Threats** > **Indicators**.

Figure 10-46 Indicators
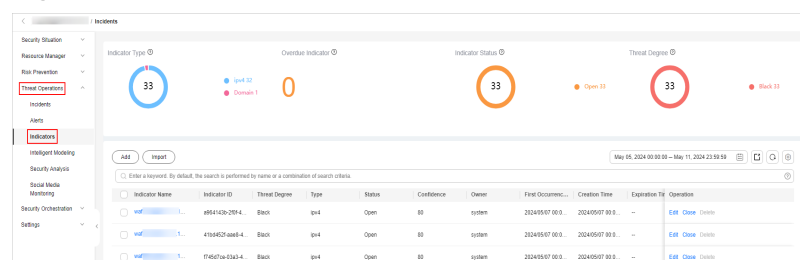
Step 6 On the **Indicators** page, view details about the indicator.

Figure 10-47 Viewing an Indicator

Table 10-19 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 Model Templates

Scenario

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

SecMaster provides multiple preconfigured model templates based on common scenarios. You can view scenario description, model principles, handling suggestions, and usage restrictions for these templates in this section.

Viewing Model Templates

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

**Step 3** Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
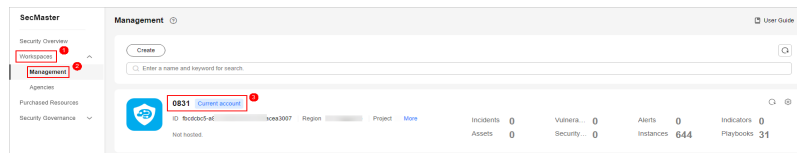
Step 5 In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**, and select the **Model Templates** tab.

Figure 10-49 Model Templates tab
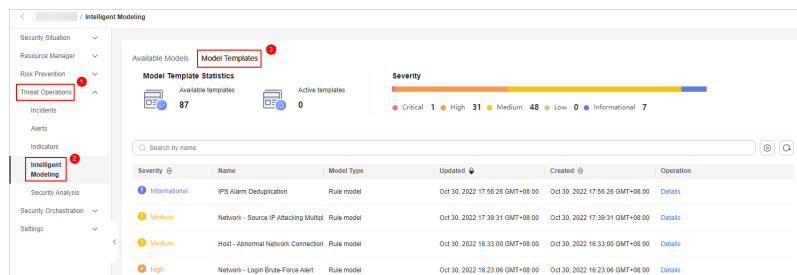
Step 6 On the **Model Templates** tab, view available model templates.

Table 10-20 Template information

Parameter	Description
Model Template Statistics	This area displays how many **Available templates** and how many **Active templates** you have.
Severity	This bar displays the number of available templates by severity levels, including **Critical**, **High**, **Medium**, **Low**, and **Informative**.
Template list	• The template list displays the severity, name, and model type of each template as well as when the template is created and upgraded. • To view details about a model template, locate the row that contains the template, click **Details** in the **Operation** column. The template details page is displayed on the right. On the details page, you can view the description, query rules, triggering conditions, and query plans of the current model template.

----End

10.4.2 Creating and Editing a Model

Scenario

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

The recommended preconfigured models in the current region can be automatically enabled in the first workspace of each region. For non-first workspaces, you need to enable them manually.

You can use a preconfigured model template to create a model. You can also create an alert model from scratch.

- **Creating an Alert Model Using a Preconfigured Model Template**
- **Creating a Custom Alert Model**
- **Editing a Model**

Limitations and Constraints

- A maximum of 100 alert models can be created in a workspace in a region for an account.
- 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 Preconfigured Model Template

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
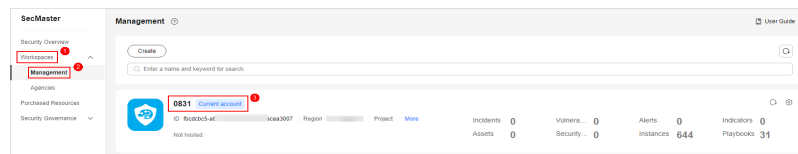
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-50 Workspace management page
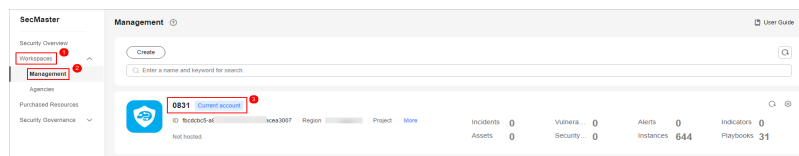
Step 5 In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**, and select the **Model Templates** tab.

Figure 10-51 Model Templates tab
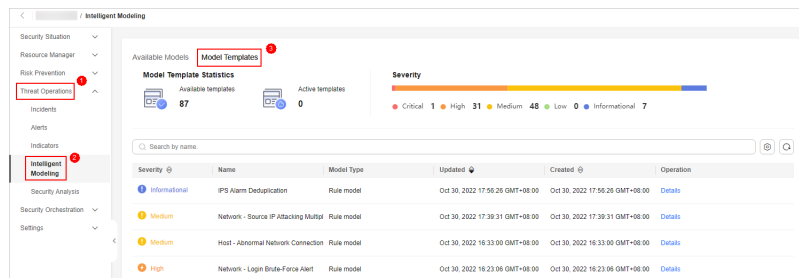
Step 6 In the model template list, click **Details** in the **Operation** column of the target model template. The template details page is displayed on the right.

Step 7 On the model template details page, click **Create Model** in the lower right corner. The page for creating an alert model is displayed.

Step 8 On the **Create Threat Model** page, configure basic information about the model by referring to **Table 10-21**.

Table 10-21 Basic alert model parameters

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

Parameter	Description
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. The status set here can be changed after the entire alert model is set successfully.

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 10-22**.

Table 10-22 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result. A query analysis statement consists of a query statement and an analysis statement. The format is **Query Statement|Analysis Statement**. For details about the syntax of query analysis statements, see **Query and Analysis Syntax Overview**. NOTE If the reserved field is of the text type, **MATCH_QUERY** is used for word segmentation queries by default.

Parameter	Description
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 trigger conditions, click **Add** and add them. A maximum of five trigger conditions can be added. If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition from top to bottom and generates all types of alerts for hit trigger conditions.
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. ● If **Suppression** is enabled, the **query stops** after an alert is generated. ● If **Suppression** is disabled, the **query is not stopped** after an alert is generated.

Step 11 After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.

Step 12 After confirming that the preview is correct, click **OK** in the lower right corner of the page.
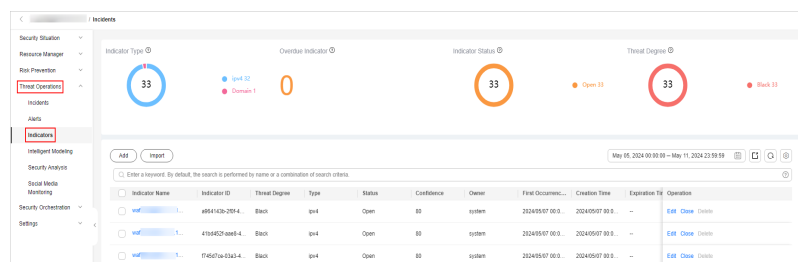
----End

Creating a Custom Alert Model

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
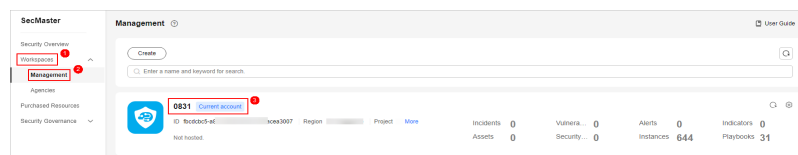
Step 5 In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**.

Figure 10-53 Available Models

Step 6 Click **Create Model** in the upper left corner of the **Available Models** tab.

Step 7 On the **Create Model** slide-out panel displayed, configure basic information about the alert model. For details about the parameters, see **Table 10-23**.

Table 10-23 Basic alert model parameters

Parameter	Description
Pipeline Name	Select the execution pipeline of the alert model.

Parameter	Description
Model Name	Name of the alert model.
Severity	Severity of the alert model. You can set the severity to Critical, High Risk, Medium Risk, Low Risk, or Warning.
Alarm Type	Alarm type displayed after the alert model is triggered.
Model Type	The default value is **Rule model**.
Description	Description of the alert model
Status	Indicates whether to enable the alert model. The status set here can be changed after the entire alert model is set successfully.

Step 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 10-24**.

Table 10-24 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result. For details about the syntax, see **Query and Analysis Syntax Overview**.
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.

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. To configure multiple trigger conditions, click **Add** and add them one by one. A maximum of five trigger conditions can be added. If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition and generates all types of alerts for hit trigger conditions.
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. - If **Suppression** is enabled, the **query stops** after an alert is generated. - If **Suppression** is disabled, the **query is not stopped** after an alert is generated.

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

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

----End

## 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.
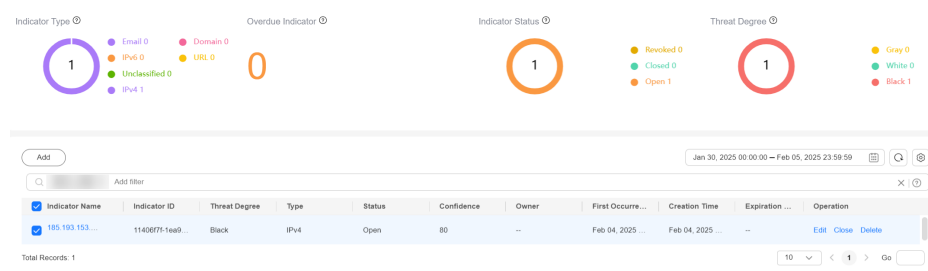
Figure 10-54 Workspace management page
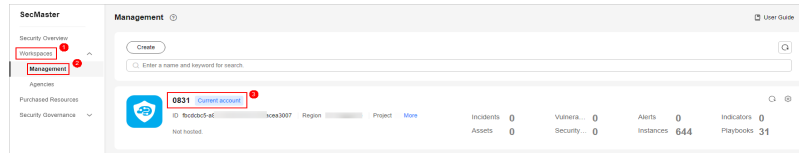
Step 5 In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**.

Figure 10-55 Available Models
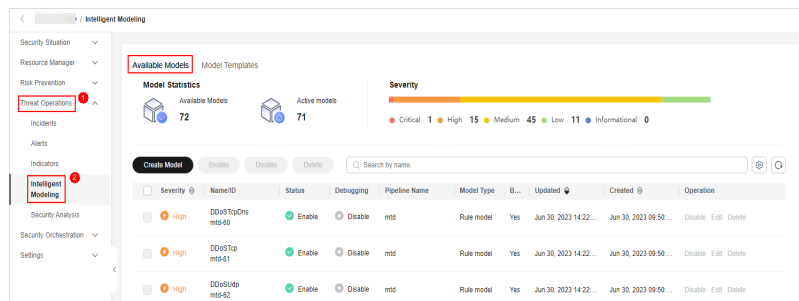
Step 6 In the available model list, click **Edit** in the **Operation** column of the target model.

Step 7 On the **Edit Model** slide-out panel, configure basic information about the alert model. For details about the parameters, see **Table 10-25**.

Table 10-25 Basic alert model parameters

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

Step 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 10-26**.

Table 10-26 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result. A query analysis statement consists of a query statement and an analysis statement. The format is **Query Statement|Analysis Statement**. For details about the syntax of query analysis statements, see **Query and Analysis Syntax Overview**. NOTE If the reserved field is of the text type, **MATCH_QUERY** is used for word segmentation queries by default.
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.

Parameter	Description
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 trigger conditions, click **Add** and add them. A maximum of five trigger conditions can be added.
	If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition from top to bottom and generates all types of alerts for hit trigger conditions.
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. ● If **Suppression** is enabled, the **query stops** after an alert is generated. ● If **Suppression** is disabled, the **query is not stopped** after an alert is generated.

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

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

----End

10.4.3 Viewing a Model

Scenario

This topic describes how to view models.

Prerequisites

A model has been created. For details, see **Creating and Editing a Model**.

Viewing a Model

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

**Step 3** Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
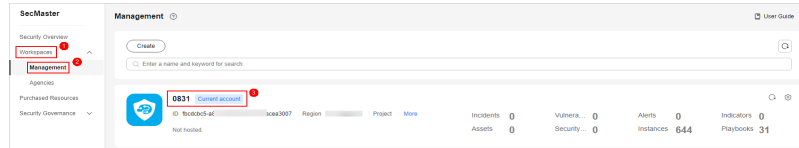
Step 5 In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**.

Figure 10-57 Available Models
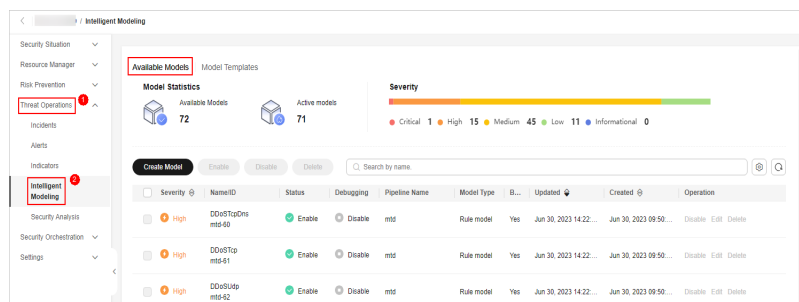
Step 6 On the **Available Models** tab, view available models.

Table 10-27 Viewing available models

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

----**End**

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.

Managing Models

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
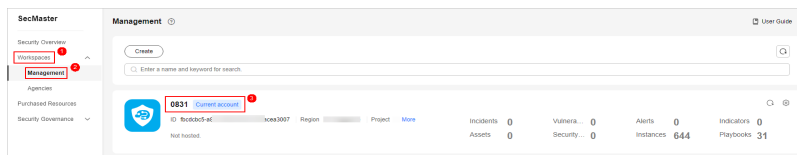
Step 5 In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**.

Figure 10-59 Available Models
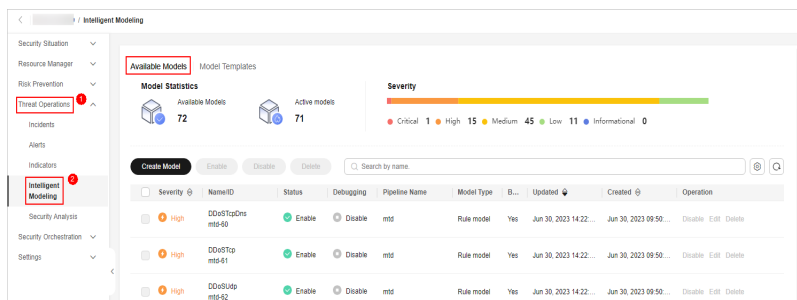
Step 6 On the **Available Models** tab, manage models.

Table 10-28 Managing 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.

Operation	Description
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**.

----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 **Cloud Service 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.

Use process

Table 10-29 Use process

Step	Description
Adding a Workspace	Add a workspace for resource isolation and control.
Integrating Data	Configure the sources of security data you need to collect. SecMaster can integrate log data of multiple Huawei Cloud products, such as services in storage, management and governance, and security domains. You can search and analyze all collected logs in SecMaster.
(Optional) **Adding a Data Space**	Create a data space for storing collected log data. For data accessed through the console, the system creates a default data space. You do not need to create a data space.
(Optional) **Creating a Pipeline**	Create pipelines for collecting, storing, and querying log data. For data accessed through the console, the system creates a default data pipeline. You do not need to create a pipeline.
Configuring Indexes	Configure indexes to narrow down the query scope. By default, indexes have been configured for some reserved fields in the accessed cloud service logs. For details, see **Log Fields**.
Querying and Analyzing Collected Data	Query and analyze the accessed data.
Downloading Logs	Download raw logs or queried and analyzed logs.
Viewing Result Charts	If you run query and analysis statements, SecMaster displays query and analysis results in charts and tables. Currently, results can be displayed in tables, line charts, bar charts, and pie charts.

10.5.2 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, field indexes are mandatory. 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**.
- Field indexes cannot be deleted.

Configuring Field Indexes

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

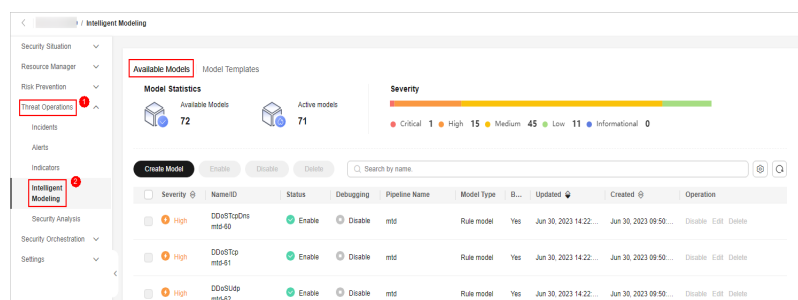**Step 3** Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
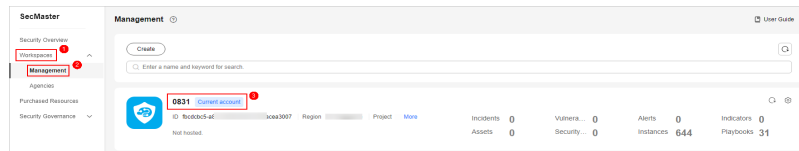
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-61 Accessing the Security Analysis tab page
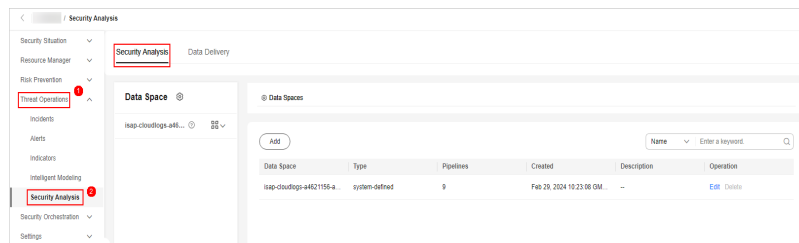
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-62 Pipeline data page
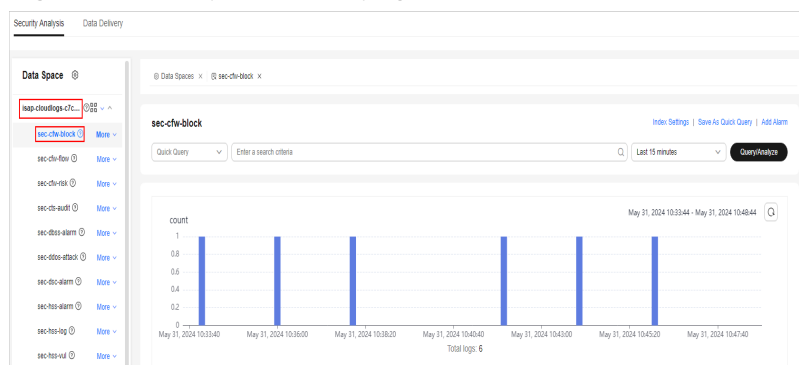
Step 7 On the pipeline page, click **Index Settings** in the upper right corner.

Step 8 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 10-30**.

Table 10-30 Parameters for index settings

Parameter	Description
Field	Log field (key)
Type	Data type of the log field value. The options are text, keyword, long, integer, double, float, date, and json.
Includes Chinese	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**.

Step 9 Click **OK**.

----End

10.5.3 Querying and Analyzing Logs

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.

- Method 1: **Executing a Query and Analysis Based on Query Criteria**
- Method 2: **Using Existing Fields for Query and Analysis**
- Method 3: **Creating a Quick Query**
- **Managing Query and Analysis Results**

Prerequisites

Data access has been completed. For details, see **Data Integration**.

Executing a Query and Analysis Based on Query Criteria

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 4 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
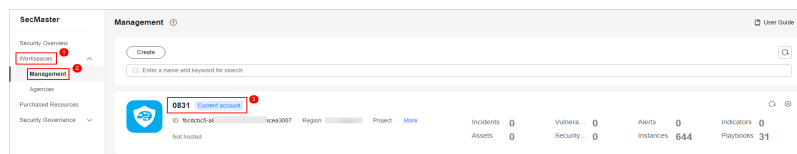
Step 5 In the navigation pane on the left, choose **Threats > Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-64 Accessing the Security Analysis tab page
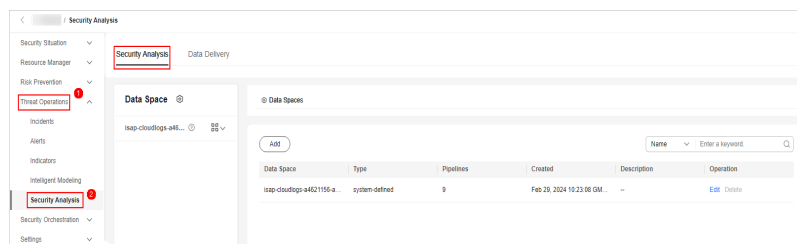
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-65 Pipeline data page
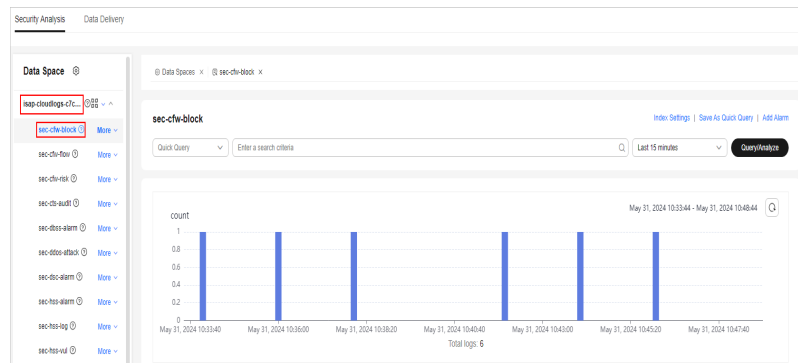
Step 7 On the pipeline data retrieval page, enter the query analysis statement.

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

📖 **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
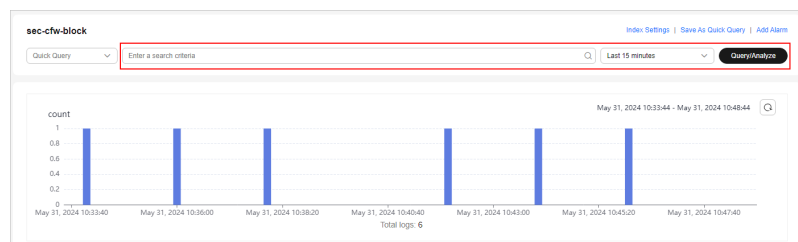
Step 8 Select **Last 15 minutes** as the time range.

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

Step 9 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
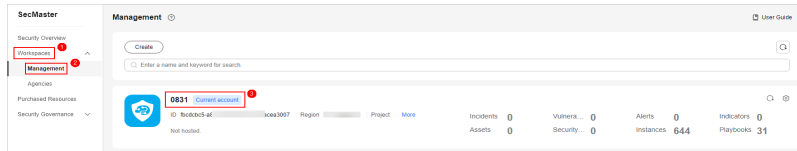
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-68 Accessing the Security Analysis tab page
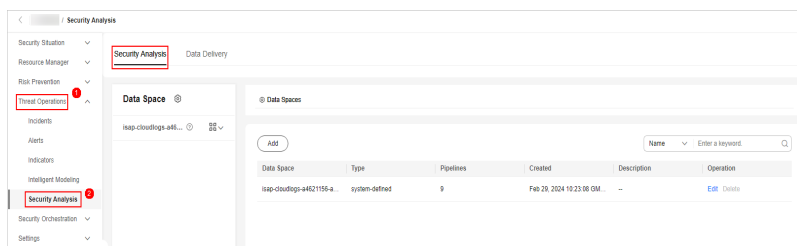
Step 6 In the **Data Spaces** tree on the left, click a data space name to show the pipeline list. Then, click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-69 Pipeline data page
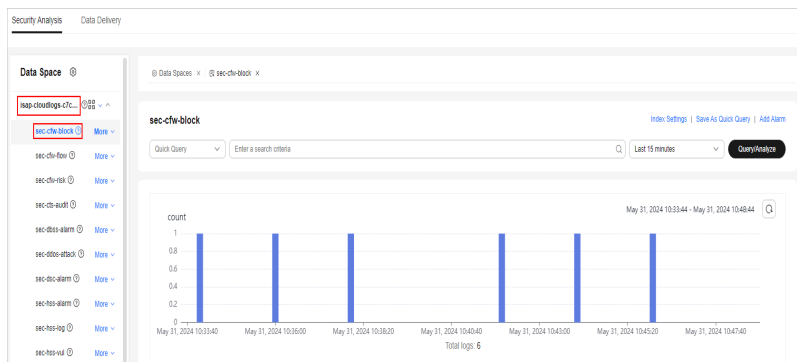
Step 7 Set search criteria.

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.

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

Figure 10-70 Filtering a Field Value (1)
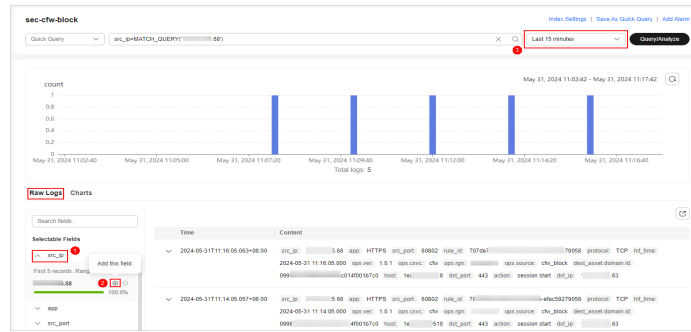
- If you have expanded the log data at a specific time point and need to filter some fields, click ⊕ (adding a field value) in front of the field name. The query box displays the matched fields. To exclude a field value, click ⊖ before the field name.

Figure 10-71 Filtering a Field Value (2)
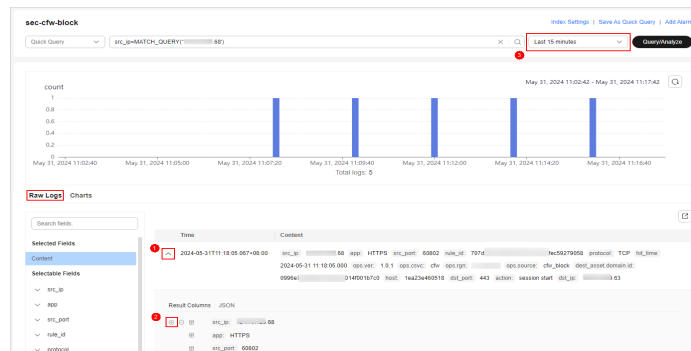
Step 8 By default, data for the last 15 minutes is queried and displayed. If you want to query log data in other time ranges, set the query time and click **Query/Analyze**.

**----End**

Creating a Quick Query

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-72 Workspace management page
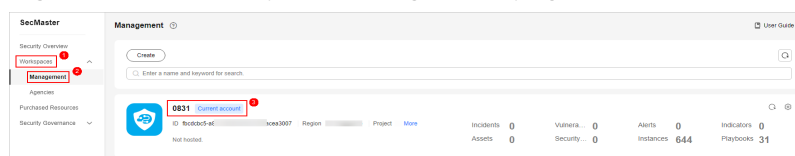
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-73 Accessing the Security Analysis tab page
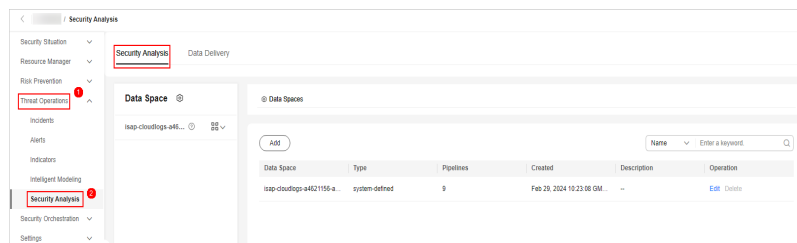
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-74 Pipeline data page
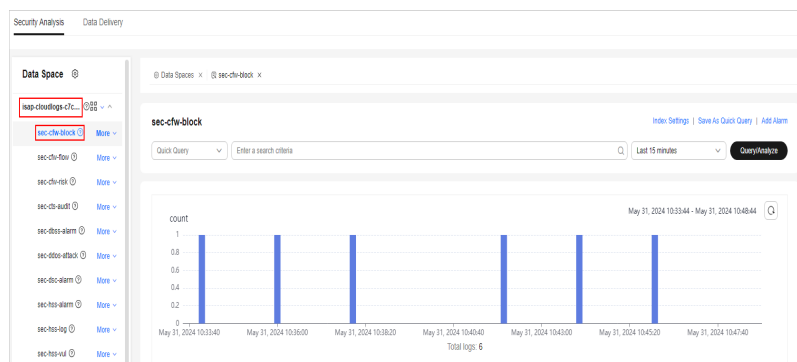
Step 7 Enter the query and analysis statement, set the time range, and click **Query/ Analyze**.

For details, see **Executing a Query and Analysis Based on Query Criteria**.

Step 8 Click **Save As Quick Query** in the upper right corner of the area and configure query parameters on the right.

Table 10-31 Parameters for a quick query

Parameter	Description
Query Name	Specify the name of the quick query.
Query statement	The system automatically generates the query statement entered in **Step 7**.

Step 9 Click **OK**.

After creating a quick query, you can click ▼ in the quick query search box on the pipeline data query and analysis page and select the target quick query name to use the quick query.

----End

Managing Query and 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 10-75 Log distribution bar chart
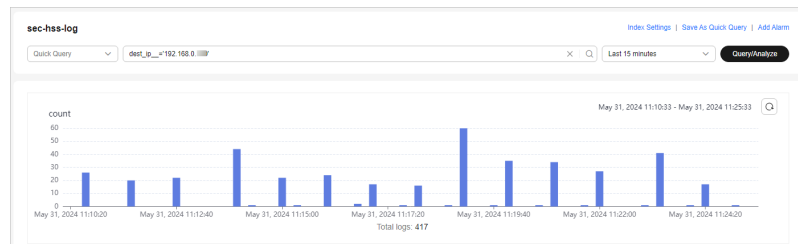
- **Raw Logs**

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

  Figure 10-76 Raw Logs
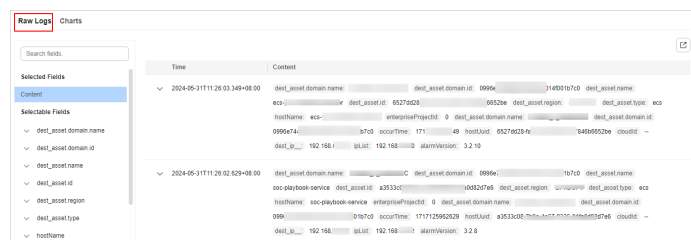
  - To display log data over time:

    - 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.

      Figure 10-77 Selecting a time range
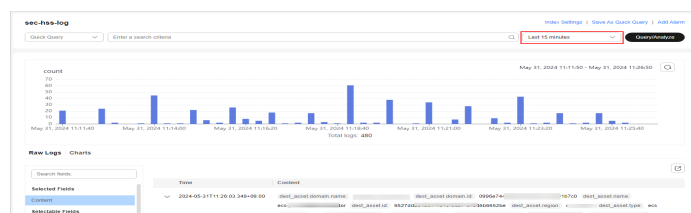
    - To view data of all fields at a specified time, click ⌄ in front of the time in the table to expand all data. By default, data is displayed in a table.

      To view data in JSON format, click the **JSON** tab. Data in JSON format is displayed on the page.

Figure 10-78 Expand to display data
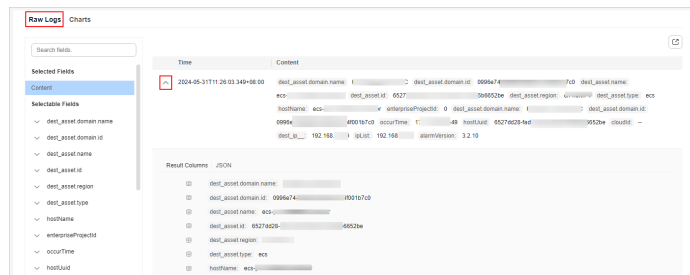
- To display or filter some fields in the list, select the fields to be displayed in the Available Fields area on the right and click ⊕ next to the field name. The fields are displayed in the log data list on the right.

Figure 10-79 Selected fields to be displayed
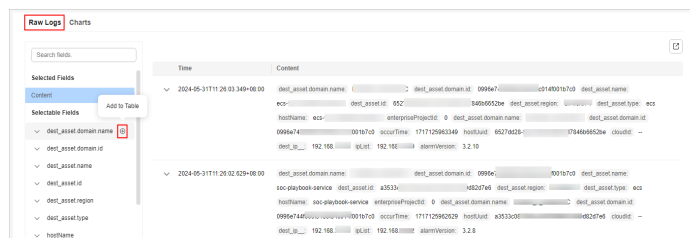
○ To adjust the field sequence: In the heading columns of the log data list on the right, select a field and then click ◄ or ► next to the field name to move the field left or right by one column with each click.

Figure 10-80 Adjusting field display sequence
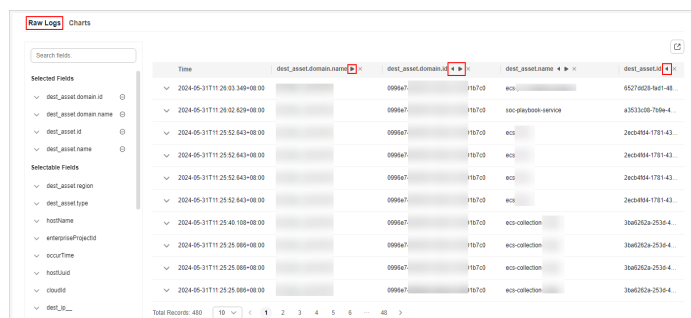
○ To cancel the display: In the table header column of the log data list on the right, select the target field, and click ✕ next to the field name, or click ⊖ next to the field name on the left.

Figure 10-81 Deselect
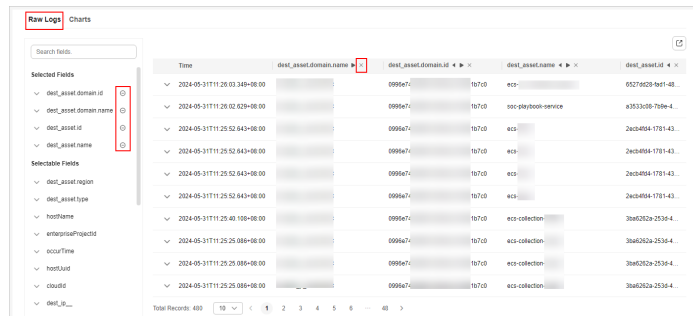
– To export logs: On the **Raw Logs** tab page, click ⬚ in the upper right corner of the page. The system automatically downloads raw logs to the local PC.

- **Charts**

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

  On the **Charts** tab, SecMaster provides query and analysis results in multiple chart types, such as tables, line charts, bar charts, and pie charts. For details, see **Viewing Results in a Chart**.

- **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 Alert 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 **Creating a Quick Query**.

10.5.4 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 10-32 Common fields

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

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

sec-waf-attack

Fields in WAF attack logs

Table 10-33 sec-waf-attack

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

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

sec-waf-access

Table 10-34 describes the fields in WAF access logs.

Table 10-34 sec-waf-access

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

Field	Type	Description
upstream_header_time	String	Time used by the backend server to receive the first byte of the response header
bind_ip	String	Retrieval IP address of the engine
engine_id	String	Unique ID of the engine
time_iso8601	Date	ISO 8601 time of the log
sni	String	Domain name requested through the SNI
tls_version	String	Version of the protocol used to establish an SSL connection
ssl_curves	String	List of curves supported by the client
ssl_session_reused	String	Whether an SSL session is reused ● **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 10-35 sec-obs-access

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

Field	Type	Description
ctx_request_id	String	Request ID, which uniquely identifies a request to be traced.
request_method	String	Request method (GET/POST).
remote_ip	String	Remote IP address, in the format of **Client IP address:Port number**.
operation	String	Operation type, for example, **GET.OBJECT**.
bucket_name	String	Bucket name.
object_name	String	Object name (file name).
query_string	String	Request query.
http_status	String	HTTP request status code, for example, 200.
content_length	String	Length of the requested content.
user_agent	String	Client agent.
storage_class	String	OBS storage class.
user_name	String	Username of the requester.
user_id	String	User ID of the requester.
domain_name	String	Domain name of the requester.
domain_id	String	Domain ID of the requester.
project_id	String	Project ID of the requester.
owner_domain_name	String	Tenant name of the bucket owner.
owner_domain_id	String	Tenant ID of the bucket owner.
owner_project_id	String	Project ID of the bucket owner.
transmission_type	String	Network type. The value can be: • **1**: intranet • **2**: public network
scheme	String	Network protocol.
http_version	String	HTTP version.
host	String	OBS domain name.
port	String	Port number.
auth_v2_v4	String	Authentication mode.
host_type	String	Access type.

Field	Type	Description
x_forwarded_for	String	IP address of the proxy client.
pub_bkt	String	Whether the bucket is accessed anonymously.
pub_obj	String	Whether an object is accessed anonymously.
website_req	String	Whether the request is a website request.
crr_req	String	Whether the request is a CRR request.
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_type	String	Response object type.
total_bytes_sent	String	Total bytes of sent content in the response header and response body.
referrer	String	Reference page.
index_read_count	String	Metadata table query latency.
persistence_read_count	String	Number of times that data is read.
vpc_id	String	ID of the VPC to which the request client belongs.
access_with_security_token	String	Access using the STS token.
copy_size	String	Copy size.

Field	Type	Description
vpcep_traffic	String	Transmission through VPCEP.
access_key	String	AK.

sec-nip-attack

Fields in IPS attack logs

Table 10-36 sec-nip-attack

Field	Type	Description
SyslogId	String	Log serial number (SN).
Vsys	String	Virtual system name.
Policy	String	Name of a security policy.
SrcIp	String	Source IP address of a packet.
DstIp	String	Destination IP address of a packet.
SrcPort	String	Source port of a packet. For an ICMP packet, the value of this field is **0**.
DstPort	String	Destination port of a packet. For an ICMP packet, the value of this field is **0**.
SrcZone	String	Source security zone of a packet.
DstZone	String	Destination security zone of a packet.
User	String	Username.
Protocol	String	Protocol of the packet detected by a signature.
Application	String	Application that the packet detected by a signature belongs to.
Profile	String	Name of a configuration file.
SignName	String	Name of a signature.
SignId	String	ID of a signature.
EventNum	String	The field is used for log mergence. Whether logs are merged is determined by the mergence frequency and conditions. The value is **1** if logs are not merged.

Field	Type	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

Table 10-37 sec-iam-audit

Field	Type	Description
uid	String	User ID
un	String	Username
did	String	Domain ID
dn	String	Domain name
src	String	Request domain name
opl	String	Operation level
op	String	Operation type
res	String	IAM service invoking result
ter	String	Source IP address
dtl	String	IAM authentication details
tn	Date	Occurrence time
ts	Long	Timestamp when the IAM service is invoked
tid	String	Trace ID
evnt	String	Incident
tobj	String	Service

sec-hss-vul

Fields in HSS vulnerability scanning results

Table 10-38 sec-hss-vul

Field	Type	Description
agentUuid	String	Agent UUID.
alarmCsn	String	Alert UUID, which is randomly generated when the master generates an alert.
alarmKey	String	Alert keyword. For an alert, it is the **msg_id** reported by the transparent transmission agent. For a vulnerability, it is generated by the master.
alarmVersion	String	Agent version.

Field		Type	Description
occurTime		Int64	Vulnerability detection time (ms).
severity		Int32	Vulnerability level defined by HSS.
hostUuid		String	UUID of the affected host.
hostName		String	Name of the affected host.
hostIp		String	Communication IP address of the affected host.
ipList		String	List of IP addresses of affected hosts.
cloudId		String	Cloud agent SN.
region		String	Region where the affected host is located.
projectId		String	ID of the affected tenant.
enterpriseProjectId		String	ID of the affected enterprise tenant.
appendInfo		Object	Vulnerability details.
appendInfo	vulId	String	Official vulnerability ID.
	type	Int32	Vulnerability type. The value can be: ● **0**: Linux ● **1**: Windows ● **2**: Web CMS
	repairNecessity	Int32	Necessity level of vulnerability fixing. The value can be: ● **1**: low-risk ● **2&3**: medium-risk ● **4**: high risk
	status	Int32	Reserved field.
	cve_ids	String	CVE ID list. Use commas (,) to separate CVE IDs.
	url	String	URL of the official website where the vulnerability details are available.
	vulNameEn	String	Vulnerability name in English.
	vulNameCn	String	Vulnerability name in Chinese.

Field		Type	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**.
	agentId	String	UUID of the associated host agent.
	projectId	String	ID of the affected tenant.

sec-hss-alarm

Fields in HSS alert logs

Table 10-39 sec-hss-alarm

Field		Type	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.
alarmVersion		String	Agent version.
occurTime		Long	Incident occurrence time (accurate to millisecond).
severity		Long	Severity.
hostUuid		String	UUID of the affected host.
hostName		String	Name of the affected host.
hostIp		String	Communication IP address of the affected host.
ipList		String	List of IP addresses of affected hosts.
cloudId		String	Cloud agent SN.
region		String	Region where the affected host is located.
projectId		String	ID of the affected tenant.
enterpriseProjectId		String	ID of the affected enterprise tenant.
appendInfo		Object	Alert details.
appendInfo	agent_id	String	Agent ID.
	version	String	Incident version.
	container_name	String	Container ID (in container security scenarios).
	image_name	String	Image name (in container security scenarios).
	event_id	String	Incident ID (GUID).
	event_name	String	Incident name.
	event_classid	String	Unique incident ID.

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

Field			Type	Description
		host_name	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_version	String	OS version.
	network_info	local_address	String	Local address.
		local_port	Integer	Local port.
		remote_address	String	Remote address.
		remote_port	Integer	Remote port.
		src_ip	String	Source IP address.
		src_port	Integer	Source port.
		src_domain	String	Source domain.
		dest_ip	String	Destination IP address.
		dest_port	Integer	Destination port.
		dest_domain	String	Destination domain.
		protocol	String	Protocol.
		app_protocol	String	Application layer protocol.

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

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

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

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

sec-hss-log

Fields in HSS security logs

Table 10-40 sec-hss-log

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

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

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

Field			Type	Description
		cloud_id	String	Cloud agent SN.
		vm_name	String	VM name.
		vm_uuid	String	VM UUID.
		container _id	String	Container ID.
		image_id	String	Image ID.
		sys_arch	String	System CPU architecture.
		os_bit	String	OS bit version.
		os_type	String	OS type.
		os_name	String	OS name.
		os_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			Type	Description
		domain_name	String	DNS domain name.
		url_path	String	URL.
		url_method	String	URL method.
		req_refer	String	URL request referrer.
		email_subject	String	Email subject.
		email_sender	String	Email sender.
		email_receiver	String	Email recipient.
		email_keyword	String	Email keyword.
	process_info	process_name	String	Process name.
		process_path	String	Process file path.
		process_pid	Integer	Process ID.
		process_uid	Integer	Process user ID.
		process_username	String	Process username.
		process_cmdline	String	Process file command line.
		process_filename	String	Process file name.
		process_start_time	Long	Process start time.
		process_gid	Integer	Process group ID.
		process_egid	Integer	Effective process group ID.
		process_euid	Integer	Effective process user ID.

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

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

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

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

sec-ddos-attack

Fields in Anti-DDoS attack logs

Table 10-41 sec-ddos-attack

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

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

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

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

sec-cts-audit

Fields in CTS logs

Table 10-42 sec-cts-audit

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

Field	Type	Description
trace_name	String	Operation name.
trace_rating	String	Level of an operation incident. The options are as follows: ● **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	Type	Description
user_agent	String	Type of OBS bucket-related operations that are not invoked using OBS SDKs.
content_length	Long	Length of the request body for performing operations on OBS buckets.
total_time	Long	Response time of the request in OBS bucket-related operations.

sec-cfw-risk

Fields in CFW attack event logs

Table 10-43 sec-cfw-risk

Field	Type	Description
event_time	Date	Attack time
action	String	Response action of CFW • **permit** • **deny**
app	String	Application type
attack_rule	String	Defense rule that works for the detected attack
attack_rule_id	String	ID of the defense rule that works for the detected attack

Field	Type	Description
attack_type	String	Type of the attack • Vulnerability exploit • Vulnerability scan • Trojan • Worms • Phishing • Web attacks • Application DDoS • Buffer overflow • Password attacks • Mail • Access control • Hacking tools • Hijacking • Protocol exception • Spam • Spyware • DDoS flood • Suspicious DNS activities • Other suspicious behaviors
dst_ip	String	Destination IP address
dst_port	String	Destination port number
packet	String	Original data packet of the attack log
protocol	String	Protocol type
level	String	Level of detected threats • **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	Type	Description
direction	String	Flow direction • **out2in**: inbound • **in2out**: outbound

sec-cfw-flow

Fields in CFW traffic logs

Table 10-44 sec-cfw-flow

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

sec-cfw-block

Fields in CFW access control logs

Table 10-45 sec-cfw-block

Field	Type	Description
hit_time	Date	Time of access

Field	Type	Description
action	String	Response action of CFW ● **permit** ● **deny**
app	String	Application type
dst_ip	String	Destination IP address
dst_port	String	Destination port number
protocol	String	Protocol type
rule_id	String	ID of the triggering rule
src_ip	String	Source IP address
src_port	String	Source port number

sec-apig-access

Fields in API Gateway access logs

Table 10-46 sec-apig-access

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

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

sec-dbss-alarm

Fields in DBSS alert logs

Table 10-47 dbss-alarm

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

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

sec-dsc-alarm

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

Table 10-48 AK SK leakage (aksk_leakage)

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

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

Table 10-49 Risky OBS bucket files (obs_risk)

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

Table 10-50 Sensitive data fields (db_risk)

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

10.5.5 Quickly Adding a Log Alert Model

Scenario

You can configure alert models for query and analysis results. In doing this, the model can generate alerts when the results match the trigger conditions.

This topic describes how to quickly configure alarm models for logs.

Prerequisites

Data access has been completed. For details, see **Data Integration**.

Quickly Adding a Log Alert Model

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
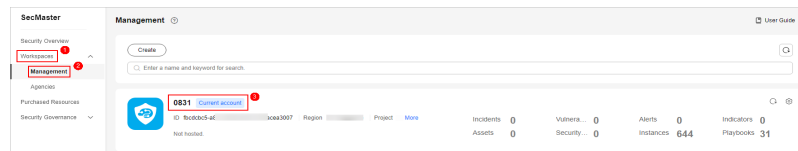
**Step 5** In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-83 Accessing the Security Analysis tab page
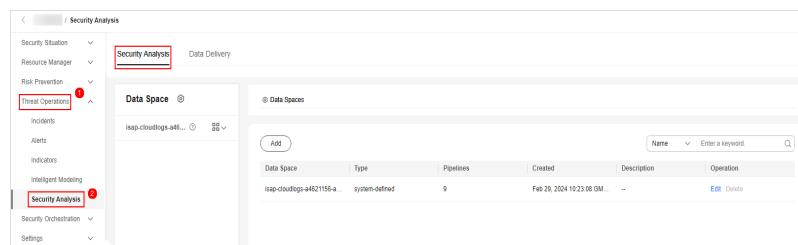
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.
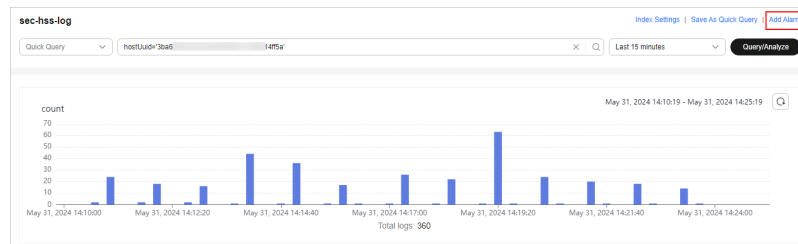
Figure 10-84 Pipeline data page
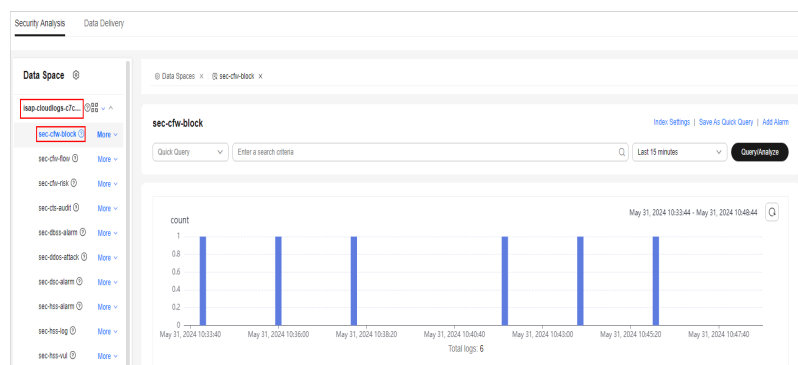
Step 7 Enter the query analysis statement, set the time range, and click **Query/Analyze**. The query analysis result is displayed.

For details, see **Querying and Analyzing Logs**.

Step 8 Click **Add Alarm** in the upper right corner of the page. The **Create Alarm Model** page is displayed.

Figure 10-85 Add Alarm

Step 9 Configure basic alarm information by referring to **Table 10-51**.

Table 10-51 Basic parameters of an alarm model

Parameter	Description
Pipeline Name	The pipeline where the alert model is executed, which is generated by the system by default.
Model Name	Name of the alarm model.
Severity	Severity of alarms reported by the alarm model. You can set the severity to **Critical**, **High**, **Medium Low**, or **Informative**.
Alarm Type	Alarm type displayed after the alarm model is triggered.
Model Type	The default value is **Rule model**.
Description	Enter the description of the alarm model.
Status	The alarm model status. You can change the alarm model status after the model is configured.

Step 10 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 11 Set the model logic. For details about the parameters, see **Table 10-52**.

Table 10-52 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result. A query analysis statement consists of a query statement and an analysis statement. The format is **Query Statement|Analysis Statement**. For details about the syntax of query analysis statements, see **Query and Analysis Syntax Overview**. **NOTE** If the reserved field is of the text type, **MATCH_QUERY** is used for word segmentation queries by default.
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 trigger conditions, click **Add** and add them. A maximum of five trigger conditions can be added. If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition from top to bottom and generates all types of alerts for hit trigger conditions.

Parameter	Description
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. ● If **Suppression** is enabled, the **query stops** after an alert is generated. ● If **Suppression** is disabled, the **query is not stopped** after an alert is generated.

Step 12 After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.

Step 13 After confirming that the preview is correct, click **OK** in the lower right corner of the page to confirm the configuration.

----End

10.5.6 Viewing Results in a Chart

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 types of charts:

- **Displaying Query and Analysis Results in a Table**
- **Displaying Query and Analysis Results in a Line Chart**
- **Displaying Query and Analysis Results in a Bar Chart**
- **Displaying Query and Analysis Results in a Pie Chart**

Procedure for Viewing Results in a Chart

The query and analysis results can be displayed in a table, line chart, bar chart, or pie chart.

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
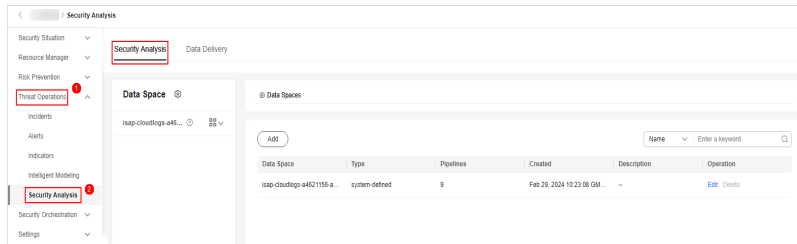
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-86 Workspace management page
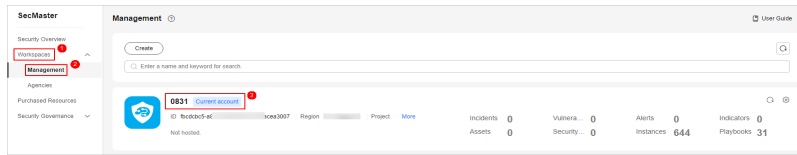
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-87 Accessing the Security Analysis tab page

Step 6 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 10-88 Pipeline data page
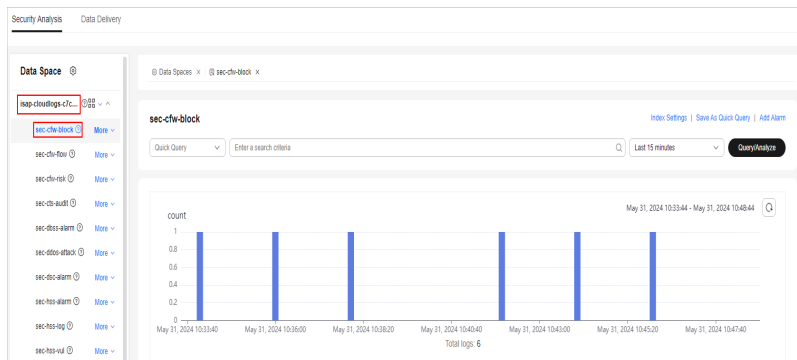
Step 7 Enter the query and analysis statement, set the time range, and click **Query/Analyze**.

Step 8 Select a chart type you need to display the query and analysis results.

- Displaying query and analysis results in a table

  Tables are the most commonly used method to display and analyze data. In SecMaster, the data results of query and analysis statements are displayed in tables by default.

  Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

  Configure table parameters.

Table 10-53 Table parameters

Parameter Category	Parameter	Description
Base Settings	Title	Customized table title.
Chart Settings	Hidden Fields	The field you want to hide it in the table.

After the chart is configured, you can preview analysis results on the left.

- Displaying query and analysis results 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.

  Click the **Charts** tab. In the **Chart Type** area on the right of the page, click ～.

  Configure line chart parameters.

Table 10-54 Line chart parameters

Parameter 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	Whether to display the legend.
	Position	This parameter is mandatory when you choose to show the legend. Position of the legend in the chart. The options are **Top**, **Bottom**, **Left**, and **Right**.

After the chart is configured, you can preview analysis results on the left.

- Displaying query and analysis results in a bar chart

  A bar chart presents categorical data with rectangular bars. It can be used to compare data and analyze trends. In SecMaster, a bar chart uses vertical bars (the width is fixed and the height indicates the value) to display data by default.

  Click the **Charts** tab. In the **Chart Type** area on the right of the page, click ⅼⅼⅼ.

Configure bar chart parameters.

Table 10-55 Bar chart parameters

Parameter 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	Whether to display the legend.
	Position	This parameter is mandatory when you choose to show the legend. Position of the legend in the chart. The options are **Top**, **Bottom**, **Left**, and **Right**.

After the chart is configured, you can preview analysis results on the left.

- Displaying query and analysis results in a pie chart

  A pie chart shows the proportion of different categories. Different categories are compared by radian.

  Click the **Charts** tab. In the **Chart Type** area on the right of the page, click
  .

  Configure pie chart parameters.

Table 10-56 Pie chart parameters

Parameter Category	Parameter	Description
Base Settings	Title	Customized line chart title.
Chart Settings	Classify	Data classification.
	Column Value	The value corresponding to the categorized data.
Legend	Show Legend	Whether to display the legend.

Parameter Category	Parameter	Description
	Position	This parameter is mandatory when you choose to show the legend. Position of the legend in the chart. The options are **Top**, **Bottom**, **Left**, and **Right**.

After the chart is configured, you can preview the analysis result on the left.

----End

10.5.7 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**.

Downloading Logs

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
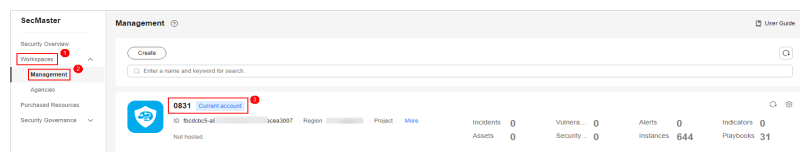
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-90 Accessing the Security Analysis tab page
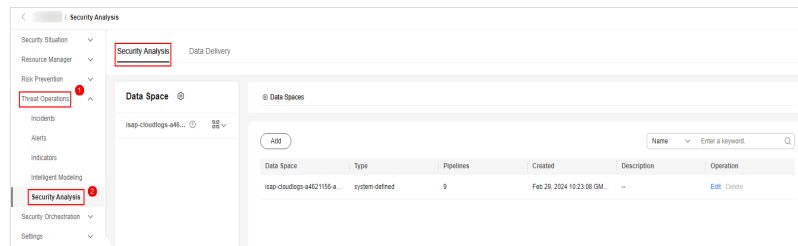
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-91 Pipeline data page
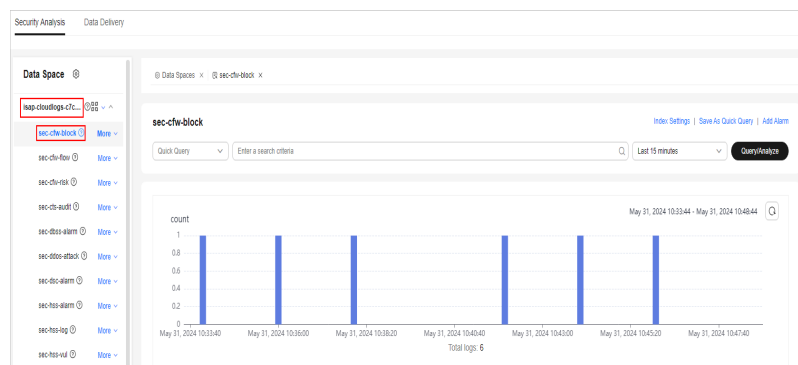
Step 7 (Optional) On the pipeline data retrieval page, enter the search criteria, select a time range, and click **Query/Analyze**.

Step 8 Download logs.

- Raw logs: On the **Raw Logs** tab page, click ⬚. The system downloads logs to the local PC.

- Chart logs: On the **Charts** tab page, click **Download**. The system downloads the logs to the local PC.

----End

10.5.8 Managing Data Spaces

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.

This topic describes how to manage data spaces.

- **Adding a Data Space**: If you need to use security analysis, data analysis, and intelligent modeling features in SecMaster, you need to create a data space.

- **Viewing Data Space Details**: You can view the details about a data space, including its name, type, and creation time.

- **Editing a Data Space**: You can modify the details about a data space after it is created.

- **Deleting a Data Space**: If you no longer need a data space, you can delete it.

Limitations and Constraints

- Adding data spaces

  A maximum of five data spaces can be created in a workspace in a region for an account.

- Deleting data spaces

  - The default data space created by the system cannot be deleted.
  - If there are pipelines in a data space, the data space cannot be deleted directly. You need to delete the pipelines before deleting the data space.

Adding a Data Space

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-92 Workspace management page
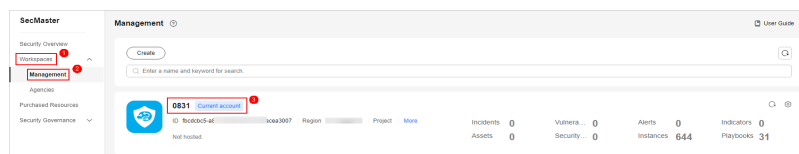
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-93 Accessing the Security Analysis tab page
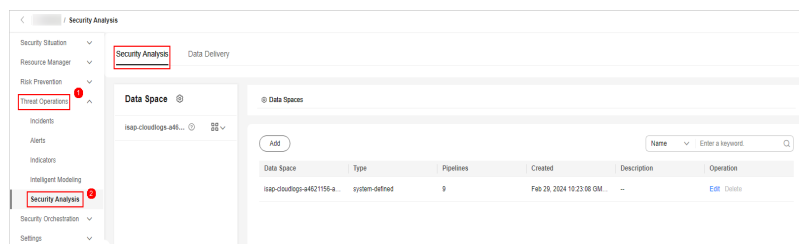
Step 6 In the upper left corner of the data space list, click **Add**. The **Add Data Space** page is displayed on the right.

Figure 10-94 Add Data Space

Step 7 On the **Add Data Space** page, set the parameters for the new data space. For details about the parameters, see **Table 10-57**.

Table 10-57 Parameters for adding a data space

Parameter	Description
Data Space	Data space name. The naming rules are as follows: ● The name can contain 5 to 63 characters. ● The name can contain letters, numbers, and hyphens (-). The name cannot start or end with a hyphen (-) or contain consecutive hyphens (-). ● The name must be unique on Huawei Cloud and cannot be the same as any other data space name.
Description	(Optional) Remarks of the data space.

Step 8 Click **OK**. The data space is added.

You can view the new data space in the data space list.

----End

Viewing Data Space Details

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
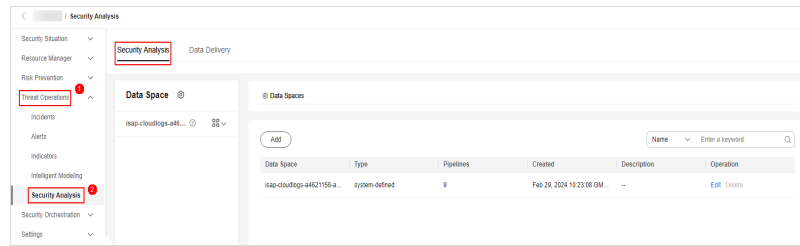
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-95 Workspace management page
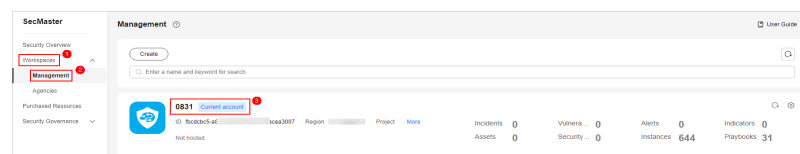
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

**Figure 10-96** Accessing the Security Analysis tab page

Step 6 On the **Data Spaces** page, view all data space information. **Table 10-58** describes related parameters.

Table 10-58 Data Space

Parameter	Description
Data Space	Data space name.
Type	Type of data in the data space. It can be: • **system-defined**: The data space is created by the system by default during data access. • **user-defined**: The data space is created by users.
Pipelines	Number of pipelines in the data space.
Created	Time the data space was created.
Description	Description of the data space.
Operation	You can edit and delete a data space in the **Operation** column.

Step 7 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 10-97 Data space details
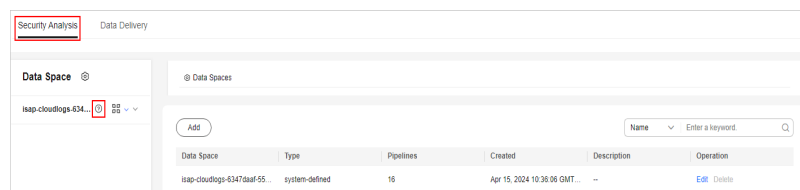
Step 8 On the data space details panel, you can view details about a data space. For details about the parameters, see **Table 10-59**.

Table 10-59 Data space details

Parameter	Description
Data Space	Data space name.
Pipelines	Number of pipelines in the data space.

Parameter	Description
Created	Time the data space was created.
Description	Description of the data space.

----End

Editing a Data Space

Step 1 Log in to the management console.

Step 2 Click ⬢ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-98 Workspace management page

Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-99 Accessing the Security Analysis tab page

Step 6 Locate the row that contains the target data space, and click **Edit** in the **Operation** column.

Figure 10-100 Edit Data Space

Step 7 In the displayed **Edit Data Space** dialog box, modify the data space details.

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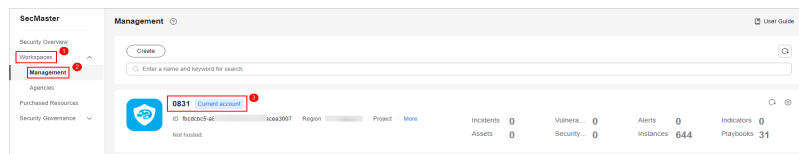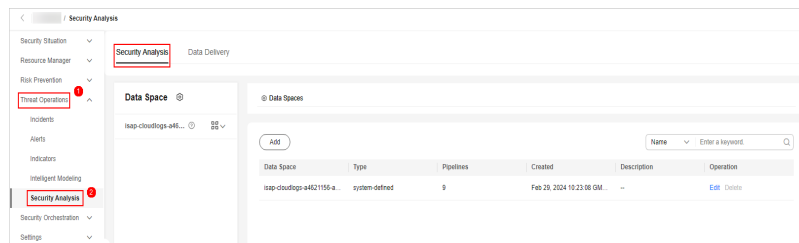
----End

Deleting a Data Space

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.
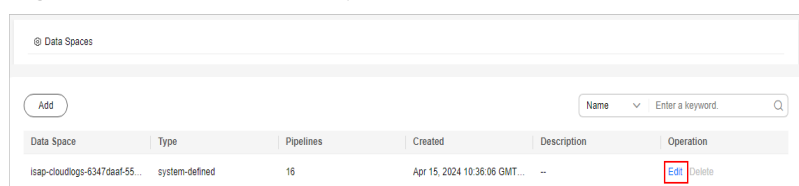
Figure 10-101 Workspace management page
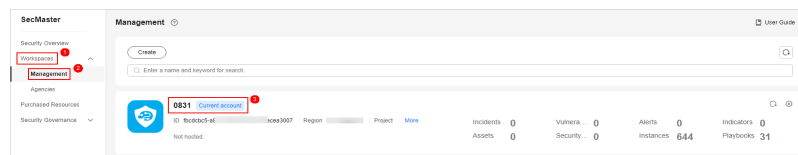
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-102 Accessing the Security Analysis tab page
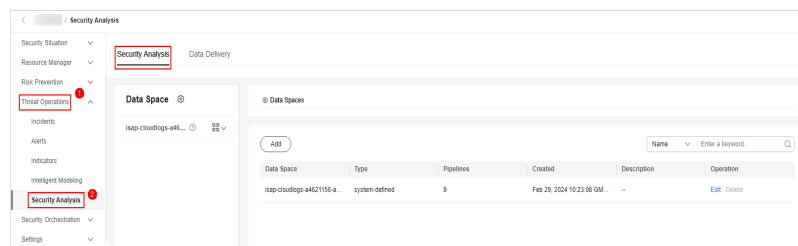
Step 6 In the row containing the target data space, click **Delete** in the **Operation** column.

Figure 10-103 Delete Data Space
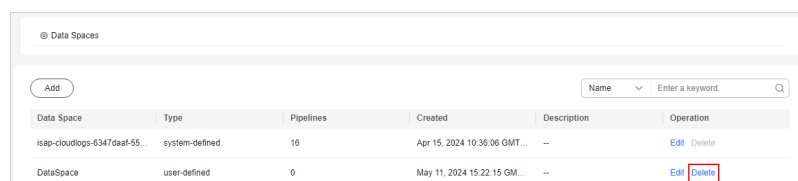
Step 7 In the dialog box displayed, click **OK**.

> ⚠️ **CAUTION**
>
> If there are pipelines in a data space, the data space cannot be deleted directly. You need to delete the pipelines before deleting the data space.

----End

10.5.9 Managing Pipelines

A data transfer message topic and a storage index form a pipeline. This topic describes how to manage data pipelines. You can:

- **Creating a Pipeline**: If you need to use security analysis, data analysis, and intelligent modeling features in SecMaster, you need to create pipelines.
- **Viewing Pipeline Details**: You can view the pipeline details, including the pipeline name, data space, and creation time.
- **Editing a Pipeline**: You can modify the pipeline information, such as the number of shards, description, and lifecycle.
- **Deleting a Pipeline**: You can delete a pipeline. Data in the pipeline will also be deleted and cannot be restored. Exercise caution when performing this operation.

Limitations and Constraints

- A maximum of 20 pipelines can be created in a data space in a region for an account.
- Pipelines created by the system **cannot be edited**.
- Pipelines created by the system **cannot be deleted**.

Creating a Pipeline

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-104 Workspace management page
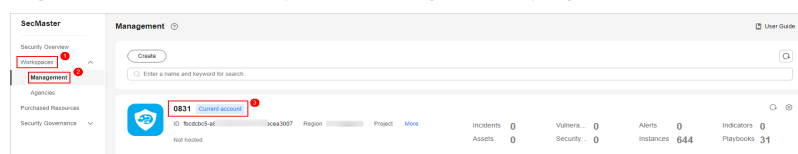
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-105 Accessing the Security Analysis tab page
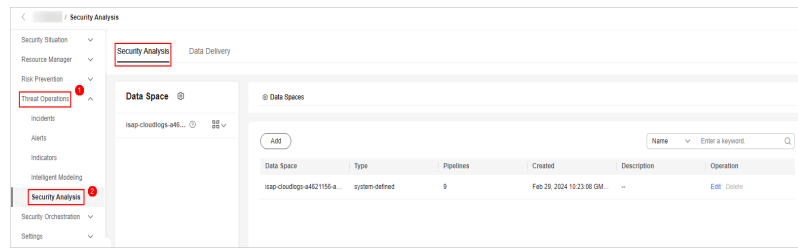
Step 6 (Optional) Add a data space. For details, see **Adding a Data Space**.

Step 7 In the data space navigation tree on the left, click ⊞ on the right of the data space name and select **Create Pipeline**.

Figure 10-106 Create Pipeline
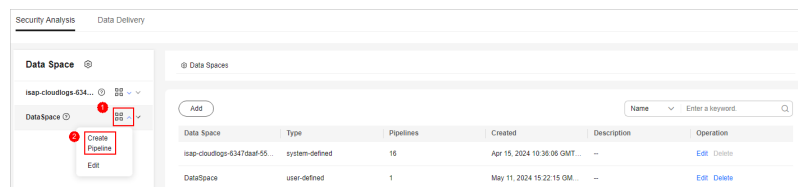
Step 8 On the **Create Pipeline** page, configure pipeline parameters. For details about the parameters, see **Table 10-60**.

Table 10-60 Parameters for creating a pipeline

Parameter	Description
Data Space	Data space the pipeline belongs to. This parameter is generated by the system by default.
Pipeline Name	Name of the pipeline. The naming rules are as follows: ● The name can contain 5 to 63 characters. ● The name can contain letters, numbers, and hyphens (-). The name cannot start or end with a hyphen (-) or contain consecutive hyphens (-). ● The name must be unique in the data space.
Shards	The number of shards of the pipeline. The value ranges from 1 to 64. An index can store a large amount of data that exceeds the hardware limits of a node. To solve this problem, Elasticsearch subdivides your index into multiple pieces called shards. When creating an index, you can specify the number of shards as required. Each shard is in itself a fully-functional and independent "index" that can be hosted on any node in the cluster.

Parameter	Description
Lifecycle	Lifecycle of data in the pipeline. Value range: 7 to 180
Description	Remarks on the pipeline. This parameter is optional.

Step 9 Click **OK**.

You can click the data space name or ▼ next to the data space to view the created pipeline.

----End

Viewing Pipeline Details

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-107 Workspace management page
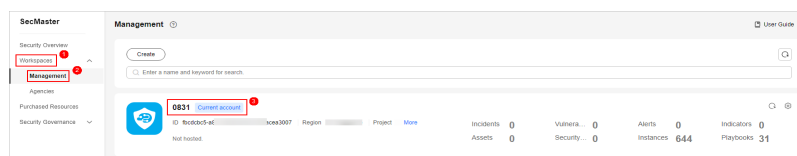
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-108 Accessing the Security Analysis tab page
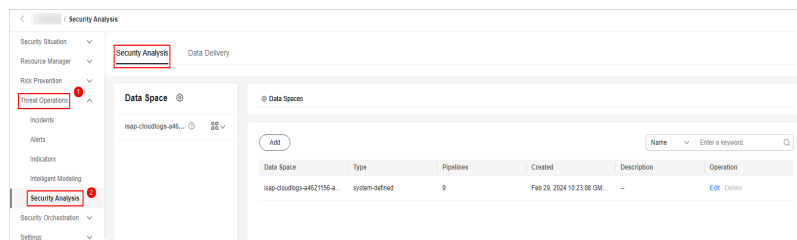
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list.

Figure 10-109 Viewing pipeline details

Step 7 Click ⑦ next to a pipeline name you want to view. The **Pipeline Details** pane is displayed on the right of the page.

Table 10-61 Pipeline parameters

Parameter	Description
Workspace Name	Name of the workspace to which the pipeline belongs.
Workspace ID	ID of the workspace to which the pipeline belongs.
Data Space Name	Name of the data space to which the pipeline belongs.
Data Space ID	ID of the data space to which the pipeline belongs.
Pipeline Name	Name of the pipeline.
Pipeline ID	ID of the pipeline.
Shards	Number of shards of the pipeline.
Lifecycle	Retention period of the data in the pipeline.
Created	Time when the pipeline was created.
Description	Description of the pipeline.

----End

Editing a Pipeline

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-110 Workspace management page
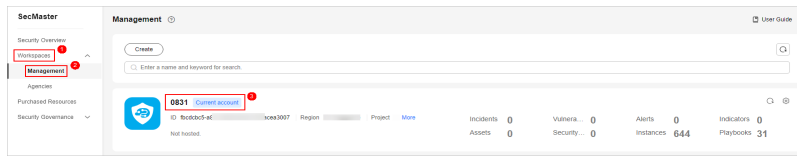
Step 5   In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-111 Accessing the Security Analysis tab page
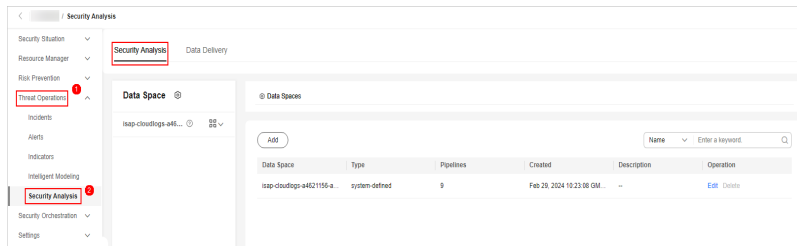
Step 6   In the data space navigation tree on the left, click a data space name to show the pipeline list.

Figure 10-112 Viewing pipeline details
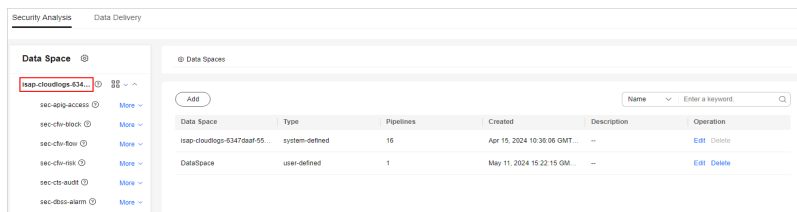
Step 7   Click **More** > **Edit** next to the pipeline name.

Figure 10-113 Entry for editing a pipeline
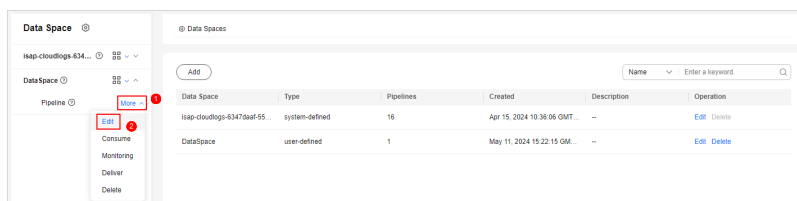
Step 8   On the **Edit Pipeline** page, configure pipeline parameters. For details about the parameters, see **Table 10-62**.

Table 10-62 Parameters for editing a pipeline

Parameter	Description
Data Space	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.

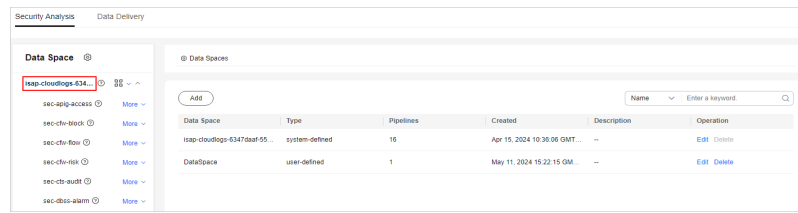| Parameter	Description
Shards	The number of shards of the pipeline. The value ranges from 1 to 64.
Lifecycle	Lifecycle of data in the pipeline. Value range: 7 to 180
Description	Remarks on the pipeline. This parameter is optional.

Step 9 Click **OK**.

----End

Deleting a Pipeline

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-114 Workspace management page
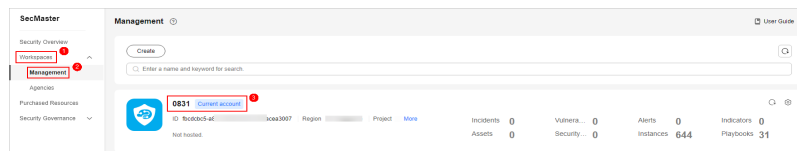
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-115 Accessing the Security Analysis tab page
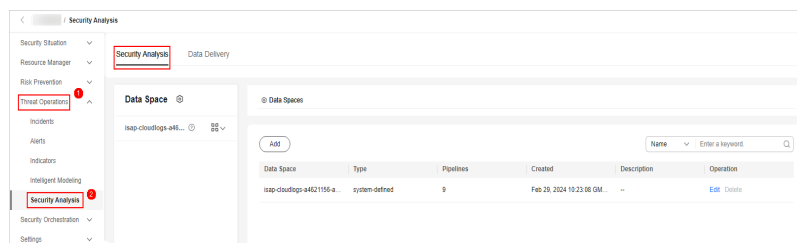
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list.

Figure 10-116 Viewing pipeline details
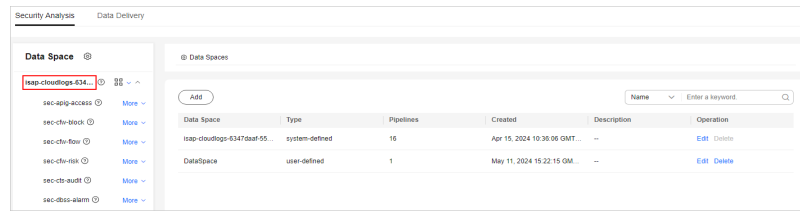
Step 7 Click **More** > **Delete** next to the pipeline name.

Figure 10-117 Deleting a pipeline
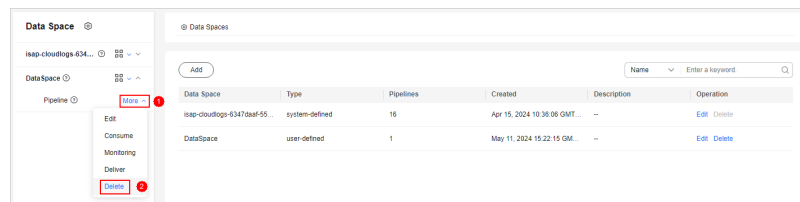
Step 8 In the dialog box displayed, click **OK**.

----End

10.5.10 Enabling 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
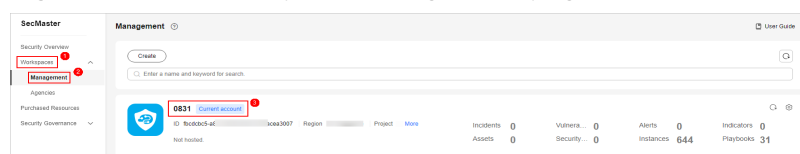
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

**Figure 10-119** Accessing the Security Analysis tab page
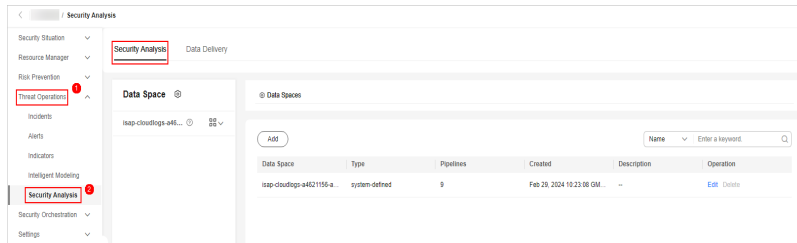
Step 6 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Consume**.

Figure 10-120 Accessing the data consumption page
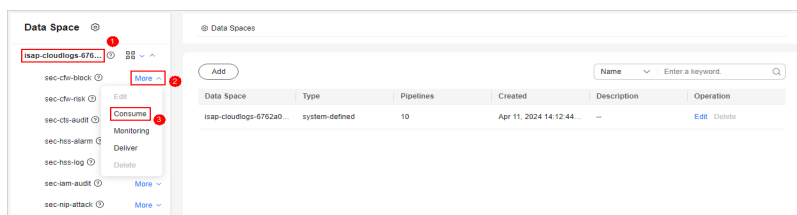
Step 7 On the Data Consumption page, click [toggle] next to Current Status to enable data consumption.

After the function is enabled, the consumption configuration information is displayed, as shown in **Table 10-63**.

Figure 10-121 Enabling Data Consumption
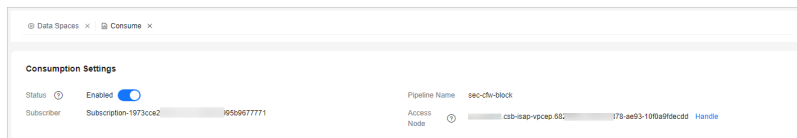
Table 10-63 Data consumption parameters

Parameter	Description
Status	Status of the data consumption function in the current pipeline
Pipeline Name	Name of the current pipeline
Subscriber	The preset subscription mode in the system. This parameter determines how data is transmitted to data consumers.
Access Node	Access node of the current data.

----End

Related Operations

After data consumption is enabled, you can click ![toggle] next to **Status** on the Data Consumption page to disable data consumption.

10.5.11 Enabling 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 ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

**Figure 10-122** Workspace management page
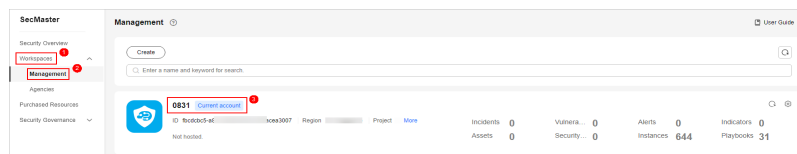
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-123 Accessing the Security Analysis tab page
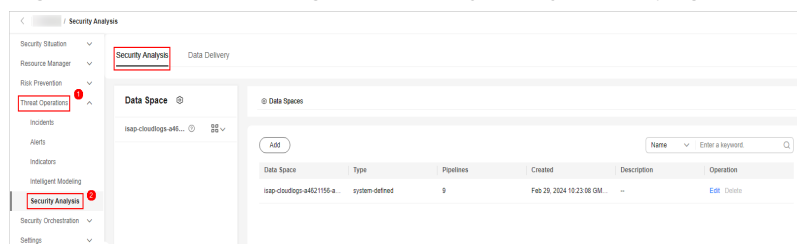
Step 6 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Monitoring**.

Figure 10-124 Data monitoring page
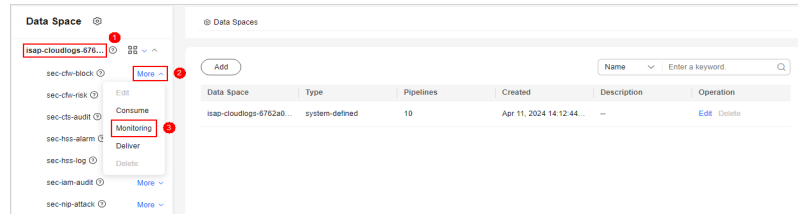
Step 7 On the pipeline monitoring page, view monitoring metrics.

Figure 10-125 Viewing monitored data
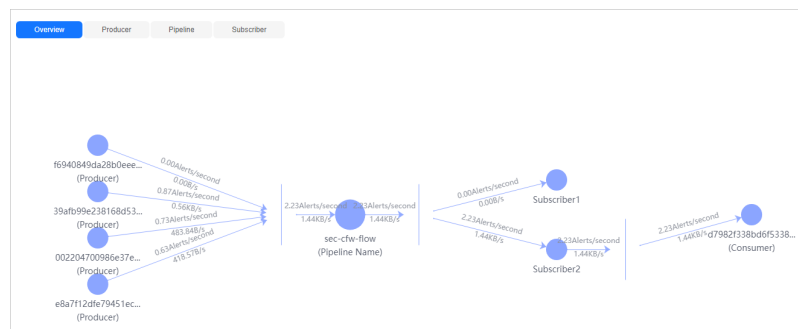
- **Overview**: Displays information such as the production rate between producers, pipelines, subscribers, and consumers in the current pipeline.

- **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 (B), pipeline production rate, pipeline consumption rate, average message size (KB), and offloaded message size (B) in a specified period (last 2/6/12/24 hours, last 7 days, or a customized period).

- Subscriber: displays the total consumption rate of subscribers, consumed data volume (B), consumed messages, and active consumers in a specified period (last 2/6/12/24 hours, last 7 days, or a user-defined period).

----End

10.6 Query and Analysis Syntax - V1

10.6.1 Query and Analysis Syntax Overview

This topic describes the query and analysis syntax used during security analysis. SecMaster supports SQL retrieval syntax. Query and analysis statements are used in the area shown in the following screenshot on the SecMaster console.

Figure 10-126 Entering a query and analysis statement
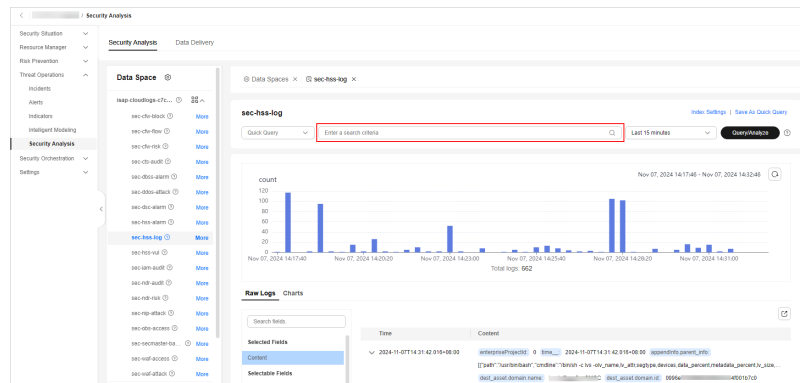
Basic Syntax

An SQL statement consists of a query statement and an analysis statement, which are separated by a vertical bar (|). Query statements can be used independently, but analysis statements must be used together with query statements.

Query Statement | Analysis Statement

Table 10-64 Basic Syntax

Statement Type	Description
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.
Analysis Statements	An analysis statement is used to calculate and collect statistics on query results.

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**.

10.6.2 Query Statements

A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.

This topic describes query statements and examples.

Syntax

A query statement can be in either of the following formats:

- If the value is only *, full data is returned without filtering.
- It consists of one or more query clauses. The clauses are connected by **NOT**, **AND**, and **OR**. **()** can be used to increase the priority of the query conditions in parentheses.

The basic structure of a query clause is as follows:

Field Name Operator Field Value

Operators lists the operators that can be used.

Operators

Table 10-65 Operator descriptions

Operator	Description
=	Queries logs in which the value of a field is equal to a certain value.
<>	Queries the logs in which the value of a field is not equal to a certain value.
>	Queries logs in which the value of a field is greater than a specified value.
<	Queries logs in which the value of a field is less than a specified value.
>=	Queries logs in which the value of a field is greater than or equal to a specified value.
<=	Queries logs in which the value of a field is less than or equal to a specified value.
IN	Queries the logs whose field values are within a specified value range.
BETWEEN	Queries the logs whose field values are in the specified range.
LIKE	Searches for logs of a field value in full text.
IS NULL	Queries logs whose field value is NULL.
IS NOT NULL	Query logs whose field value is NOT NULL.

Examples

Table 10-66 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

10.6.3 Analysis Statements

10.6.3.1 SELECT

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

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

Using * to query all fields.

```
SELECT *
```

Table 10-67 Using * to query all fields

account _numbe r	firstn ame	gend er	city	balanc e	emplo yer	state	lastna me	age
1	Amb er	M	Broga n	39225	Pyrami	IL	Duke	32
16	Hatti e	M	Dante	5686	Netag y	TN	Bond	36
13	Nane tte	F	Nogal	32838	Quility	VA	Bates	28
18	Dale	M	Orick	4180	null	MD	Adams	32

Querying a Specified Field

SELECT firstname, lastname

Table 10-68 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 10-69 Using AS to define field aliases

num
1
16
13
18

Using the DISTINCT Statement

SELECT DISTINCT age

Table 10-70 Using the DISTINCT statement

age
32
36
28

Using SQL Functions

For details about functions, see **Functions**.

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

Table 10-71 Using SQL functions

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

10.6.3.2 GROUP BY

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

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

Grouping by Field Value

```
SELECT age GROUP BY age
```

Table 10-72 Grouping by field value

age
28
32
36

Grouping by Field Alias

SELECT account_number AS num GROUP BY num

Table 10-73 Grouping by field alias

num
1
16
13
18

Grouping by Multiple Fields

SELECT account_number AS num, age GROUP BY num, age

Table 10-74 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 10-75 Using SQL functions

len	count
4	2
5	2

10.6.3.3 HAVING

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

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

Filters data based on grouping and **Aggregate Functions**.

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

Table 10-76 The HAVING function

age	MAX(balance)
28	32838
32	39225

10.6.3.4 ORDER BY

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

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

Sorting Data by Field Value

SELECT age ORDER BY age DESC

Table 10-77 Sorting by field value

age
28
32
32
36

10.6.3.5 LIMIT

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

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

Specifying the Number of Returned Records

```
SELECT * LIMIT 1
```

Table 10-78 Specifying the number of returned records

account_number	first name	gender	city	balance	employer	state	lastname	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32

Specifying the Number of Returned Records and Offsets

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

Table 10-79 Specifying the number of returned records and offsets

account_number	first name	gender	city	balance	employer	state	lastname	age
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36

10.6.3.6 Functions

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

This section describes functions.

Mathematics Functions

Table 10-80 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

Function	Purpose	Description	Example Value
divide	Division	divide(number T, number) -> T	SELECT divide(1, 0.5) LIMIT 1
e	Natural base number e	e() -> double	SELECT e() LIMIT 1
exp	Power of the natural base number e	exp(number T) -> T	SELECT exp(0.5) LIMIT 1
expm1	Subtract one from the power of the natural base number e.	expm1(number T) -> T	SELECT expm1(0.5) LIMIT 1
floor	Rounded down	floor(number T) -> T	SELECT floor(0.5) AS Rounded_Down LIMIT 1
ln	Returns the natural logarithm.	ln(number T) -> double	SELECT ln(10) LIMIT 1
log	Logarithm with T as the base	log(number T, number) -> double	SELECT log(10) LIMIT 1
log2	Logarithm with 2 as the base	log2(number T) -> double	SELECT log2(10) LIMIT 1
log10	Logarithm to base 10	log10(number T) -> double	SELECT log10(10) LIMIT 1
mod	Remainder	mod(number T, number) -> T	SELECT modulus(2, 3) LIMIT 1
multiply	Multiplication	multiply(number T, number) -> number	SELECT multiply(2, 3) LIMIT 1
pi	π	pi() -> double	SELECT pi() LIMIT 1
pow	T power of	pow(number T, number) -> T	SELECT pow(2, 3) LIMIT 1
power	T power of	power(number T) -> T, power(number T, number) -> T	SELECT power(2, 3) LIMIT 1
rand	Random number.	rand() -> number, rand(number T) -> T	SELECT rand(5) LIMIT 1
rint	Discard decimals.	rint(number T) -> T	SELECT rint(1.5) LIMIT 1

Function	Purpose	Description	Example Value
round	Round off	round(number T) -> T	SELECT round(1.5) LIMIT 1
sign	Symbol	sign(number T) -> T	SELECT sign(1.5) LIMIT 1
signum	Symbol	signum(number T) -> T	SELECT signum(0.5) LIMIT 1
sqrt	Square root	sqrt(number T) -> T	SELECT sqrt(0.5) LIMIT 1
subtract	Subtraction	subtract(number T, number) -> T	SELECT subtract(3, 2) LIMIT 1
/	Division	number / number -> number	SELECT 1 / 100 LIMIT 1
%	Remainder	number % number -> number	SELECT 1 % 100 LIMIT 1

Trigonometric Functions

Table 10-81 Trigonometric functions

Functions	Purpose	Description	Example Value
acos	Arc cosine	acos(number T) -> double	SELECT acos(0.5) LIMIT 1
asin	Arc sine	asin(number T) -> double	SELECT asin(0.5) LIMIT 1
atan	Inverse tangent	atan(number T) -> double	SELECT atan(0.5) LIMIT 1
atan2	T Arc tangent of the result of dividing U	atan2(number T, number U) -> double	SELECT atan2(1, 0.5) LIMIT 1
cos	Cosine	cos(number T) -> double	SELECT cos(0.5) LIMIT 1
cosh	hyperbolic cosine	cosh(number T) -> double	SELECT cosh(0.5) LIMIT 1
cot	Cotangent	cot(number T) -> double	SELECT cot(0.5) LIMIT 1
degrees	Converting radians into degrees	degrees(number T) -> double	SELECT degrees(0.5) LIMIT 1

Function s	Purpose	Description	Example Value
radians	Converting degrees into radians	radians(number T) -> double	SELECT radians(0.5) LIMIT 1
sin	Sine	sin(number T) -> double	SELECT sin(0.5) LIMIT 1
sinh	hyperbolic sine	sinh(number T) -> double	SELECT sinh(0.5) LIMIT 1
tan	Tangent	tan(number T) -> double	SELECT tan(0.5) LIMIT 1

Temporal Functions

Table 10-82 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

Function	Purpose	Description	Example Value
minute_of_hour	Number of minutes in the current hour	minute_of_hour(date) -> integer	SELECT minute_of_hour(date) LIMIT 1
minute_of_day	Number of minutes on the current day	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
monthname	Month Name	monthname(date) -> string	SELECT monthname(date) LIMIT 1
now	Current time.	now() -> time	SELECT now() LIMIT 1
second_of_minute	Number of seconds	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
timestamp	Date	timestamp(date) -> date	SELECT timestamp(date) LIMIT 1
year	Year	year(date) -> integer	SELECT year(date) LIMIT 1

Text Functions

Table 10-83 Text functions

Function	Purpose	Description	Example Value
ascii	ASCII value of the first character	ascii(string T) -> integer	SELECT ascii('t') LIMIT 1
concat_ws	Connection String	concat_ws(separator, string, string) -> string	SELECT concat_ws('-', 'Tutorial', 'is', 'fun!') LIMIT 1
left	Obtain a character string from left to right.	left(string T, integer) -> T	SELECT left('hello', 2) LIMIT 1
length	length	length(string) -> integer	SELECT length('hello') LIMIT 1
locate	Search for a string	locate(string, string) -> integer	SELECT locate('o', 'hello') LIMIT 1
replace	Replace strings	replace(string T, string, string) -> T	SELECT replace('hello', 'l', 'x') LIMIT 1

Function	Purpose	Description	Example Value
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
upper	Convert all letters into uppercase letters.	upper(string T) -> T	SELECT upper('helloworld') LIMIT 1

Other

Table 10-84 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

10.6.3.7 Aggregate Functions

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

This section describes some aggregate functions.

Table 10-85 Aggregate functions

Function	Purpose	Description	Example Value
avg	Average value	avg(number T) -> T	SELECT avg(age) LIMIT 1
sum	Sum	sum(number T) -> T	SELECT sum(age) LIMIT 1
min	Specifies the minimum value.	min(number T) -> T	SELECT min(age) LIMIT 1
max	Maximum value	max(number T) -> T	SELECT max(age) LIMIT 1
count	Occurrences	count(field) -> integer , count(*) -> integer , count(1) -> integer	SELECT count(age) LIMIT 1 , SELECT count(*) LIMIT 1 , SELECT count(1) LIMIT 1

10.7 Query and Analysis Syntax - V2

10.7.1 Query and Analysis Syntax Overview

This topic describes the query and analysis syntax used during security analysis. SecMaster supports SQL and SecMaster SQL retrieval syntax. Query and analysis statements are used in the area shown in the following screenshot on the SecMaster console.

Figure 10-127 Entering a query and analysis statement
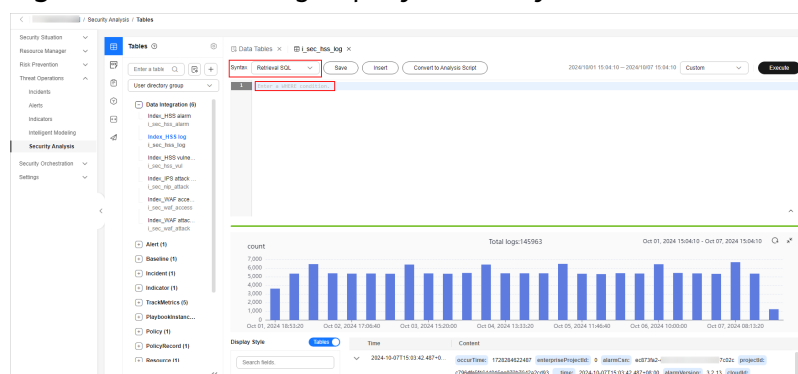
Select the query and analysis syntax as required.

- **Retrieval SQL Syntax Reference**
- **SecMaster SQL Syntax Reference**

10.7.2 Retrieval SQL Syntax Reference

10.7.2.1 Overview

Basic Syntax

An SQL statement consists of a query statement and an analysis statement, which are separated by a vertical bar (|). Query statements can be used independently, but analysis statements must be used together with query statements.

Query Statement | Analysis Statement

Table 10-86 Basic syntax

Statement Type	Description
Query Statement	A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.
Analysis Statement	An analysis statement is used to calculate and collect statistics on query results.

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.

10.7.2.2 Query Statements

A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.

This topic describes query statements and examples.

Syntax

A query statement can be in either of the following formats:

- If the value is only *, full data is returned without filtering.
- It consists of one or more query clauses. The clauses are connected by **NOT**, **AND**, and **OR**. **()** can be used to increase the priority of the query conditions in parentheses.

The basic structure of a query clause is as follows:

Field Name Operator Field Value

Operators lists the operators that can be used.

Operators

Table 10-87 Operator descriptions

Operator	Description
=	Queries logs in which the value of a field is equal to a certain value.
<>	Queries the logs in which the value of a field is not equal to a certain value.
>	Queries logs in which the value of a field is greater than a specified value.
<	Queries logs in which the value of a field is less than a specified value.
>=	Queries logs in which the value of a field is greater than or equal to a specified value.
<=	Queries logs in which the value of a field is less than or equal to a specified value.
IN	Queries the logs whose field values are within a specified value range.
BETWEEN	Queries the logs whose field values are in the specified range.
LIKE	Searches for logs of a field value in full text.
IS NULL	Queries logs whose field value is NULL.
IS NOT NULL	Query logs whose field value is NOT NULL.

Examples

Table 10-88 Example query statements

Query Requirement	Query Statement
All logs	*

Query Requirement	Query Statement
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

10.7.2.3 Analysis Statements

10.7.2.3.1 SELECT

Syntax of Analysis Statements

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

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

Using * to query all fields.

```
SELECT *
```

Table 10-89 Using * to query all fields

account _numbe r	firstn ame	gend er	city	balanc e	emplo yer	state	lastna me	age
1	Amb er	M	Broga n	39225	Pyrami	IL	Duke	32
16	Hatti e	M	Dante	5686	Netag y	TN	Bond	36
13	Nane tte	F	Nogal	32838	Quility	VA	Bates	28
18	Dale	M	Orick	4180	null	MD	Adams	32

Querying a Specified Field

SELECT firstname, lastname

Table 10-90 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 10-91 Using AS to define field aliases

num
1
16
13
18

Using the DISTINCT Statement

SELECT DISTINCT age

Table 10-92 Using the DISTINCT statement

age
32
36
28

Using SQL Functions

For details about functions, see **Functions**.

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

Table 10-93 Using SQL functions

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

10.7.2.3.2 GROUP BY

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]
```

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

Grouping by Field Value

```
SELECT age GROUP BY age
```

Table 10-94 Grouping by field value

age
28
32

age
36

Grouping by Field Alias

SELECT account_number AS num GROUP BY num

Table 10-95 Grouping by field alias

num
1
16
13
18

Grouping by Multiple Fields

SELECT account_number AS num, age GROUP BY num, age

Table 10-96 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 10-97 Using SQL functions

len	count
4	2
5	2

10.7.2.3.3 HAVING

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]
```

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

Filters data based on grouping and **Aggregate Functions**.

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

Table 10-98 The HAVING function

age	MAX(balance)
28	32838
32	39225

10.7.2.3.4 ORDER BY

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]
```

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

Sorting Data by Field Value

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

Table 10-99 Sorting by field value

age
28
32
32
36

10.7.2.3.5 LIMIT

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]
```

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

Specifying the Number of Returned Records

SELECT * LIMIT 1

Table 10-100 Specifying the number of returned records

account _numb er	first nam e	gende r	city	balan ce	emplo yer	state	lastna me	age
1	Amb er	M	Broga n	39225	Pyrami	IL	Duke	32

Specifying the Number of Returned Records and Offsets

SELECT * LIMIT 1 OFFSET 1

Table 10-101 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	M	Dante	5686	Netag y	TN	Bond	36

10.7.2.3.6 Functions

Mathematics Functions

Table 10-102 Mathematics Functions

Function	Purpose	Description	Example Value
abs	Absolute value	abs(number T) -> T	SELECT abs(0.5) LIMIT 1

Function	Purpose	Description	Example Value
add	Addition	add(number T, number) -> T	SELECT add(1, 5) LIMIT 1
cbrt	Cubic root	cbrt(number T) -> T	SELECT cbrt(0.5) LIMIT 1
ceil	Rounded up	ceil(number T) -> T	SELECT ceil(0.5) LIMIT 1
divide	Division	divide(number T, number) -> T	SELECT divide(1, 0.5) LIMIT 1
e	Natural base number e	e() -> double	SELECT e() LIMIT 1
exp	Power of the natural base number e	exp(number T) -> T	SELECT exp(0.5) LIMIT 1
expm1	Subtract one from the power of the natural base number e.	expm1(number T) -> T	SELECT expm1(0.5) LIMIT 1
floor	Rounded down	floor(number T) -> T	SELECT floor(0.5) AS Rounded_Down LIMIT 1
ln	Returns the natural logarithm.	ln(number T) -> double	SELECT ln(10) LIMIT 1
log	Logarithm with T as the base	log(number T, number) -> double	SELECT log(10) LIMIT 1
log2	Logarithm with 2 as the base	log2(number T) -> double	SELECT log2(10) LIMIT 1
log10	Logarithm to base 10	log10(number T) -> double	SELECT log10(10) LIMIT 1
mod	Remainder	mod(number T, number) -> T	SELECT modulus(2, 3) LIMIT 1
multiply	Multiplication	multiply(number T, number) -> number	SELECT multiply(2, 3) LIMIT 1
pi	π	pi() -> double	SELECT pi() LIMIT 1
pow	T power of	pow(number T, number) -> T	SELECT pow(2, 3) LIMIT 1
power	T power of	power(number T) -> T, power(number T, number) -> T	SELECT power(2, 3) LIMIT 1

Function	Purpose	Description	Example Value
rand	Random number.	rand() -> number, rand(number T) -> T	SELECT rand(5) LIMIT 1
rint	Discard decimals.	rint(number T) -> T	SELECT rint(1.5) LIMIT 1
round	Round off	round(number T) -> T	SELECT round(1.5) LIMIT 1
sign	Symbol	sign(number T) -> T	SELECT sign(1.5) LIMIT 1
signum	Symbol	signum(number T) -> T	SELECT signum(0.5) LIMIT 1
sqrt	Square root	sqrt(number T) -> T	SELECT sqrt(0.5) LIMIT 1
subtract	Subtraction	subtract(number T, number) -> T	SELECT subtract(3, 2) LIMIT 1
/	Division	number / number -> number	SELECT 1 / 100 LIMIT 1
%	Remainder	number % number -> number	SELECT 1 % 100 LIMIT 1

Trigonometric Functions

Table 10-103 Trigonometric functions

Functions	Purpose	Description	Example Value
acos	Arc cosine	acos(number T) -> double	SELECT acos(0.5) LIMIT 1
asin	Arc sine	asin(number T) -> double	SELECT asin(0.5) LIMIT 1
atan	Inverse tangent	atan(number T) -> double	SELECT atan(0.5) LIMIT 1
atan2	T Arc tangent of the result of dividing U	atan2(number T, number U) -> double	SELECT atan2(1, 0.5) LIMIT 1
cos	Cosine	cos(number T) -> double	SELECT cos(0.5) LIMIT 1
cosh	hyperbolic cosine	cosh(number T) -> double	SELECT cosh(0.5) LIMIT 1
cot	Cotangent	cot(number T) -> double	SELECT cot(0.5) LIMIT 1

Function s	Purpose	Description	Example Value
degrees	Converting radians into degrees	degrees(number T) -> double	SELECT degrees(0.5) LIMIT 1
radians	Converting degrees into radians	radians(number T) -> double	SELECT radians(0.5) LIMIT 1
sin	Sine	sin(number T) -> double	SELECT sin(0.5) LIMIT 1
sinh	hyperbolic sine	sinh(number T) -> double	SELECT sinh(0.5) LIMIT 1
tan	Tangent	tan(number T) -> double	SELECT tan(0.5) LIMIT 1

Temporal Functions

Table 10-104 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

Function	Purpose	Description	Example Value
minute_of_hour	Number of minutes in the current hour	minute_of_hour(date) -> integer	SELECT minute_of_hour(date) LIMIT 1
minute_of_day	Number of minutes on the current day	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
monthname	Month Name	monthname(date) -> string	SELECT monthname(date) LIMIT 1
now	Current time.	now() -> time	SELECT now() LIMIT 1
second_of_minute	Number of seconds	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
timestamp	Date	timestamp(date) -> date	SELECT timestamp(date) LIMIT 1
year	Year	year(date) -> integer	SELECT year(date) LIMIT 1

Text Functions

Table 10-105 Text functions

Function	Purpose	Description	Example Value
ascii	ASCII value of the first character	ascii(string T) -> integer	SELECT ascii('t') LIMIT 1
concat_ws	Connection String	concat_ws(separator, string, string) -> string	SELECT concat_ws('-', 'Tutorial', 'is', 'fun!') LIMIT 1
left	Obtain a character string from left to right.	left(string T, integer) -> T	SELECT left('hello', 2) LIMIT 1
length	length	length(string) -> integer	SELECT length('hello') LIMIT 1
locate	Search for a string	locate(string, string) -> integer	SELECT locate('o', 'hello') LIMIT 1
replace	Replace strings	replace(string T, string, string) -> T	SELECT replace('hello', 'l', 'x') LIMIT 1

Function	Purpose	Description	Example Value
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
upper	Convert all letters into uppercase letters.	upper(string T) -> T	SELECT upper('helloworld') LIMIT 1

Other

Table 10-106 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

10.7.2.3.7 Aggregate Functions

Table 10-107 Aggregate functions

Function	Purpose	Description	Example Value
avg	Average value	avg(number T) -> T	SELECT avg(age) LIMIT 1
sum	Sum	sum(number T) -> T	SELECT sum(age) LIMIT 1
min	Specifies the minimum value.	min(number T) -> T	SELECT min(age) LIMIT 1
max	Maximum value	max(number T) -> T	SELECT max(age) LIMIT 1
count	Occurrences	count(field) -> integer , count(*) -> integer , count(1) -> integer	SELECT count(age) LIMIT 1 , SELECT count(*) LIMIT 1 , SELECT count(1) LIMIT 1

10.7.3 SecMaster SQL Syntax Reference

10.7.3.1 Supported Data Types

SecMaster supports the following SQL syntax types:

STRING, BOOLEAN, BYTES, DECIMAL, TINYINT, SMALLINT, INTEGER, BIGINT, FLOAT, DOUBLE, DATE, TIME, TIMESTAMP, TIMESTAMP WITH LOCAL TIME ZONE, INTERVAL, ARRAY, MULTISET, MAP, ROW

- **Precautions**

  a. SecMaster SQL statements are compatible with the SQL syntax of Flink 1.7.2.

  b. Flink SQL uses a lexical policy for identifier (table, attribute, function names) similar to Java:

    - The case of identifiers is preserved no matter whether they are quoted.

    - Identifiers are matched case-sensitively.

    - Unlike Java, back-ticks allow identifiers to contain non-alphanumeric characters (for example, **SELECT a AS `my field` FROM t**).

    String text must be enclosed in single quotes (for example, **SELECT'Hello World'**). Duplicate a single quote for escaping (for example, **SELECT'It''s me.'**). Unicode characters are supported in string literals. If explicit Unicode points are required, use the following syntax:

▪ Use the backslash (\) as an escaping character (default): **SELECT U&'\263A'**

▪ Use a custom escaping character: **SELECT U&'#263A' UESCAPE '#'**

c. There are some restrictions when the regular expression function (REGEXP) is used:

Regular expressions are time-consuming and require 100 times performance overhead as that for addition, subtraction, multiplication, and division. Beyond that, regular expressions may enter an infinite loop in some extreme cases, causing job blocking. So LIKE is recommended. Typical regular expression functions you may use include:

REGEXP

REGEXP_REPLACE

10.7.3.2 Syntax

10.7.3.2.1 Data Query Language (DQL) Syntax

DQL Statements

- **Syntax**

```
query:
 values
 | {
     select
     | selectWithoutFrom
     | query UNION [ ALL ] query
     | query EXCEPT query
     | query INTERSECT query
   }
   [ ORDER BY orderItem [, orderItem ]* ]
   [ LIMIT { count | ALL } ]
   [ OFFSET start { ROW | ROWS } ]
   [ FETCH { FIRST | NEXT } [ count ] { ROW | ROWS } ONLY]

orderItem:
 expression [ ASC | DESC ]

select:
 SELECT [ ALL | DISTINCT ]
 { * | projectItem [, projectItem ]* }
 FROM tableExpression
 [ WHERE booleanExpression ]
 [ GROUP BY { groupItem [, groupItem ]* } ]
 [ HAVING booleanExpression ]
 [ WINDOW windowName AS windowSpec [, windowName AS windowSpec ]* ]

selectWithoutFrom:
 SELECT [ ALL | DISTINCT ]
 { * | projectItem [, projectItem ]* }

projectItem:
 expression [ [ AS ] columnAlias ]
 | tableAlias . *

tableExpression:
 tableReference [, tableReference ]*
 | tableExpression [ NATURAL ] [ LEFT | RIGHT | FULL ] JOIN tableExpression [ joinCondition ]

joinCondition:
```

```
  ON booleanExpression
| USING '(' column [, column ]* ')'

tableReference:
  tablePrimary
  [ matchRecognize ]
  [ [ AS ] alias [ '(' columnAlias [, columnAlias ]* ')' ] ]

tablePrimary:
  [ TABLE ] [ [ catalogName . ] schemaName . ] tableName
  | LATERAL TABLE '(' functionName '(' expression [, expression ]* ')' ')'
  | UNNEST '(' expression ')'

values:
  VALUES expression [, expression ]*

groupItem:
  expression
| '(' ')'
| '(' expression [, expression ]* ')'
| CUBE '(' expression [, expression ]* ')'
| ROLLUP '(' expression [, expression ]* ')'
| GROUPING SETS '(' groupItem [, groupItem ]* ')'

windowRef:
    windowName
  | windowSpec

windowSpec:
    [ windowName ]
    '('
    [ ORDER BY orderItem [, orderItem ]* ]
    [ PARTITION BY expression [, expression ]* ]
    [
        RANGE numericOrIntervalExpression {PRECEDING}
      | ROWS numericExpression {PRECEDING}
    ]
    ')'

matchRecognize:
      MATCH_RECOGNIZE '('
      [ PARTITION BY expression [, expression ]* ]
      [ ORDER BY orderItem [, orderItem ]* ]
      [ MEASURES measureColumn [, measureColumn ]* ]
      [ ONE ROW PER MATCH ]
      [ AFTER MATCH
          ( SKIP TO NEXT ROW
          | SKIP PAST LAST ROW
          | SKIP TO FIRST variable
          | SKIP TO LAST variable
          | SKIP TO variable )
      ]
      PATTERN '(' pattern ')'
      [ WITHIN intervalLiteral ]
      DEFINE variable AS condition [, variable AS condition ]*
      ')'

measureColumn:
      expression AS alias

pattern:
      patternTerm [ '|' patternTerm ]*

patternTerm:
      patternFactor [ patternFactor ]*

patternFactor:
      variable [ patternQuantifier ]
```

```
patternQuantifier:
     '*'
  | '*?'
  | '+'
  | '+?'
  | '?'
  | '??'
  | '{' { [ minRepeat ], [ maxRepeat ] } '}' ['?']
  | '{' repeat '}'
```

- **Precautions**

  a. SecMaster SQL statements are compatible with the SQL syntax of Flink 1.7.2.

  b. Flink SQL uses a lexical policy for identifier (table, attribute, function names) similar to Java:

     - The case of identifiers is preserved no matter whether they are quoted.

     - Identifiers are matched case-sensitively.

     - Unlike Java, back-ticks allow identifiers to contain non-alphanumeric characters (for example, **SELECT a AS `my field` FROM t**).

     String literals must be enclosed in single quotes (for example, **SELECT'Hello World'**). Duplicate a single quote for escaping (for example, **SELECT'It''s me.'**). Unicode characters are supported in string literals. If explicit Unicode points are required, use the following syntax:

     - Use the backslash (\) as an escaping character (default): **SELECT U&'\263A'**

     - Use a custom escaping character: **SELECT U&'#263A' UESCAPE '#'**

  c. There are some restrictions when the regular expression function (REGEXP) is used:

     Regular expressions are time-consuming and require 100 times performance overhead as that for addition, subtraction, multiplication, and division. Beyond that, regular expressions may enter an infinite loop in some extreme cases, causing job blocking. So LIKE is recommended. Typical regular expression functions you may use include:

     REGEXP

     REGEXP_REPLACE

10.7.3.3 Data Query Language (DQL) Syntax

10.7.3.3.1 SELECT

SELECT

- **Syntax Format**
  ```
  SELECT [ ALL | DISTINCT ]
  { * | projectItem [, projectItem ]* }
  FROM tableExpression
  [ WHERE booleanExpression ]
  [ GROUP BY { groupItem [, groupItem ]* } ]
  [ HAVING booleanExpression ]
  ```

- **Syntax Description**

  SELECT is used to select data from a table.

  ALL indicates that all results are returned.

  DISTINCT indicates that the duplicated results are removed.

- **Precautions**

  – The table to be queried must exist. Otherwise, an error is reported.

  – WHERE is used to specify the search condition, which can be the arithmetic operator, relational operator, or logical operator.

  – GROUP BY is used to specify the grouping field, which can be one or more multiple fields.

- **Example**

  Select the order which contains more than 3 pieces of data.

  SELECT * FROM Orders WHERE units > 3;

  Queries a group of constant data.

  select 'Lily', 'male', 'student', 17;

WHERE

- **Syntax Format**

  SELECT   { * | projectItem [, projectItem]* }
    FROM tableExpression
    [WHERE booleanExpression]

- **Syntax Description**

  This clause is used to filter the query results using the WHERE clause.

- **Precautions**

  – The to-be-queried table must exist.

  – WHERE filters the records that do not meet the requirements.

- **Example**

  Search orders which contain more than 3 pieces and fewer than 10 pieces of data.

  SELECT * FROM Orders
    WHERE units > 3 and units < 10;

HAVING

- **Function**

  This clause is used to search for the query results that meet the search condition.

- **Syntax Format**

  SELECT [ALL | DISTINCT]   { * | projectItem [, projectItem]* }
    FROM tableExpression
    [WHERE booleanExpression]
    [GROUP BY { groupItem [, groupItem]* }]
    [HAVING booleanExpression]

- **Syntax Description**

  Generally, HAVING and GROUP BY are used together. You can use GROUP BY for grouping and then use HAVING for filtering. Arithmetic operations and aggregate functions are supported in the HAVING clause.

- **Precautions**

  If the filtering condition is subject to the results of GROUP BY, the HAVING clause, rather than the WHERE clause, must be used for search.

- **Example**

  Group the **student** table according to the **name** field and search for the records in which the maximum score is higher than 95 in the group.

  ```
  SELECT name, max(score) FROM student
   GROUP BY name
   HAVING max(score) >95;
  ```

Column-Based GROUP BY

- **Function**

  This clause is used to group a table based on columns.

- **Syntax Format**

  ```
  SELECT [ ALL | DISTINCT ]   { * | projectItem [, projectItem ]* }
   FROM tableExpression
   [ WHERE booleanExpression ]
   [ GROUP BY { groupItem [, groupItem ]* } ]
  ```

- **Syntax Description**

  Column-based GROUP BY can be categorized into single-column GROUP BY and multi-column GROUP BY.

  – Single-column GROUP BY indicates that the GROUP BY clause contains only one column.

  – Multi-column GROUP BY indicates that the GROUP BY clause contains multiple columns. The table will be grouped according to all fields in the GROUP BY clause. The records whose fields are the same are grouped into one group.

- **Precautions**

  GroupBy generates update results in the stream processing table.

- **Example**

  Group the **student** table according to the score and name fields and return the grouping results.

  ```
  SELECT name,score, max(score) FROM student
   GROUP BY name,score;
  ```

Expression-Based GROUP BY

- **Function**

  This clause is used to group streams according to expressions.

- **Syntax Format**

  ```
  SELECT [ ALL | DISTINCT ]   { * | projectItem [, projectItem ]* }
   FROM tableExpression
   [ WHERE booleanExpression ]
   [ GROUP BY { groupItem [, groupItem ]* } ]
  ```

- **Syntax Description**

  groupItem can have one or more fields. The fields can be called by string functions, but cannot be called by aggregate functions.

- **Precautions**

  None

- **Example**

  Use the substring function to obtain the character string from the name field, group the **student** table according to the obtained character string, and return each sub character string and the number of records.

  ```
  SELECT substring(name,6),count(name) FROM student
   GROUP BY substring(name,6);
  ```

Grouping sets, Rollup, Cube

- **Function**

  – The GROUP BY GROUPING SETS generates a result set equivalent to that generated by multiple simple GROUP BY UNION ALL statements. Using GROUPING SETS is more efficient.

  – The ROLLUP and CUBE generate multiple groups based on certain rules and then collect statistics by group.

  – The result set generated by CUBE contains all the combinations of values in the selected columns.

  – The result set generated by ROLLUP contains the combinations of a certain layer structure in the selected columns.

- **Syntax Format**

  ```
  SELECT [ ALL | DISTINCT ]   { * | projectItem [, projectItem ]* }
   FROM tableExpression
   [ WHERE booleanExpression ]
   [ GROUP BY groupingItem]
  ```

- **Syntax Description**

  Values of **groupingItem** can be **Grouping sets(columnName [, columnName]*)**, **Rollup(columnName [, columnName]*)**, and **Cube(columnName [, columnName]*)**.

- **Precautions**

  None

- **Example**

  Return the results generated based on **user** and **product**.

  ```
  SELECT SUM(amount)
  FROM Orders
  GROUP BY GROUPING SETS ((user), (product));
  ```

GROUP BY Using HAVING

- **Function**

  This clause filters a table after grouping it using the HAVING clause.

- **Syntax Format**

  ```
  SELECT [ ALL | DISTINCT ]   { * | projectItem [, projectItem ]* }
   FROM tableExpression
   [ WHERE booleanExpression ]
   [ GROUP BY { groupItem [, groupItem ]* } ]
   [ HAVING booleanExpression ]
  ```

- **Syntax Description**

  Generally, HAVING and GROUP BY are used together. You can use GROUP BY for grouping and the HAVING for filtering.

- **Precautions**

– If the filtering condition is subject to the results of GROUP BY, the HAVING clause, rather than the WHERE clause, must be used for search. HAVING and GROUP BY are used together. Use GROUP BY for grouping and the HAVING for filtering.

– Fields used in HAVING, except for those used for aggregate functions, must exist in GROUP BY.

– The arithmetic operation and aggregate function are supported by the HAVING clause.

- **Example**

  Group the **transactions** by **num**, use the HAVING clause to search for the records in which the maximum value derived from multiplying **price** with **amount** is higher than 5000, and return the filtered results.

  ```
  SELECT num, max(price*amount) FROM transactions
   WHERE time > '2016-06-01'
   GROUP BY num
   HAVING max(price*amount)>5000;
  ```

10.7.3.3.2 UNION

Union/Union ALL/Intersect/Except

- **Syntax Format**
  ```
  query UNION [ ALL ] | Intersect | Except query
  ```

- **Syntax Description**

  – UNION is used to return the union set of multiple query results.

  – INTERSECT is used to return the intersection of multiple query results.

  – EXCEPT is used to return the difference set of multiple query results.

- **Precautions**

  – Set operations join tables from head to tail under certain conditions. The quantity of columns returned by each SELECT statement must be the same. Column types must be the same. Column names can be different.

  – By default, UNION takes only distinct records while UNION ALL does not remove duplicates from the result.

- **Example**

  Output distinct records found in either Orders1 and Orders2 tables.

  ```
  SELECT  * FROM Orders1
   UNION SELECT  * FROM Orders2;
  ```

IN

- **Syntax Format**
  ```
  SELECT [ ALL | DISTINCT ]   { * | projectItem [, projectItem ]* }
   FROM tableExpression
   WHERE column_name IN (value (, value)* ) | query
  ```

- **Syntax Description**

  The IN operator allows multiple values to be specified in the WHERE clause. It returns true if the expression exists in the given table subquery.

- **Precautions**

  The subquery table must consist of a single column, and the data type of the column must be the same as that of the expression.

- **Example**

  Return **user** and **amount** information of the products in **NewProducts** of the **Orders** table.

  ```
  SELECT user, amount
  FROM Orders
  WHERE product IN (
      SELECT product FROM NewProducts
  );
  ```

10.7.3.3.3 Window

GROUP WINDOW

- **Syntax Description**

  Group Window is defined in GROUP BY. One record is generated from each group. Group Window involves the following functions:

  – Array functions

  Table 10-108 Array functions

Grouping Window Function	Description
TUMBLE(time_attr, interval)	Defines a tumbling time window. A tumbling time window assigns rows to non-overlapping, continuous windows with a fixed duration (interval). For example, a tumbling window of 5 minutes groups rows in 5 minutes intervals. Tumbling windows can be defined on event-time (stream + batch) or processing-time (stream).
HOP(time_attr, interval, interval)	Defines a hopping time window (called sliding window in the Table API). A hopping time window has a fixed duration (second interval parameter) and hops by a specified hop interval (first interval parameter). If the hop interval is smaller than the window size, hopping windows are overlapping. Thus, rows can be assigned to multiple windows. For example, a hopping window of 15 minutes size with a 5-minute hop interval assigns each row to 3 different windows of 15-minute size, which are evaluated in an interval of 5 minutes. Hopping windows can be defined on event-time (stream + batch) or processing-time (stream).

Grouping Window Function	Description
SESSION(time_attr, interval)	Defines a session time window. Session time windows do not have a fixed duration but their bounds are defined by a time interval of inactivity, that is, a session window is closed if no event appears for a defined gap period. For example a session window with a 30 minute gap starts when a row is observed after 30 minutes inactivity (otherwise the row would be added to an existing window) and is closed if no row is added within 30 minutes. Session windows can work on event-time (stream + batch) or processing-time (stream).

⚠ **CAUTION**

In streaming mode, the **time_attr** argument of the group window function must refer to a valid time attribute that specifies the processing time or event time of rows.

- If **time_attr** is set to **event-time**, the parameter type is **timestamp(3)**.
- If **time_attr** is set to **processing-time**, you do not need to specify the type.

In batch mode, the **time_attr** parameter of the group window function must be an attribute of type timestamp.

– Window auxiliary functions

The start and end timestamps of group windows as well as time attributes can be selected with the following auxiliary functions.

Table 10-109 Window auxiliary functions

Auxiliary Function	Description
TUMBLE_START(time_attr, interval) HOP_START(time_attr, interval, interval) SESSION_START(time_attr, interval)	Returns the timestamp of the inclusive lower bound of the corresponding tumbling, hopping, or session window.

Auxiliary Function	Description
TUMBLE_END(time_attr, interval) HOP_END(time_attr, interval, interval) SESSION_END(time_attr, interval)	Returns the timestamp of the **exclusive** upper bound of the corresponding tumbling, hopping, or session window. **CAUTION** The exclusive upper bound timestamp **cannot** be used as a rowtime attribute in subsequent time-based operations, such as interval joins and group window or over window aggregations.
TUMBLE_ROWTIME(time_attr, interval) HOP_ROWTIME(time_attr, interval, interval) SESSION_ROWTIME(time_attr, interval)	Returns the timestamp of the inclusive upper bound of the corresponding tumbling, hopping, or session window. The resulting attribute is a rowtime attribute that can be used in subsequent time-based operations such as interval joins and group window or over window aggregations.
TUMBLE_PROCTIME(time_attr, interval) HOP_PROCTIME(time_attr, interval, interval) SESSION_PROCTIME(time_attr, interval)	Returns a proctime attribute that can be used in subsequent time-based operations such as interval joins and group window or over window aggregations.

⚠ **CAUTION**

Auxiliary functions must be called with the same parameters as the grouping window functions in the GROUP BY clause.

- **Example**

```
// Calculate the SUM every day (event time).
SELECT name,
    TUMBLE_START(ts, INTERVAL '1' DAY) as wStart,
    SUM(amount)
    FROM Orders
    GROUP BY TUMBLE(ts, INTERVAL '1' DAY), name;

// Calculate the SUM every day (processing time).
SELECT name,
    SUM(amount)
    FROM Orders
    GROUP BY TUMBLE(proctime, INTERVAL '1' DAY), name;

// Calculate the SUM over the recent 24 hours every hour (event time).
SELECT product,
    SUM(amount)
    FROM Orders
    GROUP BY HOP(ts, INTERVAL '1' HOUR, INTERVAL '1' DAY), product;

// Calculate the SUM of each session and an inactive interval every 12 hours (event time).
SELECT name,
    SESSION_START(ts, INTERVAL '12' HOUR) AS sStart,
    SESSION_END(ts, INTERVAL '12' HOUR) AS sEnd,
```

```
        SUM(amount)
        FROM Orders
        GROUP BY SESSION(ts, INTERVAL '12' HOUR), name;
```

TUMBLE WINDOW Extension

- **Function**

  The SecMaster TUMBLE function is enhanced as follows:

  - A tumbling window is triggered periodically to reduce latency.

    Before the tumbling window ends, the window can be periodically triggered based on the configured frequency. The compute result from the start to the current time is output, which does not affect the final output. The latest result can be viewed in each period before the window ends.

  - Data accuracy is improved.

    You can set a latency for the end of the window. The output of the window is updated according to the configured latency each time a piece of late data reaches.

- Precautions

  - If you use the INSERT statement to write results to a sink, it must support the upsert mode. Ensure that the result table supports upsert operations and the primary key is defined.

  - Latency settings only take effect for event time and not for proctime.

  - Auxiliary functions must be called with the same parameters as the grouping window functions in the GROUP BY clause.

  - If event time is used, watermark must be used. The code is as follows (**order_time** is identified as the event time column and watermark is set to 3 seconds):
    ```
    CREATE TABLE orders (
      order_id string,
      order_channel string,
      order_time timestamp(3),
      pay_amount double,
      real_pay double,
      pay_time string,
      user_id string,
      user_name string,
      area_id string,
      watermark for order_time as order_time - INTERVAL '3' SECOND
    ) WITH (
      'connector' = 'kafka',
      'topic' = '<yourTopic>',
      'properties.bootstrap.servers' = '<yourKafka>:<port>',
      'properties.group.id' = '<yourGroupId>',
      'scan.startup.mode' = 'latest-offset',
      'format' = 'json'
    );
    ```

  - If the proctime is used, you need to use the computed column. The code is as follows (**proc** is the processing time column):
    ```
    CREATE TABLE orders (
      order_id string,
      order_channel string,
      order_time timestamp(3),
      pay_amount double,
      real_pay double,
      pay_time string,
      user_id string,
    ```

```
            user_name string,
            area_id string,
            proc as proctime()
        ) WITH (
        'connector' = 'kafka',
        'topic' = '<yourTopic>',
        'properties.bootstrap.servers' = '<yourKafka>:<port>',
        'properties.group.id' = '<yourGroupId>',
        'scan.startup.mode' = 'latest-offset',
        'format' = 'json'
        );
```

- **Syntax Format**
  TUMBLE(time_attr, window_interval, period_interval, lateness_interval)

- **Parameter description**

Table 10-110 Parameters for adding a record set

Parameter	Description	Format
time_attr	Event time or processing time attribute column ● If **time_attr** is set to **event-time**, the parameter type is **timestamp(3)**. ● If **time_attr** is set to **processing-time**, you do not need to specify the type.	-
window_interval	Duration of the window	● Format 1: **INTERVAL '10' SECOND** The window interval is 10 seconds. You can change the value as needed.
period_interval	Frequency of periodic triggering within the window range. That is, before the window ends, the output result is updated at an interval specified by **period_interval** from the time when the window starts. If this parameter is not set, the periodic triggering policy is not used by default.	● Format 2: **INTERVAL '10' MINUTE** The window interval is 10 minutes. You can change the value as needed.
lateness_interval	Time to postpone the end of the window. The system continues to collect the data that reaches the window within **lateness_interval** after the window ends. The output is updated for each data that reaches the window within **lateness_interval**. **NOTE** If the time window is for processing time, **lateness_interval** does not take effect.	● Format 3: **INTERVAL '10' DAY** The window interval is 10 days. You can change the value as needed.

NOTE

Values of **period_interval** and **lateness_interval** cannot be negative numbers.

- If **period_interval** is set to **0**, periodic triggering is disabled for the window.
- If **lateness_interval** is set to **0**, the latency after the window ends is disabled.
- If neither of the two parameters is set, both periodic triggering and latency are disabled and only the regular tumbling window functions are available.
- If only the latency function needs to be used, set **period_interval** to **INTERVAL '0' SECOND**.

- Auxiliary Function

Table 10-111 Auxiliary Function

Auxiliary Function	Description
TUMBLE_START(time_attr, window_interval, period_interval, lateness_interval)	Returns the timestamp of the inclusive lower bound of the corresponding tumbling window.
TUMBLE_END(time_attr, window_interval, period_interval, lateness_interval)	Returns the timestamp of the exclusive upper bound of the corresponding tumbling window.

- **Example**

  The Kafka is used as the data source table containing the order information, and the JDBC is used as the data result table for statistics on the number of orders settled by a user within 30 seconds. The order ID and window opening time are used as primary keys to collect result statistics in real time to JDBC.

  a. Create a datasource connection for the communication with the VPC and subnet where MySQL and Kafka locate and bind the connection to the queue. Set an inbound rule for the security group to allow access of the queue, and test the connectivity of the queue using the MySQL and Kafka addresses. If the connection is successful, the datasource is bound to the queue. Otherwise, the binding fails.

  b. Run the following statement to create the **order_count** table in the MySQL Flink database:
  ```
  CREATE TABLE `flink`.`order_count` (
   `user_id` VARCHAR(32) NOT NULL,
   `window_start` TIMESTAMP NOT NULL,
   `window_end` TIMESTAMP NULL,
   `total_num` BIGINT UNSIGNED NULL,
   PRIMARY KEY (`user_id`, `window_start`)
  ) ENGINE = InnoDB
   DEFAULT CHARACTER SET = utf8mb4
   COLLATE = utf8mb4_general_ci;
  ```

  c. Create a Flink OpenSource SQL job and submit the job. In this example, the window size is 30 seconds, the triggering period is 10 seconds, and the latency is 5 seconds. That is, if the result is updated before the window ends, the intermediate result will be output every 10 seconds. After the watermark is reached and the window ends, the data whose event time is within 5 seconds of the watermark will still be processed and counted in the current window. If the event time exceeds 5 seconds of the watermark, the data will be discarded.

```
CREATE TABLE orders (
  order_id string,
  order_channel string,
  order_time timestamp(3),
  pay_amount double,
  real_pay double,
  pay_time string,
  user_id string,
  user_name string,
  area_id string,
  watermark for order_time as order_time - INTERVAL '3' SECOND
) WITH (
  'connector' = 'kafka',
  'topic' = '<yourTopic>',
  'properties.bootstrap.servers' = '<yourKafka>:<port>',
  'properties.group.id' = '<yourGroupId>',
  'scan.startup.mode' = 'latest-offset',
  'format' = 'json'
);

CREATE TABLE jdbcSink (
  user_id string,
  window_start timestamp(3),
  window_end timestamp(3),
  total_num BIGINT,
  primary key (user_id, window_start) not enforced
) WITH (
  'connector' = 'jdbc',
  'url' = 'jdbc:mysql://<yourMySQL>:3306/flink',
  'table-name' = 'order_count',
  'username' = '<yourUserName>',
  'password' = '<yourPassword>',
  'sink.buffer-flush.max-rows' = '1'
);

select
    order_id,
    TUMBLE_START(order_time, INTERVAL '30' SECOND, INTERVAL '10' SECOND, INTERVAL '5'
SECOND),
    TUMBLE_END(order_time, INTERVAL '30' SECOND, INTERVAL '10' SECOND, INTERVAL '5'
SECOND),
    COUNT(*) from orders
    GROUP BY user_id, TUMBLE(order_time, INTERVAL '30' SECOND, INTERVAL '10' SECOND,
INTERVAL '5' SECOND);
```

d. Insert data to Kafka. Assume that orders are settled at different time and
    the order data at 10:00:13 arrives late.

```
{"order_id":"202103241000000001", "order_channel":"webShop", "order_time":"2021-03-24
10:00:00", "pay_amount":"100.00", "real_pay":"100.00", "pay_time":"2021-03-24 10:02:03",
"user_id":"0001", "user_name":"Alice", "area_id":"330106"}

{"order_id":"202103241000000002", "order_channel":"webShop", "order_time":"2021-03-24
10:00:20", "pay_amount":"100.00", "real_pay":"100.00", "pay_time":"2021-03-24 10:02:03",
"user_id":"0001", "user_name":"Alice", "area_id":"330106"}

{"order_id":"202103241000000003", "order_channel":"webShop", "order_time":"2021-03-24
10:00:33", "pay_amount":"100.00", "real_pay":"100.00", "pay_time":"2021-03-24 10:02:03",
"user_id":"0001", "user_name":"Alice", "area_id":"330106"}

{"order_id":"202103241000000004", "order_channel":"webShop", "order_time":"2021-03-24
10:00:13", "pay_amount":"100.00", "real_pay":"100.00", "pay_time":"2021-03-24 10:02:03",
"user_id":"0001", "user_name":"Alice", "area_id":"330106"}
```

e. Run the following statement in the MySQL database to view the output
    result. The final result is displayed as follows because the periodic output
    result cannot be collected:

```
select * from order_count
```

user_id	window_start	window_end	total_num
0001	2021-03-24 10:00:00	2021-03-24 10:00:30	3
0001	2021-03-24 10:00:30	2021-03-24 10:01:00	1

OVER WINDOW

The difference between Over Window and Group Window is that one record is generated from one row in Over Window.

- **Syntax Format**

```
SELECT agg1(attr1) OVER (
 [PARTITION BY partition_name]
 ORDER BY proctime|rowtime
 ROWS
 BETWEEN (UNBOUNDED|rowCOUNT) PRECEDING AND CURRENT ROW FROM TABLENAME

SELECT agg1(attr1) OVER (
 [PARTITION BY partition_name]
 ORDER BY proctime|rowtime
 RANGE
 BETWEEN (UNBOUNDED|timeInterval) PRECEDING AND CURRENT ROW FROM TABLENAME
```

- **Syntax Description**

Table 10-112 Parameter description

Name	Parameter Description
PARTITION BY	Indicates the primary key of the specified group. Each group separately performs calculation.
ORDER BY	Indicates the processing time or event time as the timestamp for data.
ROWS	Indicates the count window.
RANGE	Indicates the time window.

- Precautions
  - All aggregates must be defined in the same window, that is, in the same partition, sort, and range.
  - Currently, only windows from PRECEDING (unbounded or bounded) to CURRENT ROW are supported. The range described by FOLLOWING is not supported.
  - ORDER BY must be specified for a single time attribute.

- **Example**

```
// Calculate the count and total number from syntax rules enabled to now (in proctime).
SELECT name,
    count(amount) OVER (PARTITION BY name ORDER BY proctime RANGE UNBOUNDED preceding) as cnt1,
    sum(amount) OVER (PARTITION BY name ORDER BY proctime RANGE UNBOUNDED preceding) as cnt2
    FROM Orders;

// Calculate the count and total number of the recent four records (in proctime).
SELECT name,
    count(amount) OVER (PARTITION BY name ORDER BY proctime ROWS BETWEEN 4 PRECEDING AND CURRENT ROW) as cnt1,
    sum(amount) OVER (PARTITION BY name ORDER BY proctime ROWS BETWEEN 4 PRECEDING AND CURRENT ROW) as cnt2
```

```
     FROM Orders;
```

```
// Calculate the count and total number last 60s (in eventtime). Process the events based on event
time, which is the timeattr field in Orders.
SELECT name,
    count(amount) OVER (PARTITION BY name ORDER BY timeattr RANGE BETWEEN INTERVAL '60'
SECOND PRECEDING AND CURRENT ROW) as cnt1,
    sum(amount) OVER (PARTITION BY name ORDER BY timeattr RANGE BETWEEN INTERVAL '60'
SECOND PRECEDING AND CURRENT ROW) as cnt2
    FROM Orders;
```

10.7.3.3.4 JOIN

Equi-join

- **Syntax Format**
  ```
  FROM tableExpression INNER | LEFT | RIGHT | FULL JOIN tableExpression
   ON value11 = value21 [ AND value12 = value22]
  ```

- **Precautions**

  - Currently, only equi-joins are supported, for example, joins that have at least one conjunctive condition with an equality predicate. Arbitrary cross or theta joins are not supported.

  - Tables are joined in the order in which they are specified in the FROM clause. Make sure to specify tables in an order that does not yield a cross join (Cartesian product), which are not supported and would cause a query to fail.

  - For streaming queries the required state to compute the query result might grow infinitely depending on the type of aggregation and the number of distinct grouping keys. Provide a query configuration with valid retention interval to prevent excessive state size.

- **Example**
  ```
  SELECT *
  FROM Orders INNER JOIN Product ON Orders.productId = Product.id;
  ```

  ```
  SELECT *
  FROM Orders LEFT JOIN Product ON Orders.productId = Product.id;
  ```

  ```
  SELECT *
  FROM Orders RIGHT JOIN Product ON Orders.productId = Product.id;
  ```

  ```
  SELECT *
  FROM Orders FULL OUTER JOIN Product ON Orders.productId = Product.id;
  ```

Time-windowed Join

- **Function**

  Each piece of data in a stream is joined with data in different time zones in another stream.

- **Syntax Format**
  ```
  from t1 JOIN t2 ON t1.key = t2.key AND TIMEBOUND_EXPRESSIO
  ```

- **Description**

  TIMEBOUND_EXPRESSION can be in either of the following formats:

  - L.time between LowerBound(R.time) and UpperBound(R.time)

  - R.time between LowerBound(L.time) and UpperBound(L.time)

  Comparison expression with the time attributes (L.time/R.time)

- Precautions

  A time window join requires at least one equi join predicate and a join condition that limits the time of both streams.

  For example, use two range predicates (<, <=, >=, or >), a BETWEEN predicate, or an equal predicate that compares the same type of time attributes (such as processing time and event time) in two input tables.

  For example, the following predicate is a valid window join condition:

  – ltime = rtime

  – ltime >= rtime AND ltime < rtime + INTERVAL '10' MINUTE

  – ltime BETWEEN rtime - INTERVAL '10' SECOND AND rtime + INTERVAL '5' SECOND

- **Example**

  Join all orders shipped within 4 hours with their associated shipments.

  ```
  SELECT *
  FROM Orders o, Shipments s
  WHERE o.id = s.orderId AND
      o.ordertime BETWEEN s.shiptime - INTERVAL '4' HOUR AND s.shiptime;
  ```

Expanding arrays into a relation

- Precautions

  This clause is used to return a new row for each element in the given array. Unnesting WITH ORDINALITY is not yet supported.

- **Example**

  ```
  SELECT users, tag
  FROM Orders CROSS JOIN UNNEST(tags) AS t (tag);
  ```

User-Defined Table Functions

- **Function**

  This clause is used to join a table with the results of a table function. ach row of the left (outer) table is joined with all rows produced by the corresponding call of the table function.

- Precautions

  A left outer join against a lateral table requires a TRUE literal in the ON clause.

- **Example**

  The row of the left (outer) table is dropped, if its table function call returns an empty result.

  ```
  SELECT users, tag
  FROM Orders, LATERAL TABLE(unnest_udtf(tags)) t AS tag;
  ```

  If a table function call returns an empty result, the corresponding outer row is preserved, and the result padded with null values.

  ```
  SELECT users, tag
  FROM Orders LEFT JOIN LATERAL TABLE(unnest_udtf(tags)) t AS tag ON TRUE;
  ```

Join Temporal Table Function

- **Function**

- **Precautions**

  Currently only inner join and left outer join with temporal tables are supported.

- **Example**

  Assuming Rates is a temporal table function, the join can be expressed in SQL as follows:

```
SELECT
  o_amount, r_rate
FROM
  Orders,
  LATERAL TABLE (Rates(o_proctime))
WHERE
  r_currency = o_currency;
```

Join Temporal Tables

- **Function**

  This clause is used to join the Temporal table.

- **Syntax Format**

```
SELECT column-names
FROM table1  [AS <alias1>]
[LEFT] JOIN table2 FOR SYSTEM_TIME AS OF table1.proctime [AS <alias2>]
ON table1.column-name1 = table2.key-name1
```

- **Syntax Description**

  - **table1.proctime** indicates the processing time attribute (computed column) of **table1**.

  - **FOR SYSTEM_TIME AS OF table1.proctime** indicates that when the records in the left table are joined with the dimension table on the right, only the snapshot data is used for matching the current processing time dimension table.

- **Precautions**

  Only inner and left joins are supported for temporal tables with processing time attributes.

- **Example**

  LatestRates is a temporal table that is materialized with the latest rate.

```
SELECT
  o.amount, o.currency, r.rate, o.amount * r.rate
FROM
  Orders AS o
  JOIN LatestRates FOR SYSTEM_TIME AS OF o.proctime AS r
  ON r.currency = o.currency;
```

10.7.3.3.5 OrderBy & Limit

OrderBy

- **Function**

  This clause is used to sort data in ascending order on a time attribute.

- **Precautions**

  Currently, only sorting by time attribute is supported.

- **Example**

  Sort data in ascending order on the time attribute.

```
SELECT *
FROM Orders
ORDER BY orderTime;
```

Limit

- **Function**

  This clause is used to constrain the number of rows returned.

- **Precautions**

  This clause is used in conjunction with ORDER BY to ensure that the results are deterministic.

- **Example**
  ```
  SELECT *
  FROM Orders
  ORDER BY orderTime
  LIMIT 3;
  ```

10.7.3.3.6 Top-N

Function

Top-N queries ask for the N smallest or largest values ordered by columns. Both smallest and largest values sets are considered Top-N queries. Top-N queries are useful in cases where the need is to display only the N bottom-most or the N top-most records from batch/streaming table on a condition.

Syntax Format

```
SELECT [column_list]
FROM (
  SELECT [column_list],
    ROW_NUMBER() OVER ([PARTITION BY col1[, col2...]]
      ORDER BY col1 [asc|desc][, col2 [asc|desc]...]) AS rownum
  FROM table_name)
WHERE rownum <= N [AND conditions]
```

Syntax Description

- **ROW_NUMBER()**: Allocates a unique and consecutive number to each line starting from the first line in the current partition. Currently, **ROW_NUMBER** can be used in the **over** window function only. **RANK()** and **DENSE_RANK()** will be supported soon.

- **PARTITION BY col1[, col2...]**: Specifies the partition columns. Each partition will have a Top-N result.

- **ORDER BY col1 [asc|desc][, col2 [asc|desc]...]**: Specifies the ordering columns. The ordering directions can be different for different columns.

- **WHERE rownum <= N**: Specifies a Top-N query in Flink. Where N represents the N smallest or largest records that need to be returned.

- [AND conditions]: You can add other query conditions in the where clause. Note that the other conditions can only be combined with **rownum <= N** using the **AND** logic.

Constraints

- Top N queries return updated results.
- Flink SQL will sort the input data stream according to the order key.
- So if the top N records have been changed, the changed ones will be sent as retraction/update records to downstream.
- If the top N records need to be stored in external storage, the result table should have the same unique key with the Top-N query.

Example

This is an example to get the top five products per category that have the maximum sales in real time.

```
SELECT *
  FROM (
    SELECT *,
       ROW_NUMBER() OVER (PARTITION BY category ORDER BY sales DESC) as row_num
    FROM ShopSales)
  WHERE row_num <= 5;
```

10.7.3.3.7 Deduplication

Function

Deduplication removes rows that duplicate over a set of columns, keeping only the first one or the last one.

Syntax Format

```
SELECT [column_list]
FROM (
  SELECT [column_list],
    ROW_NUMBER() OVER ([PARTITION BY col1[, col2...]]
      ORDER BY time_attr [asc|desc]) AS rownum
  FROM table_name)
WHERE rownum = 1
```

Syntax Description

- ROW_NUMBER(): Assigns a unique, sequential number to each row, starting with one.
- PARTITION BY col1[, col2...]: specifies the column of the partition, for example, the key for deduplication.
- ORDER BY time_attr [asc|desc]: Specifies the ordering column, which must be a time attribute. Currently Flink supports proctime only. Ordering by ASC means to keep the first row, ordering by DESC means to keep the last row.
- WHERE rownum = 1: The rownum = 1 is required for Flink to recognize this query is deduplication.

Precautions

None

Example

The following examples show how to remove duplicate rows on **order_id**. The proctime is an event time attribute.

```
SELECT order_id, user, product, number
  FROM (
    SELECT *,
      ROW_NUMBER() OVER (PARTITION BY order_id ORDER BY proctime ASC) as row_num
    FROM Orders)
  WHERE row_num = 1;
```

10.7.3.3.8 Reserved Keywords

Currently, the SecMaster SQL feature is being updated and improved. Some character combinations have been reserved as keywords for subsequent functions. If you want to use these characters as field names, use backquote to wrap the field names, for example, `value` and `count`.

The reserved keywords are as follows:

Table 10-113 Reserved keywords

Initials	SecMaster Reserved Keywords
A	A, ABS, ABSOLUTE, ACTION, ADA, ADD, ADMIN, AFTER, ALL, ALLOCATE, ALLOW, ALTER, ALWAYS, AND, ANALYZE, ANY, ARE, ARRAY, AS, ASC, ASENSITIVE, ASSERTION, ASSIGNMENT, ASYMMETRIC, AT, ATOMIC, ATTRIBUTE, ATTRIBUTES, AUTHORIZATION, AVG
B	BEFORE, BEGIN, BERNOULLI, BETWEEN, BIGINT, BINARY, BIT, BLOB, BOOLEAN, BOTH, BREADTH, BY, BYTES
C	C, CALL, CALLED, CARDINALITY, CASCADE, CASCADED, CASE, CAST, CATALOG, CATALOG_NAME, CEIL, CEILING, CENTURY, CHAIN, CHAR, CHARACTER, CHARACTERISTICS, CHARACTERS, CHARACTER_LENGTH, CHARACTER_SET_CATALOG, CHARACTER_SET_NAME, CHARACTER_SET_SCHEMA, CHAR_LENGTH, CHECK, CLASS_ORIGIN, CLOB, CLOSE, COALESCE, COBOL, COLLATE, COLLATION, COLLATION_CATALOG, COLLATION_NAME, COLLATION_SCHEMA, COLLECT, COLUMN, COLUMNS, COLUMN_NAME, COMMAND_FUNCTION, COMMAND_FUNCTION_CODE, COMMIT, COMMITTED, CONDITION, CONDITION_NUMBER, CONNECT, CONNECTION, CONNECTION_NAME, CONSTRAINT, CONSTRAINTS, CONSTRAINT_CATALOG, CONSTRAINT_NAME, CONSTRAINT_SCHEMA, CONSTRUCTOR, CONTAINS, CONTINUE, CONVERT, CORR, CORRESPONDING, COUNT, COVAR_POP, COVAR_SAMP, CREATE, CROSS, CUBE, CUME_DIST, CURRENT, CURRENT_CATALOG, CURRENT_DATE, CURRENT_DEFAULT_TRANSFORM_GROUP, CURRENT_PATH, CURRENT_ROLE, CURRENT_SCHEMA, CURRENT_TIME, CURRENT_TIMESTAMP, CURRENT_TRANSFORM_GROUP_FOR_TYPE, CURRENT_USER, CURSOR, CURSOR_NAME, CYCLE

Initials	SecMaster Reserved Keywords
D	DATA, DATABASE, DATE, DATETIME_INTERVAL_CODE, DATETIME_INTERVAL_PRECISION, DAY, DEALLOCATE, DEC, DECADE, DECIMAL, DECLARE, DEFAULT, DEFAULTS, DEFERRABLE, DEFERRED, DEFINED, DEFINER, DEGREE, DELETE, DENSE_RANK, DEPTH, DEREF, DERIVED, DESC, DESCRIBE, DESCRIPTION, DESCRIPTOR, DETERMINISTIC, DIAGNOSTICS, DISALLOW, DISCONNECT, DISPATCH, DISTINCT, DOMAIN, DOUBLE, DOW, DOY, DROP, DYNAMIC, DYNAMIC_FUNCTION, DYNAMIC_FUNCTION_CODE
E	EACH, ELEMENT, ELSE, END, END-EXEC, EPOCH, EQUALS, ESCAPE, EVERY,EXCEPT, EXCEPTION, EXCLUDE, EXCLUDING, EXEC, EXECUTE, EXISTS, EXP, EXPLAIN, EXTEND, EXTERNAL, EXTRACT
F	FALSE, FETCH, FILTER, FINAL, FIRST, FIRST_VALUE, FLOAT, FLOOR, FOLLOWING, FOR, FOREIGN, FORTRAN, FOUND, FRAC_SECOND, FREE, FROM, FULL, FUNCTION, FUSION
G	G, GENERAL, GENERATED, GET, GLOBAL, GO, GOTO, GRANT, GRANTED, GROUP, GROUPING
H	HAVING, HIERARCHY, HOLD, HOUR
I	IDENTITY, IMMEDIATE, IMPLEMENTATION, IMPORT, IN, INCLUDING, INCREMENT, INDICATOR, INITIALLY, INNER, INOUT, INPUT, INSENSITIVE, INSERT, INSTANCE, INSTANTIABLE, INT, INTEGER, INTERSECT, INTERSECTION, INTERVAL, INTO, INVOKER, IS, ISOLATION
J	JAVA, JOIN
K	K, KEY, KEY_MEMBER, KEY_TYPE
L	LABEL, LANGUAGE, LARGE, LAST, LAST_VALUE, LATERAL, LEADING, LEFT, LENGTH, LEVEL, LIBRARY, LIKE, LIMIT, LN, LOCAL, LOCALTIME, LOCALTIMESTAMP, LOCATOR, LOWER
M	M, MAP, MATCH, MATCHED, MAX, MAXVALUE, MEMBER, MERGE, MESSAGE_LENGTH, MESSAGE_OCTET_LENGTH, MESSAGE_TEXT, METHOD, MICROSECOND, MILLENNIUM, MIN, MINUTE, MINVALUE, MOD, MODIFIES, MODULE, MODULES, MONTH, MORE, MULTISET, MUMPS
N	NAME, NAMES, NATIONAL, NATURAL, NCHAR, NCLOB, NESTING, NEW, NEXT, NO, NONE, NORMALIZE, NORMALIZED, NOT, NULL, NULLABLE, NULLIF, NULLS, NUMBER, NUMERIC
O	OBJECT, OCTETS, OCTET_LENGTH, OF, OFFSET, OLD, ON, ONLY, OPEN, OPTION, OPTIONS, OR, ORDER, ORDERING, ORDINALITY, OTHERS, OUT, OUTER, OUTPUT, OVER, OVERLAPS, OVERLAY, OVERRIDING

Initials	SecMaster Reserved Keywords
P	PAD, PARAMETER, PARAMETER_MODE, PARAMETER_NAME, PARAMETER_ORDINAL_POSITION, PARAMETER_SPECIFIC_CATALOG, PARAMETER_SPECIFIC_NAME, PARAMETER_SPECIFIC_SCHEMA, PARTIAL, PARTITION, PASCAL, PASSTHROUGH, PATH, PERCENTILE_CONT, PERCENTILE_DISC, PERCENT_RANK, PLACING, PLAN, PLI, POSITION, POWER, PRECEDING, PRECISION, PREPARE, PRESERVE, PRIMARY, PRIOR, PRIVILEGES, PROCEDURE, PUBLIC
Q	QUARTER
R	RANGE, RANK, RAW, READ, READS, REAL, RECURSIVE, REF, REFERENCES, REFERENCING, REGR_AVGX, REGR_AVGY, REGR_COUNT, REGR_INTERCEPT, REGR_R2, REGR_SLOPE, REGR_SXX, REGR_SXY, REGR_SYY, RELATIVE, RELEASE, REPEATABLE, RESET, RESTART, RESTRICT, RESULT, RETURN, RETURNED_CARDINALITY, RETURNED_LENGTH, RETURNED_OCTET_LENGTH, RETURNED_SQLSTATE, RETURNS, REVOKE, RIGHT, ROLE, ROLLBACK, ROLLUP, ROUTINE, ROUTINE_CATALOG, ROUTINE_NAME, ROUTINE_SCHEMA, ROW, ROWS, ROW_COUNT, ROW_NUMBER
S	SAVEPOINT, SCALE, SCHEMA, SCHEMA_NAME, SCOPE, SCOPE_CATALOGS, SCOPE_NAME, SCOPE_SCHEMA, SCROLL, SEARCH, SECOND, SECTION, SECURITY, SELECT, SELF, SENSITIVE, SEQUENCE, SERIALIZABLE, SERVER, SERVER_NAME, SESSION, SESSION_USER, SET, SETS, SIMILAR, SIMPLE, SIZE, SMALLINT, SOME, SOURCE, SPACE, SPECIFIC, SPECIFICTYPE, SPECIFIC_NAME, SQL, SQLEXCEPTION, SQLSTATE, SQLWARNING, SQL_TSI_DAY, SQL_TSI_FRAC_SECOND, SQL_TSI_HOUR, SQL_TSI_MICROSECOND, SQL_TSI_MINUTE, SQL_TSI_MONTH, SQL_TSI_QUARTER, SQL_TSI_SECOND, SQL_TSI_WEEK, SQL_TSI_YEAR, SQRT, START, STATE, STATEMENT, STATIC, STDDEV_POP, STDDEV_SAMP, STREAM, STRING, STRUCTURE, STYLE, SUBCLASS_ORIGIN, SUBMULTISET, SUBSTITUTE, SUBSTRING, SUM, SYMMETRIC, SYSTEM, SYSTEM_USER
T	TABLE, TABLESAMPLE, TABLE_NAME, TEMPORARY, THEN, TIES, TIME, TIMESTAMP, TIMESTAMPADD, TIMESTAMPDIFF, TIMEZONE_HOUR, TIMEZONE_MINUTE, TINYINT, TO, TOP_LEVEL_COUNT, TRAILING, TRANSACTION, TRANSACTIONS_ACTIVE, TRANSACTIONS_COMMITTED, TRANSACTIONS_ROLLED_BACK, TRANSFORM, TRANSFORMS, TRANSLATE, TRANSLATION, TREAT, TRIGGER, TRIGGER_CATALOG, TRIGGER_NAME, TRIGGER_SCHEMA, TRIM, TRUE, TYPE
U	UESCAPE, UNBOUNDED, UNCOMMITTED, UNDER, UNION, UNIQUE, UNKNOWN, UNNAMED, UNNEST, UPDATE, UPPER, UPSERT, USAGE, USER, USER_DEFINED_TYPE_CATALOG, USER_DEFINED_TYPE_CODE, USER_DEFINED_TYPE_NAME, USER_DEFINED_TYPE_SCHEMA, USING

Initials	SecMaster Reserved Keywords
V	VALUE, VALUES, VARBINARY, VARCHAR, VARYING, VAR_POP, VAR_SAMP, VERSION, VIEW
W	WEEK, WHEN, WHENEVER, WHERE, WIDTH_BUCKET, WINDOW, WITH, WITHIN, WITHOUT, WORK, WRAPPER, WRITE
X	XML
Y	YEAR
Z	ZONE

10.8 Data Delivery

10.8.1 Data Delivery Overview

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, SecMaster supports the following data delivery destinations:

- **Other pipelines**: You can deliver log data to other pipelines.
- **OBS buckets**: You can deliver log data to Object Storage Service (OBS) buckets.
- **LTS**: You can deliver log data to Log Tank Service (LTS).

You can **manage data delivery tasks**, including viewing, suspending, starting, and deleting a data delivery task.

Advantages

- Simple operation: You only need to complete simple configurations on the console to deliver SecMaster data to other cloud products such as OBS.
- Data centralization: SecMaster has completed data centralization of different services. You only need to deliver the collected data to other cloud products such as OBS for centralized data management.
- Category management: When collecting data, the SecMaster manages the data by category. You can use this function to deliver data of different projects and types to different cloud products.

Prerequisites

- If you want to deliver data to an OBS bucket, the bucket must have private, public read, or public read/write policy enabled. Currently, parallel file buckets are not supported. For details, see **Creating an OBS Bucket**.

● To deliver data to LTS, ensure there are available log groups 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.

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

10.8.2 Delivering Logs to Other Data Pipelines

Scenario

This topic walks you through how to deliver logs to other pipelines. The main steps are as follows:

● **Step 1: Create a Data Delivery Task**

● **Step 2: Authorize the Data Delivery**

● **Step 3: View Data Delivery in the Destination Pipeline**

Limitations and Constraints

● When performing cross-account delivery, the data can only be delivered to the pipelines instead of cloud services of other accounts.

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

Step 1: Create a Data Delivery Task

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-128 Workspace management page
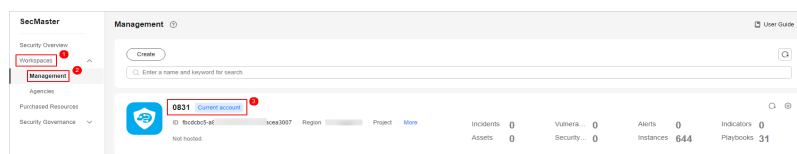
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-129 Accessing the Security Analysis tab page
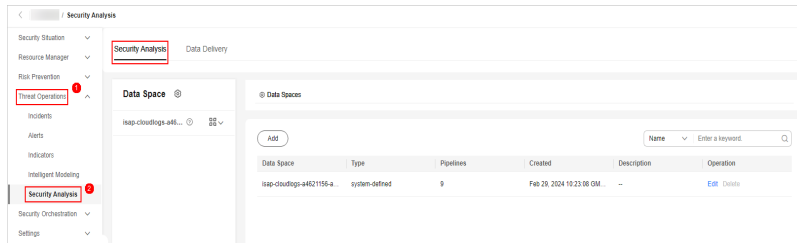
Step 6 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Deliver**.

Figure 10-130 Accessing data delivery settings page
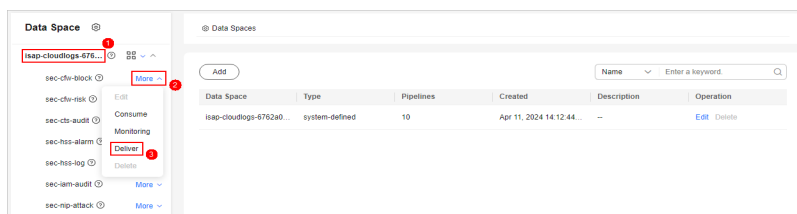
Step 7 (Optional) Confirm the authorization information, select **Agree to authorize**, and click **OK**.

Authorization is required first time you start a delivery to a specific destination type. If the destination type has been authorized, skip this step.

Step 8 On the **Create Delivery** panel, set data delivery parameters.

1. Configure basic information.

   Table 10-114 Basic Information

Parameter	Description
Delivery Name	The name you specify for the delivery.
Resource Consumption	The value is generated by default. **You do not need to configure it**.

2. Configure the data source.

   In the **Data Source Settings** area, the details about the current pipeline are displayed. **You do not need to set this parameter**.

   Table 10-115 Data source parameters

Parameter	Description
Delivery Type	Delivery destination type. The default value is **PIPE**.
Region	Region where the current pipeline is located.
Workspace	Workspace to which the current pipeline belongs.

Parameter	Description
Data Space	Data space to which the current pipeline belongs.
Pipeline	Name of the pipeline.
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 10-116**.

      Table 10-116 Destination parameters - Current account pipeline

Parameter	Description
Account Type	Account type for the data delivery destination. Select **Current**.
Delivery Type	Delivery type. Select **PIPE**.
Workspace	Workspace where the destination pipeline is located.
Data Space	Data space where the destination pipeline is located.
Pipeline	Pipeline where the destination pipeline is located.
Written To	The value is generated by default. You do not need to configure it.

      ▪ Cross-account delivery: Deliver the current pipeline data to the pipeline of another account. For details about the parameters, see **Table 10-117**.

      Table 10-117 Destination parameters - Pipelines of other account

Parameter	Description
Account Type	Account type for the data delivery destination. Select **Other** in this case.
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 pipeline is located. For details about how to query the workspace ID, see **Step 7**.
Data Space ID	ID of the data space where the destination pipeline is located. For details about how to query the data space ID, see **Step 7**.
Pipeline ID	ID of the destination pipeline. For details about how to query the pipeline ID, see **Step 7**.
Written To	The value is generated by default. You do not need to configure it.

4. Under **Access Authorization**, view the permissions granted in **Step 7**.

    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**.

----End

Step 2: Authorize the Data Delivery

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-131 Workspace management page
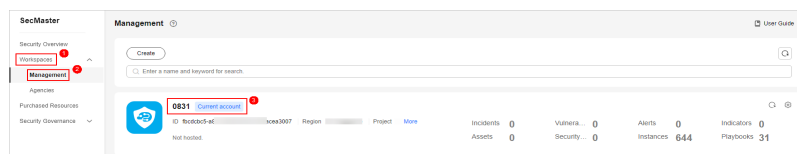
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Step 6 On the **Data Delivery** tab, 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 10-132 Authorization for data delivery
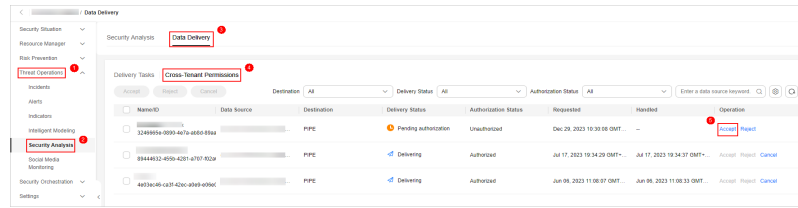
After the authorization is granted, the authorization status of the target delivery task is updated to **Authorized**. You can go to the delivery destination to view the delivery details.

----End

Step 3: View Data Delivery in the Destination Pipeline

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-133 Workspace management page
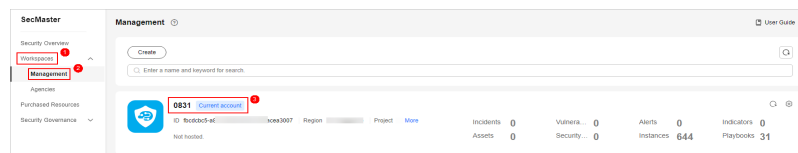
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-134 Accessing the Security Analysis tab page
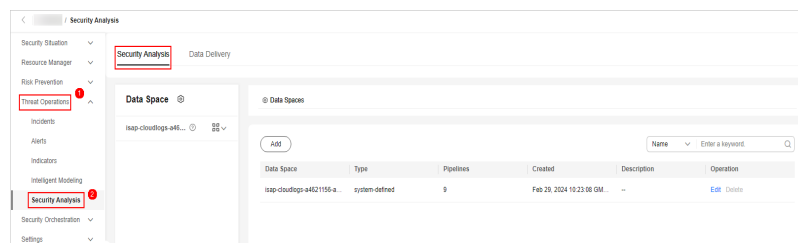
Step 6 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-135 Pipeline data page
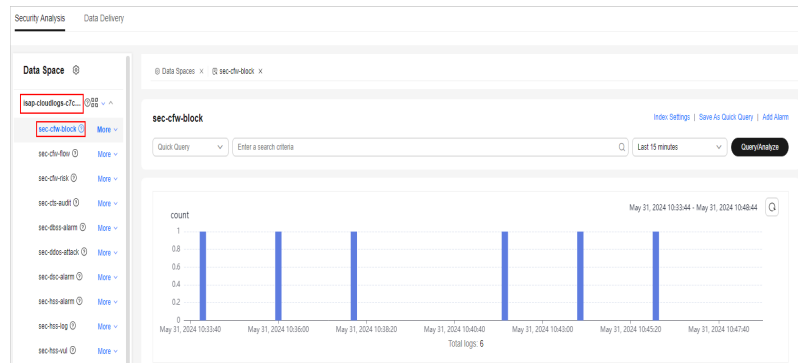
Step 7 In the target pipeline, view the delivery log.

----End

Operations Related to Data Delivery Authorization

On the **Cross-tenant Permissions** tab page, you can select to **Reject** or **Cancel** the authorization.

Table 10-118 Cross-tenant permission authorization options

Operation	Description
Reject	In the row containing the target delivery task, click **Reject** in the **Operation** column to reject the authorization.
	To reject authorization in batches, select all tasks to be rejected and click **Reject** in the upper left corner of the list.
Cancel	1. In the row containing the target delivery task, click **Cancel** in the **Operation** column to cancel the authorization. To cancel authorization in batches, select all tasks to be canceled and click **Cancel** in the upper left corner of the list. 2. In the displayed dialog box, click **OK**.

10.8.3 Delivering Logs to OBS

Scenarios

This topic walks you through how to deliver logs to an OBS bucket. The main steps are as follows:

Step 1: Create a Data Delivery Task

Step 2: Authorize the Data Delivery

Step 3: View the Delivered Data in OBS

Limitations and Constraints

- When performing cross-account delivery, the data can only be delivered to the pipelines instead of cloud services of other accounts.
- If the new data delivery is cross-account, you need to log in to SecMaster using the destination account and perform authorization.

Step 1: Create a Data Delivery Task

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-136 Workspace management page
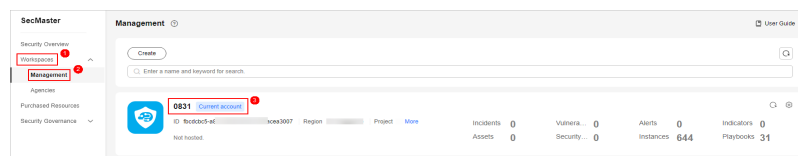
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-137 Accessing the Security Analysis tab page
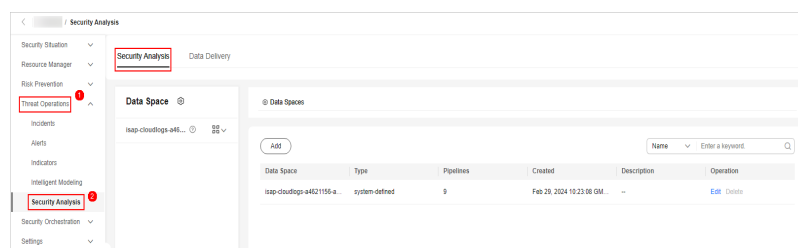
Step 6 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Deliver**.

Figure 10-138 Accessing data delivery settings page
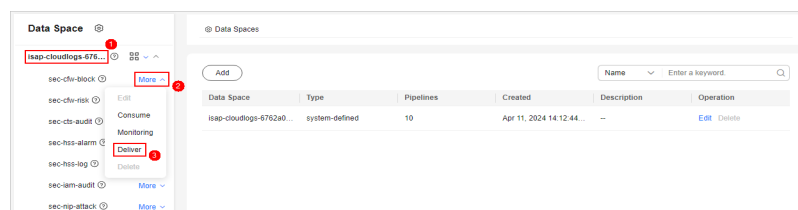
Step 7 (Optional) Confirm the authorization information, select **Agree to authorize**, and click **OK**.

Authorization is required first time you start a delivery to a specific destination type. If the destination type has been authorized, skip this step.

Step 8 On the **Create Delivery** panel, set data delivery parameters.

1. Configure basic information.

   Table 10-119 Basic Information

Parameter	Description
Delivery Name	The name you specify for the delivery.
Resource Consumption	The value is generated by default. **You do not need to configure it**.

2. Configure the data source.

   In the **Data Source Settings** area, the details about the current pipeline are displayed. **You do not need to set this parameter**.

   Table 10-120 Data source parameters

Parameter	Description
Delivery Type	Delivery destination type. The default value is **PIPE**.
Region	Region where the current pipeline is located.
Workspaces	Workspace to which the current pipeline belongs.
Data Space	Data space to which the current pipeline belongs.
Pipeline	Name of the pipeline.
Data Read Policy	Data read policy of the current pipeline.
Read By	Identity of the data source reader.

3. Configure the delivery destination.

   – **OBS**: Deliver the pipeline data to OBS. For details about the parameter settings, see **Table 10-121**.

     Note that the OBS bucket you use must have private, public read, or public read/write policy enabled. Currently, parallel file buckets are not supported. For details, see **Creating an OBS Bucket**.

Table 10-121 Data delivery destination - OBS

Parameter	Description
Account Type	Account type for the data delivery destination. When you deliver data to OBS, only the **Current** account type can be selected.
Delivery Type	Delivery type. Select **OBS** in this case.
Bucket Name	Name of the destination OBS bucket.
Written To	The value is generated by default. You do not need to configure it.

4. Under **Access Authorization**, view the permissions granted in **Step 7**.

    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**.

----End

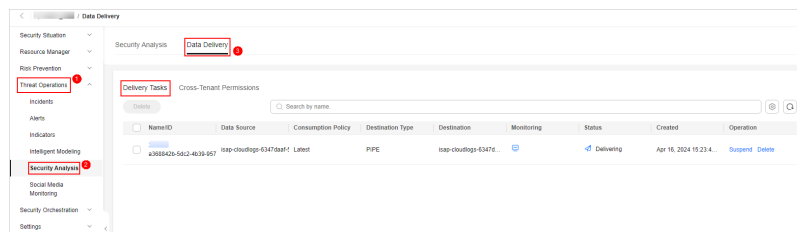## Step 2: Authorize the Data Delivery

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-139 Workspace management page
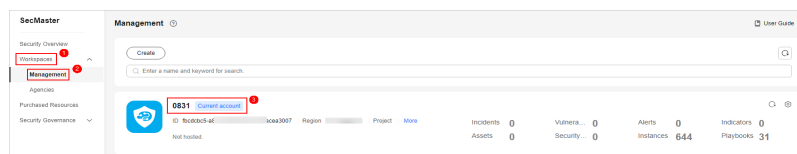
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Step 6 On the **Data Delivery** tab, 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 above the list.

Figure 10-140 Data delivery authorization
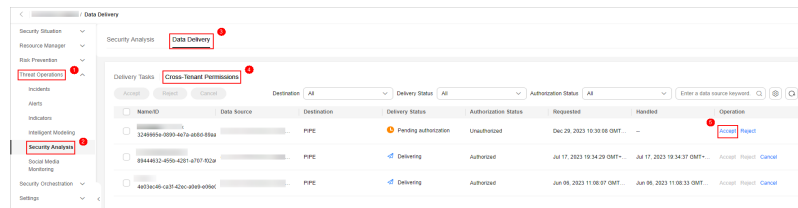
After the authorization is granted, the authorization status of the target delivery task is updated to **Authorized**. You can go to the delivery destination to view the delivery details.

----End

Step 3: View the Delivered Data in OBS

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

**Step 3** Click ☰ in the upper left corner of the page and choose **Storage** > **Object Storage Service**. The bucket list page is displayed.

Step 4 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 5 On the OBS bucket details page, view the delivery log information.

----End

Operations Related to Data Delivery Authorization

On the **Cross-tenant Permissions** tab page, you can select to **Reject** or **Cancel** the authorization.

Table 10-122 Cross-tenant permissions management

Operation	Method
Reject	In the row containing the target delivery task, click **Reject** in the **Operation** column to reject the authorization. To reject authorization in batches, select all tasks to be rejected and click **Reject** in the upper left corner of the list.

Operation	Method
Cancel	1. In the row containing the target delivery task, click **Cancel** in the **Operation** column to cancel the authorization. To cancel authorization in batches, select all tasks to be canceled and click **Cancel** in the upper left corner of the list. 2. In the displayed dialog box, click **OK**.

10.8.4 Delivering Logs to LTS

Scenario

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

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

This topic walks you through how to deliver integrated logs to LTS. The procedure is as follows:

- **Step 1: Create a Data Delivery Task**
- **Step 2: Authorize the Data Delivery**
- **Step 3: View the Delivered Data in 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**.

Step 1: Create a Data Delivery Task

Step 1 Log in to the management console.

Step 2 Click ⚲ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-141 Workspace management page
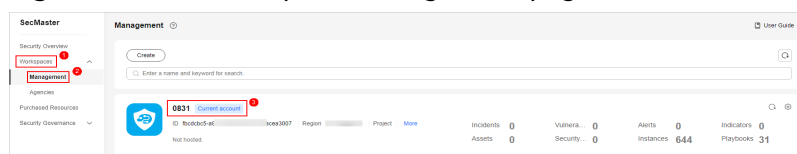
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.

Figure 10-142 Accessing the Security Analysis tab page
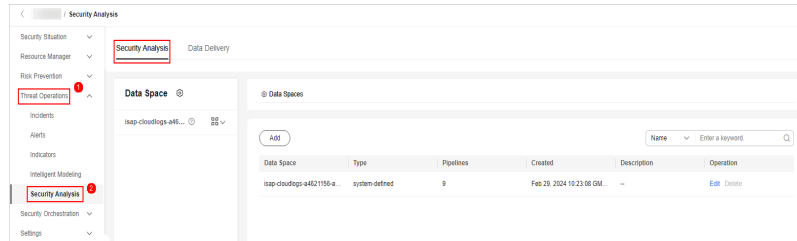
Step 6 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Deliver**.

Figure 10-143 Accessing data delivery settings page
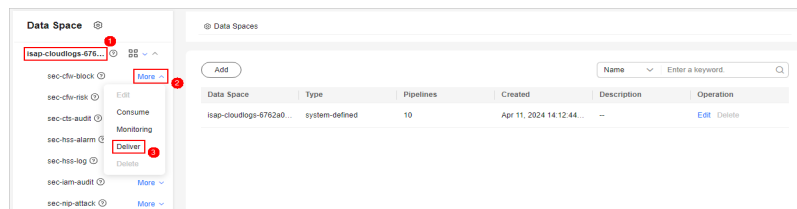
Step 7 (Optional) Authorization is required first time you start a delivery to a specific destination type. If the destination type has been authorized, skip this step.

Confirm the authorization information, select **Agree to authorize** and click **OK**.

Step 8 On the **Create Delivery** panel, 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 9 Under **Access Authorization**, view the permissions granted in **Step 7**.

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 10 Click **OK**.

----End

Step 2: Authorize the Data Delivery

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
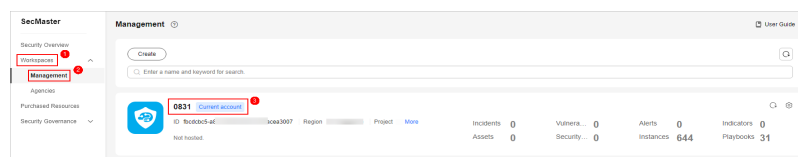
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Step 6 On the **Data Delivery** tab, 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 above the list.

Figure 10-145 Authorization for data delivery
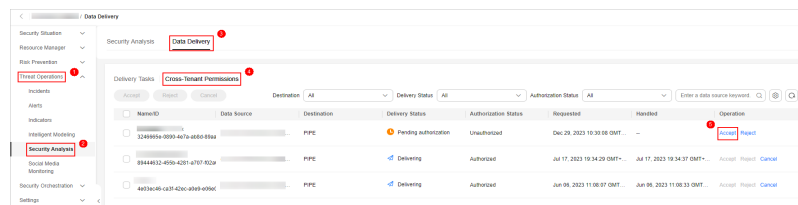
After the authorization is granted, the authorization status of the target delivery task is updated to **Authorized**. You can go to the delivery destination to view the delivery details.

----End

Step 3: View the Delivered Data in LTS

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Management & Governance** > **Log Tank Service**.

Step 4 In the log group list on the **Log Management** page, locate the log group for which you want to add data delivery and click ˅ before the log group name.

Step 5 Click the name of the log stream selected during data delivery. The log stream details page is displayed.

Step 6 On the log stream details page, view the delivered logs.

----End

Operations Related to Data Delivery Authorization

On the **Cross-tenant Permissions** tab page, you can select to **Reject** or **Cancel** the authorization.

Table 10-123 Cross-tenant permissions management

Operation	Method
Reject	In the row containing the target delivery task, click **Reject** in the **Operation** column to reject the authorization.
	To reject authorization in batches, select all tasks to be rejected and click **Reject** in the upper left corner of the list.
Cancel	1. In the row containing the target delivery task, click **Cancel** in the **Operation** column to cancel the authorization. To cancel authorization in batches, select all tasks to be canceled and click **Cancel** in the upper left corner of the list.
	2. In the displayed dialog box, click **OK**.

10.8.5 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 management console and select a region or project.

**Step 3** Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
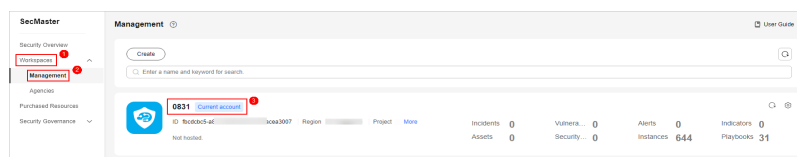
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Figure 10-147 Data Delivery tab page
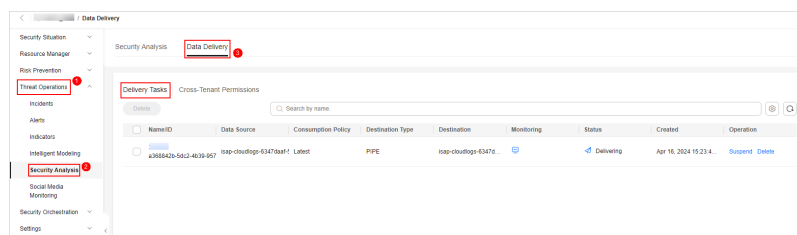
Step 6 On the delivery task list page, view existing delivery tasks.

Table 10-124 Delivery task parameters

Operation	Description
Name/ID	Delivery task name and ID
Data Source	Pipeline where the data source is located
Consumption Policy	Consumption policy of a delivery task
Destination Type	Type of the data delivery destination
Destination	Data delivery destination
Monitoring	Data delivery monitoring status. You can click the monitoring icon to view the data consumption information.
Status	Status of a delivery task

Operation	Description
Created	Time when a delivery task is created
Operation	You can delete or suspend a data delivery task.

----End

Suspending a Delivery Task

After a data delivery task is added and authorized, the delivery task status changes to **Delivering**. To stop the delivery, you can suspend the target delivery task.

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
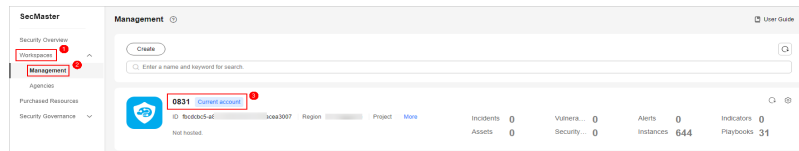
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Figure 10-149 Data Delivery tab page
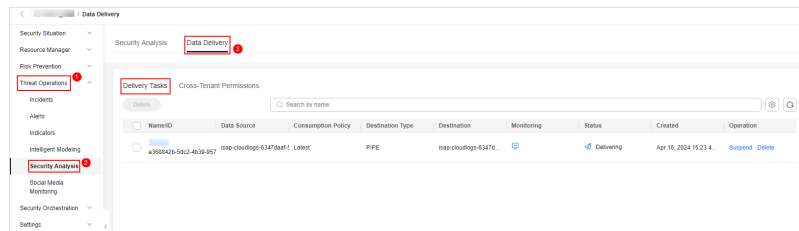
Step 6 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Suspend** in the **Operation** column.

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 ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-150 Workspace management page
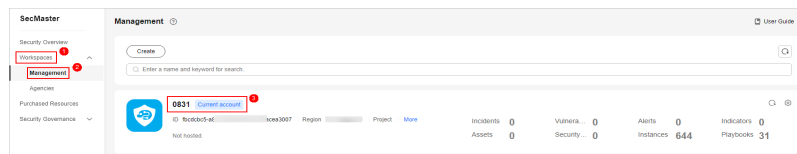
Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Figure 10-151 Data Delivery tab page

Step 6 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 ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Threats** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Figure 10-153 Data Delivery tab page
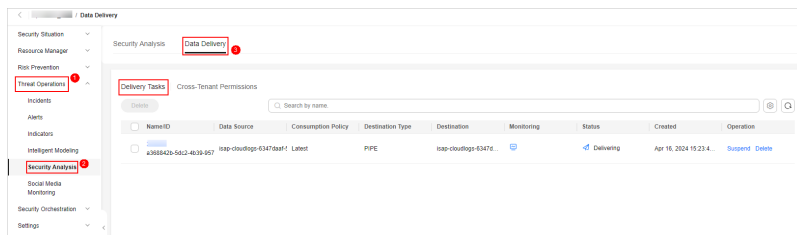
Step 6 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Delete** in the **Operation** column and click **OK** in the displayed dialog box.

----End

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.

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

- Definition:
  - A playbook is a formal representation of the security operations workflow in a security orchestration system. A playbook converts the security operations workflows and procedures into a machine-readable work flow. A playbook is a predefined, structured response plan used to handle specific types of incidents or threats. A playbook explicitly lists the steps and actions to be taken under certain trigger conditions, such as the detection of a specific security incident.

    Playbooks embody the logic of security protection controls and schedule security capabilities. Playbooks are flexible and scalable. They can be modified and extended based on actual requirements to adapt to ever-changing security threats and service requirements.

    A playbook can have only one workflow.

  - A workflow is a collaborative work mode that integrates various capabilities related to security operation, such as tools, technologies, workflows, and personnel. It consists of multiple connected components. After defined in a workflow, these components can be triggered externally. For example, when a new service ticket is generated, the automatic service ticket review workflow is automatically triggered. You can use the visual canvas to define component actions for each node in a workflow.

A workflow is a response mode when a playbook is triggered. Workflows convert instructions and procedures in the corresponding playbook into specific actions and execution steps.

- Relationships and differences
  - Relationship: A playbook provides guidance and rules for secure operations, and its workflow is responsible for converting these rules into specific execution steps and actions. A playbook and its workflow depend on each other. The playbook guides the execution of the workflow, while the workflow implements the intent and requirements of the playbook.
  - Differences: There are also some differences between playbooks and workflows. First, playbooks focus more on defining and describing security operation processes and regulations, so they focus on the overall framework and policies. Workflows focus more on specific actions and execution steps, so they focus on how to convert requirements in playbooks into actual actions. Second, playbooks are flexible and scalable, and can be modified and extended as required. However, workflows are relatively fixed. Once the design is complete, they need to follow the specified steps.

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

Limitations and Constraints

- In a workspace of an account, the schedule interval of a playbook cannot be less than 5 minutes.
- The maximum number of retries within a day in a workspace of an account is as follows:
  - Manual retries: 100. After a retry, the playbook cannot be retried until the current execution is complete.
  - API retries: 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 workspace of an account, a maximum of 50 classification & mapping templates can be created.
  - In a workspace of an 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 an account.

Security Orchestration Process

The process of using security orchestration is as follows.

Figure 11-1 Security orchestration process
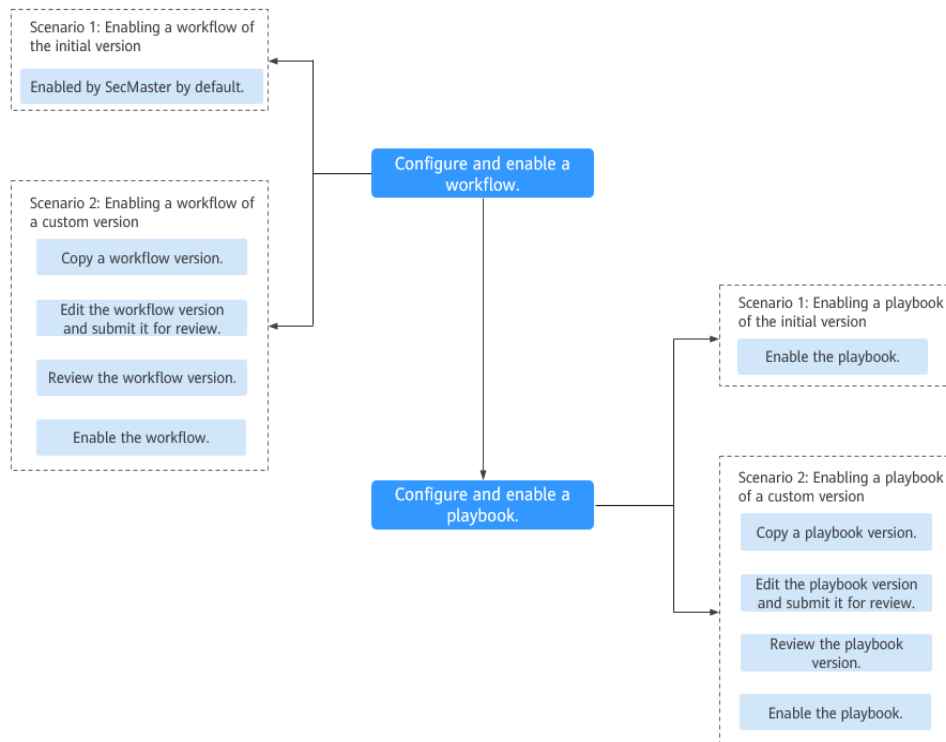
Table 11-1 Procedure

No.	Operation	Description
1	**Enabling a Workflow**	A workflow determines how a playbook responds to threats when it is triggered. SecMaster provides some preconfigured workflows, such as WAF one-click unblocking, HSS alert synchronization, and alert metric extraction.
		Workflows can be enabled in the following scenarios:
		● Scenario 1: Using a workflow of the initial version The initial version (V1) of a workflow is automatically enabled.
		● Scenario 2: Using a workflow of a custom version You can copy the initial version of a workflow and edit it to create a custom workflow version. To enable a custom workflow version, take the following steps:
		1. **Copy a workflow version**.
		2. **Edit and submit the workflow version**.
		3. **Review the workflow version**.
		4. **Enable the workflow**.

No.	Operation	Description
2	**Enabling a Playbook**	A playbook describes how SecMaster handles a type of security issues. Playbooks express security operations process of SecMaster in the entire security orchestration system.
		SecMaster provides some preconfigured playbooks such as **Fetching Indicator from alert**, **Synchronization of HSS alert status**, and **Automatic disabling of repeated alerts**. Most preconfigured 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.
		Playbooks can be enabled in the following scenarios:
		● Scenario 1: Using a playbook of the initial version The initial version (V1) of a playbook is activated by default. So you can enable a playbook of the initial version directly. For details, see **Enabling a Playbook**.
		● Scenario 2: Using a playbook of a custom version If you want to use a playbook that is not enabled, you can modify the playbook version and then enable it. To enable a custom playbook version, take the following steps:
		1. **Copy a playbook of a version**.
		2. **Edit and submit the playbook version**.
		3. **Review the playbook version**.
		4. **Enable the playbook**.

11.2 Playbook Orchestration Management

11.2.1 Enabling a Workflow

A workflow determines how a playbook responds to threats when it is triggered. SecMaster provides some preconfigured workflows, such as WAF one-click

unblocking, HSS alert synchronization, and alert metric extraction. The initial version (V1) of a workflow is automatically enabled. You can edit existing workflow versions to create custom workflows.

This topic describes how to configure and enable custom workflows. The procedure is as follows:

- **Copy a workflow version**.
- **Editing and Submitting a Workflow Version**
- **Review the workflow version**.
- **Enable the workflow**.

Prerequisites

The workflow must have an activated version. For details, see **Managing Workflow Versions**.

Copying a Workflow Version

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
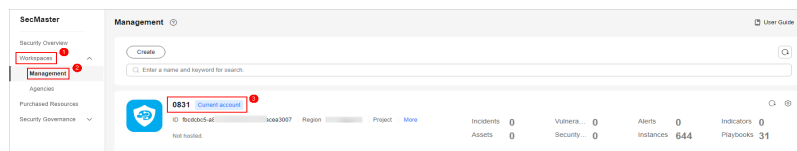
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-3 Workflows tab
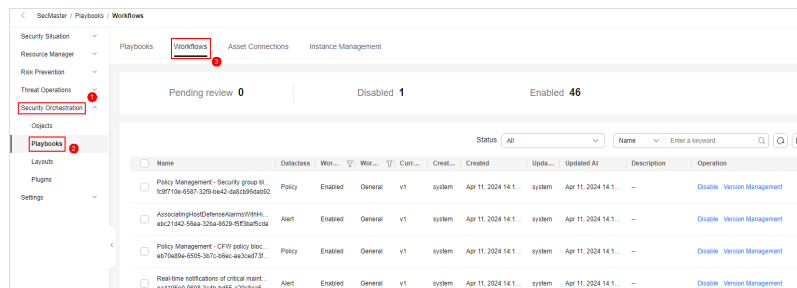
Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-4 Version Management page

Step 7 On the **Version Management** slide-out panel for the workflow, in the **Version Information** area, locate the row containing the target workflow version, and click **Clone** in the **Operation** column.

Step 8 In the displayed dialog box, click **OK**.

----End

Editing and Submitting a Workflow Version

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-5 Workspace management page

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-6 Workflows tab

Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-7 Version Management page
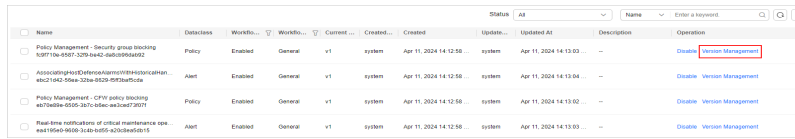
Step 7 On the **Version Management** slide-out panel for the workflow, in the **Version Information** area, locate the row containing the target workflow version, and click **Edit** in the **Operation** column.

Step 8 On the workflow canvas, drag basic, workflow, and plug-in nodes from **Resource Libraries** on the left to the canvas on the right.

Table 11-2 Resource Libraries parameters

Parameter			Description
Basic	Basic Node	StartEvent	The start of the workflow. Each workflow can have only one start node. The entire workflow starts from the start node.
		EndEvent	The end of the 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. The subsequent nodes in the workflow continue to be executed only after the user task is completed. **Table 11-3** describes the manual review parameters.
		SubProcess	Another workflow added in the workflow. It is equivalent to the loop body in the workflow.
	System Gateway	ExclusiveGateway	For an exclusive, diverging gateway, the workflow chooses only the path that matches the conditional expression to proceed. For an exclusive, converging gateway, the workflow chooses the path arrives the gateway first to proceed.
		ParallelGateway	For a parallel, diverging gateway, the workflow executes all paths arrive the gateway. For a parallel, converging gateway, the workflow executes the subsequent node only when all paths arrive the gateway. (If one path fails, the entire workflow fails.)

Parameter			Description
		InclusiveGateway	For an inclusive, diverging gateway, the workflow executes all paths that match conditional expressions.
			For an inclusive, converging gateway, the workflow executes the subsequent node only when all paths executed during diverging arrive the gateway. (If one path fails, the entire workflow fails.)
Workflows			You can select all released workflows in the current workspace.
Plug-ins			You can select all plug-ins in the current workspace.

Table 11-3 UserTask parameters

Parameter	Description
Primary key ID	A primary key ID is generated by the system. You can change it if needed.
Name	Name of the manual review node.
Valid Till	Time the manual review node expires.
Description	Description of the manual review node.
View Parameters	Click ≫ . On the **Select Context** pane displayed, select a parameter. To add a parameter, click **Add Parameter**.
Manual Processing Parameters	Input Parameter Key. To add a parameter, click **Add Parameter**.

Step 9 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
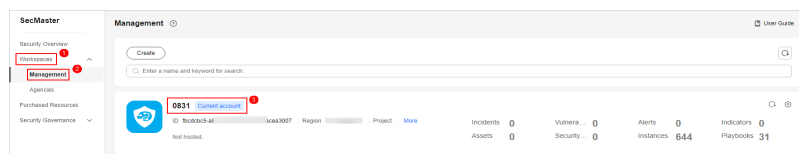
Reviewing a Workflow Version

Step 1 Log in to the management console.

Step 2 Click ◉ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
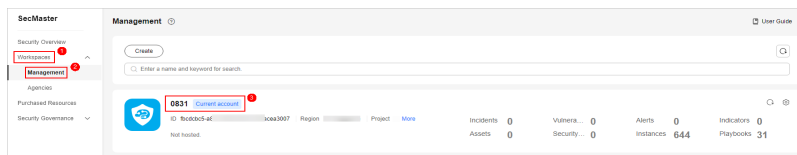
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-8 Workspace management page
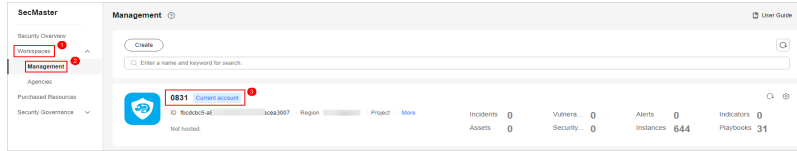
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-9 Workflows tab
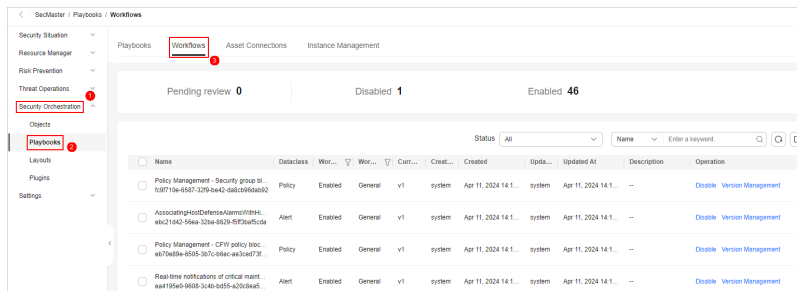
Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-10 Version Management page
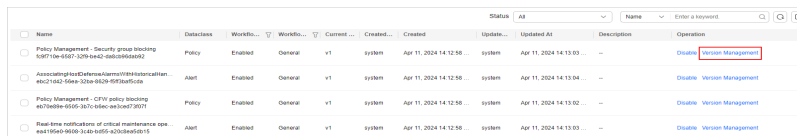
Step 7 On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target workflow.

Step 8 Set **Comment**. Table 11-4 describes the parameters.

Table 11-4 Workflow review parameters

Parameter	Description
Comment	Select the review conclusion. ● **Passed**: If the workflow version is approved, the status of the workflow version changes to **Activated**. ● **Reject**. If the workflow version is rejected, the status of the workflow version changes to **Rejected**. You can edit the workflow version and submit it again.
Reason for Rejection	Enter the review comment. This parameter is mandatory when **Reject** is selected for **Comment**.

📖 NOTE

- You can edit a rejected workflow version. For details, see **Managing Workflow Versions**.
- Workflow version status change:

  If the current workflow has only one workflow version, the status of the approved workflow version **Status** is **Activated** by default.

Step 9 Click **OK** to complete the workflow version review.

----End

Enabling a Workflow

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-11 Workspace management page
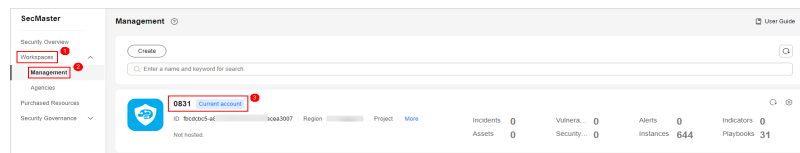
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-12 Workflows tab
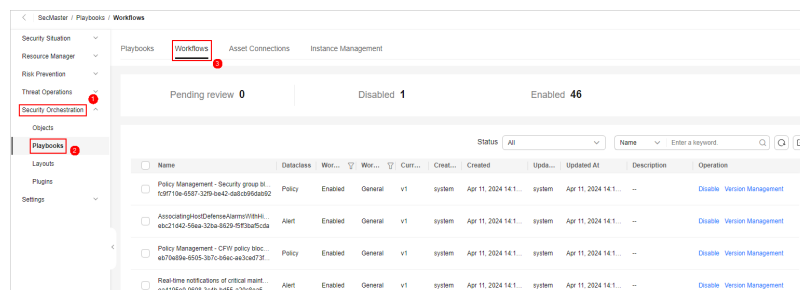
Step 6 In the row containing the target workflow, click **Enable** in the **Operation** column.

Step 7 In the slide-out panel that is displayed, select the workflow version to be enabled and click **OK**.

----End

11.2.2 Enabling a Playbook

A playbook describes how SecMaster handles a type of security issues. Playbooks express security operations process of SecMaster in the entire security orchestration system.

SecMaster provides some preconfigured playbooks such as **Fetching Indicator from alert**, **Synchronization of HSS alert status**, and **Automatic disabling of repeated alerts**. Most preconfigured 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, 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.

- Scenario 1: The initial version (V1) of a playbook is activated by default. So you can enable a playbook of the initial version directly. For details, see **Enabling a Playbook**.

- Scenario 2: If you want to use a playbook that is not enabled, you can modify the playbook version and then enable it. To enable a custom playbook version, take the following steps:
  - **Copy a playbook version**.
  - **Edit and submit the playbook version**.
  - **Reviewing a Playbook Version**
  - **Enabling a Playbook**

Prerequisites

- The workflow associated with the playbook has been enabled. For details, see **Enabling a Workflow**.

- The playbook has an activated version. For details, see **Activating/ Deactivating a Playbook Version**.
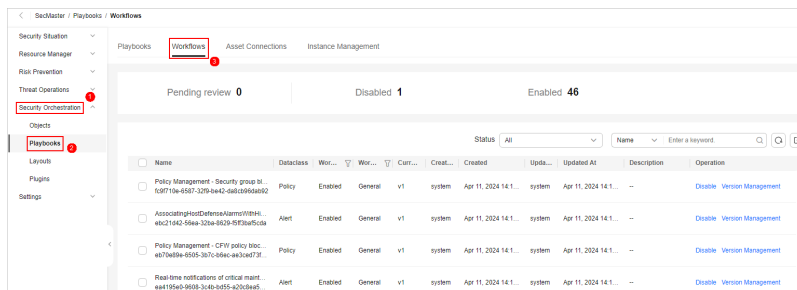
Copying a Playbook Version

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-13 Workspace management page
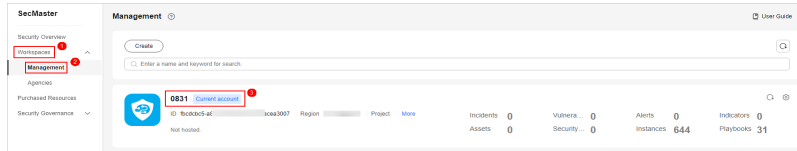
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-14 Accessing the Playbooks tab
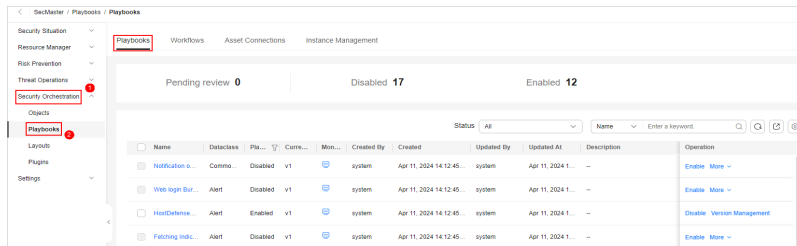
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-15 Version Management slide-out panel
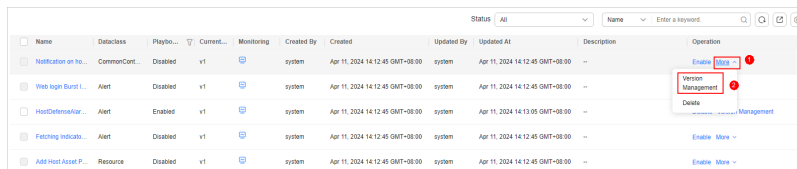
Step 7 On the **Version Management** slide-out panel, in the **Version Information** area, locate the row containing the desired playbook version, and click **Clone** in the **Operation** column.

Step 8 In the displayed dialog box, click **OK**.

**----End**

Editing and Submitting a Playbook Version

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
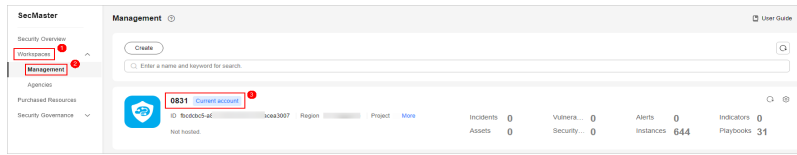
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-17 Accessing the Playbooks tab
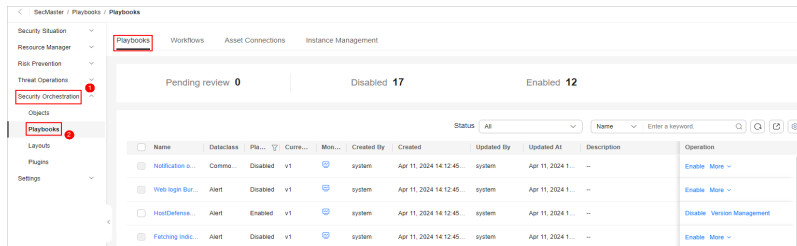
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-18 Version Management slide-out panel
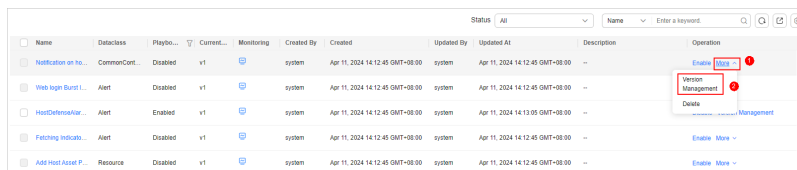
Step 7 On the **Version Management** slide-out panel, in the **Version Information** area, locate the row containing the desired playbook version, and click **Edit** in the **Operation** column.

Step 8 On the page for editing a playbook version, edit the version information.

Step 9 Click **OK**.

Step 10 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 11 In the confirmation dialog box, click **OK** to submit the playbook version.

📖 **NOTE**

- After the playbook version is submitted, **Version Status** changes to **Pending review**.
- After a playbook version is submitted, it cannot be edited. To edit it, create a version or reject it during review.

----End

Reviewing a Playbook Version

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-19 Workspace management page
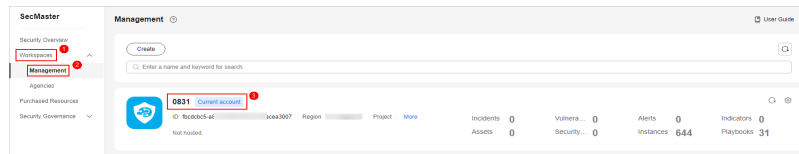
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-20 Accessing the Playbooks tab
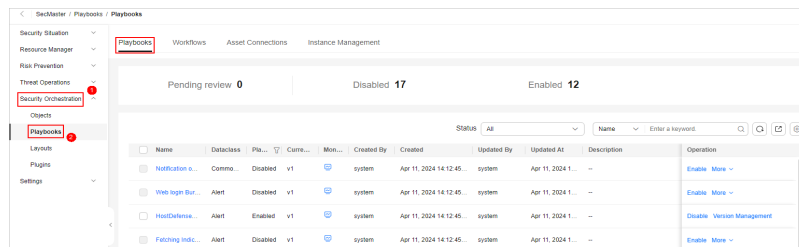
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-21 Version Management slide-out panel
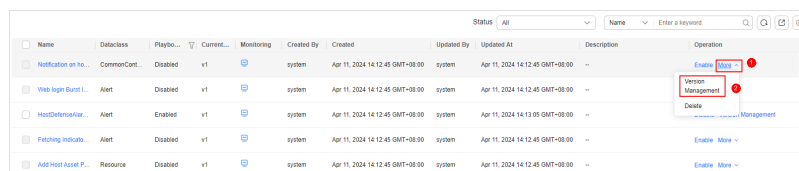
Step 7 On the **Version Management** slide-out panel, click **Review**.

Step 8 On the **Review Playbook Version** page, enter the review information. **Table 11-5** describes the parameters for reviewing a playbook version.

Table 11-5 Parameters for reviewing a playbook version

Parameter	Description
Comment	Select the review conclusion. **Passed**: If the playbook version is approved, the status of the workflow version changes to **Activated**. **Reject**. If the playbook version is rejected, the status of the workflow version changes to **Rejected**. You can edit the workflow version and submit it again.

Parameter	Description
Reason for Rejection	This parameter is mandatory when **Comment** is **Reject**. Enter the review comment. This parameter is mandatory when **Reject** is selected for **Comment**.

☐ NOTE

If there is only one version available for the current playbook, the version is in the **Activated** state by default after being approved.

Step 9 Click **OK** to complete the playbook version review.

----End

Enabling a Playbook

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-23 Accessing the Playbooks tab
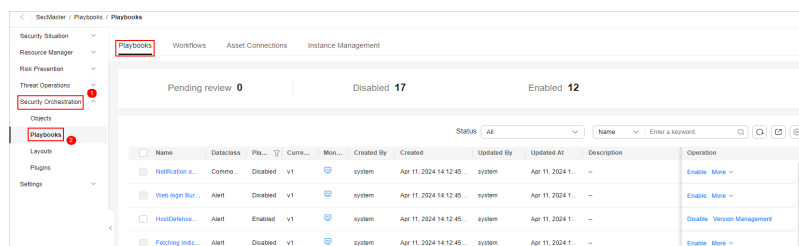
Step 6 In the **Operation** column of the target playbook, click **Enable**.

Step 7 Select the playbook version you want to enable and click **OK**.

----End

11.2.3 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-25 Workflows tab
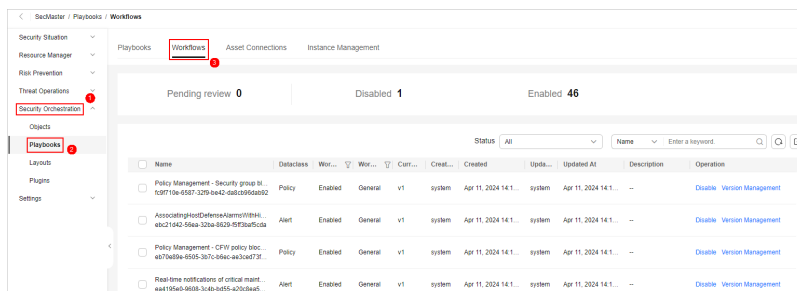
Step 6 On the **Workflows** page, view details about the created workflow.

Figure 11-26 Viewing workflows

- The numbers of **Pending review**, **Not enabled**, and **Enabled** workflows are displayed above the workflow list.
- View information about existing workflows in the workflow list.

  If there are many workflows displayed, use filters to search for a specific one.

Table 11-6 Workflow parameters

Parameter	Description
Name	Workflow name
Dataclass	Data class corresponding to a workflow.
Workflow Status	Current status of a workflow. The status can be **Enabled** or **Disabled**.
Workflow Type	Current type of a workflow.
Current Version	Current version of a workflow.
Created By	User who creates the workflow.
Created	Time when a workflow was created
Updated By	User who modifies the workflow last time.
Updated At	Time when a workflow is last updated.
Description	A description of the workflow.
Operation	You can perform operations such as enabling and managing versions in the **Operation** column.

- To view details about a workflow, click its name to access its details page.

----End

Exporting Workflows

☐ **NOTE**

Workflows in the **Enabled** state can be exported.

Step 1 Log in to the managuent console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-27 Workspace management page
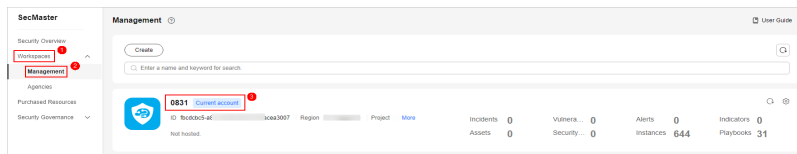
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-28 Workflows tab

Step 6 On the **Workflows** tab page, select the workflows to be exported and click ⧉ in the upper right corner of the list.

Step 7 In the dialog box that is displayed, click **OK**. The system exports the workflows to the local host.

----End

Deleting Workflows

📖 **NOTE**

All of the following conditions must be met before you can delete a workflow:

● The workflow is in the **Disabled** state.

● The workflow does not contain an activated workflow version.

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-29 Workspace management page
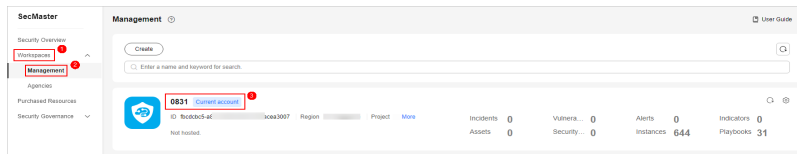
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-30 Workflows tab
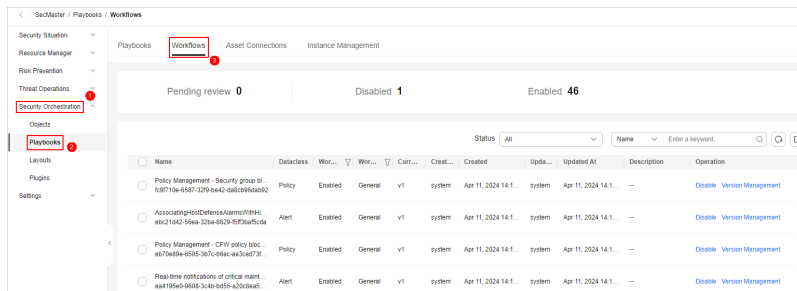
Step 6 On the **Workflows** tab page, locate the row containing the target workflow and click **Delete** in the **Operation** column.

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

📖 **NOTE**

During deletion, all historical versions in the current workflow are deleted by default. Deleted versions cannot be restored.

----End

Disabling a Workflow

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-31 Workspace management page
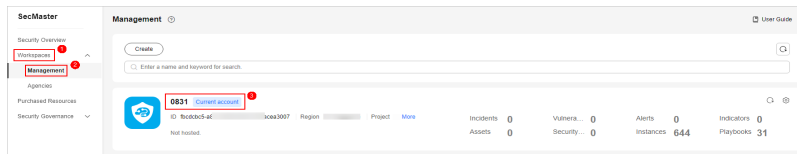
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-32 Workflows tab
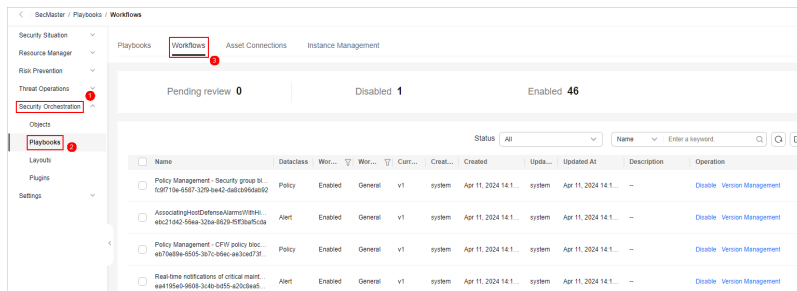
Step 6 In the row containing the target workflow, click **Disable** in the **Operation** column.

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

----End

11.2.4 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 management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-33 Workspace management page
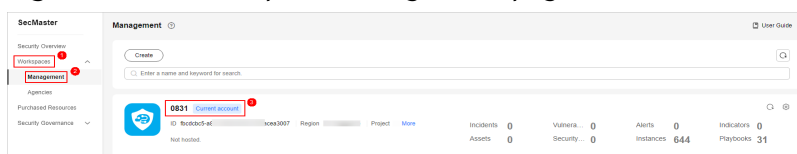
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-34 Workflows tab
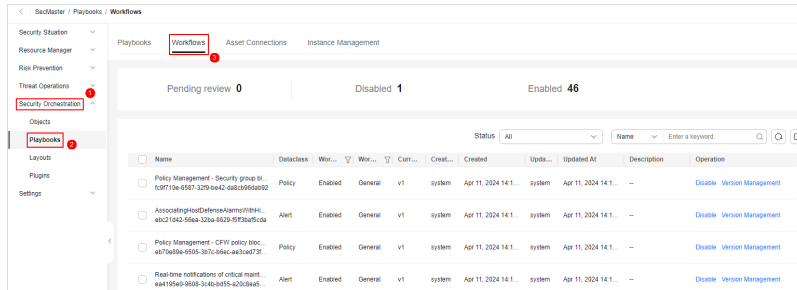
Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-35 Version Management page
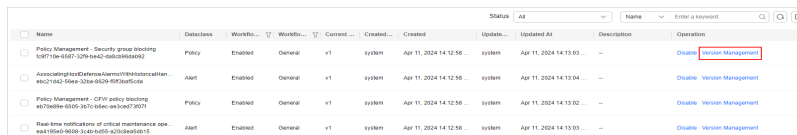
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Copy** in the **Operation** column.

Step 8 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 management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
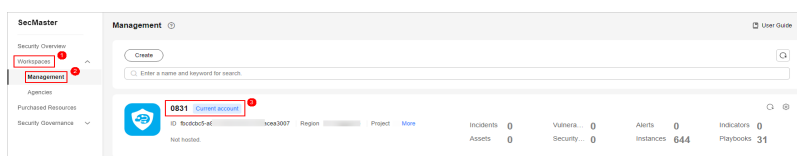
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-37 Workflows tab
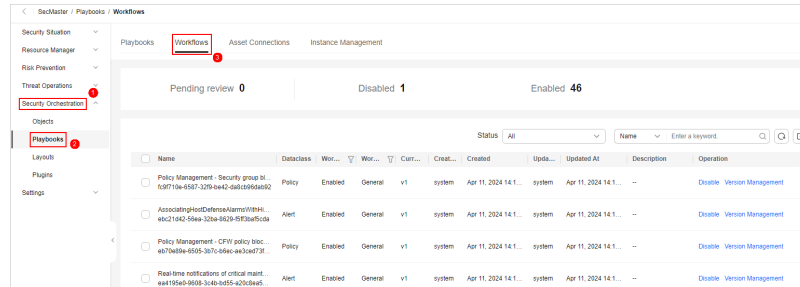
Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-38 Version Management page
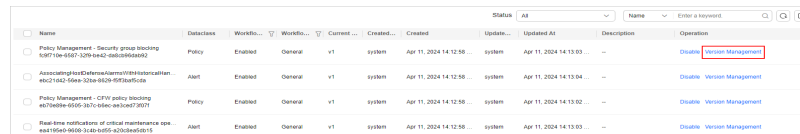
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Edit** in the **Operation** column.

Step 8 On the workflow canvas, drag basic, workflow, and plug-in nodes from **Resource Libraries** on the left to the canvas on the right.

Table 11-7 Resource Libraries parameters

Parameter			Description
Basic	Basic Node	StartEvent	The start of the workflow. Each workflow can have only one start node. The entire workflow starts from the start node.
		EndEvent	The end of the 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. The subsequent nodes in the workflow continue to be executed only after the user task is completed. **Table 11-8** describes the manual review parameters.
		Step	Another workflow added in the workflow. It is equivalent to the loop body in the workflow.

Parameter			Description
	System Gateway	ExclusiveGateway	For diverged line flows, the workflow chooses only the first line flow that matches the conditional expression to proceed. During line flow converging, the workflow chooses the line flow first arrives to proceed.
		ParallelGateway	During line diverging, all lines are executed. During line converging, the subsequent node can be executed only when all lines arrive. (If one line fails, the entire workflow fails.)
		InclusiveGateway	During line diverging, all lines that match conditional expressions are executed. The subsequent node can be executed only when all executed diverged lines arrive the inclusive gateway. (If one line fails, the entire workflow fails.)
Workflows			You can select all released workflows in the current workspace.
Plug-ins			You can select all plug-ins in the current workspace.

Table 11-8 UserTask parameters

Parameter	Description
Primary key ID	A primary key ID is generated by the system. You can change it if needed.
Name	Name of the manual review node.
Valid Till	Time the manual review node expires.
Description	Description of the manual review node.
View Parameters	Click 》. On the **Select Context** pane displayed, select a parameter. To add a parameter, click **Add Parameter**.
Manual Processing Parameters	Input Parameter Key. To add a parameter, click **Add Parameter**.

Step 9 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 [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-39 Workspace management page
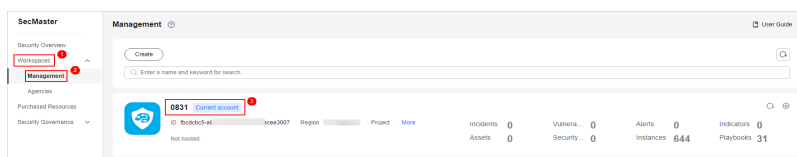
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-40 Workflows tab
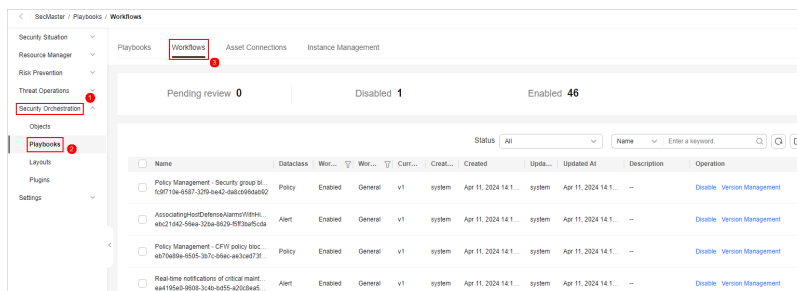
Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-41 Version Management page
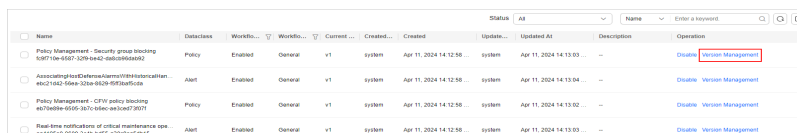
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Submit** in the **Operation** column.

Figure 11-42 Submitting a workflow version
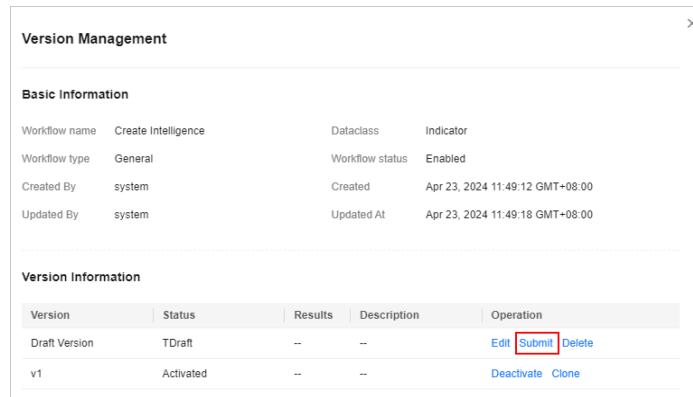
Step 8 In the confirmation dialog box, click **OK** to submit the workflow version.

☐ 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.
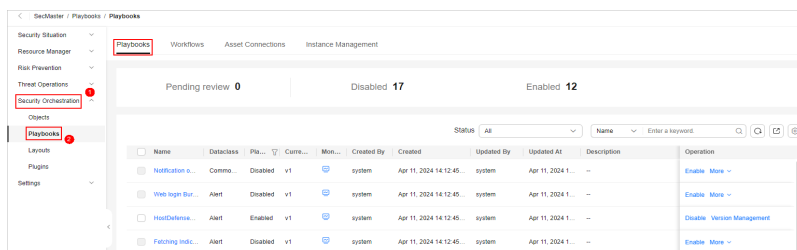
Step 1 Log in to the management console.

Step 2 Click ⬥ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-43 Workspace management page
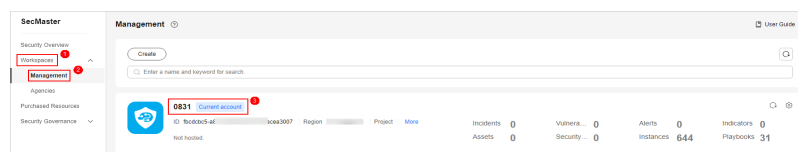
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-44 Workflows tab
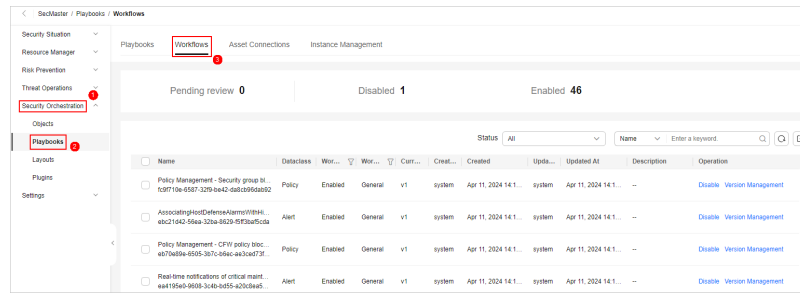
Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-45 Version Management page
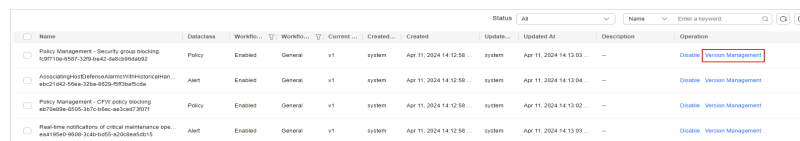
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Activate** or **Deactivate** in the **Operation** column.

Figure 11-46 Example deactivating a workflow version
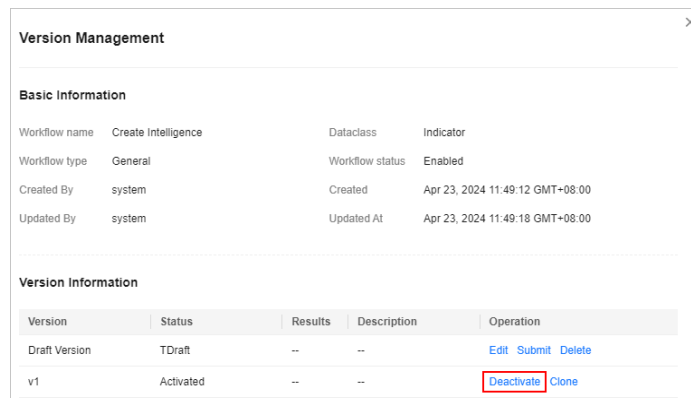
**Step 8** In the dialog box that is displayed, click **OK**.

----End

Deleting a Workflow Version

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-47 Workspace management page
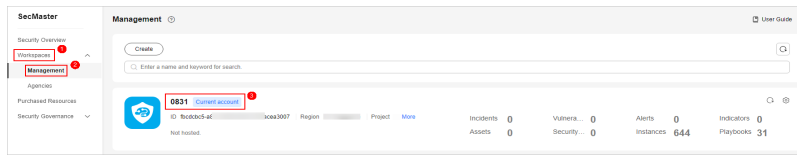
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

Figure 11-48 Workflows tab
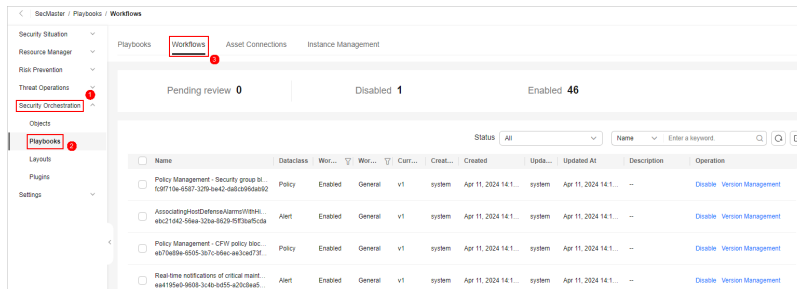
Step 6 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-49 Version Management page
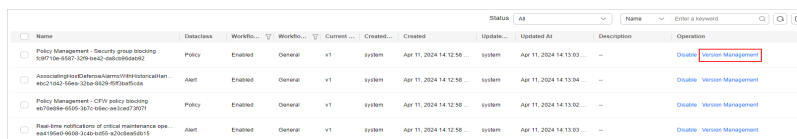
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row of the target workflow version, and click **Delete** in the **Operation** column.

Step 8 In the displayed dialog box, click **OK**.

📖 **NOTE**

Deleted workflow versions cannot be retrieved. Exercise caution when performing this operation.

----End

11.2.5 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 ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
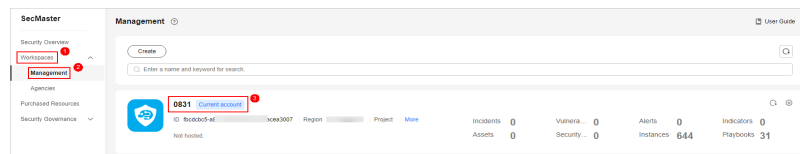
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-51 Accessing the Playbooks tab
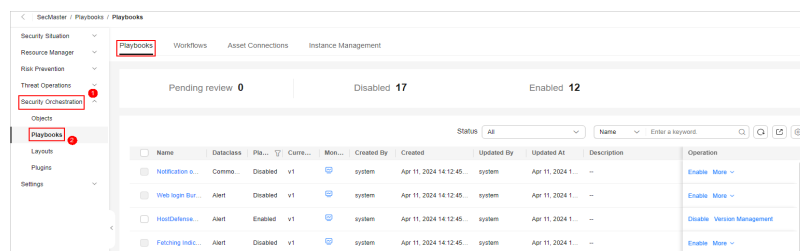
Step 6 On the **Playbooks** tab page, view playbook information.

Figure 11-52 Viewing playbook information
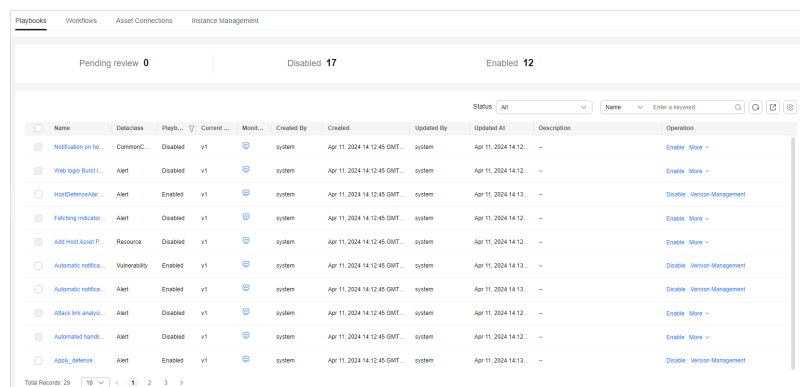
- The numbers of **Pending review**, **Not enabled**, and **Enabled** playbooks are displayed above the playbook list.
- View the information about existing playbooks.

  If there are many playbooks displayed, use filters to search for a specific one.

  To view details about a playbook, click its name to go to its details page.

Table 11-9 Playbook parameters

Parameter	Description
Name	Name of the playbook to be created.
Dataclass	Data class of the playbook
Playbook Status	Current status of the playbook The status can be Enabled or Disabled.
Current Version	Current version of the playbook
Monitoring	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, and minimum running duration. Average running duration = Total running duration of instances/Total number of instances. – Instance Status Statistics: allows you to view the total number of running instances, the number of successfully running instances, the number of running instances, the number of failed instances, and the number of terminated instances.
Created By	User who creates the playbook
Created	Time when a playbook is created.
Updated By	User who last modified the playbook
Updated At	Time when the playbook was last updated.
Description	Description of a playbook

----End

Exporting Playbooks

☐ **NOTE**

SecMaster supports the export of playbooks whose **Status** is **Enabled**.

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
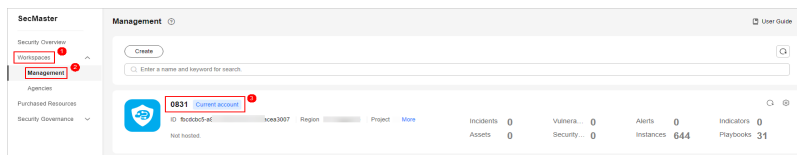
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-54 Accessing the Playbooks tab

Step 6 Select the playbooks to be exported and click ![icon] in the upper right corner of the list. The dialog box for confirming the export is displayed.

Step 7 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 ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-56 Accessing the Playbooks tab

Step 6 In the **Operation** column of the target playbook, click **Disable**. A confirmation dialog box is displayed.

Step 7 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 management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-58 Accessing the Playbooks tab
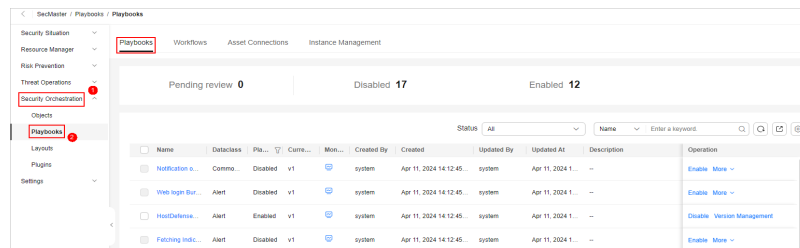
Step 6 In the **Operation** column of the playbook to be deleted, click **Delete**.

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

📖 **NOTE**

> Deleting a playbook will delete all its versions by default. Deleted playbook versions cannot be restored. Exercise caution when performing this operation.

----End

11.2.6 Managing Playbook Versions

Scenario

This section describes how to manage playbook versions, including **Previewing Playbook Versions**, **Editing a Playbook Version**, **Activating/Deactivating a Playbook Version**, **Copying a Playbook Version**, and **Deleting a Playbook Version**.

Previewing Playbook Versions

📖 **NOTE**

> The draft version cannot be previewed.

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
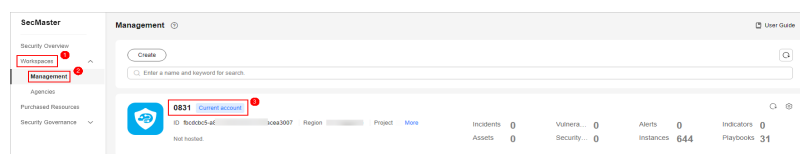
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-60 Accessing the Playbooks tab
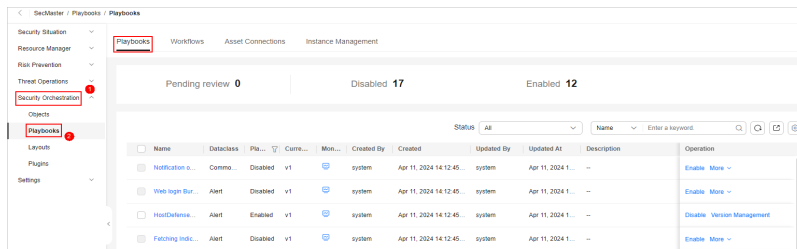
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-61 Version Management slide-out panel
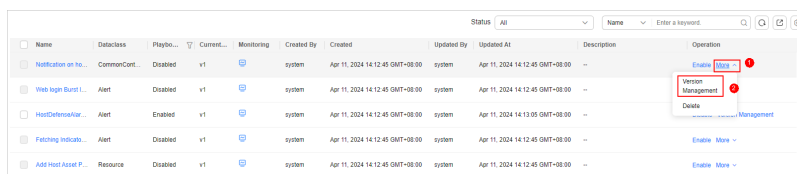
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Preview** in the **Operation** column.

Step 8 On the playbook version preview page, you can view the details about the target playbook version, including **Basic Information**, **Version Information**, and **Matching Workflow**.

----End

Editing a Playbook Version

📖 **NOTE**

Only playbook versions whose version status is **Unsubmitted** can be edited.

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
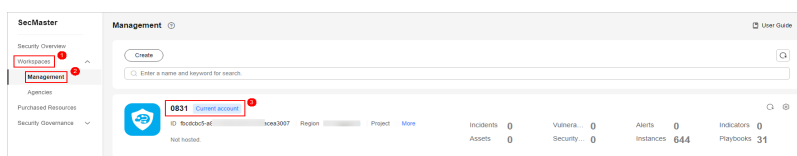
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-63 Accessing the Playbooks tab
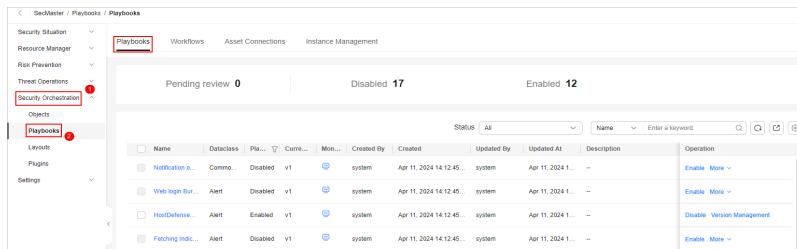
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-64 Version Management slide-out panel
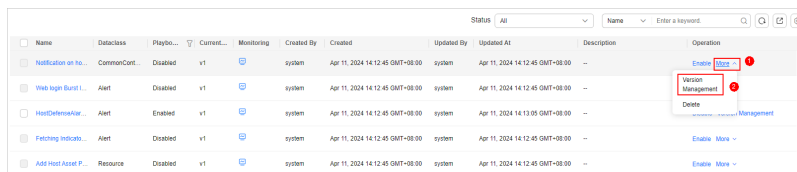
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Edit** in the **Operation** column.

Step 8 On the page for editing a playbook version, edit the version information.

Step 9 Click **OK**.

----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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
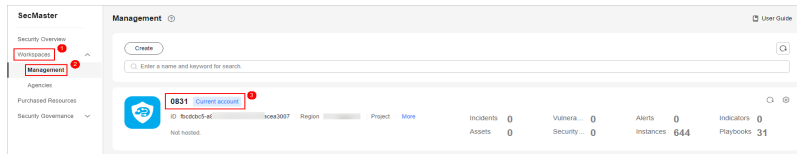
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-66 Accessing the Playbooks tab
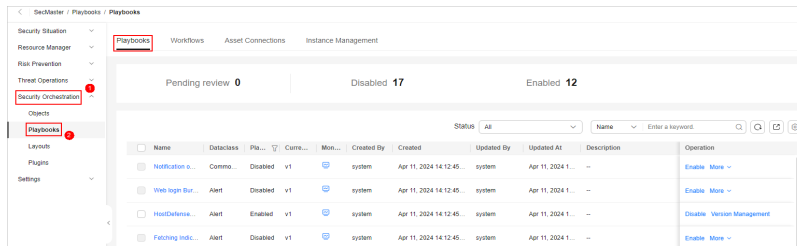
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-67 Version Management slide-out panel
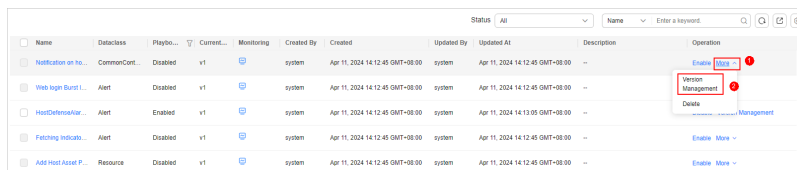
Step 7 On the **Version Management** page, in the version information area, locate the row containing the desired playbook version, and click **Activate** or **Deactivate** in the **Operation** column.

----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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-68 Workspace management page
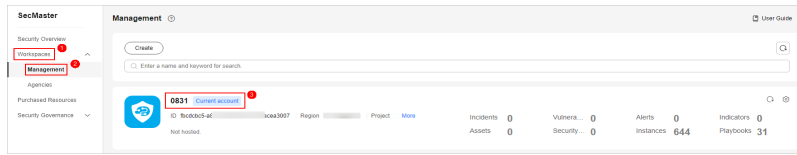
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-69 Accessing the Playbooks tab
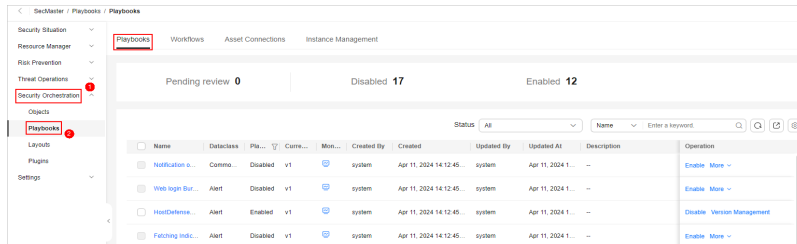
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-70 Version Management slide-out panel
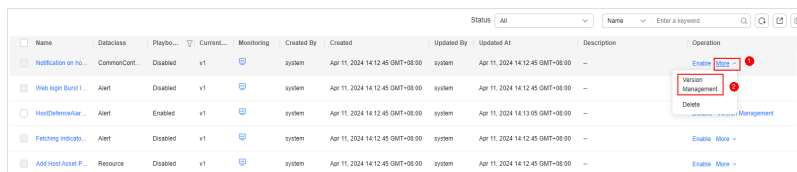
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Copy** in the **Operation** column.

Step 8 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-71 Workspace management page
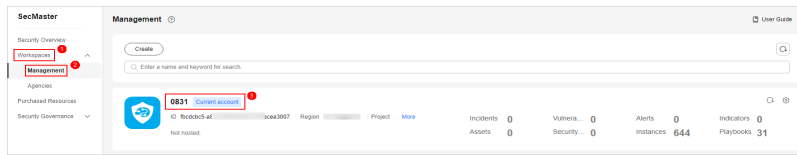
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 11-72 Accessing the Playbooks tab
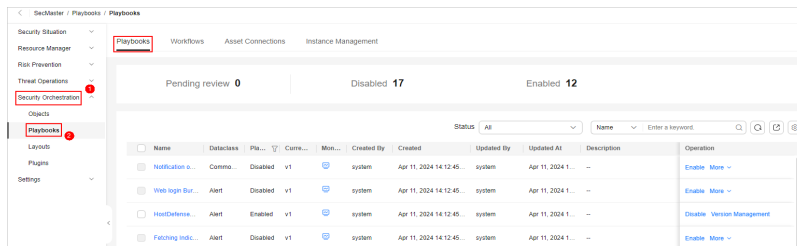
Step 6 On the **Playbooks** tab, click **Version Management** in the **Operation** column of the playbook.

Figure 11-73 Version Management slide-out panel
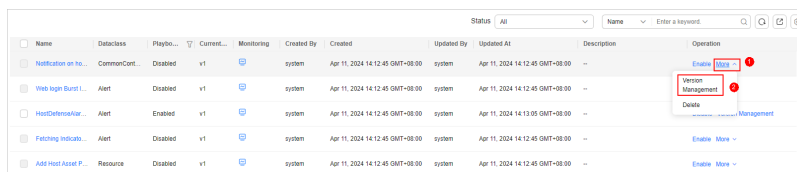
Step 7 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Delete** in the **Operation** column.

📖 **NOTE**

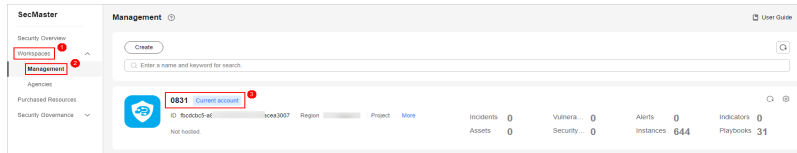> After a playbook version is deleted, it cannot be retrieved. Exercise caution when performing this operation.

----End

11.2.7 Managing Asset Connections

Scenarios

- **Definition**: An asset connection consists of the domain name and authentication parameters required by each plug-in node set during the security orchestration process.

- **Function**: During security orchestration, each plug-in node transfers the domain name to be connected and the authentication information, such as the username, password, and account AK/SK, to establish connections.

- **Relationship between asset connections and plug-ins**: Plug-ins access other cloud services or third-party services through domain names and authentication. So, domain name parameters (endpoints) and authentication parameters (username/password, account AK/SK, etc.) are defined in the login

credential parameters of plug-ins. An asset connection configures login credential parameters for a plug-in. In a workflow, each plug-in node is associated with different asset connections so that the plug-in can access different services.

This topic describes how to manage asset connections, including **Adding an Asset Connection**, **Viewing Asset Connections**, **Editing an Asset Connection**, and **Deleting an Asset Connection**.

Adding an Asset Connection

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

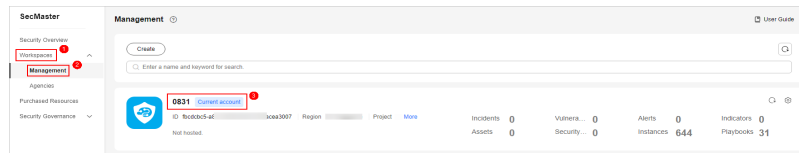**Figure 11-74** Workspace management page
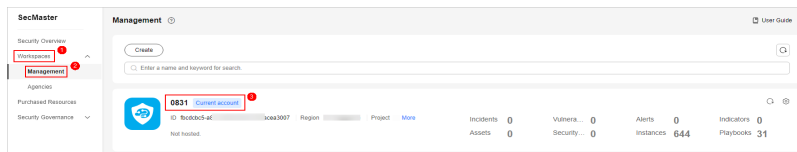
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-75 Asset Connections tab
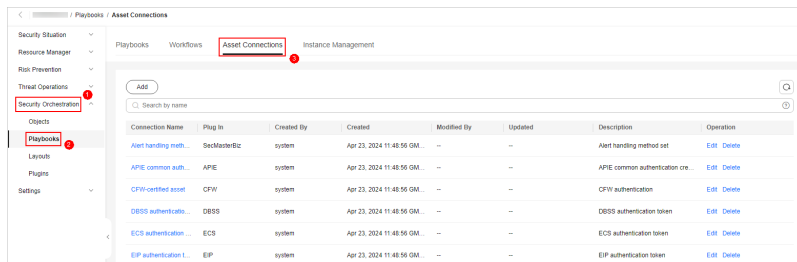
Step 6 On the **Asset Connections** tab page, click **Add**. The slide-out panel **Add** is displayed on the right.

Step 7 On the panel, set asset connection parameters. For details about the parameters, see **Table 11-10**.

Table 11-10 Asset connection parameters

Parameter	Description
Connection Name	Enter the 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 the asset connection. For details about the plug-in, see **Viewing Plug-in Details**.
Connection Type	Select the type of the asset connection. ● Cloud service agency: If a Huawei cloud service plug-in is used, the cloud service agency is recommended. You do not need to manually enter authentication parameters such as the domain name, username, and password. The system automatically obtains the domain name (endpoint) of the corresponding cloud service based on the plug-in name and uses the cloud service agency for authentication. ● AK&SK: You need to manually enter the domain name (endpoint) and provide an AK and SK for authentication. ● Username and password: You need to manually enter the domain name (endpoint) and provide a username and password for authentication. ● Others: Some plug-ins have other authentication parameters in addition to the preceding authentication parameters. Set these parameters based on the plug-in login credential parameter guide.
Credential	Enter the credential information, such as the endpoint, AK, and SK, based on the selected connection type.

Step 8 Click **OK**. You can query the created asset connection in the asset connection list.

----End

Viewing Asset Connections

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
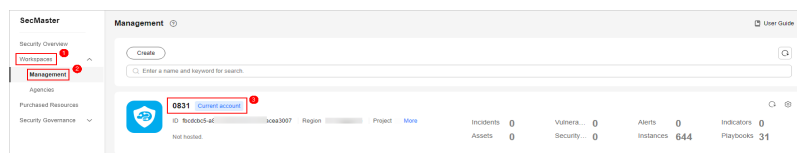
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-76 Workspace management page

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-77 Asset Connections tab
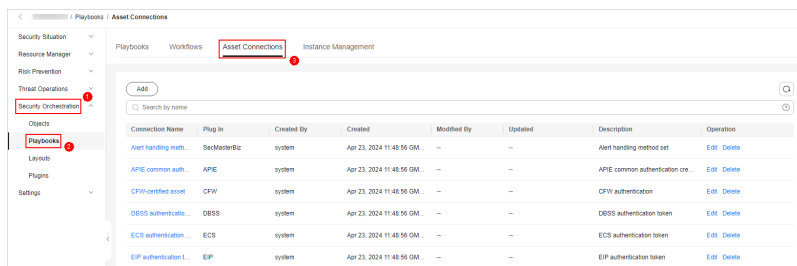
Step 6 On the **Asset Connections** tab page, view information about asset connections.

Figure 11-78 Viewing asset connections
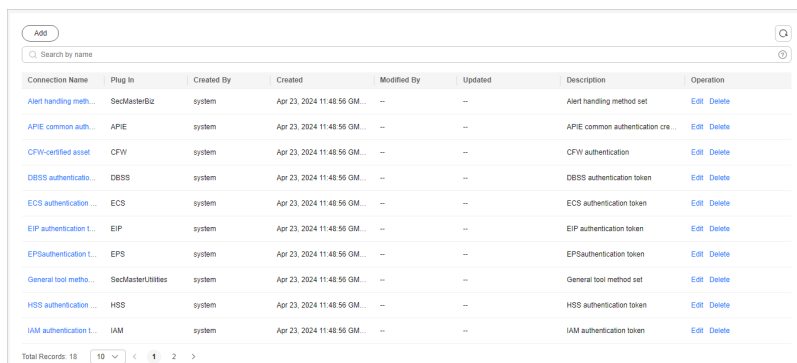
- In the asset connection list, you can view the name, plug-in, and creator of an asset connection.

- If there are many asset connections displayed, use filters to search for a specific one.

- To view details about an asset connection, click its name to go to its **Detail** panel.

----End

Editing an Asset Connection

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-80 Asset Connections tab
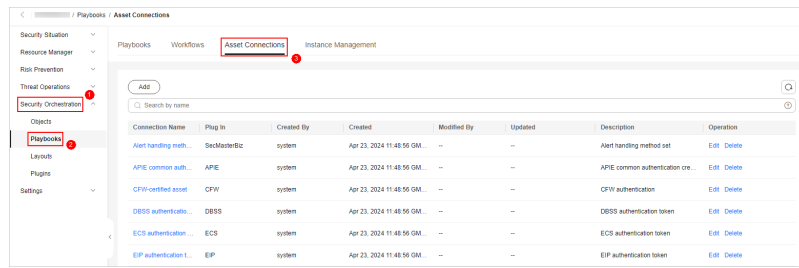
**Step 6** In the row containing a desired asset connection, click **Edit** in the **Operation** column. The slide-out panel **Edit** is displayed.

Step 7 On the **Edit** panel, edit asset connection parameters. For details about the parameters, see **Table 11-11**.

Table 11-11 Asset connection parameters

Parameter	Description
Connection Name	Enter the 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 the asset connection. For details about plug-ins, see **Viewing Plug-in Details**.
Created By	The creator of the asset connection. This parameter **cannot be modified**.

Parameter	Description
Created	Time when the asset connection is created. This parameter **cannot be modified**.
Modified By	The user who last modifies the asset connection. This parameter **cannot be modified**.
Connection Type	Select the type of the asset connection.
Credential	Enter the credential information, such as AK and SK, based on the selected connection type.

Step 8 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 management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

**Figure 11-81** Workspace management page

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-82 Asset Connections tab
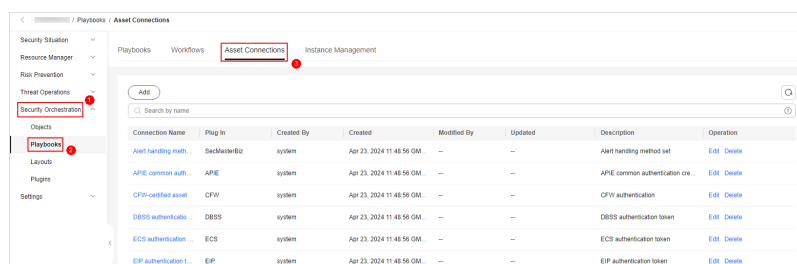
Step 6 Locate the row that contains a desired asset connection, click **Delete** in the **Operation** column.

Step 7 In the confirmation dialog box, enter **DELETE** and click **OK**.

📖 **NOTE**

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

----End

11.2.8 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 in a workspace of an account is as follows:

- Manual retries: 100. After a retry, the playbook cannot be retried until the current execution is complete.

- API retries: 100. After a retry, the playbook cannot be retried until the current execution is complete.

Viewing Monitored Playbook Instances

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-83 Workspace management page
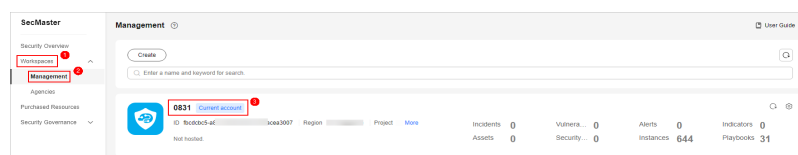
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Instance Management** tab.

Figure 11-84 Instance Management page
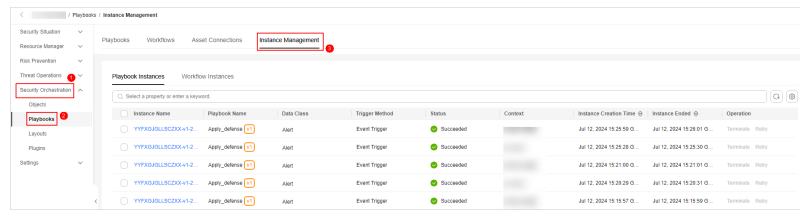
Step 6 On the **Instance Management** tab, click the **Playbook Instances** or **Workflow Instances** tab, and view the instance information. For details about the parameters, see **Table 11-12**.

Figure 11-85 Instances
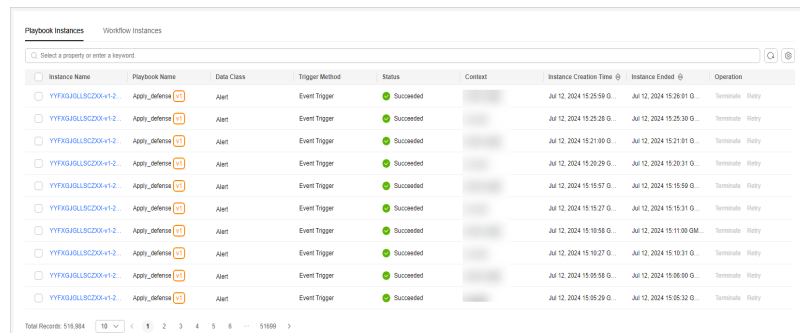
- You can view the total number of instances below the instance list. You can view a maximum of 10,000 instance records page by page. To view more than 10,000 records, optimize the filter criteria.
- An instance can be stored for a maximum of 180 days.
- To view details about an instance, click the instance name. On the displayed page, you can view the instance workflow, workflow nodes, start time, and end time.

Table 11-12 Parameters in the instance list

Parameter	Description
Instance Name	Name of the instance generated by the system.
Playbook Name	Name of the playbook corresponding to the instance.
Data Class	Operation object of a playbook
Trigger Method	Triggering mode of an instance ● **Timer Trigger** ● **Event Trigger**

Parameter	Description
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.

----End

Related Operations

- To stop a running instance, click **Terminate** in the **Operation** column of the target instance. After an instance is terminated, no operations are supported.

- To start a failed instance, click **Retry** in the **Operation** column.

  You can retry instances up to 100 times a day in a single workspace. After a retry, the playbook cannot be retried until the current execution is complete.

11.3 Operation Object Management

11.3.1 Operation Object Management Overview

- **Data class**: A data class is required for a playbook and workflow running for security orchestration and response. The playbook is triggered by data objects. A data object is the specific instance of a data class. Common data classes include alerts, incidents, indicators, and vulnerabilities. You can view data classes by referring to **Viewing Data Classes**.

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

impact of an exception. In addition, alerts can be classified by severity, such as critical, major, and minor, so that O&M personnel can determine which alerts need to be handled first based on their severity. The purpose of an alert is to notify related personnel in a timely manner so that they can make a quick response and take measures to fix the problem. Common alert types include web tamper protection, abnormal process behavior, and abnormal network connections. For more details, see **Managing Alert Types**.

- **Incident**: An incident is a broad concept. It can include but is not limited to alerts. It can be a part of normal system operations, exceptions, or errors. In the O&M and security fields, an incident usually refers to a problem or fault that has occurred and needs to be focused on, investigated, and handled. An incident may be triggered by one or more alerts or other factors, such as user operations and system logs. An incident is usually used to record and report historical activities in a system for analysis and audits. For more details, see **Managing Incident Types**.
- **Indicator**: For details, see **Viewing Threat Intelligence Types**.
- **Vulnerability**: Common vulnerability types include Linux software vulnerabilities, Windows OS vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities. For more details, see **Managing Vulnerability Types**.
- **Custom type**: You can add custom data classes. For details, see **Viewing Custom Types**.
- **Classification & mapping**: A categorical mapping indicates the relationship of data sources and data objects (the specific instance of data classes). For details, see **Managing Categorical Mappings**.

11.3.2 Viewing Data Classes

The playbook and workflow running in security orchestration and response need to be bound to a data class. The playbook is triggered by a data object (instance of the data class). The data class supports the following operations:

- **Viewing Data Classes**

Viewing Data Classes

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-86 Workspace management page
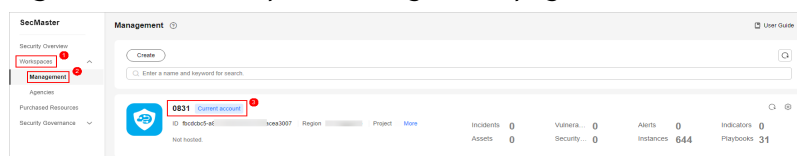
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. The **Data Class** tab page is displayed by default.

Figure 11-87 Accessing the Data Class tab
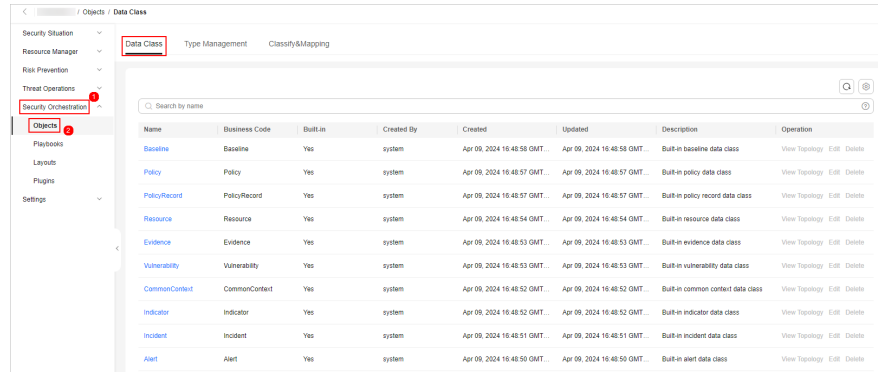
Step 6 In the data class list, view the existing data class information.

- If there are many data classes displayed, use filters to search for a specific one.

- In the data class list, you can view the data class name, service code, and whether the data class is a built-in data class.

- To view details about a data class, click the name of the target data class. The details page of the target data class is displayed on the right.

  On the data class details page, you can view the basic information and fields about the data class.

----End

11.3.3 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 management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance > SecMaster**.

Step 4 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
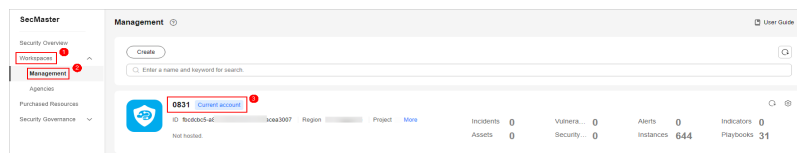
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-89 Type Management page
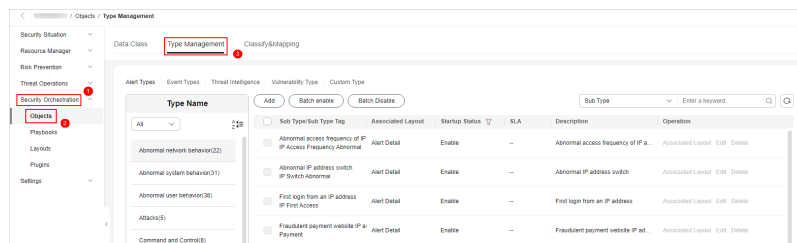
Step 6 On the **Type Management** page, click the **Alert Type** tab.

Step 7 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 11-13**.

If there are many subtypes, you can select the **Sub Type** or **Associated Layout** and enter the corresponding keyword for search.

Table 11-13 Alert type parameters

Parameter	Description
Sub Type/Sub Type Tag	Name and ID of an alert subtype.

| Parameter	Description
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.
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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-90 Workspace management page
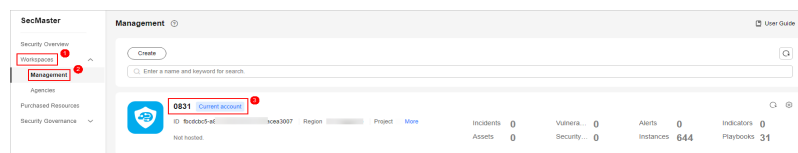
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-91 Type Management page
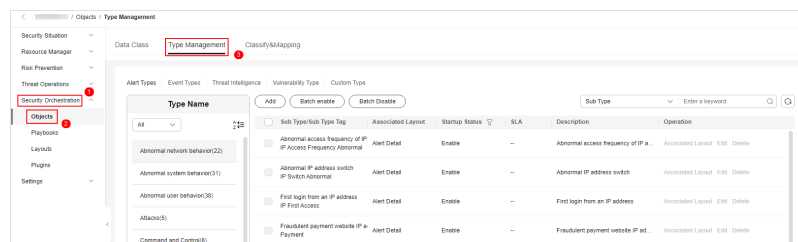
Step 6 On the **Type Management** page, click the **Alert Type** tab.

Step 7 On the **Alert Types** tab, click **Add**. On the **Add Alert Type** slide-out panel, set alert type parameters.

Table 11-14 Parameters for adding an alert type

Parameter	Description
Type Name	Customize the name of the new alert type.
Type Tag	Enter the alert type ID. The keyword must comply with the upper camel case naming rules, for example, **TypeTag**.
Sub Type	Enter the subtype of the alert type.
Sub Type Tag	Enter the alert subtype ID. The keyword must comply with the upper camel case naming rules, for example, **SubTypeName**.
Startup Status	Indicates whether an alert type is enabled.
SLA	Set the SLA processing time of the alert.
Description	Description of a user-defined alert type

🔖 **NOTE**

After a customized alert type is added, the **Type Name**, **Type Tag**, and **Sub Type Tag** parameters cannot be modified.

Step 8 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, preset 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-92 Workspace management page
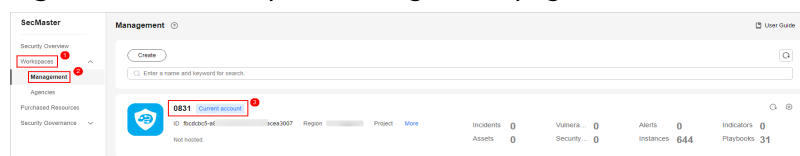
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-93 Type Management page
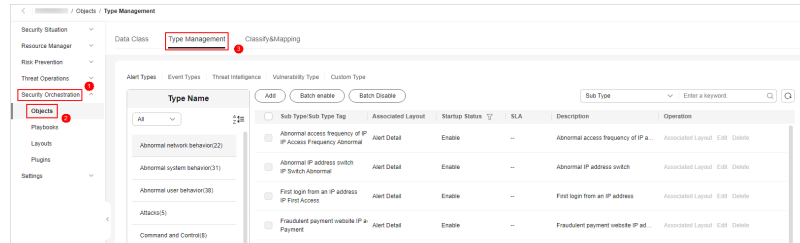
Step 6 On the **Type Management** page, click the **Alert Type** tab.

Step 7 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 8 In the **Associate Layout** dialog box, select the target layout and click **OK**.

----End

Editing an Alert Type

📖 **NOTE**

- Currently, the preset 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
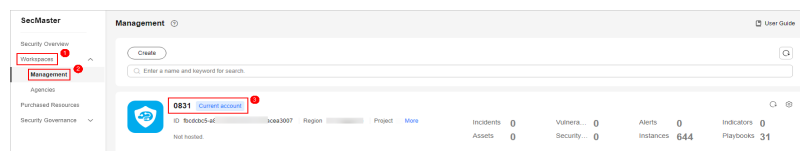
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-95 Type Management page
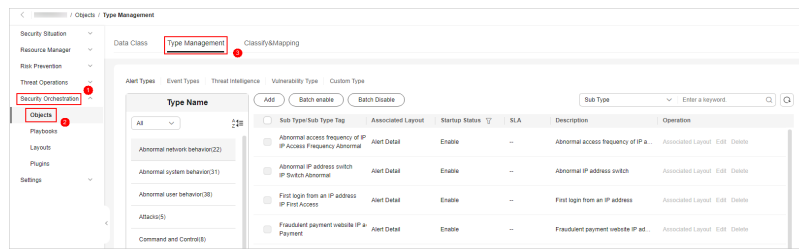
Step 6 On the **Type Management** page, click the **Alert Type** tab.

Step 7 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 8 On the alert list page on the right, locate the row that contains the target type and click **Edit** in the **Operation** column.

Step 9 On the displayed page, modify the parameters of the alert type.

Table 11-15 Parameters for editing an alert type

Parameter	Description
Type Name	Name of an alert type, which **cannot** be modified.
Type ID	Alert type ID, which **cannot** be modified.
Sub Type	Enter the subtype of the alert type.
Sub Type Tag	Alert subtype ID, which **cannot** be modified.
Status	Sets the startup status of an alert type.
SLA	Set the SLA processing time of the alert.
Description	Description of a custom alert type

Step 10 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-96 Workspace management page
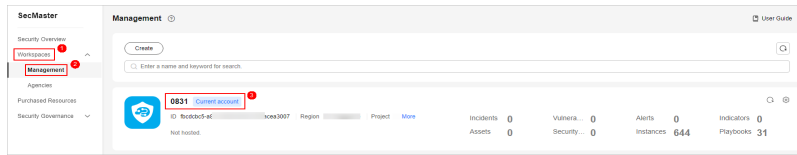
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-97 Type Management page
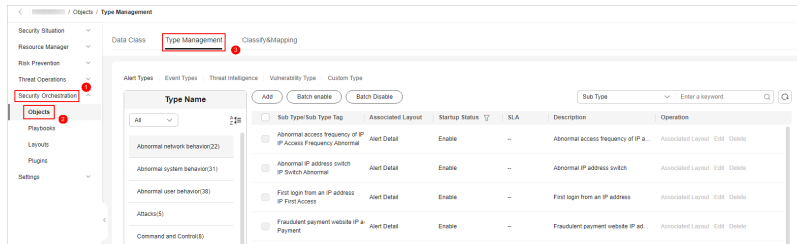
Step 6 On the **Type Management** page, click the **Alert Type** tab.

Step 7 On the **Alert Types** tab, manage alert types.

📖 **NOTE**

- The built-in alert types are enabled by default. You do not need to manually enable them.
- Currently, built-in alert types cannot be disabled or deleted.
- Currently, built-in alert types cannot be deleted.

Table 11-16 Managing an alert type

Operation	Description
Enable	1. On the **Alert Types** tab, select the types you want to enable and click **Batch enable**. Alternatively, locate the row containing the alert type you want to enable, click **Disable** in the **Status** column. 2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the status of the target type changes to **Enable**, the target type is enabled successfully.

Operation	Description
Disable	1. On the **Alert Types** tab, select the types you want to disable and click **Batch Disable**. Alternatively, locate the row containing the alert type to be disabled, click **Enable** in the **Status** column. 2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the **Status** of the target type changes to **Disable**, the target type is disabled successfully.
Delete	1. On the alert type management page, select the type to be deleted and click **Delete** in the **Operation** column. 2. In the displayed dialog box, enter **DELETE** and click **OK**.

----End

11.3.4 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.

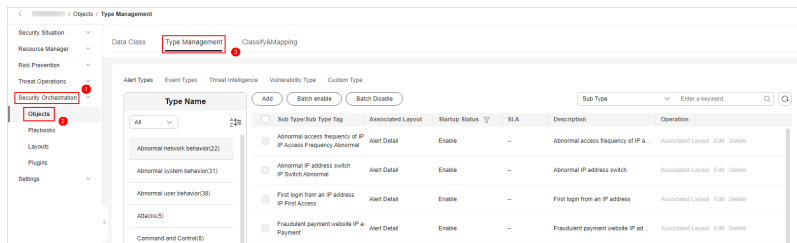## Viewing Incident Types

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-98 Workspace management page
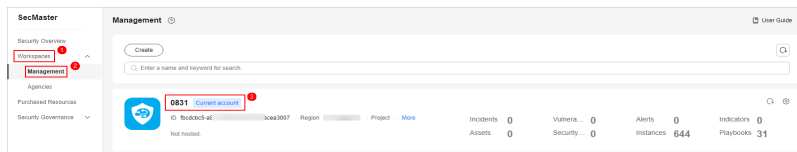
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-99 Type Management page

Step 6 On the **Type Management** page, click the **Event Types** tab.

Step 7 On the **Event Types** tab, view the details about existing incident types. For details about the parameters, see **Table 11-17**.

Table 11-17 Incident type parameters

Parameter	Description
Type Name	Name of an incident type
Sub Type/Sub Type Tag	Name and ID of an incident subtype
Associated Layout	Layout associated with the incident type
Startup Status	Indicates whether an incident type is enabled. ● Enable: The current type has been enabled. ● Disabled: The current type has been disabled.
SLA	SLA processing time of an incident type
Description	Description of an incident type
Operation	You can edit and delete incident types.

----End

Adding an Incident Type

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

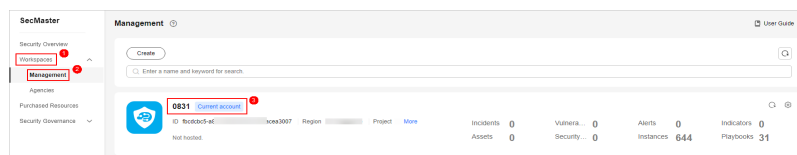**Figure 11-100** Workspace management page
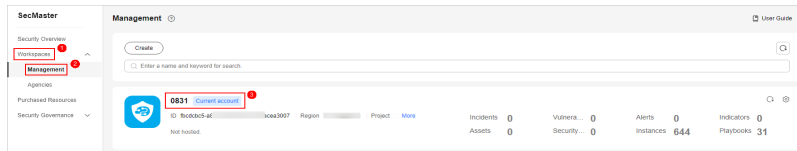
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-101 Type Management page
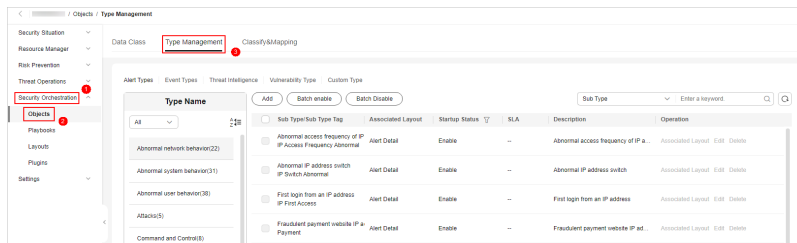
Step 6 On the **Type Management** page, click the **Event Types** tab.

Step 7 On the **Event Types** tab, click **Add**. On the **Add Event Type** slide-out panel, set incident type parameters.

Table 11-18 Incident type parameters

Parameter	Description
Type Name	Customized name of an incident type.
Type Tag	Enter the incident type ID. The keyword must comply with the upper camel case naming rules, for example, **TypeTag**.
Sub Type	Enter the subtype of the incident type.

Parameter	Description
Sub Type Tag	Enter the incident subtype ID. The keyword must comply with the upper camel case naming rules, for example, **SubTypeName**.
Startup Status	Indicates whether an incident type is enabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

NOTE

> After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Step 8 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 [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-102 Workspace management page

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-103 Type Management page
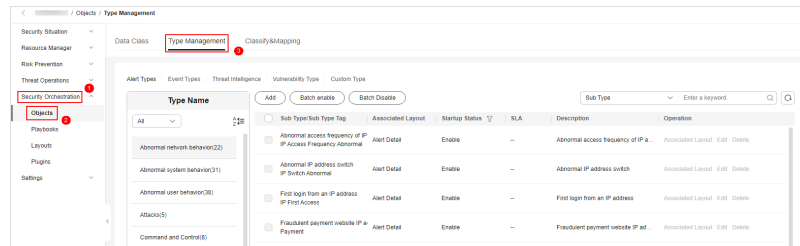
Step 6 On the **Type Management** page, click the **Event Types** tab.

Step 7 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 8 In the **Associate Layout** dialog box, select the target layout and click **OK**.

----End

Editing an Incident Type

> 📖 **NOTE**
>
> ● Currently, the built-in incident type cannot be edited.
> ● After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-104 Workspace management page
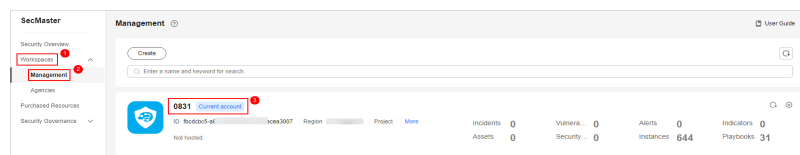
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-105 Type Management page
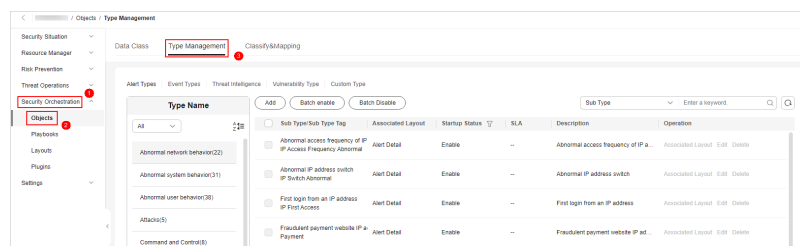
Step 6 On the **Type Management** page, click the **Event Types** tab.

Step 7 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 8 On the **Event Type** page, click **Edit** in the **Operation** column of the target type to be edited.

Step 9 In the **Edit Event Type** dialog box, edit parameters.

Table 11-19 Incident type parameters

| Parameter	Description
Type Name	Name of an incident type, which **cannot** be modified.
Type Tag	Incident type ID, which **cannot** be modified.
Sub Type	Enter the subtype of the incident type.
Sub Type Tag	Incident subtype ID, which **cannot** be modified.
Startup Status	Indicates whether an incident type is enabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

Step 10 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-106 Workspace management page
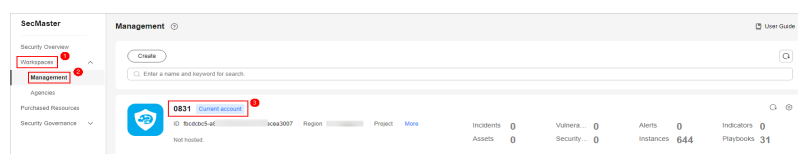
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-107 Type Management page
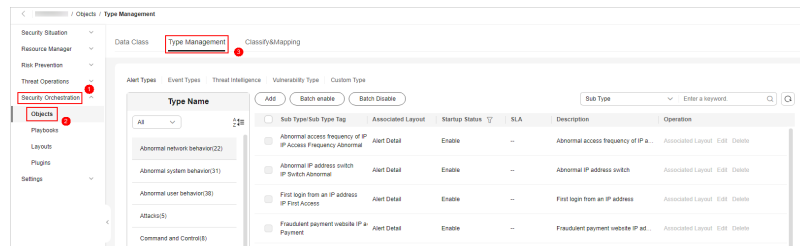
Step 6 On the **Type Management** page, click the **Event Types** tab.

Step 7 On the incident type tab, manage incident types.

> **NOTE**
>
> - The built-in incident types are enabled by default. You do not need to manually enable them.
> - Currently, built-in incident (event) types cannot be disabled or deleted.

Table 11-20 Managing existing incident types

Operation	Description
Enable	1. On the type management page, select the type to be enabled and click **Batch Enable**. Alternatively, locate the row containing the incident type to be enabled, click **Disable** in the **Status** column.
	2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the status of the target type changes to **Enable**, the target type is enabled successfully.
Disable	1. On the **Event Type** page, select the type to be disabled and click **Batch Disable**. Alternatively, locate the row containing the incident type to be disabled, click **Enable** in the **Status** column.
	2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the **Status** of the target type changes to **Disable**, the target type is disabled successfully.
Delete	1. On the incident type management page, select the type to be deleted and click **Delete** in the **Operation** column.
	2. In the displayed dialog box, enter **DELETE** and click **OK**.

----End

11.3.5 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.
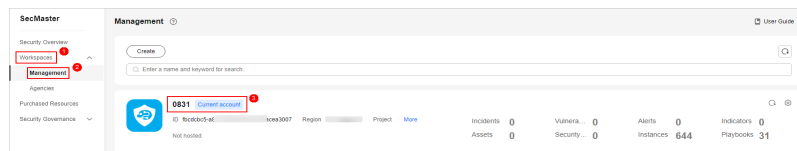
Viewing Threat Intelligence Types

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
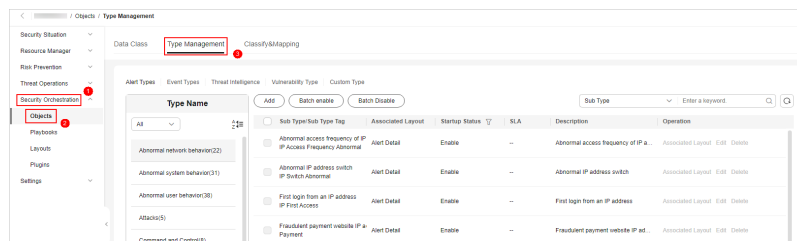
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-108 Workspace management page

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-109 Type Management page

Step 6 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 7 On the **Threat Intelligence** page, view details. For details about the parameters, see **Table 11-21**.

Table 11-21 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.
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

11.3.6 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.
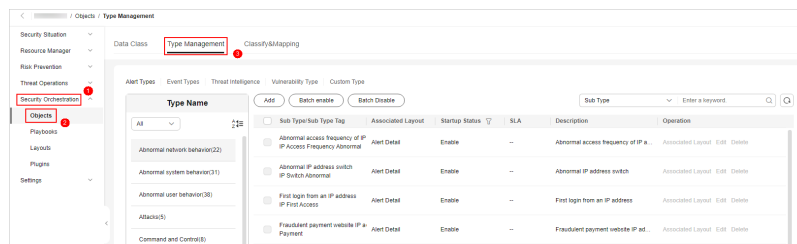
Viewing Existing Vulnerability Types

Step 1 Log in to the management console.

Step 2 Click ▢ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
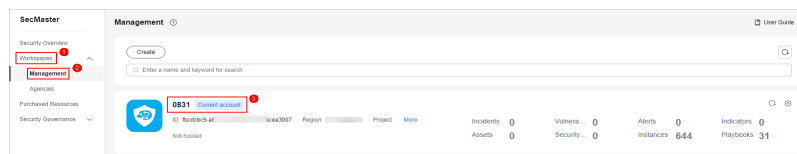
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-111 Type Management page

Step 6 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 7 On the **Vulnerability Type** tab page, view details about existing vulnerability types. For details about the parameters, see **Table 11-22**.

Table 11-22 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

| Parameter	Description
Operation	You can edit and delete vulnerability types.

----End
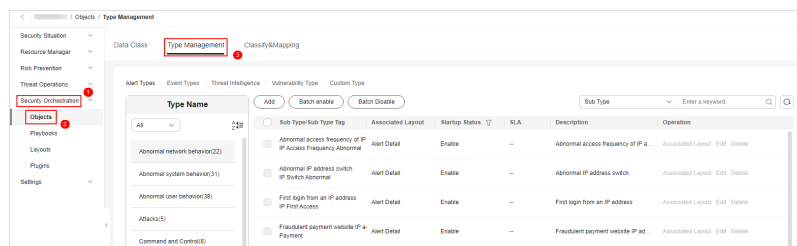
Adding a Vulnerability Type

Step 1 Log in to the management console.

Step 2 Click ⬢ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-112 Workspace management page
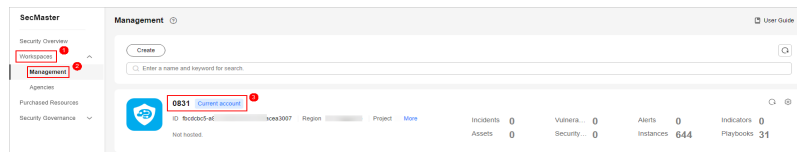
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-113 Type Management page

Step 6 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 7 On the **Vulnerability Type** page, click **Add**. On the **Add Vulnerability Type** slide-out panel, set type parameters.

Table 11-23 Vulnerability type parameters

Parameter	Description
Type Name	Name of the vulnerability type to be added.

Parameter	Description
Type Tag	Enter the vulnerability type ID. The keyword must comply with the upper camel case naming rules, for example, **TypeTag**.
Startup Status	Indicates the enabling status of the vulnerability type:
Description	Description of a user-defined vulnerability

☐ NOTE

After a user-defined vulnerability type is added, the **Type ID** cannot be modified.

Step 8 In the lower right corner of the page, click **Confirm**.

After the threat intelligence type is added, you can view the new type in the table on the **Vulnerability Type** page.

----End

Associating a Vulnerability Type with a Layout

☐ NOTE

Currently, built-in vulnerability types do not support customized layouts.

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
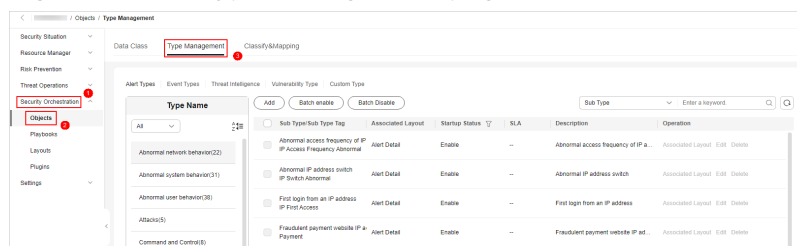
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-114 Workspace management page
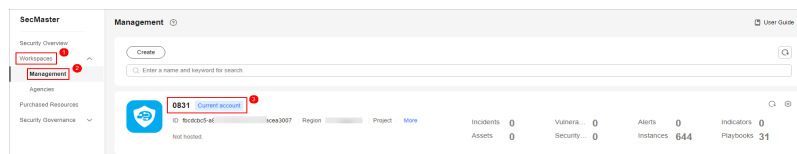
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-115 Type Management page

Step 6 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 7 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 8 In the **Associate Layout** dialog box, select the target layout and click **OK**.

----End

Editing a Vulnerability Type

☐ NOTE

- Currently, the built-in vulnerability types cannot be edited.
- After a user-defined vulnerability type is added, the type ID cannot be modified.

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-116 Workspace management page
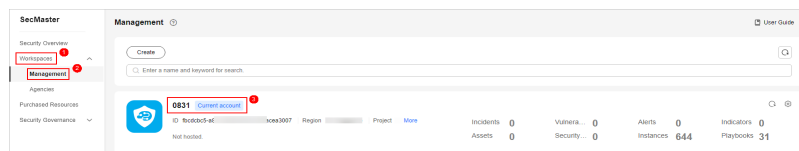
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-117 Type Management page
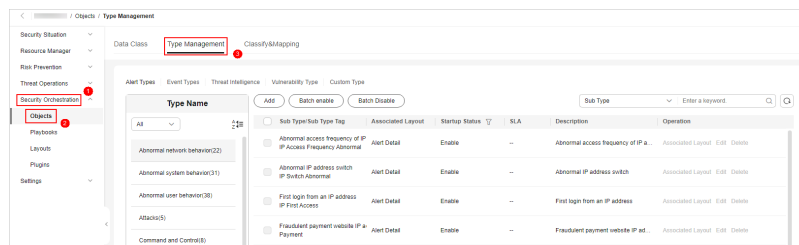
Step 6 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 7 On the **Vulnerability Type** page, select the type to be edited and click **Edit** in the **Operation** column of the target type.

Step 8 On the displayed page, edit the parameter information of the corresponding type.

Table 11-24 Vulnerability type parameters

Parameter	Description
Type Name	Name of a user-defined vulnerability type
Type Tag	Vulnerability type ID, which **cannot** be modified.
Startup Status	Set the enabling status of the vulnerability type:
Description	Description of a user-defined vulnerability

Step 9 In the lower right corner of the page, click **OK**.

----End
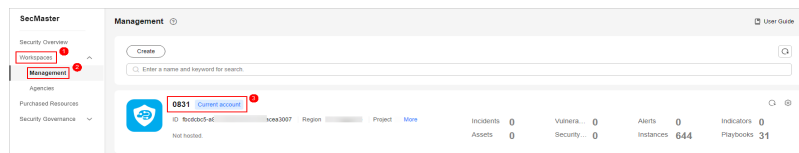
Managing a Vulnerability Type

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-118 Workspace management page

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-119 Type Management page
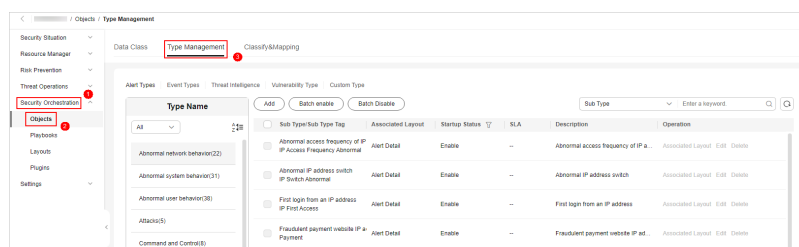
Step 6 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 7 On the vulnerability type tab, manage vulnerability types.

📖 **NOTE**

- Built-in vulnerability types are enabled by default. You do not need to manually enable them.
- Currently, the built-in vulnerability types cannot be disabled or deleted.

Table 11-25 Managing a vulnerability type

Operation	Description
Enable	1. On the **Vulnerability Type** page, select the type to be enabled and click **Batch Enable**. Alternatively, locate the row containing the vulnerability type to be enabled, click **Disable** in the **Status** column. 2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the status of the target type changes to **Enable**, the target type is enabled successfully.
Disable	1. On the **Vulnerability Type** page, select the type to be disabled and click **Batch Disable**. Alternatively, locate the row containing the vulnerability type to be disabled, click **Enable** in the **Status** column. 2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the **Status** of the target type changes to **Disable**, the target type is disabled successfully.
Delete	1. On the **Vulnerability Type** tab, select the vulnerability type to be deleted and click **Delete** in the **Operation** column. 2. In the displayed dialog box, enter **DELETE** and click **OK**.

----End

11.3.7 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
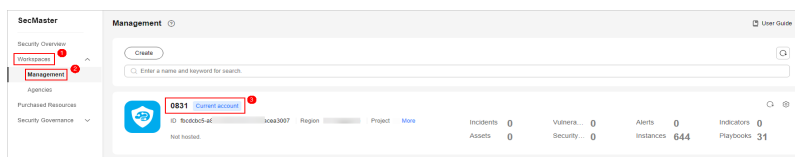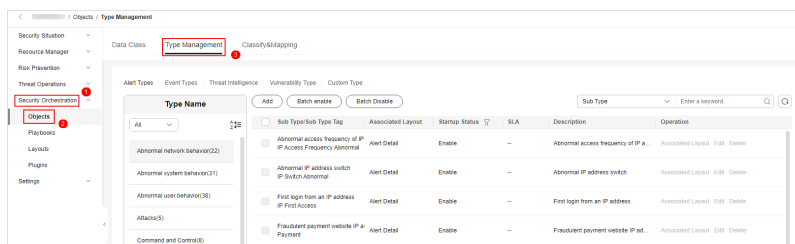
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-120 Workspace management page

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-121 Type Management page

Step 6 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

11.3.8 Managing Categorical Mappings

Categorical mappings are used to match alert types and map alert fields for cloud service alerts.

This section describes how to manage categories and mappings, including **Viewing Categorical Mappings**, **Creating a Categorical Mapping**, **Copying a Categorical Mapping**, **Editing a Categorical Mapping**, and **Enabling, Disabling, and Deleting a Categorical Mapping**.

Limitations and Constraints

- In a workspace of an account, a maximum of 50 classification & mapping templates can be created.
- In a workspace of an 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 an account.

Viewing Categorical Mappings

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-122 Workspace management page
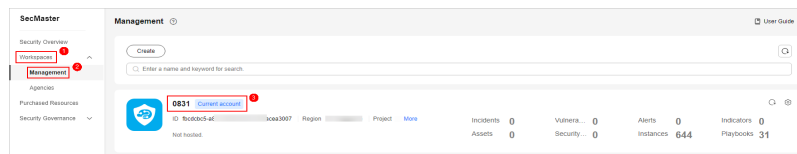
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-123 Classify&Mapping tab
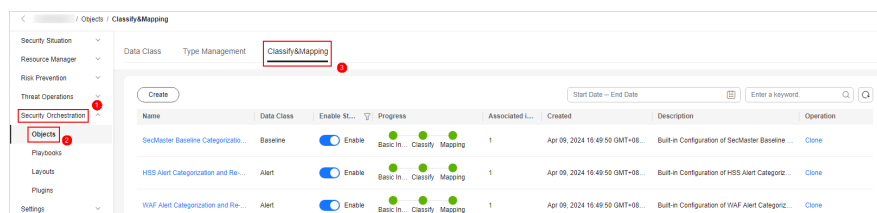
Step 6 On the **Classify&Mapping** tab, view details about the created categorical mappings.

- In the categorical mapping list, view details such as the categorical mapping name, data class, and number of associated plug-in instances.
- If there are many categorical mappings, use filters and keywords to search for a specific one.
- To edit a categorical mapping, click its name to go to the edit page.

  On the edit page, you can edit details about the categorical mapping.
- In the categorical mapping list, you can also enable, disable, clone, and delete a categorical mapping.

----End

Creating a Categorical Mapping

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
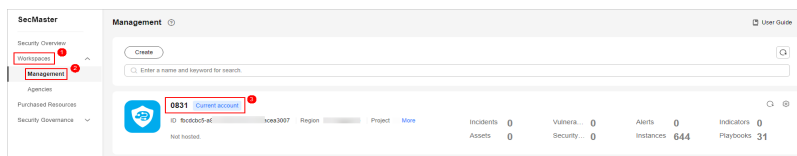
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-125 Classify&Mapping tab
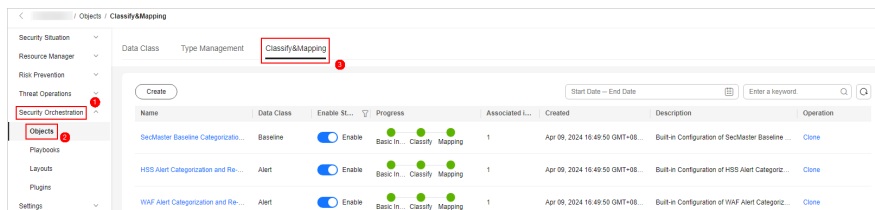
Step 6 On the **Classify&Mapping** tab, click **Create**.

Step 7 On the **Create Categorical Mapping** page, set categorical mapping parameters.

Figure 11-126 Create Categorical Mapping
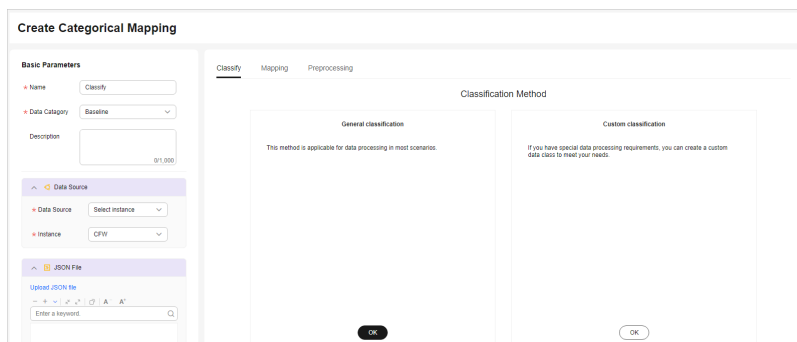
1. In the **Basic Parameters** area on the left, configure basic information about the categorical mapping. For details about the parameters, see **Table 11-26**.

Table 11-26 Configuring basic information

Parameter	Description
Name	Name of a user-defined categorical mapping.
Data Category	Select the corresponding data class.
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 method 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

Copying a Categorical Mapping

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

**Figure 11-127** Workspace management page
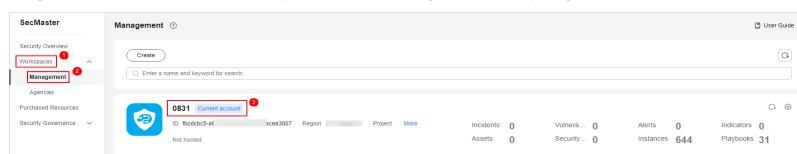
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-128 Classify&Mapping tab

Step 6 On the **Classify&Mapping** page, click **Clone** in the **Operation** column of the target categorical mapping.

Step 7 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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-130 Classify&Mapping tab
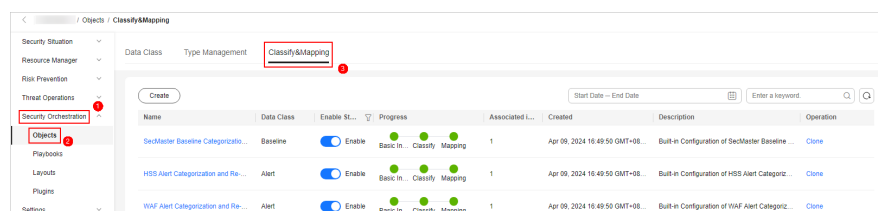
Step 6 On the **Classify&Mapping** page, click the target categorical mapping name to go to the edit page.

Step 7 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 11-26**.

Table 11-27 Configuring basic information

Parameter	Description
Name	Name of a user-defined categorical mapping.
Data Category	This field cannot be edited.
Description	Description of the custom categorical mapping.

2. In the **Data Source** area on the left, select the data source for the categorical mapping.

   If **Data Source** is set to **Upload JSON file**, you need to click **Upload JSON file** and upload the JSON file.

3. On the **Classify** tab on the right, select a classification method 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

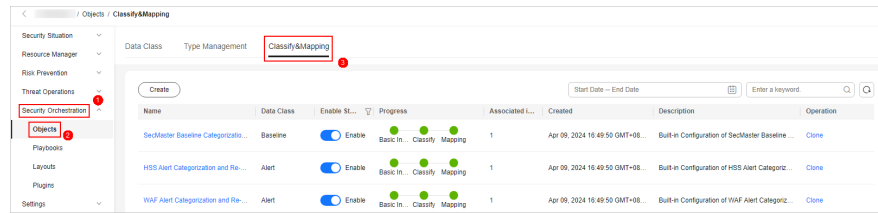## Enabling, Disabling, and Deleting a Categorical Mapping

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-131 Workspace management page
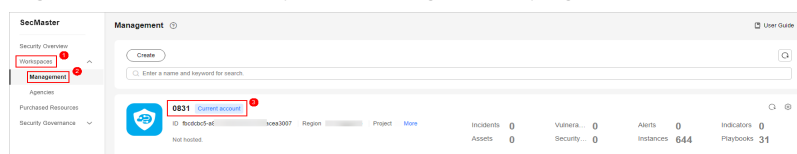
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

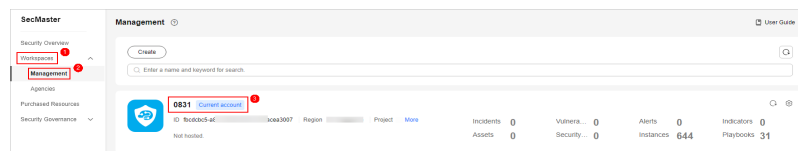**Figure 11-132** Classify&Mapping tab
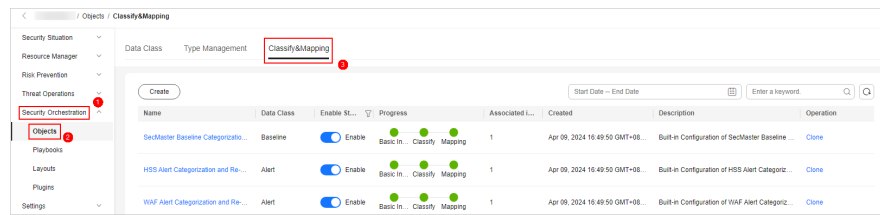
Step 6 On the **Classify&Mapping** tab, manage categorical mappings.

📖 **NOTE**

- Custom categorical mappings cannot be enabled or disabled.
- Currently, built-in categorical mappings cannot be deleted.

Table 11-28 Managing categorical mappings

Operation	Description
Enable	Locate the row containing the target categorical mapping and click **Disable** in the **Status** column. If the status changes to **Enable**, the categorical mapping has been enabled.
Disable	Locate the row containing your desired categorical mapping and click **Enable** in the **Status** column. If the status changes to **Disable**, the categorical mapping has been disabled.

Delete	1. Click **Delete** in the **Operation** column of the target categorical mapping.
	2. In the displayed pane on the right, click **Delete**.
	    NOTE
	    – If a categorical mapping is deleted, the plug-ins and connections associated with the categorical mapping will be stopped immediately.
	    – Deleted categorical mappings cannot be restored. Exercise caution when performing this operation.

----End

11.4 Creating a Custom Layout

11.4.1 Viewing Layouts

Scenario

There are multiple page layouts, such as the **Alert List**, **Indicator Details**, and **Vulnerability Details** layouts.

This topic describes how to check a layout.

Viewing an Existing Layout

Step 1 Log in to the management console.

Step 2 Click ⬚ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
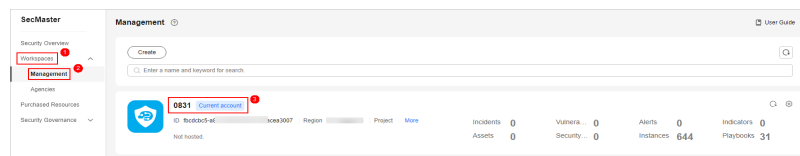
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Layouts**.

Figure 11-134 Layouts page
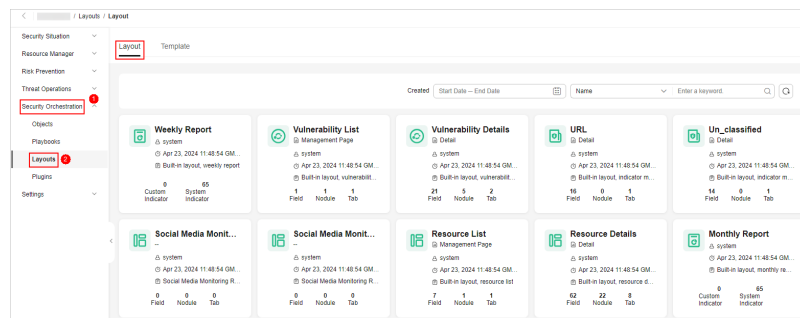
Step 6 On the layout management page, view existing layouts.

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

11.4.2 Viewing a Layout Template

Scenarios

There are many management page and details page templates, for example, alert, incident, and vulnerability management templates.

This section describes how to view layout templates you have.

Viewing a Layout Template

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-135 Workspace management page
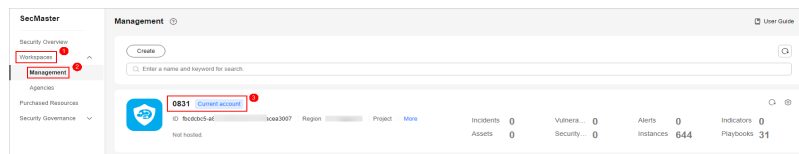
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Layouts**. On the displayed page, click the **Template** tab.

Figure 11-136 Layout template tab
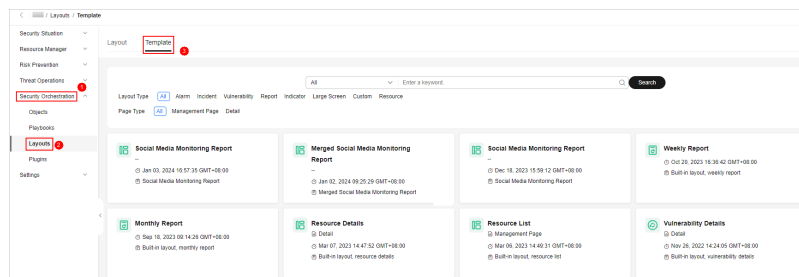
Step 6 On the **Template** tab, view the template information.

You can search for a specified layout template by **Layout Type** or **Page Type**.

- You can view the name, page type, and creation time of a template.
- You can edit the name and layout of a template.

----End

11.5 Viewing Plug-in Details

Scenario

This section describes how to view SecMaster built-in plug-ins and their details.

Viewing Plug-in Details

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![menu icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-137 Workspace management page
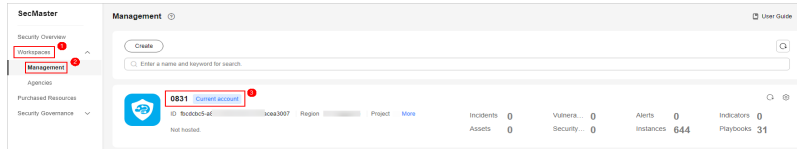
Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Plugins**.

Figure 11-138 Plugins page
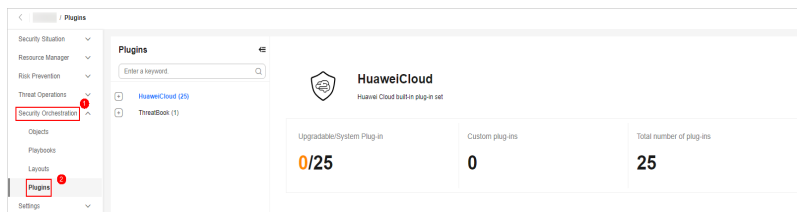
Step 6 On the **Plugins** page, view plug-in details.

- 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 Playbook Overview

12.1 Ransomware Incident Response Solution

Incident Type: Ransomware Attacks

Ransomware is a special type of malware designed to deny a user or organization access to files on their computers. So ransomware attacks are classified as denial-of-access (DoS) attacks. Ransomware uses technical means to restrict victims from accessing their own systems or data in the systems, such as documents, emails, databases, and source code. To remove the restrictions, victims have to pay ransom to attackers.

Once a ransomware attack succeeded, it is hard to take measures to interrupt the attack or mitigate the damage. So, it is important to take preventive measures to reduce such attacks.

This document describes a series of measures and strategies designed to effectively control and respond to ransomware attacks.

Incident Response Solution: Ransomware Host Isolation Playbook

The **Ransomware host isolation** playbook preconfigured in SecMaster automatically isolates compromised hosts. When a ransomware alert is generated, the playbook adds the affected hosts to a security group and blocks all inbound and outbound traffic to isolate the hosts. This move is crucial to ransomware protection.

Figure 12-1 Host isolation - Malware
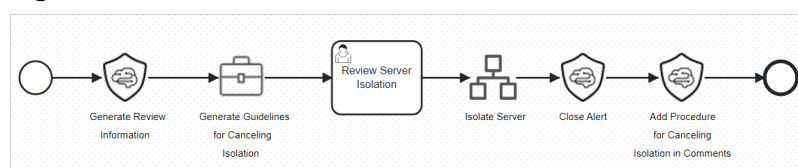
Incident Response Process

Step 1 **Obtain, store, and record evidence**.

Based on your cloud environment configurations, you can identify potential ransomware incidents from many sources, including:

1. An IT employee reported that an ECS could not be accessed over SSH or other similar methods.

   New ECSs can be created and no alerts are reported by Cloud Eye, but the ECS is inaccessible.

2. A service ticket has been triggered by abnormal metrics or logs of an ECS instance and generated in your service ticket system.

3. A network fault error was reported on the ECS console or by Cloud Eye for an ECS.

4. Attackers received ransomware requests through other communication channels (such as emails).

5. Cloud security services or other security tools detected that an ECS instance was attacked.

6. Your cloud or other third-party monitoring systems generated alerts or reported abnormal metrics.

7. If an event is identified as a security incident, it is critical to assess its impact scope, including the number of affected resources and the sensitivity of the data involved.

8. Check whether there are any known events that may cause service interruptions or affect instance metrics. For example, the number of network metrics in Cloud Eye increases due to ongoing events.

9. Use Cloud Eye or other application performance monitoring tools to compare the recorded performance baseline metrics of the application with the current abnormal metrics to check if there are any abnormal behavior.

10. Identify the classifications of data stored in ECS instances, OBS buckets, or other storage media.

11. Ensure that a service ticket has been created for an incident. If no tickets are generated automatically, manually create one.

12. If there is a service ticket already, locate the alert or metric associated with the issue.

    Locate the reason for automatically generated service tickets or record the alerts or notifications for manually generated service tickets. Locate the events or other reasons for service interruptions. If no events or reasons can be located, record the actual attack medium.

13. Check logs to identify when the ransomware attack occurred.

    You can use Cloud Trace Service (CTS) to collect, store, and query operation records of all cloud resources.

14. Identify and record the impact on and experience of end users.

    If users are affected, record the details about how the attack occurred step by step in the service ticket to help with the attack medium identification and mitigation measure preparation.

15. Identify the roles involved in the incident based on the incident response plan of your organization. Notify relevant roles, including legal personnel, technical

teams, and developers, and ensure that they are added to the service ticket and war rooms for continuous responses.

16. Ensure that the legal counsel of your organization is aware of and involved in the internal response to and external communication about the incident, and add colleagues responsible for public or external communication to the service ticket so that they can fulfill their communication responsibilities in a timely manner. If local or federal regulations require the reporting of such incidents, notify the authorities concerned and seek guidance from their legal counsel or law enforcement on the collection of evidence and the preservation of the chain of custody. Reporting such incidents to open databases, government agencies, or non-governmental organizations may also help to advance the response to such incidents, even if it is not required by laws or regulations.

Step 2 **Contain incidents**.

Early detection of abnormal user behavior or network activities is the key to reducing the impact of ransomware incidents. You can take the following actions to contain an incident. You can follow the procedure below and work with the legal and compliance team of your organization to take any necessary response measures and continue the incident response process.

1. Determine the type of ransomware involved in the attack. Common ransomware types are as follows:
   - Encryption ransomware: This type of ransomware encrypts files and objects for ransom.
   - Lock-in ransomware: This type of ransomware locks the access to a specific device.
   - Other types: Emerging types or types that are not recorded yet.

2. For workloads affected by attacks, you can modify security groups, OBS bucket policies, or related identity and access management policies to isolate networks or Internet connections, minimizing the possibility of attack spreading, or minimizing the chances of attackers accessing these resources.

   Note that sometimes modifying a security group may not achieve the expected effect due to connection tracking.

3. Evaluate whether the ECS instance needs to be restored. If the instance belongs to an auto scaling group, remove the instance from the group. If the event is related to a vulnerability in OSs, update the OSs and ensure that the vulnerability has been fixed.

4. Check operation logs on CTS to see if there are unauthorized operations, such as creating unauthorized IAM users, policies, roles, or temporary credentials. If any, delete the unauthorized IAM users, roles, and policies, and revoke all temporary credentials.

5. If the attack medium is related to unpatched software, OS updates, or expired anti-malware or antivirus tools, ensure that all ECS instances are updated to the latest OSs and all software packages and patches are up to date, and the virus feature codes and definition files on all ECSs are the latest. You can perform the following operations: For a variable architecture, patch it immediately. For an immutable architecture, deploy it again.

6. According to the update in **5**, delete all remaining resources that are identified as at risk of infection. These resources may possibly have accessed the same

media through which the ransomware was downloaded, by email, visiting infected websites, or by other means. For resources managed through auto scaling, focus on identifying attack media and take measures to prevent other resources from being infected through the same media.

Step 3 **Eradicate incidents**.

1. Assess whether the impact of an incident is limited to a specific part of the environment. If the ransomware data can be restored from a backup or snapshot, restore the data from the backup or snapshot.

    Investigating incidents in an isolated environment for root cause analysis is recommended as it is helpful in implementing controls to prevent similar incidents in the future.

2. Use the latest antivirus or anti-malware software to eliminate ransomware.

    Exercise caution when performing this operation because it may alert attackers. It is recommended that you view locked or encrypted objects in an isolated forensic environment, for example, removing network access permissions from infected ECS instances.

3. Delete all malware identified during forensic analysis and identify intrusion metrics.

4. If a ransomware virus has been identified, check whether there are available third-party decryption tools or other online resources that may help decrypt data.

Step 4 **Recover from incidents**.

1. Determine the restoration points of all restoration operations performed from the backup.

2. Check the backup policy to see whether all objects and files can be restored. This depends on the lifecycle policy applied to the resources.

3. Use the forensic method to confirm that the data is secure before the restoration, and then restore the data from the backup or restore the data to an earlier snapshot of the ECS instance.

4. If you have successfully restored data using any open-source decryption tool, delete the data from the instance and perform necessary analysis to confirm that the data is secure. Then, restore the instance. Alternatively, you can terminate or isolate the instance, create an instance, and restore the data to the new instance.

5. If neither restoring data from backups nor decrypting data is feasible, evaluate the possibility of restarting in a new environment.

Step 5 **Perform post-incident activities**.

1. Document and apply lessons learned from simulations and real incidents to subsequent processes and procedures. This will help better understand how the incident occurred in the system configuration and processes (e.g., where weaknesses exist, where automation may fail, and where there is a lack of visibility) and how to enhance its overall security posture.

2. If you have identified the initial attack medium or entry point, find out what is the best way to reduce the similar risk.

    For example, if malware is initially accessed through an unpatched public-facing ECS instance and you have applied the missing patch to all current

instances, consider how to improve the patch management process to test and apply the patch more quickly and consistently to prevent similar problems in the future.

3. If you have developed technical measures to address a particular threat, assess the probability that these steps will be automatically performed when the relevant threat is detected. Automated responses can help mitigate threats more quickly, thereby minimizing the scope and severity of the impact.

4. Collect lessons learned from all roles in the response process and update your incident response plan, disaster recovery plan, and this response plan as needed. New technical capabilities and personnel skills should be considered and funded as well to fill the gaps identified.

----End

12.2 Attack Link Analysis Alert Notification

12.2.1 Playbook Overview

Background

An attack link is an important concept in the cyber security field. It refers to a series of attack steps and paths taken by an attacker on a target network or system to achieve an attack purpose. Using these steps and paths, an attacker can sneakingly penetrate into the target system and do what they want.

The attack link has great harm to the target network or system. Once an attacker successfully constructs an attack link and breaks through the defense measures of the target system, the attacker can perform any operation on the target system, including stealing sensitive information, damaging system data, and paralyzing system services. These hazards not only cause economic losses, but also may have a serious impact on national security and social stability.

Response Solution

If a domain name is attacked, the attacker usually further hacks into backend servers. This playbook analyzes attack chains and generates alerts. Once this playbook discovers that attacks are approaching servers, it notifies operations personnel.

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 affected assets that are marked by HSS alerts through asset associations. By default, a maximum of three 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 three 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.

Incident Response

Step 1 **Obtain, store, and record evidence**.

1. Based on your environment configurations on the cloud, use HSS and WAF to detect alerts.

2. Access affected ECSs over SSH and check the instance status and monitoring information to see if there are any exceptions. Alerts you receive from other channels are supported.

3. Once an attack is confirmed as an incident, the affected scope, attacked machines, affected services, and data information need to be assessed.

4. Use SecMaster to convert alerts into incidents and continue to monitor and record incident details. For details, see **Converting Alerts to Incidents**.

5. In addition, log information can be traced. All related log information can be reviewed through security analysis, and recorded in the incident management module for subsequent operation tracing.

Step 2 **Contain incidents**.

1. Determine the attack type, affected servers, and service processes based on alerts and logs.

2. Use scripts, such as isolation, killing, and policy blocking scripts, to kill processes, isolate software, and taken other actions to reduce subsequent impacts.

3. Check the infection scope. If there is an infection risk, check and handle it in a timely manner.

4. Other playbooks and workflows can also be used for risk control, such as host isolation. Security group access control policies can be used to isolate infected machines and contain risks from further spreading.

Step 3 **Eradicate incidents**.

1. Evaluate whether the affected servers need to be hardened and restored. If the server has been compromised, you need to harden and restore it based on the source tracing result. If attacks are caused by security credential leakage, delete any unauthorized IAM users, roles, and policies, and revoke credentials to improve host security.

2. Check affected hosts for vulnerabilities, outdated software, and unpatched vulnerabilities. These may cause more hosts to be affected. You can go to the **Vulnerabilities** page and fix the vulnerabilities for the affected hosts. Check for risky configurations. You can go to the **Baseline Inspection** and rectify risky configurations in a timely manner.

3. Evaluate the impact scope. If other hosts have been affected, handle all affected hosts.

Step 4 **Recover from incidents**.

1. Determine the restoration points of all restoration operations performed from the backup.

2. Check the backup policy to see whether all objects and files can be restored. This depends on the lifecycle policy applied to the resources.

3. Use the forensic method to confirm that the data is secure before the restoration, and then restore the data from the backup or restore the data to an earlier snapshot of the ECS instance.

4. If you have successfully restored data using any open-source decryption tool, delete the data from the instance and perform necessary analysis to confirm that the data is secure. Then, restore the instance. Alternatively, you can terminate or isolate the instance, create an instance, and restore the data to the new instance.

5. If neither restoring data from backups nor decrypting data is feasible, evaluate the possibility of restarting in a new environment.

Step 5 **Perform post-incident activities**.

1. Analyze alert details in the entire alert handling process, continuously operate and optimize the model, and improve the model alarm accuracy. If an alert is related to a service but there is no risk, the alert can be filtered by a model.

2. Deeply analyze why the alert is generated and continuously optimize asset protection policies to reduce resource risks and the attack surface.

3. Optimize the automated response playbooks and workflows based on the actual service scenario. For example, you can replace the manual review policy with the automated review policy to improve the response efficiency and handle risks more quickly.

4. Analyze risk and attack links to enable pre-event risk control.

----End

12.2.2 Configuring Playbooks

Scenarios

This topic describes how to configure the playbook. After you configure this playbook, once this playbook discovers that attacks are approaching servers, it notifies operations personnel.

Prerequisites

- You have enabled access to HSS and WAF alerts on the **SecMaster** > **Data Integration**.

  You have enabled access to HSS and WAF logs and enable the function to automatically convert logs into alerts for HSS. For details about how to enable HSS and WAF alert access in SecMaster, see **Data Integration**.

Figure 12-2 Alert access
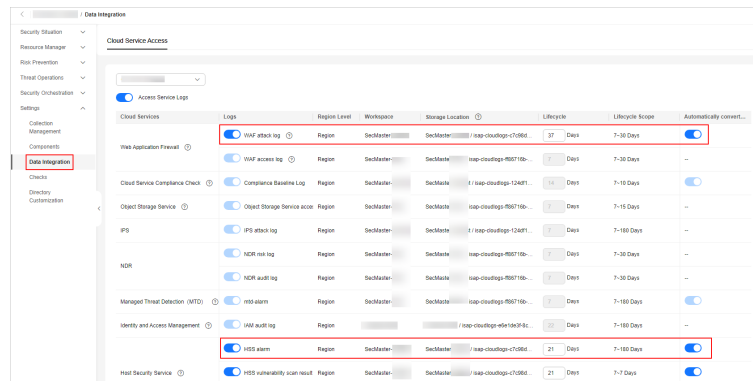
- On the **Resource Manager** page in the current SecMaster workspace, click an asset name. On the asset details page displayed, associate the website asset with the server asset.

Figure 12-3 Associated Assets
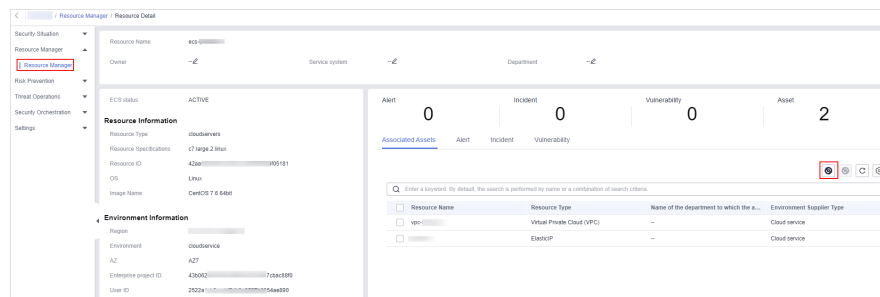
- SecMaster has obtained the **SMN FullAccess** permission, which specifies all permissions of SMN.

Table 12-1 Description

Permission	Description	Principal	Usage
SMN FullAccess	All permissions for SMN.	SecMaster_Agency	SecMaster uses SMN to send playbook execution notifications.

Perform the following steps to check whether SecMaster has obtained the **SMN FullAccess** permission: If the permission is not allocated, allocate it to SecMaster by referring to **Authorizing SecMaster**.

a. Log in to the console as the administrator.

b. Click in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

c. In the navigation pane on the left, choose **Agencies**. On the **Agencies** page, click **SecMaster_Agency** and then click the **Permissions** tab to view all authorization records of **SecMaster_Agency**.

Figure 12-4 Viewing Agency Authorization Records

Step 1: Create and Subscribe to a Topic

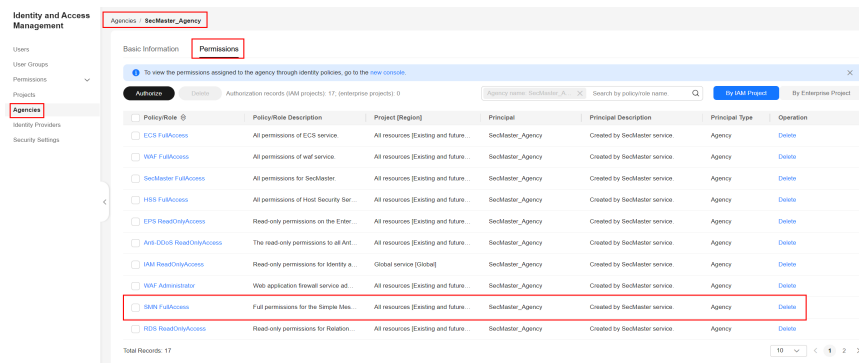The **Attack link analysis alert notification** workflow needs to use Simple Message Notification (SMN) to create and subscribe to a notification topic.

1. Log in to the management console.

2. In the upper left corner of the page, click ☰ and choose **Management & Governance** > **Simple Message Notification**.

3. Create a topic.

   a. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

   Figure 12-5 Create Topic

   b. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.

   - **Topic Name**: Set it to **SecMaster-Notification**.

   - **Display Name**: **SecMaster notification topic** is recommended.

   - Retain the default settings for other parameters.

   ⚠️ **CAUTION**

   Topic Name must be to **SecMaster-Notification**, or playbooks may fail to be executed.

   ---

4. Add a subscription.

   a. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.

     b.   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.

5.   Confirm the subscription.

    After a subscription is added, a confirmation email will be sent to the email address set in **4**. Click the subscription confirmation link in the email. A page for a successful subscription will be displayed.

Step 2: Configure and Enable the Playbook

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.

1.   Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

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

Figure 12-6 Workspace management page
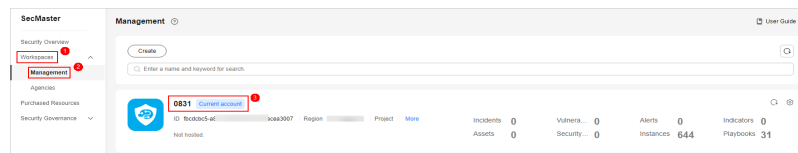
3.   In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 12-7 Accessing the Playbooks tab
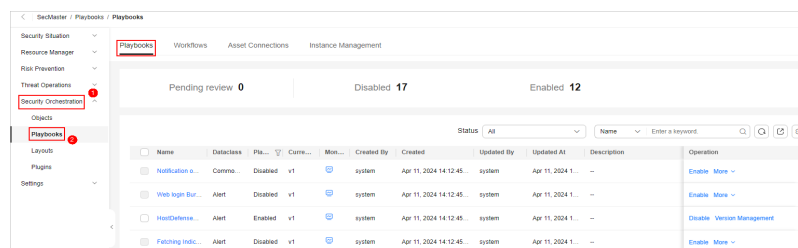
4.   On the **Playbooks** page, locate the row that contains the **Attack link analysis alert notification** playbook and click **Enable** in the **Operation** column.

5.   In the dialog box displayed, select the initial playbook version v1 and click **OK**.

Implementation Effect

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 12-8 Associated alerts
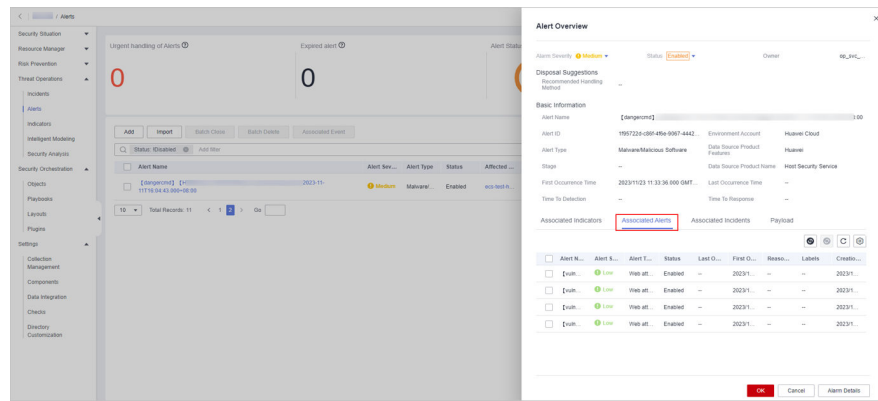
Comments on the corresponding alert added to the playbook

Figure 12-9 Comment
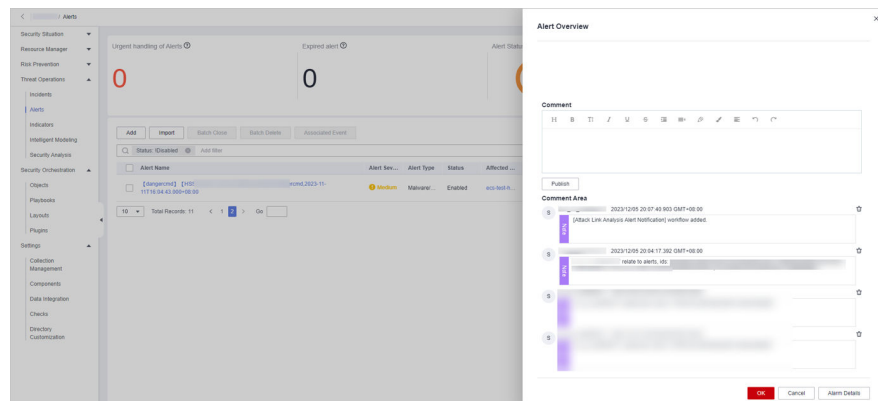
Alert notification email sent to specified personnel

Figure 12-10 Email notifications
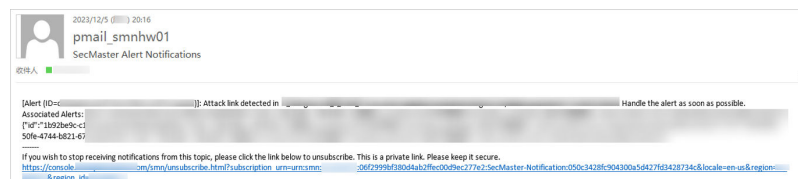
12.3 HSS Isolation and Killing of Malware

12.3.1 Playbook Overview

Background

A malware attack is a process of spreading malware (such as viruses, worms, Trojans, and ransomware) to users through emails, remote downloads, and malicious advertisements, and executing malicious programs on target hosts. In this way, the attacker can manipulate remote hosts, hack the network system,

steal sensitive information, or carry out other malicious activities. Such attacks pose a serious threat to the security of computer systems, networks, and personal devices, and may cause data leakage, system breakdown, personal privacy leakage, financial loss, and other security risks.

To solve the preceding problems, the required solution should effectively identify malicious programs such as backdoors, Trojans, mining software, worms, and viruses, and detect unknown malicious programs and virus variants on hosts through program feature and behavior detection, AI image fingerprint algorithms, and cloud-based antivirus. It can also detect ransomware embedded in media such as web pages, software, emails, and storage media. It is critical to prevent such attacks and reduce risks.

The following describes how this playbook isolates and kills malware and ransomware.

Response Solutions

This built-in playbook automatically isolates and kills malware detected on servers protected by HSS.

The HSS file isolation and killing playbook has matched the HSS file isolation and killing workflow. When a malware or ransomware alert is generated, the system checks the HSS version used for the attacked asset. If the professional edition or later is used but automatic isolation and killing are not enabled, the isolation and killing conditions are met. After the isolation and killing are manually approved, the alert is handled by this playbook. If the malware is successfully isolated, the alert is closed. If the playbook fails to isolate the malware, a comment is added, indicating that manual actions are required.

Incident Response

Step 1 **Obtain, store, and record evidence**.

1. Based on your environment configurations on the cloud, you can configure anti-virus and HIPS tests in HSS to detect security threats, such as malware and ransomware.

2. You can access the ECS using SSH and view the instance status and monitoring information to check whether any exception occurs. You can also check attack information or ransomware indicators you receive through other channels to discover potential threats.

3. Once an attack is confirmed as an incident, the affected scope, attacked machines, affected services, and data information need to be assessed.

4. Use SecMaster to convert alerts into incidents and continue to monitor and record incident details. For details, see **Converting Alerts to Incidents**.

5. In addition, log information can be traced. All related log information can be reviewed through security analysis, and recorded in the incident management module for subsequent operation tracing.

Step 2 **Contain incidents**.

1. Determine the attack type, affected servers, and service processes based on alerts and logs.

2. Use the HSS file isolation and killing playbook to kill and isolate compromised processes and software. This will reduce the further security risks.

3. Check the infection scope. If there is an infection risk, check and handle it in a timely manner.

4. Other playbooks and workflows can also be used for risk control, such as host isolation. Security group access control policies can be used to isolate infected machines and contain risks from further spreading.

Step 3 **Eradicate incidents**.

1. Evaluate whether the affected servers need to be hardened and restored. If the server has been compromised, you need to harden and restore it based on the source tracing result. If attacks are caused by security credential leakage, delete any unauthorized IAM users, roles, and policies, and revoke credentials to improve host security.

2. Check affected hosts for vulnerabilities, outdated software, and unpatched vulnerabilities. These may cause more hosts to be affected. You can go to the **Vulnerabilities** page and fix the vulnerabilities for the affected hosts. Check for risky configurations. You can go to the **Baseline Inspection** and rectify risky configurations in a timely manner.

3. Evaluate the impact scope. If other hosts have been affected, handle all affected hosts.

Step 4 **Recover from incidents**.

1. Determine the restoration points of all restoration operations performed from the backup.

2. Check the backup policy to see whether all objects and files can be restored. This depends on the lifecycle policy applied to the resources.

3. Use the forensic method to confirm that the data is secure before the restoration, and then restore the data from the backup or restore the data to an earlier snapshot of the ECS instance.

4. If you have successfully restored data using any open-source decryption tool, delete the data from the instance and perform necessary analysis to confirm that the data is secure. Then, restore the instance. Alternatively, you can terminate or isolate the instance, create an instance, and restore the data to the new instance.

5. If neither restoring data from backups nor decrypting data is feasible, evaluate the possibility of restarting in a new environment.

Step 5 **Perform post-incident activities**.

1. Analyze alert details in the entire alert handling process, continuously operate and optimize the model, and improve the model alarm accuracy. If an alert is related to a service but there is no risk, the alert can be filtered by a model.

2. Deeply analyze why the alert is generated and continuously optimize asset protection policies to reduce resource risks and the attack surface.

3. Optimize the automated response playbooks and workflows based on the actual service scenario. For example, you can replace the manual review policy with the automated review policy to improve the response efficiency and handle risks more quickly.

4. Perform risk analysis based on all similar malware and ransomware attack points to control risks before incidents occur.

----End

12.3.2 Configuring Playbooks

Scenarios

The following describes how to enable this playbook and use it to handle malware and ransomware alerts.

Prerequisites

You have enabled access to HSS alerts and toggled on the automatic converting logs into alerts function on the **Settings** > **Data Integration** page in the current workspace. For details, see **Data Integration**.

Figure 12-11 Accessing HSS alerts
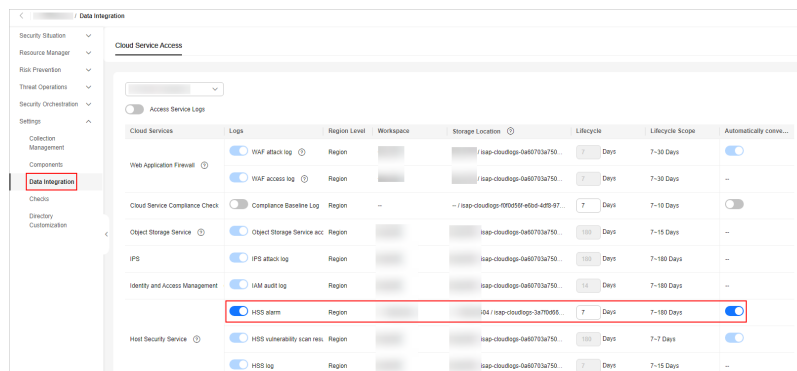
Configuring and Enabling a Playbook

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.

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 12-12 Workspace management page
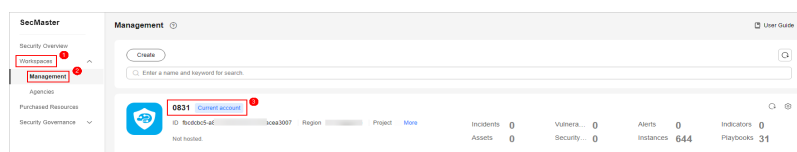
Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 12-13 Accessing the Playbooks tab
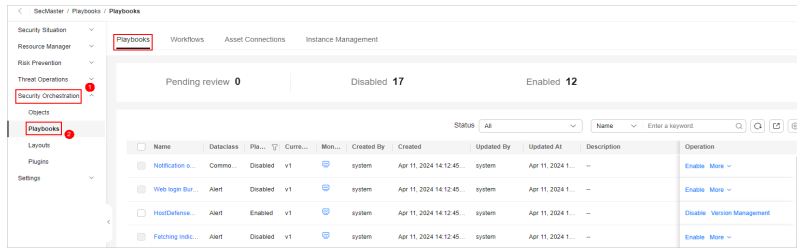
Step 5 On the **Playbooks** page, locate the row that contains the **HSS isolation and killing of malware** playbook and click **Enable** in the **Operation** column.

Step 6 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

Implementation Effect

- The malware has been killed and the alert is closed automatically.

Figure 12-14 Alerts automatically closed
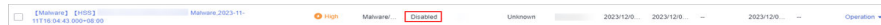
If the malware is isolated and killed, a comment will be left indicating that the alert has been cleared.

Figure 12-15 Comment on succeeded isolation and killing of malware
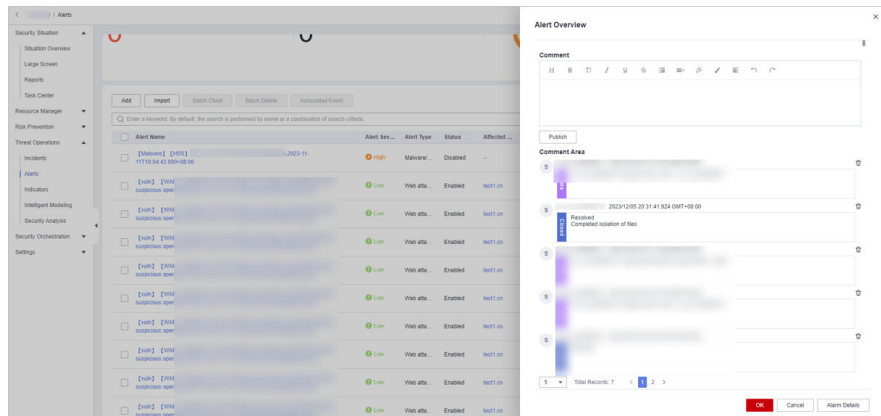
- If the malware fails to be isolated or killed, a comment will be left indicating that manual handling is required.

Figure 12-16 Comment on failed isolation and killing of malware
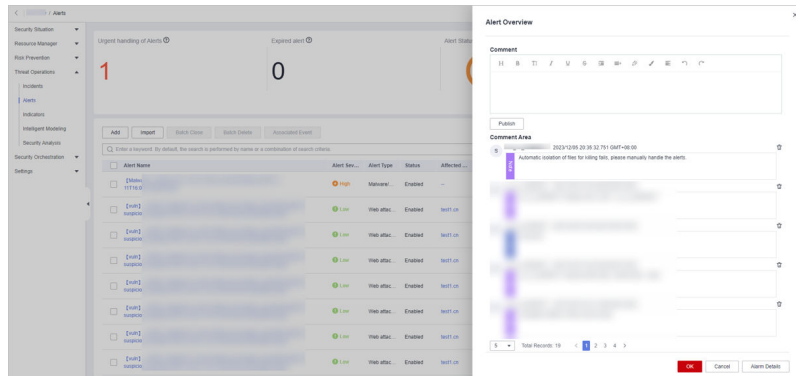
12.4 Automatic Renaming of Alert Names

Playbook Overview

This built-in playbook can automatically rename alerts. You can customize alert names with this playbook to meet your needs.

The **Auto Alert Renaming** playbook has matched the **Auto Alert Renaming** workflow. To configure this playbook, you need to configure the matched workflow and plug-ins the workflow uses.

The **Auto Alert Renaming** workflow has four plug-in nodes, one for obtaining alert type IDs, one for obtaining alert details, one 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 12-17 Automatic renaming of alarm names workflow
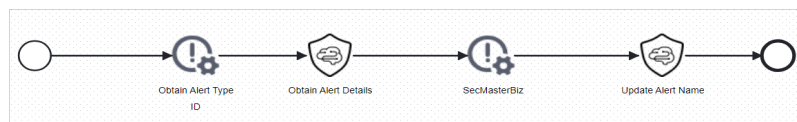
Limitations and Constraints

Currently, only names for web shell attack alerts can be modified.

Configuring and Enabling the Playbook

This topic walks you through on how to configure the SecMasterBiz node, enable the **Auto Alert Renaming** workflow, and enable the **Auto Alert Renaming** 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 12-18 Workspace management page
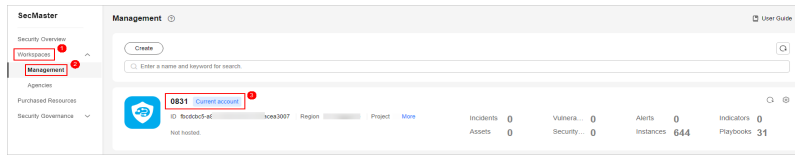
Step 4 Configure and enable the workflow.

1. Copy a workflow version.

   a. In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, select the **Workflows** tab.

      Figure 12-19 Workflows tab
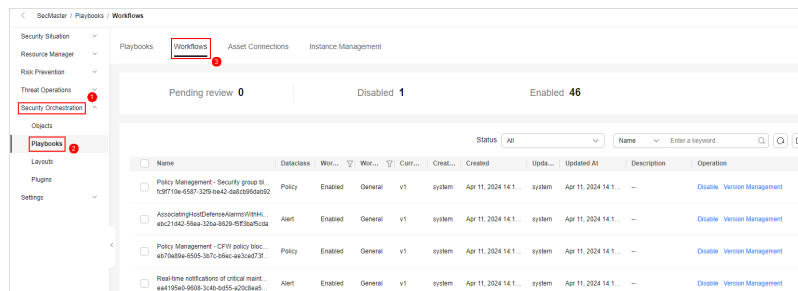
   b. Locate the row containing the **Auto Alert Renaming** workflow. In the **Operation** column, click **Version Management**.

      Figure 12-20 Version Management page
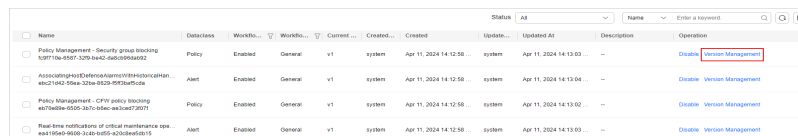
   c. On the **Version Management** page displayed, go to the **Version Information** area, locate the row where the initial version (v1) is listed, and click **Clone** in the **Operation** column.

   d. In the displayed dialog box, click **OK**.

2. Edit and submit the workflow version.

   a. On the **Version Management** slide-out panel for the **Auto Alert Renaming** workflow, go to the **Version Information** area, locate the row containing the copied workflow version, and click **Edit** in the **Operation** column.

   b. On the drawing page, click the **SecMasterBiz** plug-in and configure **Input** parameters on the pane displayed from the left.

      Details about SecMasterBiz plug-in parameters are listed below.

Figure 12-21 SecMasterBiz plug-in
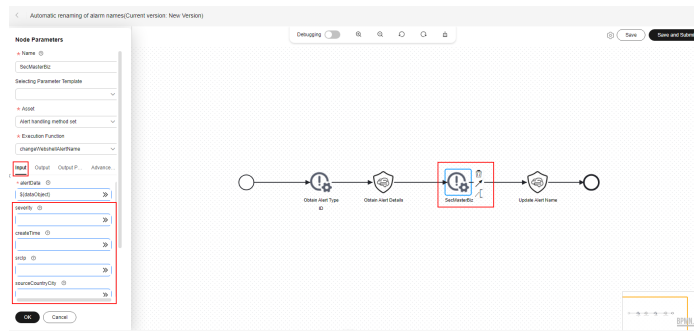
SecMasterBiz is a plug-in used in the workflow for automatically renaming alert names. It analyzes and processes web shell alert names. You can combine alert names in the way you want and let the system return the alert names as you configured.

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 **y**, this parameter is selected. If you enter **n**, this parameter is not selected. If you leave this parameter blank, this parameter is not selected.

Table 12-2 Parameter configuration description

Parameter	Description	Value Range
severity	Alert severity.	y/n
createTime	Time the alert was created.	y/n
srcIp	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

c. After the configuration is complete, click **Save and Submit** in the upper right corner. In the dialog box displayed, click **OK**.

3. Review the workflow version.

a. On the **Workflows** page, locate the **Auto Alert Renaming** workflow and click **Version Management** in the **Operation** column.

      b.   On the displayed **Version Management** page, locate the row that contains the edited workflow version, and click **Review** in the **Operation** column.

      c.   In the displayed dialog box, set **Comment** to **Passed** and click **OK**.

  4.   Activate the workflow version.

      a.   On the **Version Management** page, locate the row that contains the reviewed workflow version and click **Activate** in the **Operation** column.

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

      After a workflow version is activated, the workflow is enabled by default.

Step 5   Configure and enable the playbook.

  1.   In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 12-22 Accessing the Playbooks tab
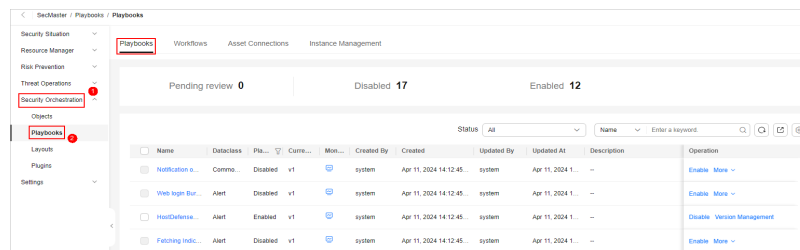
  2.   On the **Playbooks**, locate the row that contains the playbook for automatically renaming alert names, and click **Enable** in the **Operation** column.

  3.   In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

Verifying the Playbook

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.

Step 1   In the navigation pane on the left, choose **Threats** > **Alerts**.

Figure 12-23 Alerts
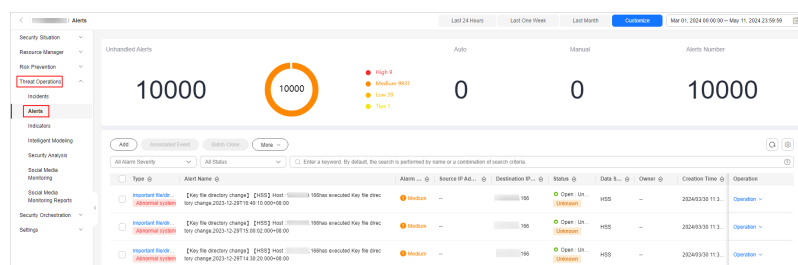
Step 2   Click **Add**. Configure parameters in the **Add** slide-out panel.

  ●   **Alert Name**: Enter a name for the alert.

- **Alert Type**: Select **Web attacks** and then **Web shell**.

- First Occurrence Time: Set the time when the alert occurs for the first time.

- **Debugging data**: Select **Yes**.

- **Description**: Description of the custom alert.

- Retain default values for other parameters.

Step 3 Click **OK**.

Step 4 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 12-24 Output when no parameters are selected (default)

Figure 12-25 Output when only severity is selected

----End

Implementation Effect

The following figure shows default alert names.

Figure 12-26 Before processing

The following figure shows customized alert names.

Figure 12-27 After processing
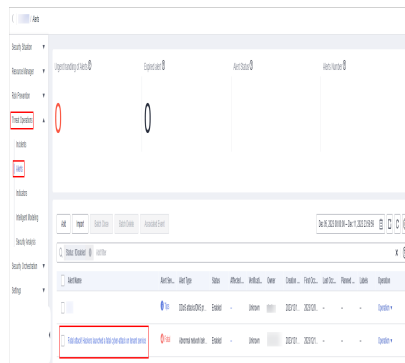
12.5 Auto High-Risk Vulnerability Notification

Playbook Overview

This playbook can automatically notify of high-risk server vulnerabilities to operations personnel.

The **Automatic notification of high-risk vulnerabilities** playbook has been matched the **Auto High-Risk Vulnerability 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.

If a high-risk vulnerability was reported by HSS, SMN sends a notification to operations personnel.

Figure 12-28 Auto high-risk vulnerability notification workflow
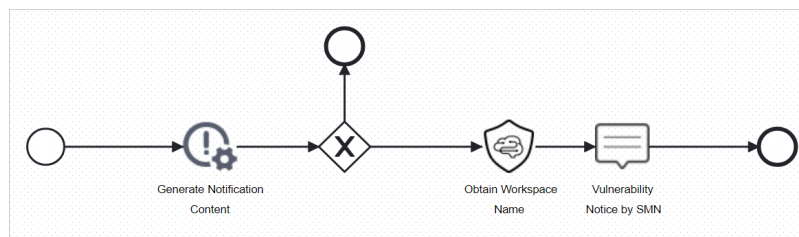
Prerequisites

- You have enabled Host Security Service (HSS) alarm access on the **Data Integration** page under the **Settings** pane. For details, see **Data Integration**.

Figure 12-29 Access to HSS alerts

To view integrated data, choose **Risk Prevention** > **Vulnerabilities**.

Figure 12-30 Viewing vulnerabilities

- SecMaster has obtained the **SMN FullAccess** permission, which specifies all permissions of SMN.
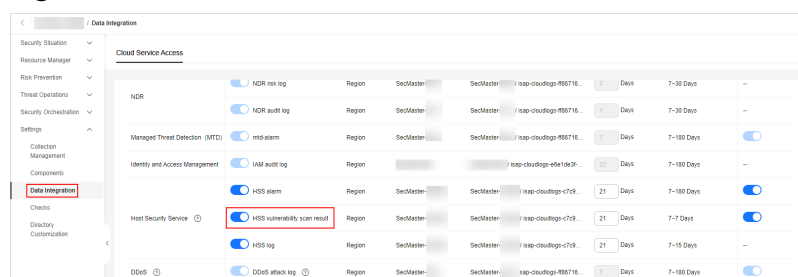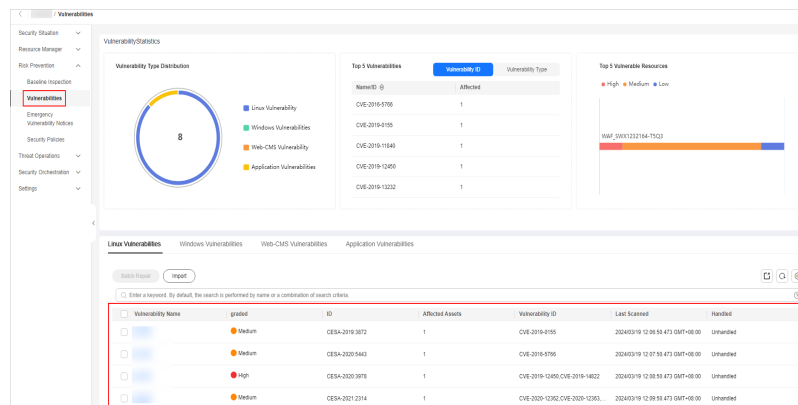
Table 12-3 Description

Permission	Description	Principal	Usage
SMN FullAccess	All permissions for SMN.	SecMaster_Agency	SecMaster uses SMN to send playbook execution notifications.

Perform the following steps to check whether SecMaster has obtained the **SMN FullAccess** permission: If the permission is not allocated, allocate it to SecMaster by referring to **Authorizing SecMaster**.

a. Log in to the console as the administrator.

b. Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

c. In the navigation pane on the left, choose **Agencies**. On the **Agencies** page, click **SecMaster_Agency** and then click the **Permissions** tab to view all authorization records of **SecMaster_Agency**.

Figure 12-31 Viewing Agency Authorization Records
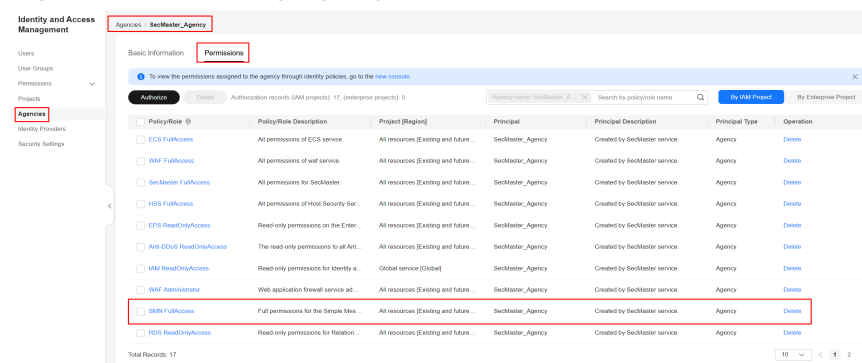
Step 1: Create and Subscribe to a Topic

The **Auto High-Risk Vulnerability Notification** workflow uses Simple Message Notification (SMN) to send notifications. You need to create and subscribe to a topic for receiving notifications.

1. Log in to the management console.

2. In the upper left corner of the page, click ☰ and choose **Management & Governance** > **Simple Message Notification**.

3. Create a topic.

   a. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.
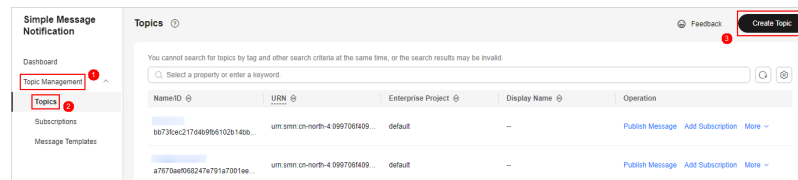
   Figure 12-32 Create Topic

   b. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.

      ▪ **Topic Name**: Set it to **SecMaster-Notification**.

      ▪ **Display Name**: **SecMaster notification topic** is recommended.

      ▪ Retain the default settings for other parameters.

   ⚠️ **CAUTION**

   Topic Name must be to **SecMaster-Notification**, or playbooks may fail to be executed.

   ---

4. Add a subscription.

   a. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.

   b. 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.

5. Confirm the subscription.

   After a subscription is added, a confirmation email will be sent to the email address set in **4**. Click the subscription confirmation link in the email. A page for a successful subscription will be displayed.

Step 3: Configure and Enable the Playbook

In SecMaster, the initial version (V1) of the **Auto High-Risk Vulnerability Notification** 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.

1. On the **Playbooks** page, locate the row that contains the **Playbooks** playbook and click **Automatic notification of high-risk vulnerabilities** in the **Enable** column.

2. In the dialog box displayed, select the initial playbook version v1 and click **OK**.

12.6 Automatic Notification of High-Risk Alerts

Playbook Overview

This playbook can automatically notify you of new high-risk alerts after removing repeated ones.

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.

Figure 12-33 Automatic notification of high-risk alerts workflow
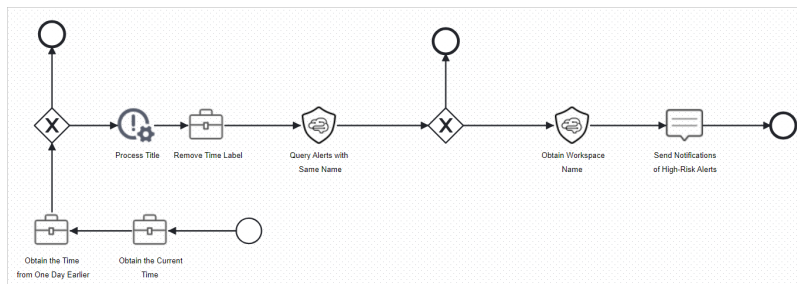
Prerequisites

- SecMaster has obtained the **SMN FullAccess** permission, which specifies all permissions of SMN.

Table 12-4 Description

Permission	Description	Principal	Usage
SMN FullAccess	All permissions for SMN.	SecMaster_Agency	SecMaster uses SMN to send playbook execution notifications.

Perform the following steps to check whether SecMaster has obtained the **SMN FullAccess** permission: If the permission is not allocated, allocate it to SecMaster by referring to **Authorizing SecMaster**.

a. Log in to the console as the administrator.

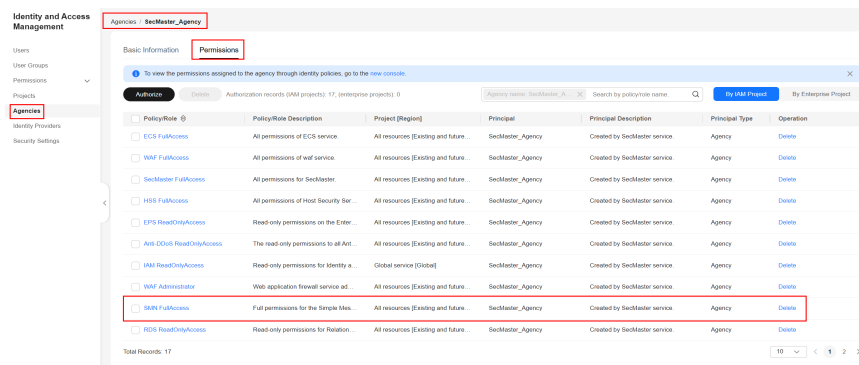b. Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

c. In the navigation pane on the left, choose **Agencies**. On the **Agencies** page, click **SecMaster_Agency** and then click the **Permissions** tab to view all authorization records of **SecMaster_Agency**.

Figure 12-34 Viewing Agency Authorization Records

Step 1: Create and Subscribe to a Topic

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.

1. Log in to the management console.

2. In the upper left corner of the page, click ☰ and choose **Management & Governance** > **Simple Message Notification**.

3. Create a topic.

   a. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

   Figure 12-35 Create Topic

   b. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.

   - **Topic Name**: Set it to **SecMaster-Notification**.

   - **Display Name**: **SecMaster notification topic** is recommended.

■ Retain the default settings for other parameters.

> ⚠ CAUTION
>
> **Topic Name** must be to **SecMaster-Notification**, or playbooks may fail to be executed.

4. Add a subscription.

   a. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.

   b. 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.

5. Confirm the subscription.

   After a subscription is added, a confirmation email will be sent to the email address set in **4**. Click the subscription confirmation link in the email. A page for a successful subscription will be displayed.

Step 2: Configure and Enable the Playbook

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.

1. Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

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

   Figure 12-36 Workspace management page
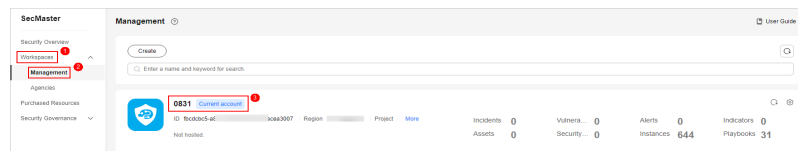
3. In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 12-37 Accessing the Playbooks tab
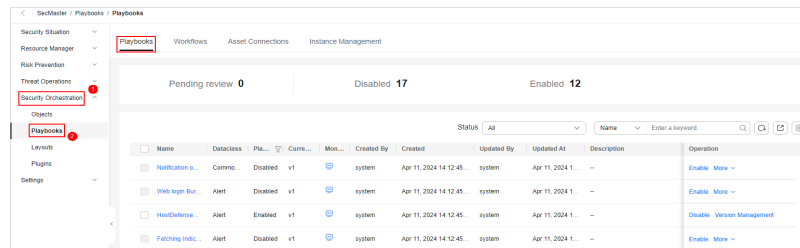
4. On the **Playbooks** page, locate the row that contains the **Automatic notification of high-risk alerts** playbook and click **Enable** in the **Operation** column.

5. In the dialog box displayed, select the initial playbook version v1 and click **OK**.

Implementation Effect

This following figure shows an email example sent when the playbook was triggered by high-risk alerts.

Figure 12-38 Alert notification email
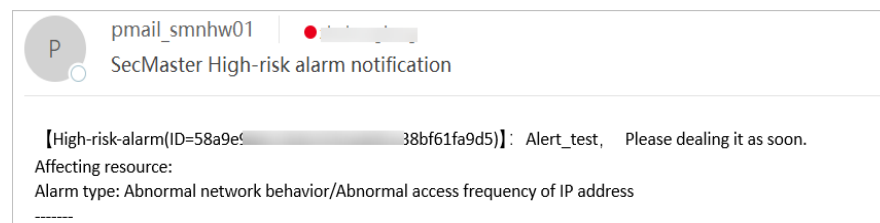
12.7 Auto Blocking for High-risk Alerts

Playbook Overview

SecMaster provides a playbook for automatic blocking of high-risk alerts. This playbook can automatically scan high-risk alerts for source IP addresses that are identified by ThreatBook as medium and high risk and block them in the services, such as WAF, CFW, and VPC security groups, where the high-risk alerts have been generated.

The **Auto Blocking for High-Risk Alerts** playbook has matched the **Auto Blocking for High-Risk Alerts** workflow.

Figure 12-39 Auto Blocking for High-risk Alerts
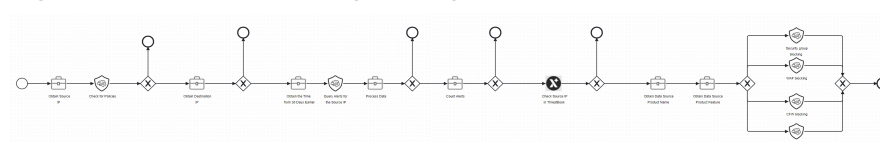
Prerequisites

- You have enabled access to WAF access logs or WAF attack logs on the **Data Integration** page under **Settings** in the current workspace. For details, see **Data Integration**.

Figure 12-40 Enabling access to WAF logs
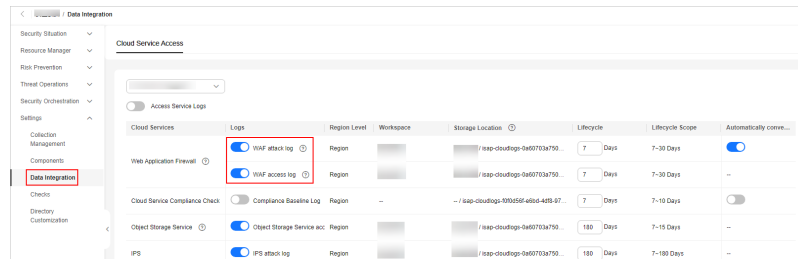
- You have available quota for querying indicators in ThreatBook.

Step 1: Configure an Asset Connection

Before using the **Auto Blocking for High-Risk Alerts** workflow, configure the API key of the ThreatBook plug-in used for the workflow first. You can obtain it in the **threatbook authentication token** asset connection.

1. Log in to the management console.

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

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
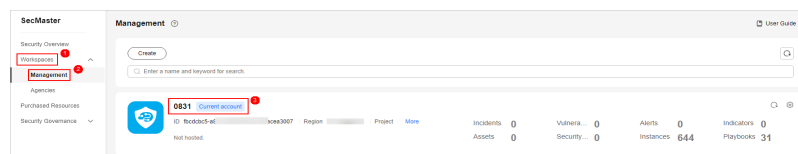
4. In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 12-42 Asset Connections tab
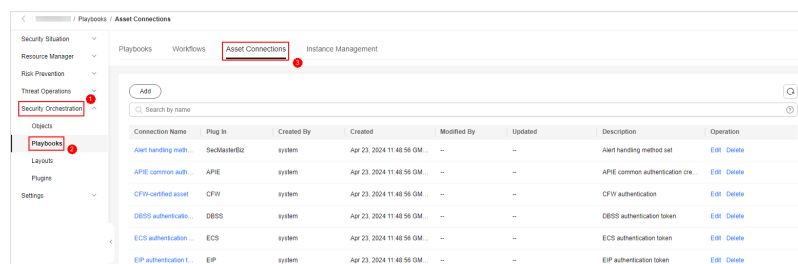
5. On the **Asset connection** page, locate the row that contains the **threatbook authentication token** asset connection and click **Edit** in the **Operation** column.

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.

7. Click **OK**.

Step 2: Configure and Enable the Playbook

In SecMaster, the initial version (V1) of the **Auto Blocking for High-Risk Alerts** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Auto Blocking for High-Risk Alerts** playbook is also activated by default. To use it, you only need to enable it.

1. On the **Playbooks** page, locate the row that contains the **Auto Blocking for High-Risk Alerts** playbook and click **Enable** in the **Operation** column.

2. In the dialog box displayed, select the initial playbook version v1 and click **OK**.

Implementation Effect

The following uses WAF as an example.

If an IP address is blocked, it will 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 an address group in the WAF blacklist.

Figure 12-43 Blacklist and Whitelist
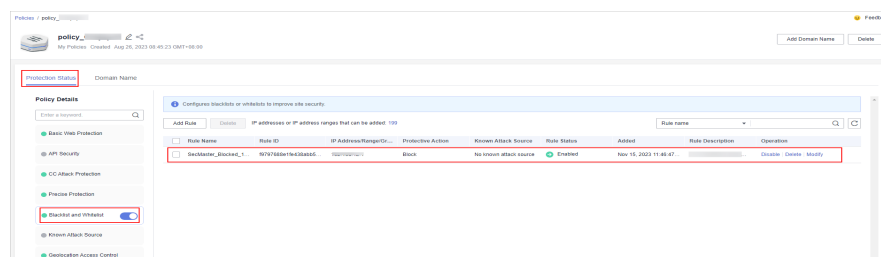
12.8 Real-time Notification of Critical Organization and Management Operations

Playbook Overview

This built-in playbook can notify you of key O&M operations by email in real time.

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.

Prerequisites

- You have enabled access to CTS logs on the **Data Integration** page under **Settings** in the current workspace. For details, see **Data Integration**.

  Figure 12-44 Access to CTS logs
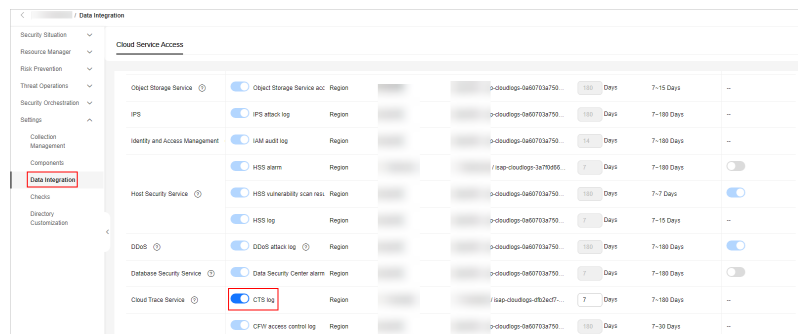
- The corresponding O&M defense model has been enabled. For details, see **Step 2: Enable the Alert Model**.

- SecMaster has obtained the **SMN FullAccess** permission, which specifies all permissions of SMN.

  Table 12-5 Description

Permission	Description	Principal	Usage
SMN FullAccess	All permissions for SMN.	SecMaster_Agency	SecMaster uses SMN to send playbook execution notifications.

  Perform the following steps to check whether SecMaster has obtained the **SMN FullAccess** permission: If the permission is not allocated, allocate it to SecMaster by referring to **Authorizing SecMaster**.

a. Log in to the console as the administrator.

b. Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

c. In the navigation pane on the left, choose **Agencies**. On the **Agencies** page, click **SecMaster_Agency** and then click the **Permissions** tab to view all authorization records of **SecMaster_Agency**.

Figure 12-45 Viewing Agency Authorization Records
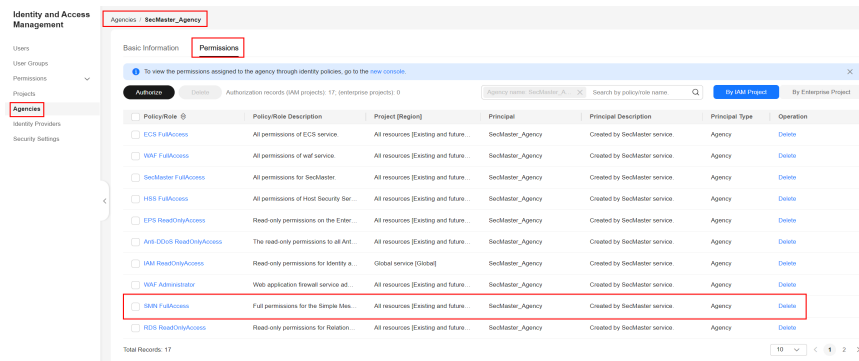
Step 1: Create and Subscribe to a Topic

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.

1. Log in to the management console.

2. In the upper left corner of the page, click ☰ and choose **Management & Governance** > **Simple Message Notification**.

3. Create a topic.

    a. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

    Figure 12-46 Create Topic

    b. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.

    ▪ **Topic Name**: Set it to **SecMaster-Notification**.

    ▪ **Display Name**: **SecMaster notification topic** is recommended.

    ▪ Retain the default settings for other parameters.

⚠ **CAUTION**

Topic Name must be to **SecMaster-Notification**, or playbooks may fail to be executed.

4. Add a subscription.

   a. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.

   b. 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.

5. Confirm the subscription.

   After a subscription is added, a confirmation email will be sent to the email address set in **4**. Click the subscription confirmation link in the email. A page for a successful subscription will be displayed.

Step 2: Enable the Alert Model

Before using the **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.

1. Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

2. 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
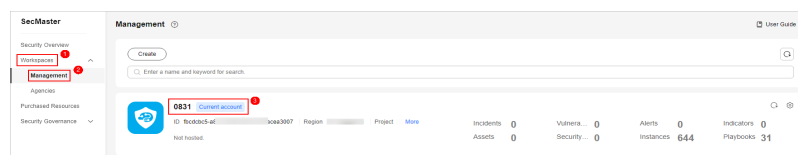
3. In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**, and select the **Model Templates** tab.

Figure 12-48 Model Templates tab
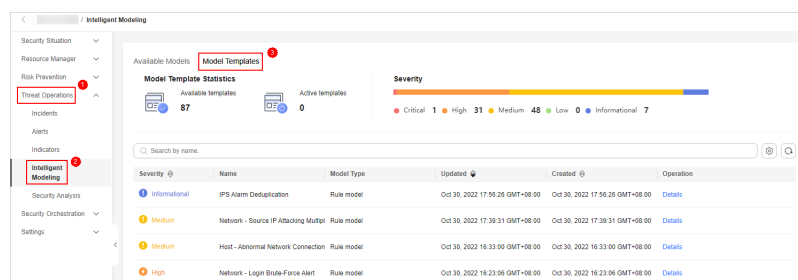
4. In the model template list, click **Details** in the **Operation** column of the target model template. The template details page is displayed on the right.

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

6. On the **Create Threat Model** page, configure basic information about the model.

   – **Pipeline Name**: Select an execution pipeline for the alert model.

   Table 12-6 Available pipelines

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 for other parameters.

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.

8. Set the model logic. You are advised to retain the default settings.

9. Complete all settings and click **Next** in the lower right corner of the page.

10. Review all settings and click **OK** in the lower right corner of the page.

11. Repeat **4** to **10** to create alert models with other templates.

12. In the navigation pane on the left, choose **Threats** > **Intelligent Modeling**.

    Figure 12-49 Available Models
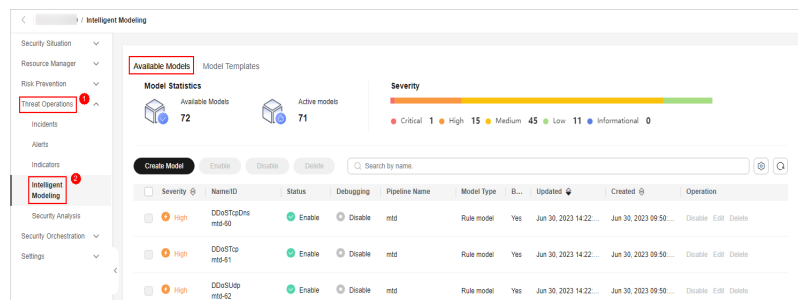
13. To enable models in batches, select all models you want to enable and click **Enable** in the upper left corner of the list.

    If the model status changes to **Enable**, the model is successfully started.

Step 3: Configure and Enable the Playbook

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.

1. In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 12-50 Accessing the Playbooks tab
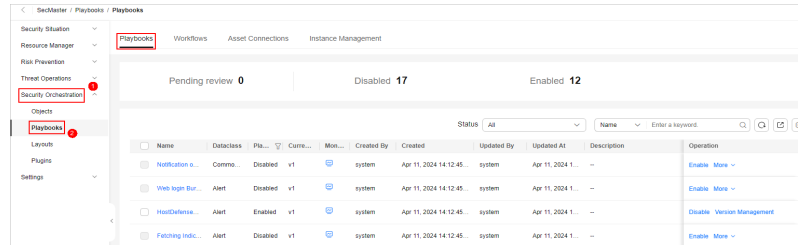
2. On the **Playbooks** page, locate the row that contains the **Real-time notification of critical Organization and Management operations** playbook and click **Enable** in the **Operation** column.

3. In the dialog box displayed, select the initial playbook version v1 and click **OK**.

Implementation Effect

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 12-51 Operation notifications
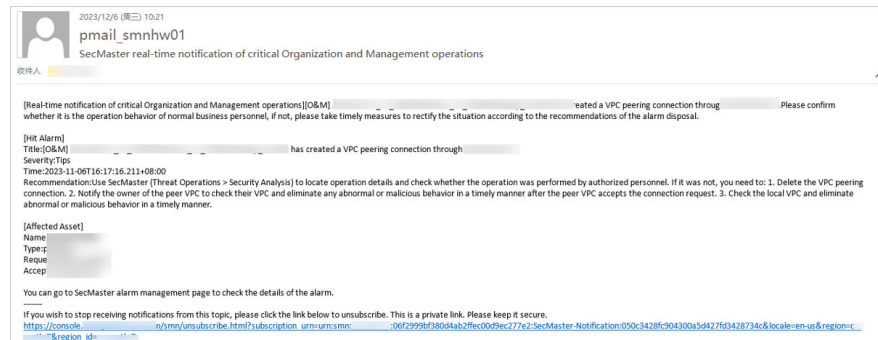
13 Settings

13.1 Data Integration

13.1.1 Cloud Service 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.

Table 13-1 Log access supported by SecMaster

Cate gory	Service	Servi ce Type	Log	Log Descripti on	Supported Region
Host securi ty	Host Security Service (HSS)	Tenan t-side cloud servic e	hss-alarm	HSS security alarms	AP-Singapore, CN-Hong Kong, TR-Istanbul, AP-Bangkok, AF-Johannesburg, LA-Mexico City2 (converged in LA-Mexico City1), LA-Sao Paulo1, LA-Santiago, AP-Jakarta, ME-Riyadh, and AF-Cairo
			hss-vul	HSS vulnerabil ity scan results	
			hss-log	HSS security logs	
			hss-baseli ne	HSS baseline check	AP-Singapore, CN-Hong Kong, TR-Istanbul, AP-Bangkok, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1, LA-Santiago, AP-Jakarta, ME-Riyadh, and AF-Cairo

Cate gory	Service	Servi ce Type	Log	Log Descripti on	Supported Region
Appli catio n securi ty	Web Applicatio n Firewall (WAF)	Tenan t-side cloud servic e	waf-attac k	WAF attack logs	AP-Singapore, CN-Hong Kong, TR-Istanbul, AP-Bangkok, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1, LA-Santiago, AP-Jakarta, ME-Riyadh, and AF-Cairo
			waf-acces s	WAF access logs	
	API Gateway (APIG)	Tenan t-side cloud servic e	apig-acces s	APIG request logs	NA
	Cloud Trace Service (CTS)	Tenan t-side cloud servic e	cts-audit	CTS logs	AP-Singapore, CN-Hong Kong, TR-Istanbul, AP-Bangkok, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1, LA-Santiago, AP-Jakarta, ME-Riyadh, and AF-Cairo
Netw ork securi ty	NIP	Huaw ei devic e	nip-attac k	IPS attack logs	AP-Singapore and AF-Johannesburg
	DDoS	Huaw ei devic e	ddos-attac k	Anti-DDoS attack logs	AF-Johannesburg and AP-Jakarta
	Cloud Firewall (CFW)	Tenan t-side cloud servic e	cfw-block	Access control logs	AP-Singapore, CN-Hong Kong, TR-Istanbul, AP-Bangkok, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1, LA-Santiago, AP-Jakarta, ME-Riyadh, and AF-Cairo
			cfw-flow	Traffic logs	
			cfw-risk	Attack logs	
O&M securi ty	Cloud Bastion Host (CBH)	Tenan t-side cloud servic e	cbh-audit	Bastion host audit logs	NA

Cate gory	Service	Servi ce Type	Log	Log Descripti on	Supported Region
Data securi ty	Object Storage Service (OBS)	Tenan t-side cloud servic e	obs-acces s	OBS access logs	LA-Mexico City2
	Database Security Service (DBSS)	Tenan t-side cloud servic e	dbss-alarm	DBSS alarm logs	NA
	Data Security Center (DSC)	Tenan t-side cloud servic e	dsc-alarm	DSC alarm logs	AP-Singapore, CN-Hong Kong, TR-Istanbul, AP-Bangkok, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1, LA-Santiago, AP-Jakarta, ME-Riyadh, and AF-Cairo
Identi ty securi ty	Identity and Access Managem ent (IAM)	Tenan t-side cloud servic e	iam-audit	IAM audit logs	NA
Cloud securi ty	Managed Threat Detection (MTD)	Tenan t-side cloud servic e	mtd-alarm	MTD alarm logs	AP-Singapore, CN-Hong Kong, AP-Bangkok, AF-Johannesburg, LA-Sao Paulo1, and LA-Santiago
	SecMaste r	Tenan t-side cloud servic e	secm aster-baseli ne	SecMaste r baseline inspection	AP-Singapore, CN-Hong Kong, TR-Istanbul, AP-Bangkok, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1, LA-Santiago, AP-Jakarta, ME-Riyadh, and AF-Cairo

13.1.2 Enabling Log Access

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 **Cloud Service Log Access Supported by SecMaster**.

For the first workspace in each region, most types of logs recommended by SecMaster will be automatically loaded. For non-first workspaces, you need to configure log data access manually.

📖 **NOTE**

> You are advised to enable access to asset details, asset alerts, baseline inspection results, vulnerability data, and logs in one workspace. This will make it easier for centralized security operations and association analysis.

This topic describes how to access logs and view where logs are stored.

Limitations and Constraints

It takes about 10 minutes for the log access settings to take effect.

Allowing SecMaster to Access Cloud Service Logs

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-1 Workspace management page
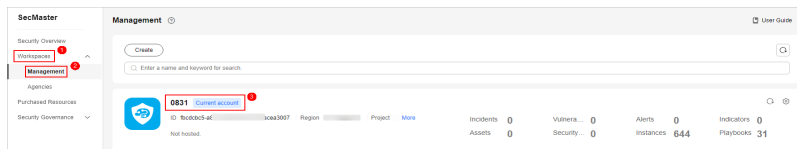
Step 5 In the navigation pane on the left, choose **Settings** > **Data Integration**.

Figure 13-2 Data Integration page
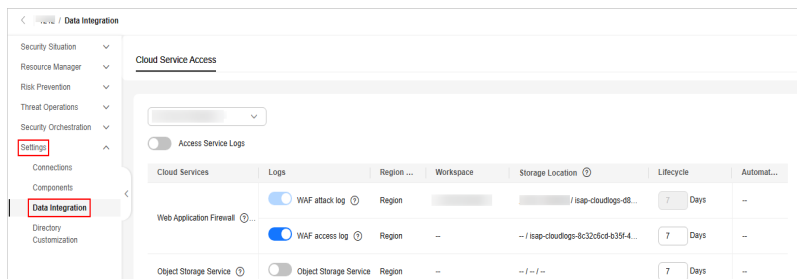
Step 6 Locate the target cloud service and click 🔘 in the **Logs** column.

To access logs of cloud services supported in the current region, click 🔘 on the left of **Access Service Logs**.

Step 7 Set the lifecycle.

Set the data storage duration as required.

Step 8 Set **Automatically converts alarms**.

Locate the row containing the target security products. In the **Automatically converts alarms** column of that row, click ⬤ to enable the function. After that, SecMaster will automatically convert cloud service logs into alerts when the logs meet certain alert rules. Those alerts will be displayed on the **Alerts** page.

📖 **NOTE**

- If this function is disabled, logs that meet certain alert rules will not be converted into 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 9 Click **Save**. In the displayed dialog box, click **OK**.

📖 **NOTE**

It takes about 10 minutes for the log access settings to take effect. After the access completes, a default data space and pipeline are created.

----End

Viewing Logs and Storage Locations

After log integration, choose **Security Analysis** > **Security Data Tables** and view integrated logs.

1. Go to the target workspace. In the navigation pane on the left, choose **Threats** > **Security Analysis**. The **Security Analysis** page is displayed.
2. 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 page displayed on the right, you can search the pipeline data.

   You can view the integrated logs on the pipeline data query page.

Related Operations

- Canceling Data Access

  a. In the **Logs** column of the target cloud services, click ⬤ to disable the access to cloud service logs.

  b. Click **Save**.

- Editing the Data Access Lifecycle

  a. In the **Lifecycle** column of the target cloud services, enter the data storage period.

  b. Click **Save**.

- Canceling Automatic Converting Logs into Alarms

  a. In the **Automatically converts alarms** column of the target cloud products, click ⬤ to disable the alarms.

b.	Click **Save**.

13.2 Log Data Collection

13.2.1 Data Collection Overview

You can enable access to third-party (non-Huawei Cloud) logs in SecMaster. SecMaster uses Logstash to collect logs from many types of sources. Logs are comprehensively collected for historical data analysis, associated data analysis, and unknown threat detection.

Figure 13-3 Data collection
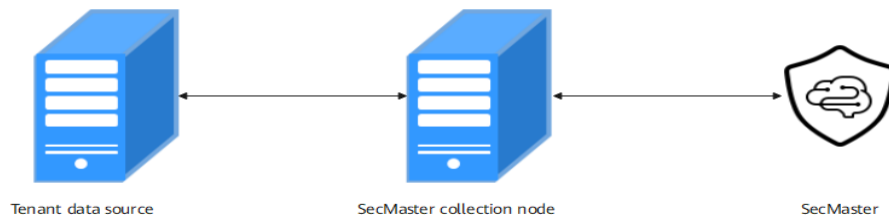
Data Collection Principles

The basic principle of data collection is as follows: SecMaster uses a component controller (isap-agent) that is installed on your ECSs to manage the collection component Logstash, and Logstash transfer security data in your organization or between you and SecMaster.

Figure 13-4 Functional architecture of the collection system
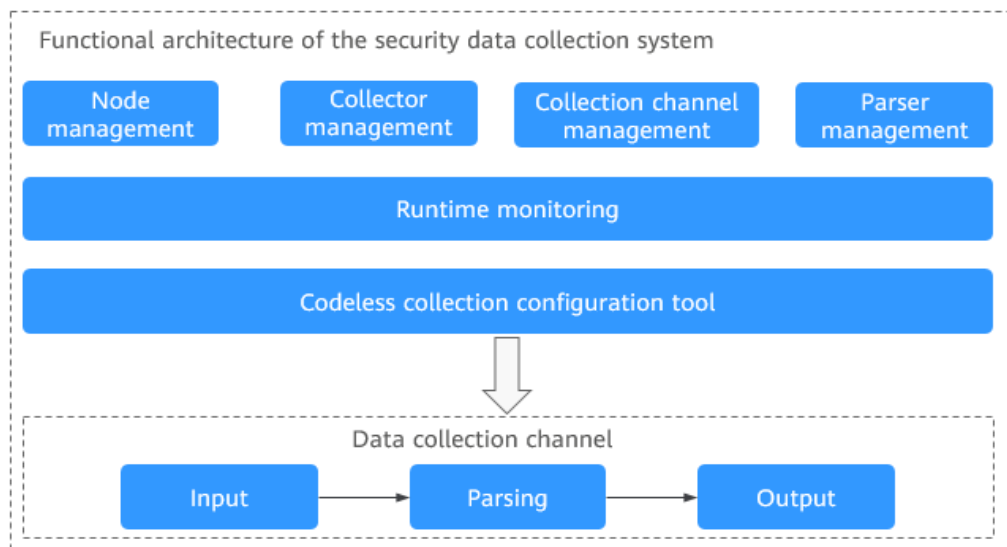
Description

- Collector: custom Logstash. A collector node is a custom combination of Logstash+ component controller (isap-agent).

- Node: If you install SecMaster component controller isap-agent on an ECS and use IAM to authorize SecMaster to manage the ECS, the ECS is called a node. You need to deliver data collection engine Logstash to managed nodes on the **Components** page.

- Component: A component is a custom Logstash that works as a data aggregation engine to receive and send security log data.

- Connector: A connector is a basic element for Logstash. It defines the way Logstash receives source data and the standards it follows during the process. Each connector has a source end and a destination end. Source ends and destination ends are used for data inputs and outputs, respectively. The SecMaster pipeline is used for log data transmission between SecMaster and your devices.

- Parser: A parser is a basic element for configuring custom Logstash. Parsers mainly work as filters in Logstash. SecMaster preconfigures varied types of filters and provides them as parsers. In just a few clicks on the SecMaster console, you can use parsers to generate native scripts to set complex filters for Logstash. In doing this, you can convert raw logs into the format you need.

- Collection channel: A collection channel is equivalent to a Logstash pipeline. Multiple pipelines can be configured in Logstash. Each pipeline consists of the input, filter, and output parts. Pipelines work independently and do not affect each other. You can deploy a pipeline for multiple nodes. A pipeline is considered one collection channel no matter how many nodes it is configured for.

Limitations and Constraints

- Currently, the data collection component controller can run on Linux ECSs running the x86_64 architecture.

- Only IAM users can be used to install component controller and check details on the console. The IAM user can have only the minimum permissions assigned. For details, see **Preparations**.

Collector Specifications

The following table describes the specifications of the ECSs that are selected as nodes in collection management.

Table 13-2 Collector Specifications

vCPUs	Memory	System Disk	Data Disk	Referenced Processing Capability
4 vCPUs	8 GB	50 GB	100 GB	2,000 EPS @ 1 KB 4,000 EPS @ 500 B

vCPUs	Memory	System Disk	Data Disk	Referenced Processing Capability
8 vCPUs	16 GB	50 GB	100 GB	5,000 EPS @ 1 KB 10,000 EPS @ 500 B
16 vCPUs	32 GB	50 GB	100 GB	10,000 EPS @ 1 KB 20,000 EPS @ 500 B
32 vCPUs	64 GB	50 GB	100 GB	20,000 EPS @ 1 KB 40,000 EPS @ 500 B
64 vCPUs	128 GB	50 GB	100 GB	40,000 EPS @ 1 KB 80,000 EPS @ 500 B

NOTE

- The ECS must have at least two vCPUs and 4 GB of memory. A disk of at least 100 GB must be attached as the directory disk.

- The log volume usually increases in proportion to the server specifications. Generally, you are advised to increase the log volume based on the specifications in the table. If there is huge pressure on a collector, you can deploy multiple collectors and manage them centrally through collection channels. This can distribute the log forwarding pressure across collectors.

- Before installing the component controller, you are advised to mount a disk and use the disk partitioning script to allocate the disk. To ensure the installation and running of Logstash, the directory partition must have more than 100 GB of free space.

Log Source Limit

You can add as many as log sources you need to the collectors as long as your cloud resources can accommodate those logs. You can scale cloud resources anytime to meet your needs.

Data Collection Process

Figure 13-5 Data collection process

Table 13-3 Description of the data collection process

No.	Step	Description
1	**Managing Nodes**	Select or purchase an ECS and install the component controller on the ECS to complete node management.
2	**Installing Components**	Install data collection engine Logstash on the **Components** tab to complete component installation.

No.	Step	Description
3	**Configuring Connectors**	Configure the source and destination connectors. Select a connector as required and set parameters.
4	**(Optional) Configuring a Parser**	Configure codeless parsers on the console based on your needs.
5	**Configuring a Collection Channel**	Configure the connection channels, associate it with a node, and deliver the Logstash pipeline configuration to complete the data collection configuration.
6	Verifying the Collection Result	After the collection channel is configured, check whether data is collected. If logs are sent to the SecMaster pipeline, you can query the result on the SecMaster **Security Analysis** page.

Data Collection Configuration Removal Process

Figure 13-6 Data collection configuration removal process
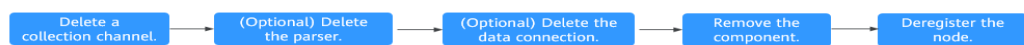
Table 13-4 Description of the data collection configuration removal process

No.	Step	Description
1	Deleting a collection channel	On the **Collection Channels** page, stop and delete the Logstash pipeline configuration. Note: All collection channels on related nodes must be stopped and deleted first.
2	(Optional) Deleting a parser	If a parser is configured, delete it on the **Parsers** tab.
3	(Optional) Deleting a data connection	If a data connection is added, delete the source and destination connectors on the **Connections** tab.
4	Removing a component	Delete the collection engine Logstash installed on the node and remove the component.

No.	Step	Description
5	Deregistering a node	Remove the component controller to complete node deregistration. Note: Deregistering a node does not delete the ECS and endpoint resources. If the data collection function is no longer used, you need to manually release the resources. For details, see **How Do I Release an ECS or VPC Endpoint?** and **Deleting a VPC Endpoint**.

13.2.2 Adding a Node

Scenario

This topic describes how to install the component controller (isap-agent) to add a node, as well as edit a node.

⚠️ **CAUTION**

The recommended installation path is **/opt/cloud**. This section also uses this path as an example. You can use other installation paths. Make sure change the path when you refer to the example here. For example, if the installation path is **/tmp**, change the installation path in this section to **/tmp**.

Preparations

- **Creating an IAM user with the minimum permission**

  IAM is used for data collection authorization. You need to create an IAM user with the minimum permission to access SecMaster APIs and disable verification rules such as MFA for the user.

  a. Log in to the management console.

  b. Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

  c. Create a user group.

     i. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **Create User Group** in the upper right corner.

     ii. On the **Create User Group** page, specify user group name and description.

        ○ **Name**: Set this parameter to **Tenant collection**.

        ○ **Description**: Enter a description.

     iii. Click **OK**.

  d. Assign permissions to the user group.

i. In the navigation pane on the left, choose **Permissions** > **Policies/ Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.

ii. Configure a policy.

○ **Policy Name**: Set this parameter to **Least permission policy for tenant collection**.

○ **Policy View**: Select **JSON**.

○ **Policy Content**: Copy the following content and paste it in the text box.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secmaster:workspace:get",
                "secmaster:node:create",
                "secmaster:node:monitor",
                "secmaster:node:taskQueueDetail" ,
                "secmaster:node:updateTaskNodeStatus"
            ]
        }
    ]
}
```

iii. Click **OK**.

e. Assign permissions to the created user group.

i. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **Tenant collection**.

ii. On the **Permissions** tab, click **Authorize**.

iii. On the **Select Policy/Role** page, search for and select the **Least permission policy for tenant collection** added in **d**, and click **Next**.

iv. Set the minimum authorization scope. Select **All resources** for **Scope**. After the setting is complete, click **OK**.

v. Verify the authorization. The policy will be listed on the page.

f. **Create a user**.

During the creation, enable **Programmatic access**, **Access key**, and **Password**.

g. Add the operation account to the user group.

i. In the navigation pane on the left, choose **User Groups**.

ii. In the **Tenant collection** user group row, click **Manage User** in the **Operation** column.

iii. In the displayed **Manage User** dialog box, select users added in **f**.

iv. Click **OK**.

● **Checking the disk space**

Check the disk space in the **/opt** directory of the ECS where you will install the component controller and make sure the space is not smaller than 100 GB.

a. Remotely log in to the ECS where you want to install the component controller.

- 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 component controller on the server as user **root**.

b. Run the **df -h** command to check whether more than 100 GB space is reserved in the **/opt** directory of the disk. At least 2 vCPUs and 4 GB of memory are required.

Figure 13-7 Checking disks

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**.

To ensure that the **/opt** directory has more than 100 GB free disk space allocated, you can use the disk partitioning script to allocate the disk. For details, see **Partitioning a Disk**.

Creating a Node

Step 1 Check operations in **Preparations** and log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-8 Workspace management page
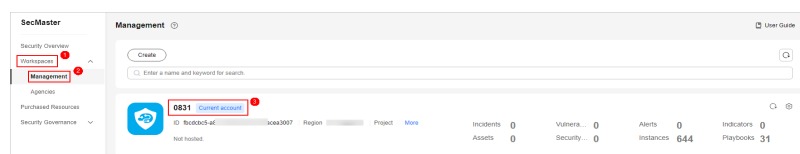
Step 5 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 13-9 Node management page
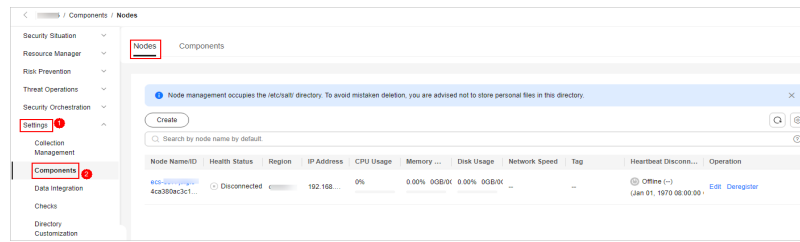
Step 6 On the **Nodes** tab, click **Create**. The **Create Node** page is displayed on the right.

Step 7 On the **Create Node** page, configure a channel.

1. In the **Network Channel Settings** area, select the VPC and subnet the target ECS belongs to.

2. In the network channel list, click **Config** in the **Operation** column of each channel. In the displayed confirmation dialog box, click **Confirm**.

📖 **NOTE**

VPC endpoints you use for log collection are billed. For details about pricing, see **Billing Overview**.

If you no longer need to collect log data, you need to manually release the VPC endpoints used. For details, see **Deleting a VPC Endpoint**.

Step 8 Click **Next** in the lower right corner of the page to go to the **Script Installation Verification** page.

Step 9 Select the ECS OS, follow the step, and click 🗗 to copy the command for installing the component controller.

Figure 13-10 Copying the installation command
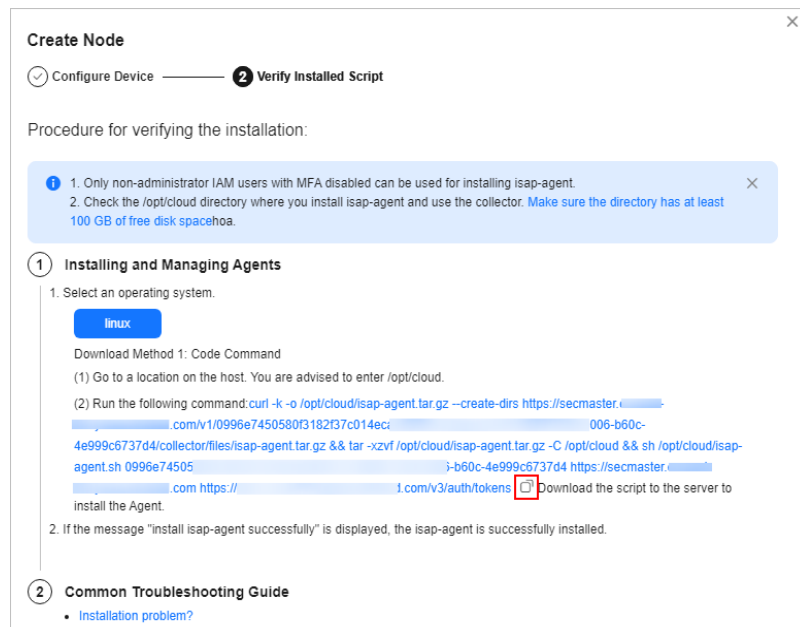
Step 10 Install the component controller.

1. Remotely log in to the ECS where you want to install the component controller.

- 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 component controller on the server as user **root**.

2. Run the command copied in **Step 9** as user **root** to install the controller on the ECS.

3. Enter the IAM username and password created in **Preparations** as prompted.

4. If **install isap-agent successfully** is displayed, the component controller is installed.

Figure 13-11 Installed

If the installation fails, rectify the fault by referring to **Troubleshooting the Component Controller Installation Failure**. If the system displays a message indicating that the memory is insufficient, rectify the fault by referring to **Partitioning a Disk**.

Step 11 After confirming that installation has been completed, return to the page for adding nodes and click **Confirm** in the lower right corner of the page.

You can view new nodes on the **Nodes** tab.

Figure 13-12 New node added
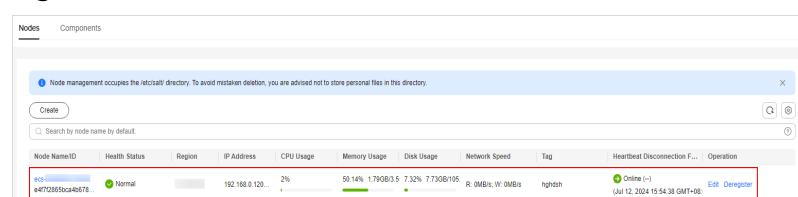
----End

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 management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-13 Workspace management page
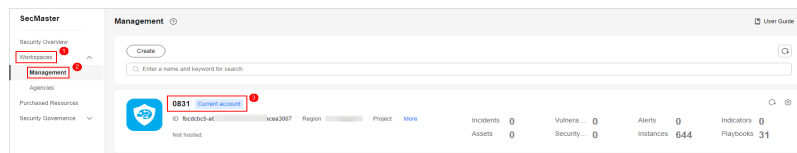
Step 5 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 13-14 Node management page

Step 6 On the **Nodes** tab, locate the row that contains the target node and click **Edit** in the **Operation** column.

Step 7 On the **Edit Node** panel, edit the node information.

Table 13-5 Parameters of node information

Parameter	Description
Data Center	User-defined data center name
Network Plane	Select the network plane of the node.
Tag	Set the tag for the node.
Description	Description of a user-defined node.
Maintained By	Select a node owner.

Step 8   Click **Confirm**.

----End

Related Operations

You can also view node information or deregister a node. For details, see **Managing Nodes and Components**.

13.2.3 Configuring a Component

Scenario

This topic describes how to configure Logstash. Logstash works as the log collection component in SecMaster.

Configuring a Component

Step 1   Log in to the management console.

Step 2   Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3   Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4   In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-15 Workspace management page
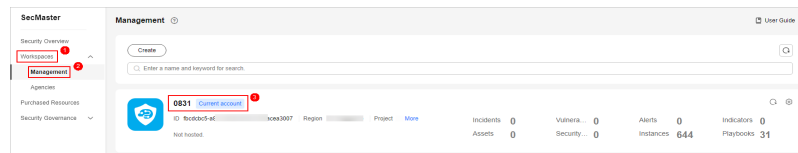
Step 5   In the navigation pane on the left, choose **Settings** > **Components**. Then, select the **Components** tab.

Figure 13-16 Accessing the Components tab
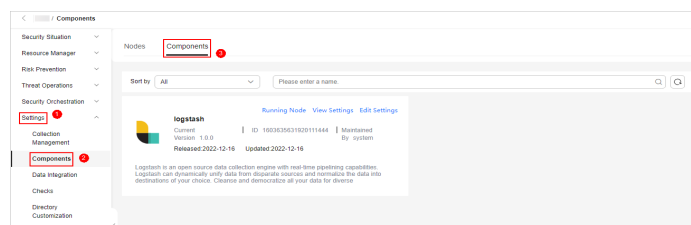
Step 6   On the **Components** tab page, click **Edit Settings** in the upper right corner of the component to be viewed. The configuration management page of the component is displayed on the right.

Step 7   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 8 Click **Save and Apply** in the lower right corner of the page.

Wait for a period of time. When the component status changes to **Applied completed**, the Logstash collector has been installed on the current node.

Figure 13-17 Configuration completed

----**End**
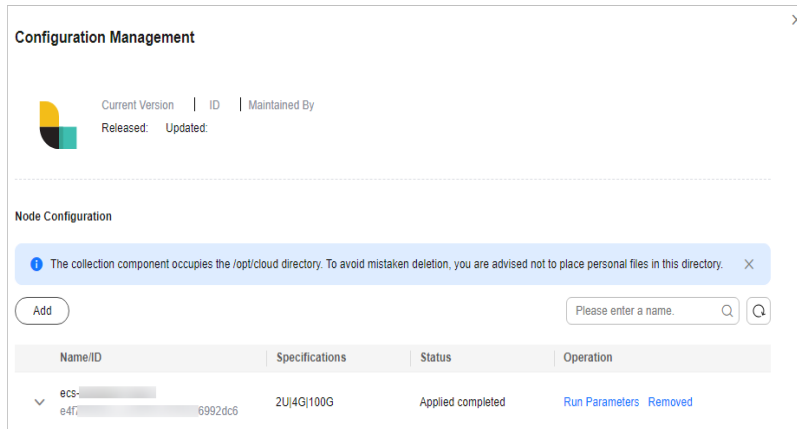
Related Operations

You can view component details. For details, see **Viewing Component Details**.

13.2.4 Adding a Connection

Scenario

This topic describes how to add and edit a connection. You can configure and edit connection sources and destinations for log transfers.

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 management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-18 Workspace management page
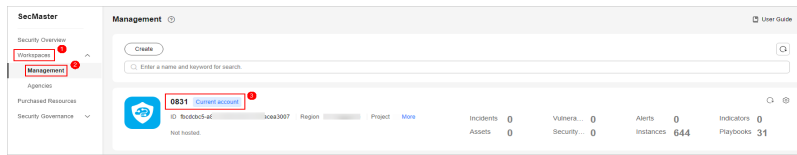
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**.

Figure 13-19 Accessing the connection management page
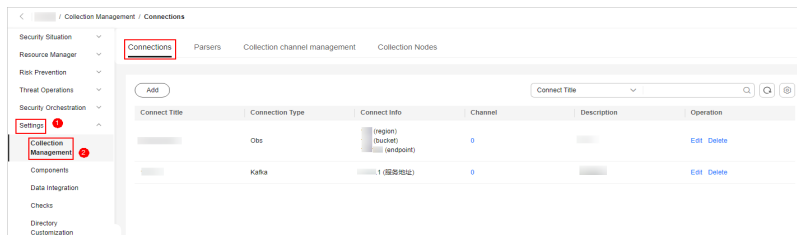
Step 6 Add a data connection source.

1. On the **Connections** tab, click **Add**.

2. Configure the data connection source details.

   – **Connection Method**: Select **Source**.

   – **Connection Type**: Select the type of the data source.

   – Set other parameters based on the selected connection type. For details about the parameters, see **Source Connectors**.

3. After the setting is complete, click **Confirm** in the lower right corner of the page.

Step 7 Add a data connection destination.

1. On the **Connections** tab, click **Add**.

2. Configure the data connection destination details.

   – **Connection Method**: Select **Destination**.

   – **Connection Type**: Select the type of the data destination.

   – Set other parameters based on the selected connection type. For details about the parameters, see **Destination Connectors**.

3. After the setting is complete, click **Confirm** in the lower right corner of the page.

----End

Editing a Data Connection

📖 **NOTE**

After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed.

For example, if you select **File** as the data source type when adding a data connection, you can modify only the parameters in the file type but cannot change the **File** type.

Step 1 Log in to the management console.

Step 2 Click 🔲 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-20 Workspace management page
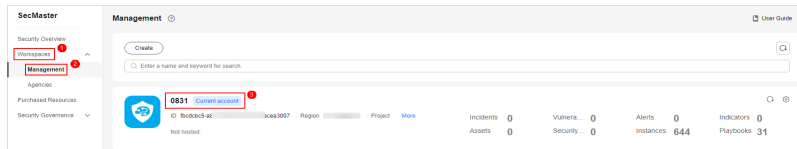
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**.

Figure 13-21 Accessing the connection management page
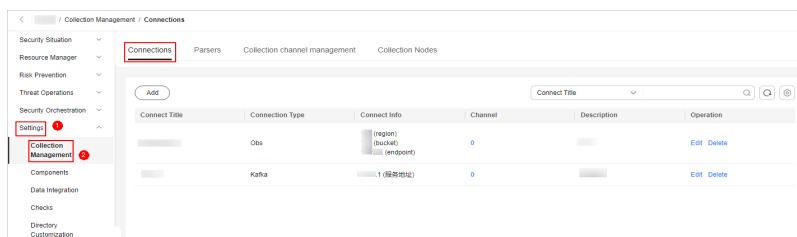
Step 6 On the **Connections** page, locate the row that contains the target connection and click **Edit** in the **Operation** column.

Step 7 On the displayed page, edit the data source type.

Step 8 Check the settings and click **Confirm** in the lower right corner of the page.

----End

Related Operations

You can view connection details and delete a connection. For details, see **Managing Connections**.

13.2.5 Creating and Editing a Parser

Scenario

SecMaster provides some preconfigured parsers for quick use. You can use the parsers you need.

Table 13-6 Parser scenario description

Type	Scenario
Quick access	The source data can be directly transmitted without being processed.
Template	When you need to clear data sources or process fields, you can select a template based on the application scenario and create a parser.
Custom	You can create custom parsers and configure parsing rules to meet your needs, such as clearing data sources, processing fields, and more.

This topic describes how to add and edit a log parser. With a log parser, you can convert the log format in a codeless manner. In SecMaster, you can configure log parsers in two ways:

- Using a template: SecMaster provides some log parser (rule) templates. You can use them to configure parsers quickly.

- Creating custom parsers: If the log parser (rule) templates SecMaster provides for you cannot meet your log conversion requirements, you can create custom log parsers (rules).

Creating a Parser

**Step 1** Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
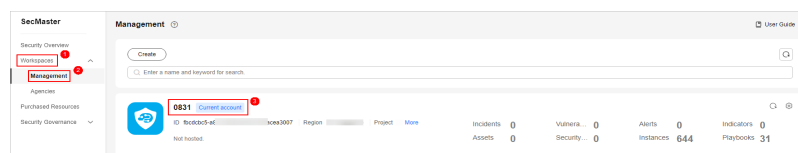
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 13-23 Accessing the Parsers tab
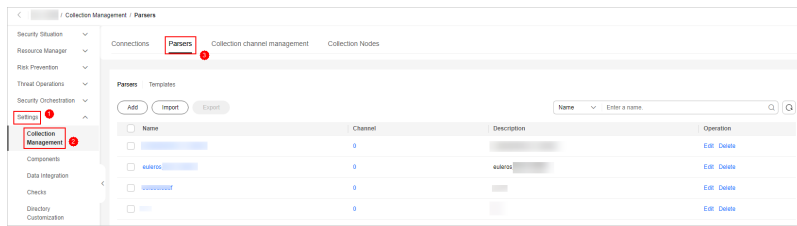
Step 6 **Customize a parser** or **create a parser from a template**.

- **Customizing a parser**

  a. On the **Parsers** tab page, click **Add**.

  b. On the **Parsers** tab page, set parameters.

Table 13-7 Parameters for adding a parser

Parameter		Description
Basic Information	Parser Name	Set the parser name.
	Description	Enter the parser description.

Rules		Set the parsing rule of the parser. Perform the following steps:
		
		1. Click **Add** and select a rule type.
		
		  ○ **Parsing rule**: Select the parsing rule of the parser. For details about the parameters, see **Parser 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** page, click the **Templates** tab.

  b. On the displayed page, locate the row that contains the target template, click **Created by Template** in the **Operation** column.

  c. On the **Parsers** tab page, set parameters.

Table 13-8 Parameters for adding a parser

Parameter		Description
Basic Information	Parser Name	Parser name, which is automatically generated by the system based on the template and can be changed.
	Description	Parser description, which is automatically generated by the system based on the template and can be modified.
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 rule**: Select the parsing rule of the parser. For details about the parameters, see **Parser Rules**.
		▪ **Conditional control**: Select the conditions for the parser. You can select **If**, **Else**, or **Else if**.

d. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

Editing a Parser

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-24 Workspace management page
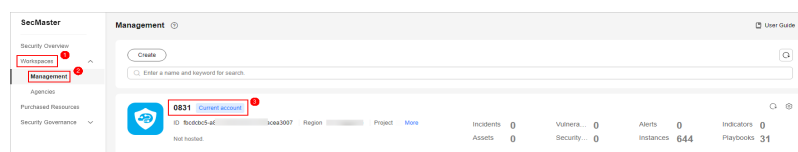
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 13-25 Accessing the Parsers tab

Step 6 On the **Parsers** tab, locate the row containing your desired parser and click **Edit** in the **Operation** column.

Step 7 In the **Edit Parser** dialog box, edit the parser information.

Table 13-9 Editing a parser

Parameter		Description
Basic Information	Parser Name	Set the parser name.
	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 rule**: Select the parsing rule of the parser. For details about the parameters, see **Parser Rules**.
		• **Conditional control**: Select the conditional control principle of the parser.

Step 8 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

Related Operations

You can view parsers, as well as import, export, and delete a parser. For details, see **Managing Parsers**.

13.2.6 Adding and Editing a Collection Channel

Scenario

This topic describes how to add and edit a log collection channel to connect functional components and let SecMaster and the log collector work properly.

Adding a Channel Group

Before adding a collection channel, you need to add a connection group.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-26 Workspace management page
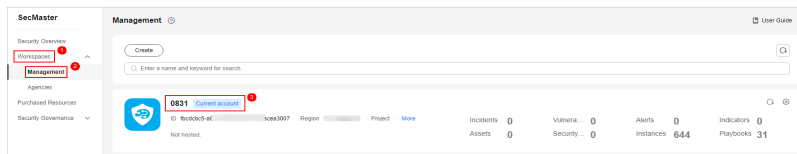
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 13-27 Collection channel management tab page
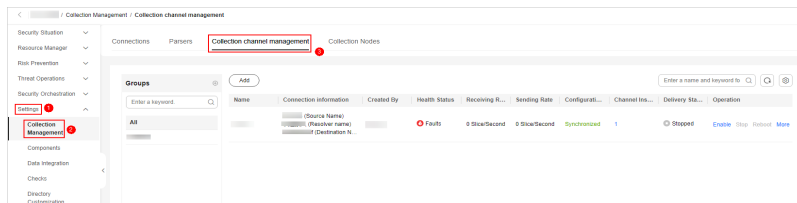
Step 6 Add a channel group.

1. On the **Collection Channels** tab, click on the right of **Groups**.

2. Enter a group name and click .

To edit or delete a group, hover the cursor over the group name and click the edit or deletion icon.

----End

Adding a Collection Channel

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-28 Workspace management page

Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 13-29 Collection channel management tab page
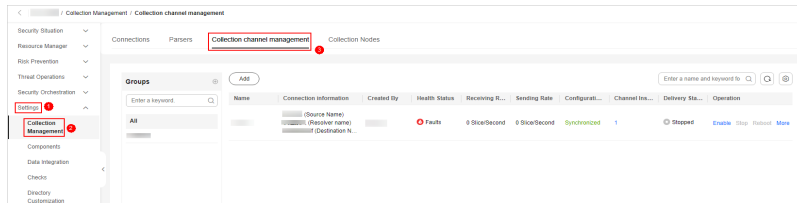
Step 6 On the right of the group list, click **Add**.

Step 7 On the displayed page, in the **Basic Configuration** phase, configure basic information.

Table 13-10 Basic configuration parameters

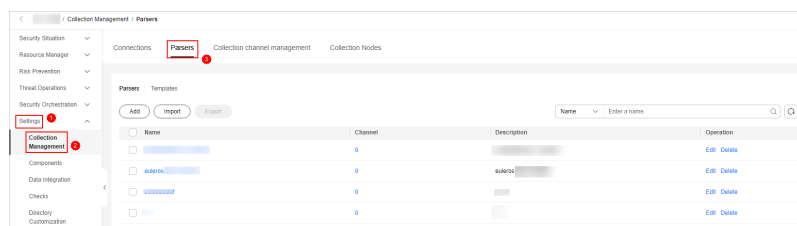| Parameter		Description
Basic Information	Title	User-defined collection channel name.
	Channel grouping	Select the group to which the collection channel belongs.
	(Optional) Description	(Optional) Enter the description of the collection channel.
Configure Source	Source Name	Select the source name of the collection channel. After you select a source, the system automatically generates the information about the selected source.
Destination	Destination Name	Select the destination name of the collection channel. After you select a destination, the system automatically generates the information about the selected destination.

Step 8 After the basic configuration is complete, click **Next** in the lower right corner of the page.

Step 9 On the **Configure Parser** page, select a parser. You can check its details.

If no parser is available or you want to create a parser, click **Create** and create one. For details, see **Creating and Editing a Parser**.

Step 10 After the parser is configured, click **Next** in the lower right corner of the page.

Step 11 On the **Select Node** page, click **Create**. In the **Add Node** dialog box displayed, select a node and click **OK**.

- Running parameters: You can configure running parameters for added nodes by taking the following steps:

  a. In the node list, locate the row that contains the target node, and click **Running parameters** in the **Operation** column.

  b. Click **Add Configuration** and select a key and value.

    If you need to optimize the running parameters of a collection channel, SecMaster provides optimization parameters **pipeline.batch.size**, **pipeline.workers**, and **pipeline.batch.delay** for your choice. If no optimizations are required, delete related configurations.

    Table 13-11 Parameter configuration description

Parameter	Type	Description
pipeline.batch.size	int	This parameter specifies the number of events that can be collected by each worker thread each time. A larger value indicates a higher efficiency. However, the memory overhead also increases. You can increase the heap space in **jvm.options**.
pipeline.workers	int	This parameter specifies the number of worker threads in the pipeline. The default value is the number of CPU cores.
pipeline.batch.delay	int	This parameter specifies the delay to submit the current pipeline. You can use this parameter to increase message submission times and system consumption efficiency.

- To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.

Step 12 After the running node is selected, click **Next** in the lower right corner of the page.

Step 13 On the **Preview Channel Details** page, confirm the configuration and click **Save and Execute**.

If the collection channel healthy status is **Normal**, all collection channels are successfully delivered. The following table describes the statuses of collection channels.

Table 13-12 Health status of a collection channel

Monitoring Status	Description
Healthy	The collection channel is successfully delivered.
Abnormal	Some collection channels are successfully delivered, and some are abnormal.
Faulty	The collection channel has not been delivered. This status changes according to the heartbeat status, and there is a delay. Generally, the monitoring status is reported every 30 seconds.

----End

Editing a collection channel

Step 1 Log in to the management console.

Step 2 Click ⬤ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.
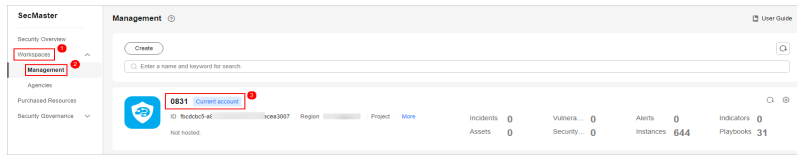
Figure 13-30 Workspace management page
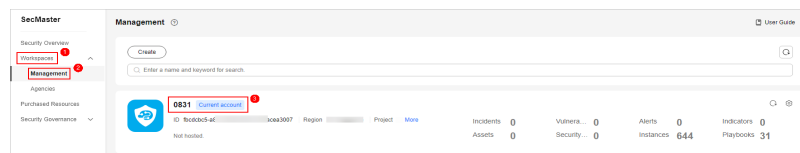
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 13-31 Collection channel management tab page
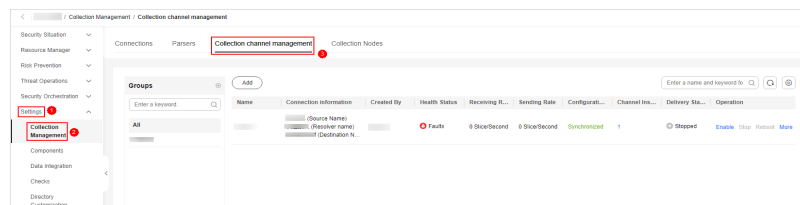
Step 6 In the collection channel list, locate the row that contains the target channel, click **More** > **Edit** in the **Operation** column. The **Edit Collection Channel** page is displayed.

Step 7 On the displayed page, in the **Basic Configuration** phase, configure basic information.

Table 13-13 Basic configuration parameters

Parameter		Description
Basic Information	Channel Name	User-defined collection channel name.
	Channel grouping	Select the group to which the collection channel belongs.
	(Optional) Description	(Optional) Enter the description of the collection channel.
Source Configuration	Source Name	Select the source name of the collection channel. After you select a source, the system automatically generates the information about the selected source.
	Destination Name	Select the destination name of the collection channel. After you select a destination, the system automatically generates the information about the selected destination.

Step 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 **Creating and Editing a Parser**.

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 select a key and value.

- To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.

Step 12 After the running node is selected, click **Next** in the lower right corner of the page.

Step 13 On the **Preview Channel Details** page, confirm the configuration and click **Save and Execute**.

----End

Related Operations

For details about how to view, delete, enable, disable, and restart a collection channel, see **Managing Collection Channels**.

13.2.7 Managing Connections

Scenarios

This section describes how to perform the following operations: **Deleting a Data Connection** and **Deleting a Data Connection**.

Viewing Connections

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-32 Workspace management page
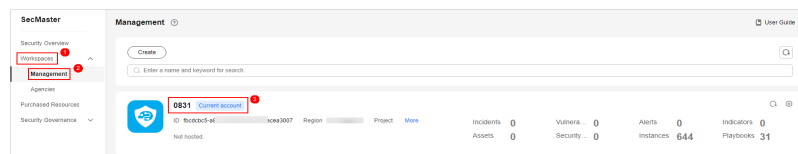
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**.

Figure 13-33 Accessing the connection management page
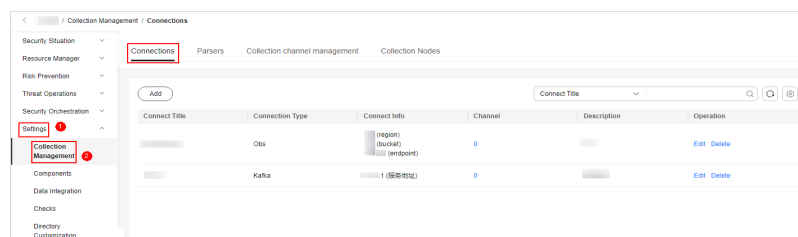
Step 6 On the **Connections** tab, view connection details.

Table 13-14 Connection parameters

Parameter	Description
Connection Name	Connection name
Connection Type	Connection type

Parameter	Description
Connection Info	Information about the connection
Channel	Number of channels that are used by the connection
Description	Description of the connection
Operation	Operations such as editing or deleting connections

----End

Deleting a Data Connection

Step 1 Log in to the management console.

Step 2 Click [icon] in the upper left corner of the management console and select a region or project.

Step 3 Click [icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-34 Workspace management page

Step 5 In the navigation pane on the left, choose **Settings** > **Collections**.

Figure 13-35 Accessing the connection management page

Step 6 On the Connections page, locate the row that contains the target connection and click **Delete** in the **Operation** column.

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

----End

13.2.8 Managing Parsers

Scenarios

This topic describes how to perform the following operations: **Viewing Parsers**, **Importing a Parser**, **Exporting a Parser**, and **Deleting a Parser**.

Viewing Parsers

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-36 Workspace management page
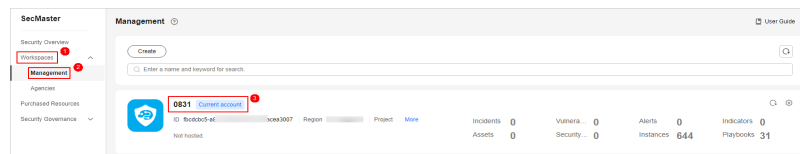
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 13-37 Accessing the Parsers tab

Step 6 On the **Parsers** page, view the detailed information about parsers.

Table 13-15 Parsers parameters

Parameter	Description
Name	Name of the parser.
Channel	Number of channels that are used by the parser
Description	Description of the parser.
Operation	Operations such as editing or deleting the parser

Step 7 On the **Parsers** page, click the **Templates** tab.

Step 8 On the **Templates** tab displayed, view the parser templates you can use.

Table 13-16 Parser template parameters

Parameter	Description
Name	Name of a parser template
Description	Description of the parser template
Operation	Creating a parser from a template.

----End

Importing a Parser

📖 NOTE

- Only .json files no larger than 1 MB can be imported.
- A maximum of five parser files can be imported at a time, and each parser file can contain a maximum of 100 parsers.

Step 1 Log in to the management console.

Step 2 Click 🌐 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-38 Workspace management page
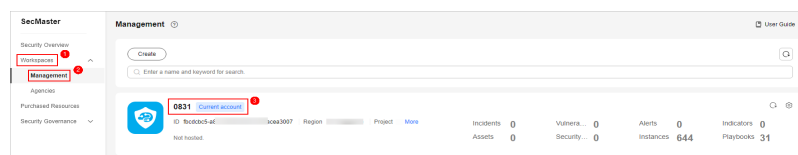
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 13-39 Accessing the Parsers tab
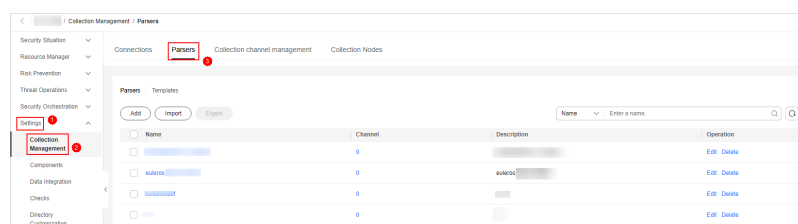
Step 6 On the **Parsers** tab, click **Import** in the upper left corner above the parser list.

Step 7 In the displayed **Import** dialog box, click **Select File** and select the JSON file you want to import.

> ⚠️ **CAUTION**
>
> - Only .json files no larger than 1 MB can be imported.
> - A maximum of five parser files can be imported at a time, and each parser file can contain a maximum of 100 parsers.

Step 8 Click **OK**.

You can view imported parsers in the parser list.

**----End**

Exporting a Parser

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-40 Workspace management page

Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 13-41 Accessing the Parsers tab

Step 6 On the **Parsers** page, select the parsers you want to export and click **Export** above the list.

The system automatically downloads the parser file in .json format to your local PC.
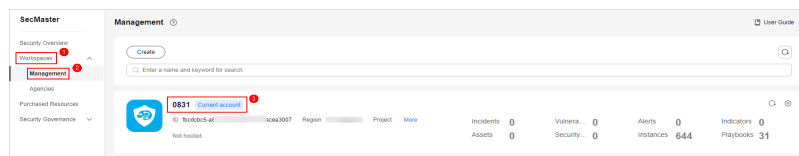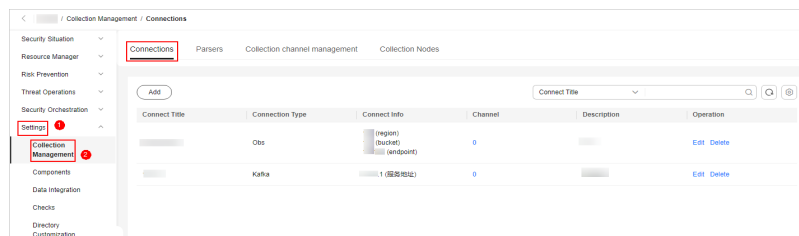
----End

Deleting a Parser

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 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
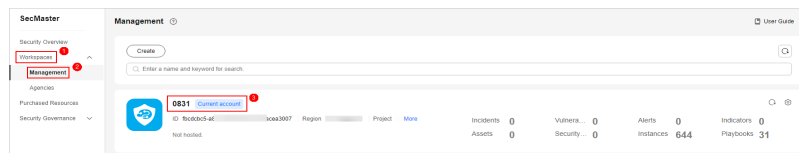
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Parsers** tab.

Figure 13-43 Accessing the Parsers tab

Step 6 On the **Parsers** tab, locate the row that contains the target parser and click **Delete** in the **Operation** column.

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

----End

13.2.9 Managing Collection Channels

Scenarios

This topic describes how to perform the following operations: **Viewing Collection Channels**, **Deleting a Collection Channel**, and **Enabling, Disabling, and Restarting a Collection Channel**.

Viewing Collection Channels

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-44 Workspace management page
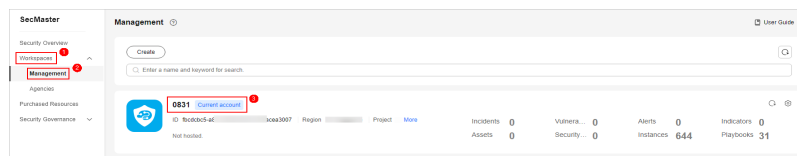
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 13-45 Collection channel management tab page
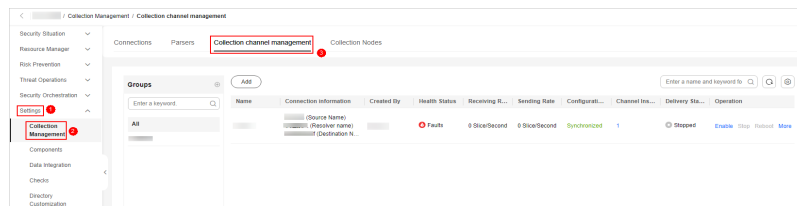
Step 6 On the **Collection Channels** page, view the detailed information about collection channels.

Table 13-17 Collection channel parameters

Parameter	Description
Groups	List of collection channel groups and group names.
Name	Name of the collection channel.
Connection information	Collect channel connection information.
Created By	Creator of the collection channel.
Health Status	Health status of the collection channel.
Receiving Rate	Data receiving rate of the collection channel.
Sending Rate	Data sending rate of the collection channel.
Configuration Status	Configuration status of the collection channel.

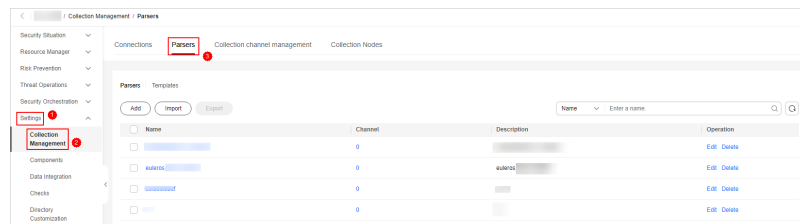| Parameter	Description
Channel Instance	Number of collection channels.
Delivery Status	Status of a collection channel.
Operation	Operations such as editing and disabling a collection channel.

----End

Deleting a Collection Channel

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-46 Workspace management page

Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 13-47 Collection channel management tab page

Step 6 In the collection channel list, locate the row that contains the target channel, click **More** > **Delete** in the **Operation** column.

☐ NOTE

You can delete a collection channel only when it is stopped.

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

----End

## Enabling, Disabling, and Restarting a Collection Channel

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-48 Workspace management page
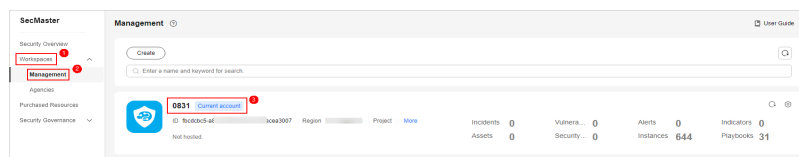
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Channels** tab.

Figure 13-49 Collection channel management tab page
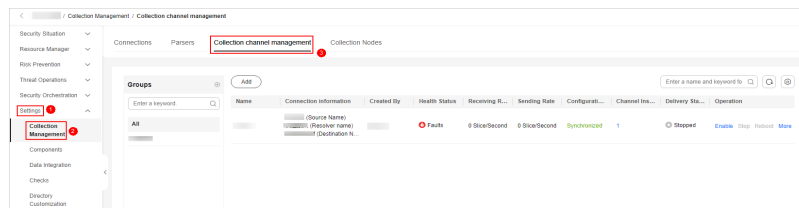
Step 6 In the collection stream management list, locate the row that contains the target stream and click **Enable**, **Stop**, or **Restart** in the **Operation** column.

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

----End

13.2.10 Viewing Collection Nodes

Scenario

This topic describes how to view collection nodes details.
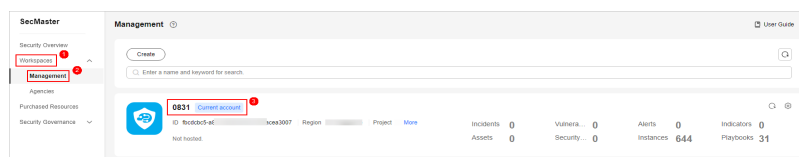
Viewing Collection Nodes

Step 1 Log in to the management console.

Step 2 Click ▣ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
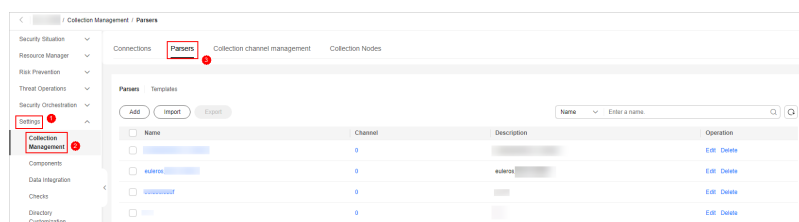
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-50 Workspace management page
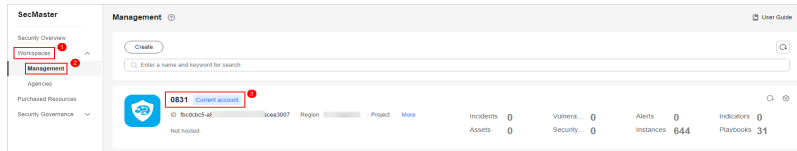
Step 5 In the navigation pane on the left, choose **Settings** > **Collections**. Then, select the **Collection Nodes** tab.

Figure 13-51 Accessing the Collection Nodes page
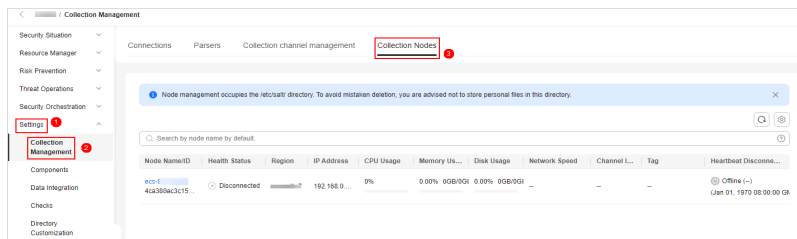
Step 6 On the **Collection Nodes** page, view the detailed information about collection nodes.

If there are many nodes displayed, use filters to search for a specific one.

To view details about a node, click its name to go to its details page.

Table 13-18 Collection node parameters

Parameter	Description
Node Name/ID	Name or ID of a node
Health Status	Node health status
Region	Region where the node is located
IP Address	Node IP address
CPU Usage	CPU usage of the node
Memory Usage	Memory usage of the node
Disk Usage	Node disk usage
Network Speed	Network rate of a node
Label	Label information of a node
Heartbeat Expiration Mark	Indicates whether the node is disconnected due to heartbeat expiration. If no heartbeat message is sent within 15 minutes, the node is marked as **Disconnected**.

----End

13.2.11 Managing Nodes and Components

Scenarios

This topic describes **Viewing Node Details**, **Deregistering a Node**, and **Viewing Component Details**.
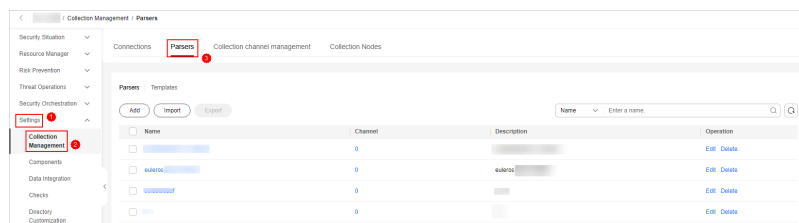
Viewing Node Details

Step 1 Log in to the management console.

Step 2 Click ⬛ in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-52 Workspace management page
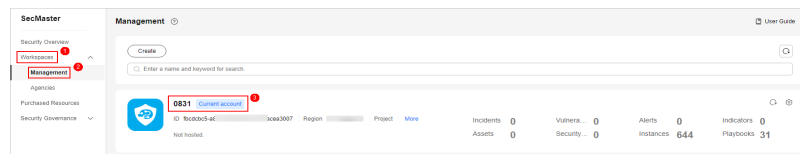
Step 5 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 13-53 Node management page
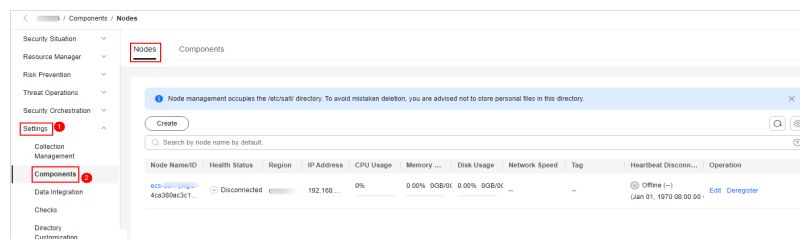
Step 6 On the **Nodes** tab, view the details about nodes.

If there are many nodes displayed, use filters to search for a specific one.

Table 13-19 Collection node 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. If no heartbeat message is sent within 15 minutes, the node is marked as **Disconnected**.

Step 7 To view details about a node, click the node name.

----End

Deregistering a Node

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-54 Workspace management page
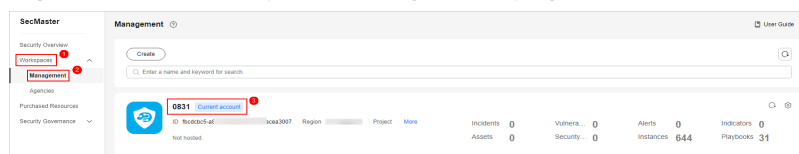
Step 5 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 13-55 Node management page
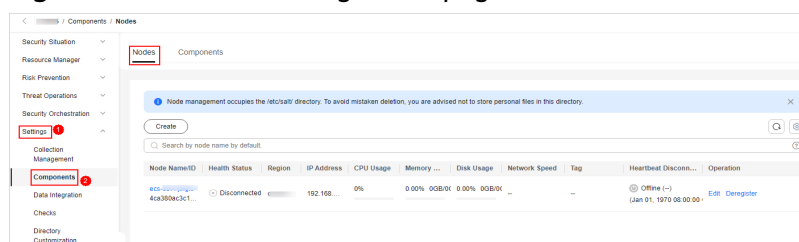
Step 6 On the **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.

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

📖 NOTE

Only the node is deregistered. The ECS and endpoint interface resources are not deleted. If you no longer need the data collection function, you need to manually release those resources. For details, see **Deleting ECSs** and **Deleting a VPC Endpoint**.
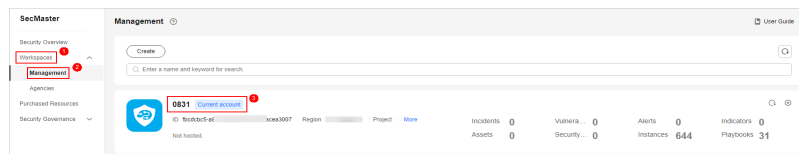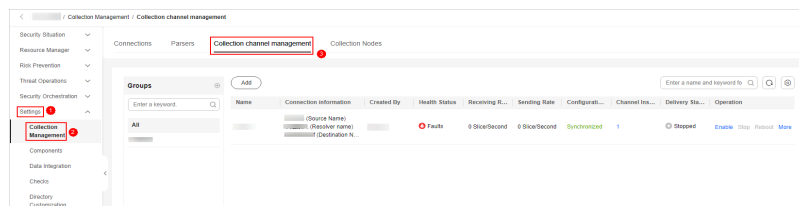
----End

Viewing Component Details

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-56 Workspace management page
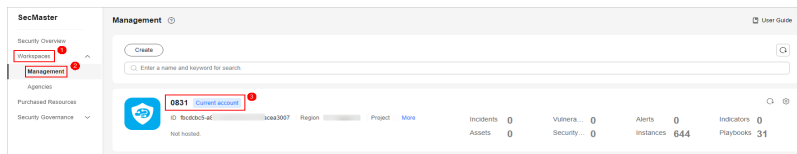
Step 5 In the navigation pane on the left, choose **Settings** > **Components**. Then, select the **Components** tab.

Figure 13-57 Accessing the Components tab
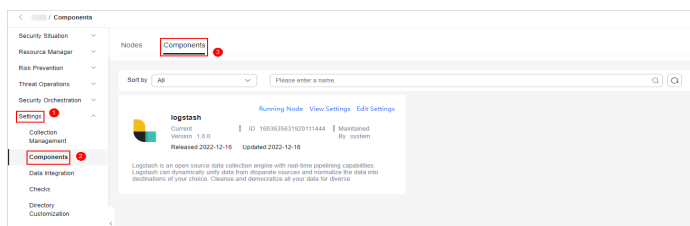
Step 6 On the **Components** page, view the component details.

● **Running Node**

Click **Running Node** in the upper right corner of a component. The running node information of the component is displayed on the right.

● **View Settings**

Click **View Settings** in the upper right corner of the component to be viewed. The configuration details about the component are displayed on the right.

● **Edit Settings**

   a. Click **Edit Settings** in the upper right corner of the component to be viewed. The **Configuration Management** panel of the component is displayed on the right.

   b. In the **Node Configuration** area, edit the node configuration information.

   ▪ Adding a node: Click **Add** in the upper left corner of the node list. In the **Add Node** dialog box displayed, select a node and click **OK**.

   ▪ Editing node parameters: Click ⌄ next to the node name to expand the node configuration information and edit the node parameters.

   ▪ Running parameters: Locate the row that contains the target node, click **Run Parameter** in the **Operation** column.

   ▪ Removing a node: Locate the row that contains the target node and click **Removed** in the **Operation** column.

   ▪ Batch deletion: Select the nodes you want to remove and click **Batch Remove** in the upper left corner of the list.

   ▪ Viewing historical versions: Click **Historical Version** in the lower right corner of the panel.

   c. Click **Save and Apply** in the lower right corner of the page.

   ----End

13.2.12 Partitioning a Disk

To keep collectors healthy for you to collect security data, there are some limitations and constraints.

● Only non-administrator IAM users can be used for installing isap-agent.

● Make sure the **/opt/cloud** directory where you install isap-agent and use the collector has at least 100 GB of free disk space.

When you install the isap-agent in the **/opt** directory on an ECS, if the message shown in **Figure 13-58** is displayed, the space of the **/opt** directory is insufficient.

Figure 13-58 Insufficient disk space error

To ensure at least 100 GB space is available in the directory where the component controller isap-agent is installed, you may need to partition the disk.

The procedure is as follows:

Step 1 Buy and attach a disk.

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the region and project.

3. In the upper left corner of the page, click ☰ and choose **Compute** > **Elastic Cloud Server**. In the ECS list, click the name of the ECS where isap-agent is installed to go to the ECS details page.

4. Click the **Disks** tab. On the displayed page, click **Add Disk**.

5. On the displayed page, buy a disk with **Disk Specifications** set to **100 GiB**.

   For details, see **Purchasing an EVS Disk**.

6. After the disk is successfully attached, you can view the attached disk on the **Disks** tab for the ECS.

Figure 13-59 Disks attached
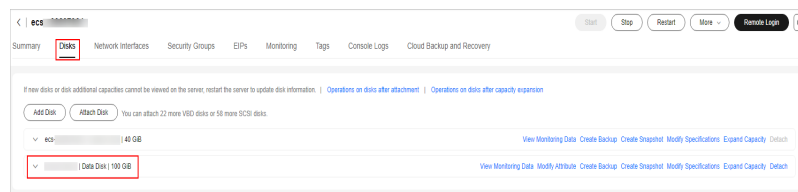
After a data disk is attached to a server, you must log in to the server and initialize the disk before you can use the disk. For details about how to initialize a data disk, see **Initializing an EVS Data Disk**.

Step 2 Partition the disk.

1. Log in to the node where isap-agent is installed and run the following command to check the disk usage:

   lsblk

   Figure 13-60 Checking the disk size on a node
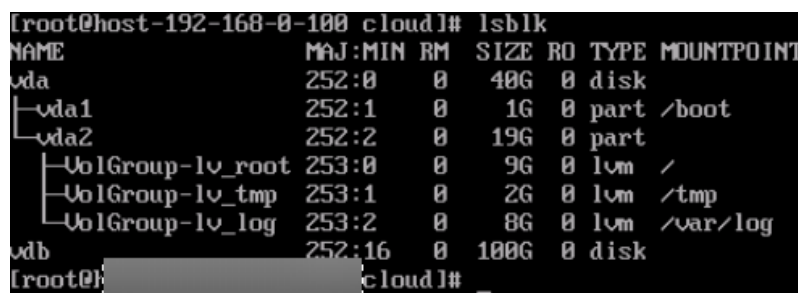
2. Run the following command to partition the disk:

   sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition

   If the following information is displayed, the disk is partitioned successfully.

Figure 13-61 Disk partitions

Step 3 Reinstall the component controller isap-agent. For details, see **Managing Nodes**.

----End

13.2.13 Logstash Configuration Description

The data collector Logstash for tenant-side collection is customized by SecMaster. In different transmission scenarios, you can adjust parameter settings to obtain an optimal performance. This topic mainly covers how to tune log4j2.properties and jvm.options.

JVM Running Memory Configuration

Figure 13-62 jvm.options
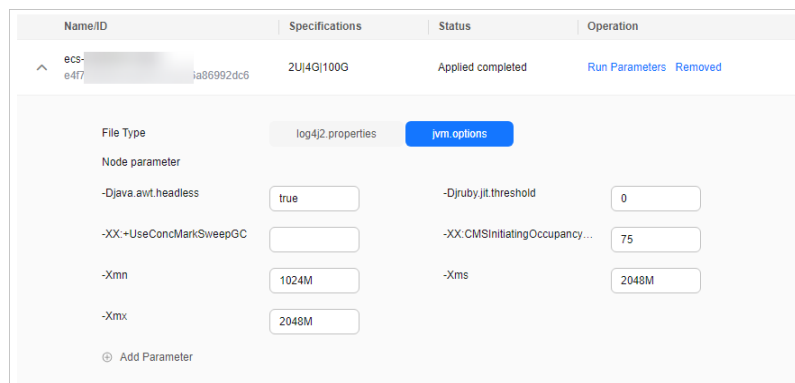
Table 13-20 JVM running memory configuration

Parameter	Configur ation Type	Default Value	Description
-Djava.awt.headles s	boolean	true	Server side configuration. If it is set to "true", you can run an application in headless mode (without a keyboard or display). This parameter is used for data related services.
-XX:+UseConcMark SweepGC	boolean	false	Concurrent Mark Sweep (CMS) garbage collector for the old generation.

Parameter	Configuration Type	Default Value	Description
-Xmn	String	1024M	The size of the heap for the young generation. If the collection pressure is high, adjust this value. The larger the heap size for the young generation, the smaller the number of garbage collection times, and the higher the collection efficiency. **Xmn** must be smaller than **Xmx**.
-Xmx	String	2048M	The total (maximum) heap size. A proper **Xmx** can prevent JVM from using excessive system resources to keep the application available and stable. If this parameter is set to a very small value, the collector will start garbage collection over and over again. This will affect collector performance.
-Djruby.jit.threshold	number	0	The specified method invocation count. When this threshold is reached, the JIT compiler of JRuby attempts to compile the local code of the method. You can adjust this value to obtain an optimal balance between startup time (compilation cost) and execution time performance
-XX:CMSInitiatingOccupancyFraction	number	75	CMS garbage collector. When the old generation usage reaches 75%, CMS garbage collection is triggered.
-Xms	String	20248M	The initial Java heap size. When JVM starts, it attempts to allocate the specified amount of memory to the heap. A proper initial heap size will free you from frequent heap size adjustments while the application is running.

log4j2 log configuration

Figure 13-63 log4j2.properties
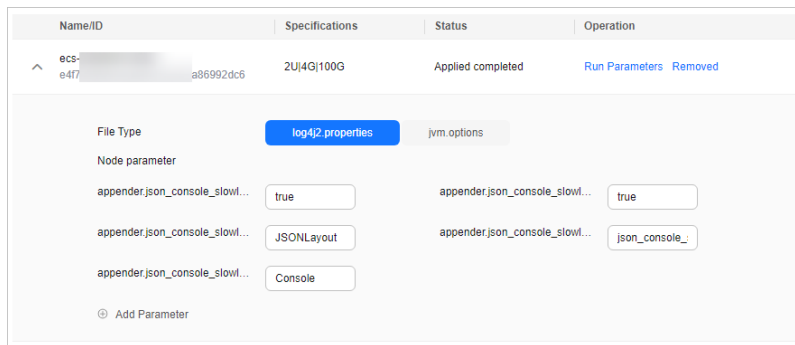
Table 13-21 log4j2 log configuration

Parameter	Configuration Type	Default Value	Description
appender.json_console_slowlog.layout.compact	boolean	true	JSON slow query log output.
appender.json_console_slowlog.layout.type	String	JSONLayout	Layout type of JSON slow query logs. Retain the default value.
appender.json_console_slowlog.type	String	Console	Type of JSON slow query logs. Default value: **Console**, which means that logs are directly displayed on the console.
appender.json_console_slowlog.layout.eventEol	boolean	true	JSON slow query log output.
appender.json_console_slowlog.name	String	json_console_slowlog	Name of the JSON slow query log. Retain the default value.

13.2.14 Connector Rules

Source Connectors

SecMaster provides a wide range of source connectors for you to collect security data from your security products.

Table 13-22 Source connector types

Connector Type	In-use Logstash	Description
TCP	tcp	This collector is used to receive TCP logs. For details about the configuration rules, see **Table 13-23**.
UDP	udp	This collector is used to receive UDP logs. For details about the configuration rules, see **Table 13-24**.
OBS	obs	This collector is used to obtain log data from an OBS bucket. For details about the configuration rules, see **Table 13-25**.
Kafka	kafka	This collector is used to obtain Kafka network log data. For details about the configuration rules, see **Table 13-26**.
SecMaster	pipe	This collector is used to transfer SecMaster data to you. For details about the configuration rules, see **Table 13-27**.
Elasticsearch	elasticsearch	This collector is used to read data from the Elasticsearch cluster. For details about the configuration rules, see **Table 13-28**.

Table 13-23 TCP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Port	port	number	1025	Yes	Port number of the collection node.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Codec	codec	string	plain	Yes	Encoding format ● **Plain**: Reads the original content. ● **Json**: Processes the content in JSON format.
Packet label	type	string	tcp	Yes	Used to label logs.
SSL_enable	ssl_enable	boolean	false	No	Whether to enable SSL verification.
SSL certificate	ssl_cert	file	null	No	Certificate.
SSL key	ssl_key	file	--	No	SSL key file.
SSL key	ssl_key_passphrase	string	--	No	SSL certificate key.

Table 13-24 UDP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Port	port	number	1025	Yes	Port number of the collection node.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Codec	codec	string	plain	Yes	Decoding type • **Plain**: Reads the original content. • **Json**: Processes the content in JSON format.
Packet label	type	string	udp	No	Packet label, which is used for subsequent processing.
Queue size	queue_size	number	20000	No	Queue size.
Number of bytes in the receiving buffer	receive_buffer _bytes	number	20000	No	Number of bytes in the receiving buffer
Buffer size	buffer_size	number	10000	No	Buffer size
Worker thread	workers	number	1	No	Number of worker threads

Table 13-25 OBS connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
region	region	string	--	Yes	region
Bucket	bucket	string	demo-obs-sec-mrd-datas	Yes	OBS bucket name
endpoint	endpoint	string	https://obs.huawei.com	Yes	Endpoint address. Note that https must be added.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
AK	ak	string	--	No	AK
SK	sk	string	--	No	SK
Prefix	prefix	string	/test	No	Prefix of the folder for log reads
Cache folder	temporary_directory	string	/temp	No	Cache folder for log reads
Packet label	type	string	--	No	Packet label
Memory path	sincedb_path	string	/opt/cloud/ logstash/ pipeline/ file_name	No	Log read position. This parameter is used to prevent full-text traversal caused by restart.

Table 13-26 Kafka connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Service address	bootstrap_servers	string	--	Yes	Service address
Topics	topics	array	logstash	Yes	Topics. Multiple topics can be consumed at the same time.
Consumer threads	consumer_threads	number	1	Yes	Consumer threads

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Auto offset reset	auto_offset_reset	string	latest	No	Offset reset ● **Earliest**: Read the earliest message. ● **Latest**: Read the latest messages.
SSL certificate	ssl_truststore_location	file	--	No	SSL certificate This parameter is mandatory when SSL is selected.
SSL key	ssl_truststore_password	string	--	No	SSL key This parameter is mandatory when SSL is selected.
Security protocol	security_protocol	string	SASL_SSL	No	Security protocol
SASL connection configuration	sasl_jaas_config	string	--	No	SASL connection configuration
Encrypted	is_pw_encrypted	string	false	No	Encrypted
SASL mechanism	sasl_mechanism	string	PLAIN	No	sasl_mechanism
Group ID	group_id	string	--	No	group_id

Set **sasl_jaas_config** based on the Kafka specifications. Example:

● Plaintext connection configuration
  org.apache.kafka.common.security.plain.PlainLoginModule required username='*kafka user*'password='*kafka password*';

● Ciphertext connection configuration
  org.apache.kafka.common.security.scram.ScramLoginModule required username='*kafka user name*'password='*kafka password*';

Table 13-27 Pipe connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Type	type	string	Tenant	Yes	Type
Pipeline	pipeId	string	--	Yes	Pipeline ID
domain_name	domain_name	string	domain_name	Yes	Domain name of the IAM user
User_name	user_name	string	user_name	Yes	Username of the IAM user
Password	user_password	string	--	Yes	Username of the IAM user
Subscription type	subscription_type	string	true	No	Subscription type • **Shared**: shared mode • **Exclusive**: exclusive mode • **Failover**: disaster recovery mode
Subscription Start	subscription_initial_position	string	true	No	Subscription Start

Table 13-28 Elasticsearch connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Hosts	hosts	array	--	Yes	Host IP address
Index	index	string	--	Yes	Index
Retrieval statement	query	string	--	Yes	Retrieval statement
User_name	user	string	--	Yes	User_name
Password	user_password	string	--	Yes	Password

Rule	Logstash Settings	Type	Default Value	Man dator y	Description
Queries	size	number	20	Yes	Queries
Scroll	scroll	string	5m	Yes	Volume
Docinfo	docinfo	boolean	true	Yes	Document
Is pw encrypted	is_pw_encrypt ed	boolean	true	Yes	Whether to enable encryption
Whether to enable SSL	ssl	boolean	true	No	Whether to enable SSL
Ssl	ca_file	file	--	No	Certificate file
SsL_certificate _verification	ssl_certificate_ verification	boolean	true	No	SSL certificate verification

Destination Connectors

SecMaster provides a wide range of destination connectors for you to collect security data from your security products.

Table 13-29 Destination connectors

Connector Type	In-use Logstash	Description
TCP	tcp	This collector is used to send TCP logs. For details about the configuration rules, see **Table 13-30**.
UDP	udp	This collector is used to send UD logs. For details about the configuration rules, see **Table 13-31**.
Kafka	kafka	This collector is used to write logs to Kafka message queues. For details about the configuration rules, see **Table 13-32**.
OBS	obs	This collector is used to write logs to OBS buckets. For details about the configuration rules, see **Table 13-33**.
SecMaster pipeline	pipe	This collector is used to write logs to the SecMaster pipeline. For details about the configuration rules, see **Table 13-34**.

Table 13-30 TCP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Port	port	number	1025	Yes	Port
Codec	codec	string	plain	Yes	Decoding type, which can be **Json_lines** or **Plain**. ● **Plain**: Reads the original content. ● **Json_lines**: Processes the content in JSON format.
Hosts	host	string	192.168.0.66	Yes	Host address Note: The network between the host and the node is normal.
SSL certificate	ssl_cert	file	--	No	SSL certificates
Whether to enable SSL	ssl_enable	boolean	false	No	Whether to enable SSL authentication
SSL key	ssl_key	file	--	No	SSL certificate file
SSL key	ssl_key_passphrase	string	--	No	SSL certificate key

Table 13-31 UDP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Hosts	host	string	--	Yes	Host IP address. Note: The network between the host and the node is normal.
Port	port	number	1025	Yes	Port
Decoding type	codec	string	json_lines	Yes	Decoding type, which can be **Json_lines** or **Plain**. ● **Plain**: Reads the original content. ● **Json_lines**: Processes the content in JSON format.
Retry count	retry_count	number	3	No	Time of retry attempts
Retry backoff (ms)	retry_backoff_ms	number	200	No	Retry backoff (ms)

Table 13-32 Kafka connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Service address	bootstrap_servers	string	--	Yes	Service address, for example, 192.168.21.21:9092,192.168.21.24:9999.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Topics	topic_id	string	logstash	Yes	Topics
Decoding type	codec	string	plain	Yes	Decoding type, which can be **Json** or **Plain**.
Maximum length of the request	max_request_size	number	10485760	Yes	Maximum length of the request
SSL certificate	ssl_truststore_location	file	--	No	SSL certificates This parameter is mandatory when SSL is selected.
SSL key	ssl_truststore_password	string	--	No	SSL key This parameter is mandatory when SSL is selected.
Security protocol	security_protocol	string	PLAINTEXT	No	Security protocol
SASL connection configuration	sasl_jaas_config	string	--	No	SASL connection configuration
is_pw_encrypted	is_pw_encrypted	string	true	No	Whether to encrypt the value.
SASL mechanism	sasl_mechanism	string	PLAIN	No	sasl_mechanism

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Set **sasl_jaas_config** based on the Kafka specifications. The following is an example: ● Plaintext connection configuration org.apache.kafka.common.security.plain.PlainLoginModule required username='*kafka user*'password='*kafka password*'; ● Ciphertext connection configuration org.apache.kafka.common.security.scram.ScramLoginModule required username='*kafka user name*'password='*kafka password*';					

Table 13-33 OBS connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
region	region	string	--	Yes	region
Bucket	bucket	string	demo-obs-sec-mrd-datas	Yes	Bucket name
endpoint	endpoint	string	https://obs.huawei.com	Yes	endpoint
Cache folder	temporary_directory	string	/temp/logstash/	Yes	Cache path
Encoding type	codec	string	plain	No	Encoding format: plain or JSON
AK	ak	string	--	No	AK
SK	sk	string	--	No	SK
Prefix	prefix	string	test	No	Path prefix.
Encoding format	encoding	string	gzip	No	Encoding format: gzip or pure file

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Memory path	sincedb_path	string	/opt/ cloud/ logstash/ pipeline/ file_name	No	Log read position. This parameter is used to prevent full-text traversal caused by restart.

Table 13-34 Pipe connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Type	type	string	Tenant	Yes	Type
Pipeline	pipeId	string	--	Yes	Pipeline
AK	ak	string	--	Yes	AK This parameter is mandatory when the platform type is selected.
SK	sk	string	--	Yes	SK This parameter is mandatory when the platform type is selected.
domain_name	domain_name	string	domain_name	Yes	Domain name of the IAM user This parameter is mandatory when the tenant type is selected.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
User_name	user_name	string	user_name	Yes	Username of the IAM user This parameter is mandatory when the tenant type is selected.
Password	user_password	string	--	Yes	Password of the IAM user This parameter is mandatory when the tenant type is selected.
Compression type	compression_type	string	NONE	No	Packet compression type
Block if the queue is full	block_if_queue_full	boolean	true	No	Whether to block the access if the queue is full.
Enable batch processing	enable_batching	boolean	true	No	Whether to enable batch processing.

13.2.15 Parser Rules

The tenant-side data collection uses custom Logstash collectors for data transmission. Parsers mainly work as codeless filters in Logstash. Currently, the following types of Logstash filter plugins are supported.

Table 13-35 Supported types

Parser	Plug-in in Logstash	Description
Key-Value filter	kv	Parses key-value pairs. For details about parsing rules, see **Table 13-36**.

Parser	Plug-in in Logstash	Description
Mutate filter	mutate	Performs general mutations on fields. For details about parsing rules, see **Table 13-37**.
Grok filter	grok	Parses regular expressions. For details about parsing rules, see **Table 13-38**.
Date filter	date	Parses the date. For details about parsing rules, see **Table 13-39**.
Drop filter	drop	Deletes packets. There is no specific rule. If you use this parser, logs received will be deleted.
Prune filter	prune	Parses blacklists and whitelists. For details about parsing rules, see **Table 13-40**.
CSV filter	csv	Parses the CSV data. For details about parsing rules, see **Table 13-41**.
Function filter	ruby	Executes ruby code. For details about parsing rules, see **Table 13-42**.
JSON filter	json	Converts the JSON data. For details about parsing rules, see **Table 13-43**.
Split filter	split	Splits data. For details about parsing rules, see **Table 13-44**.
Clone filter	clone	Duplicates data. For details about parsing rules, see **Table 13-45**.
UUID filter	uuid	Parses UUIDs. For details about parsing rules, see **Table 13-46**.

Table 13-36 Kv filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Source	source	string	source	Yes	Defines the fields to be translated.
Target	target	string	message	No	Defines the target fields.
Field_split	field_split	string	,	No	Splits fields.
Value_split	value_split	string	=	No	Splits fields.

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Trim_key	trim_key	string	--	No	Removes spaces from the key.
Trim_value	trim_value	string	--	No	Removes spaces from the value.
Allow_duplicate_values	allow_duplicate_values	boolean	true	No	Allows duplicate values.
Default_keys	default_keys	array	--	No	Adds keys.
Exclude_keys	exclude_keys	array	--	No	Excludes certain keys.
Include_keys	include_keys	array	--	No	Includes certain keys.
Prefix	prefix	string	--	No	Performs prefix matches.
Recursive	recursive	boolean	true	No	Performs Recursive parsing.
Transform_key	transform_key	string	--	No	Transforms keys.
Add_field	add_field	hash	--	No	Adds fields.
add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.
Remove_tag	remove_tag	array	--	No	Removes tags.
Id	id	string	--	No	ID.
Whitespace	whitespace	string	strict/ lenient	No	Allows whitespace characters.
Remove_char_key	remove_char_key	string	<>[](),	No	Removes characters from the key.

Table 13-37 Mutate filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Convert	convert	hash	--	No	Converts a field's value into a different type.
Join	join	hash	--	No	Joins arrays.
Lowercase	lowercase	array	--	No	Converts characters into its lowercase equivalent.
Coerce	coerce	hash	--	No	Sets the default value of a field.
Rename	rename	hash	--	No	Renames fields.
Replace	replace	hash	--	No	Replaces the value of a field with a new value.
Split	split	hash	--	No	Split a field to an array.
Strip	strip	array	--	No	Strips spaces from fields.
Update	update	hash	--	No	Updates fields.
Uppercase	uppercase	array	--	No	Converts characters into its uppercase equivalent.
Add_field	add_field	hash	--	No	Adds fields.
Add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.
Remove_tag	remove_tag	array	--	No	Removes tags.
ID	id	string	--	No	Id
Copy	copy	hash	--	No	Copies fields.

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Gsub	gsub	array	--	No	Replaces the gsub value.

Table 13-38 Grok filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
match	match	hash	--	Yes	Performs regex matches.
Break_on_match	break_on_match	boolean	true	No	Breaks on the first match.
Overwrite	overwrite	array	message	No	Overwrites fields.
Add_field	add_field	hash	--	No	Adds fields.
Add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.
Remove_tag	remove_tag	array	--	No	Removes tags.
Id	id	string	--	No	Id

Table 13-39 Date filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Match	match	array	--	Yes	Performs regex match.
Target	target	string	timestamp	Yes	Target fields.
Add_field	add_field	hash	--	No	Adds fields.
Add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Remove_tag	remove_tag	array	--	No	Removes tags.
Id	id	string	test	No	Id
Locale	locale	string	--	No	Locale
Timezone	Specifies the time zone.	string	+8:00	No	Specifies the time zone.

Table 13-40 Prune filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Blacklist_names	blacklist_names	array	--	No	Excludes fields whose names match specified regular expressions.
Blacklist_values	blacklist_values	array	--	No	Excludes specified fields if their values match one of the supplied regular expressions.
Whitelist_names	whitelist_names	array	--	No	Includes specified fields only if their names match specified regular expressions.
Whitelist_values	whitelist_values	array	--	No	Includes specified fields only if their values match one of the supplied regular expressions.

Table 13-41 CSV filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Source	source	string	message	No	Defines the fields to be parsed.
Columns	columns	array	--	No	Defines a list of column names.
Separator	separator	string	,	No	Defines the column separator value.
Skip_empty_columns	skip_empty_columns	boolean	true	No	Defines whether empty columns can be skipped.

Table 13-42 Function filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Filter_length	filter_length	number	10	No	Controls the field length.
Set_time	set_time	ruby_time	123	No	Sets a time.

Table 13-43 JSON filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Source	source	string	message	Yes	Defines source fields.
Skip_on_invalid_json	skip_on_invalid_json	boolean	true	No	Skips invalid json fields.
Add_field	add_field	hash	null	No	Adds fields.
Add_tag	add_tag	array	null	No	Adds tags.

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Remove_field	remove_field	array	null	No	Removes fields.
Remove_tag	remove_tag	array	null	No	Removes tags.
Target	target	string	message	No	Defines target fields.

Table 13-44 Split filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Field	field	string	message	Yes	Defines fields to be split.

Table 13-45 Clone filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Clone	clones	array	--	Yes	Defines the list of fields to be cloned.

Table 13-46 UUID filter

Parsing Rule	Logstash Configuration Item	Type	Default Value	Mandatory	Description
Target	target	string	uuid	Yes	Target fields.
Overwrite	overwrite	boolean	true	Yes	Defines whether to overwrite.

13.2.16 Upgrading the Component Controller

Scenarios

This topic describes how to upgrade the component controller from salt-minion to isap-agent for tenant-side data collection. salt-minion was used as component controller in earlier tenant-side data collection.

📖 **NOTE**

The upgrade does not affect the data plane.

Preparing for the Upgrade

IAM is used for data collection authorization. You need to create an IAM user with the minimum permission to access SecMaster APIs and disable verification rules such as MFA for the user.

1. Log in to the management console.

2. Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

3. Create a user group.

   a. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **Create User Group** in the upper right corner.

   b. On the **Create User Group** page, specify user group name and description.

      ▪ **Name**: Set this parameter to **Tenant collection**.

      ▪ **Description**: Enter a description.

   c. Click **OK**.

4. Assign permissions to the user group.

   a. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.

   b. Configure a policy.

      ▪ **Policy Name**: Set this parameter to **Least permission policy for tenant collection**.

      ▪ **Policy View**: Select **JSON**.

      ▪ **Policy Content**: Copy the following content and paste it in the text box.
      ```
      {
        "Version": "1.1",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": [
              "secmaster:workspace:get",
              "secmaster:node:create",
              "secmaster:node:monitor",
              "secmaster:node:taskQueueDetail" ,
      ```

```
            "secmaster:node:updateTaskNodeStatus"
          ]
        }
      ]
    }
```

    c.   Click **OK**.

5.   Assign permissions to the created user group.

    a.   In the navigation pane on the left, choose **User Groups**. On the displayed page, click **Tenant collection**.

    b.   On the **Permissions** tab, click **Authorize**.

    c.   On the **Select Policy/Role** page, search for and select the **Least permission policy for tenant collection** added in **4**, and click **Next**.

    d.   Set the minimum authorization scope. Select **All resources** for **Scope**. After the setting is complete, click **OK**.

    e.   Verify the authorization. The policy will be listed on the page.

6.   **Create a user**.

During the creation, enable **Programmatic access**, **Access key**, and **Password**.

7.   Add the operation account to the user group.

    a.   In the navigation pane on the left, choose **User Groups**.

    b.   In the **Tenant collection** user group row, click **Manage User** in the **Operation** column.

    c.   In the displayed **Manage User** dialog box, select users added in **6**.

    d.   Click **OK**.

Upgrading the Component Controller

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-64 Workspace management page
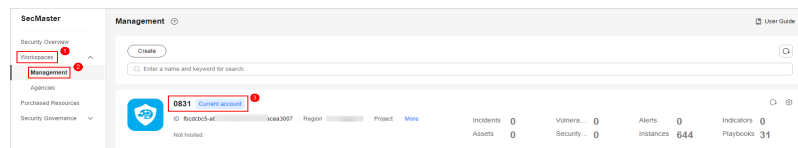
Step 5 Deregister a node.

1.   In the navigation pane on the left, choose **Settings** > **Components**. On the displayed **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.

Figure 13-65 Deregistering a node

2. In the displayed dialog box, click **OK**.

   The node is deregistered successfully, and its **Health Status** changes to **Disconnected**.

Figure 13-66 Health Status

Step 6 Copy the script.

1. On the **Nodes** page, click **Create**.

2. On the **Create Node** page, click **Next**. On the **Verify installed Script** page, copy the script.

Figure 13-67 Copying the installed script

Step 7 Install the component controller.

1. Use a remote management tool, such as Xftp, SecureFX, WinSCP, PuTTY, or Xshell, to log in to the disconnected ECS node.

2. Run the command copied in **Step 6.2** as user **root** to install the Agent on the ECS.

Figure 13-68 Installing the agent

3. Enter the IAM username and password created in **Preparing for the Upgrade** as prompted.

4. If information similar to the following is displayed, the agent is successfully installed:

   install isap-agent successfully

5. Go to the SecMaster console and check the node status on the **Nodes** page under **Settings**.

Figure 13-69 Checking node status
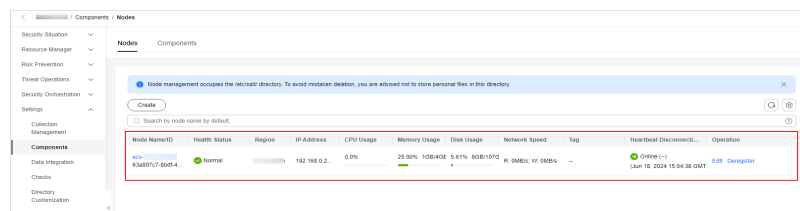
Step 8 Delete the old management channel.

1. Choose **Settings** > **Components** > **Nodes** and click **Create**. On the **Create Node** pane displayed, click **Delete** in the **Operation** column in the row of each the management.

Figure 13-70 Deleting a management channel
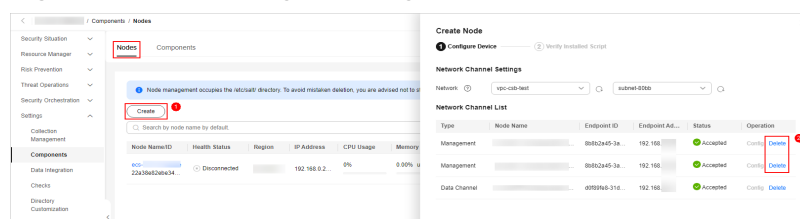
2. In the displayed dialog box, click **OK**.

----End

13.3 Customizing Directories

Scenario

You can customize directories on SecMaster. This section includes the following content:

- **Viewing Existing Directories**
- **Changing Layout**

Limitations and Constraints

- Built-in directories **cannot** be edited or deleted.

Viewing Existing Directories

Step 1 Log in to the management console.

Step 2 Click ![icon] in the upper left corner of the management console and select a region or project.

Step 3 Click ![menu icon] in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.
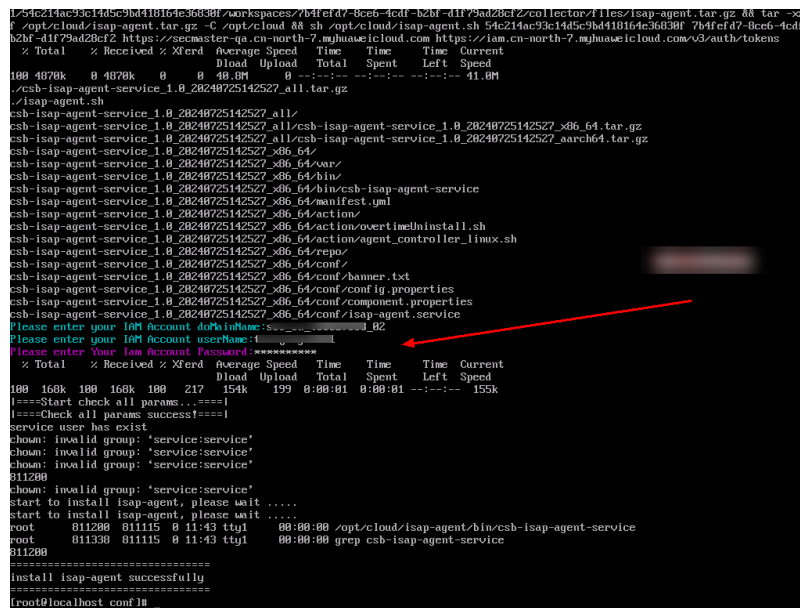
Figure 13-71 Workspace management page
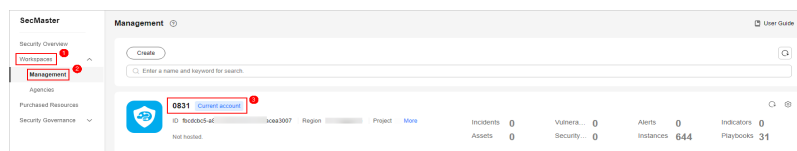
Step 5 In the navigation tree on the left, choose **Settings** > **Directory Customization**.

Figure 13-72 Directory Customization page
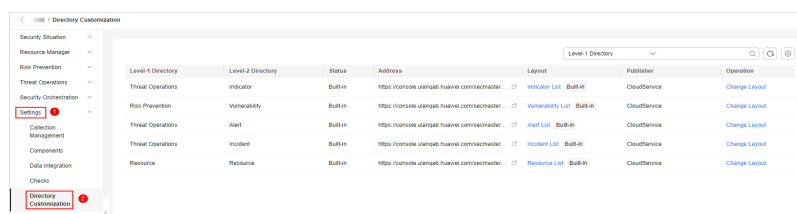
Step 6 In the directory list, view the directory details.

Table 13-47 Directory parameters

Parameter	Description
Level-1 Directory	Name of the level-1 directory to which the directory belongs
Level-2 Directory	Name of the level-2 directory to which the directory belongs
Status	Type of the directory.
Address	Address of the directory.
Layout	Layout associated with the directory.
Publisher	Publisher of the directory. The default publisher of a built-in directory is **Huawei Cloud**.
Operation	Operations you can do for the directory, such as changing the layout.

----End

Changing Layout

Step 1 Log in to the management console.

Step 2 Click 🔘 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-73 Workspace management page
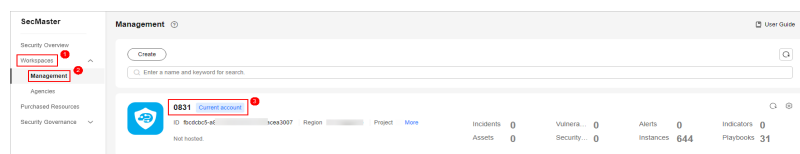
Step 5 In the navigation tree on the left, choose **Settings** > **Directory Customization**.

Figure 13-74 Directory Customization page
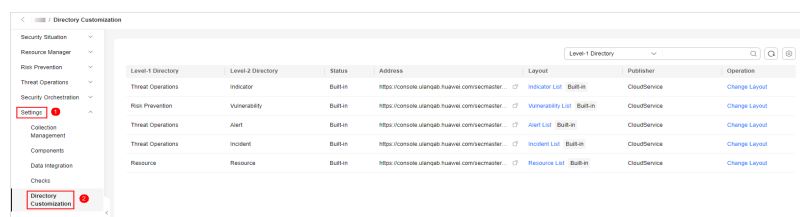
Step 6 Click **Changing layout** in the **Operation** column of the target directory.

Step 7 On the **Changing layout** page, select the layout to be changed.

Step 8 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.

Table 14-1 System-defined permissions supported by SecMaster

Policy Name	Description	Type
SecMaster FullAccess	All permissions of SecMaster.	System-defined policy
SecMaster ReadOnlyAccess	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	System-defined policy

Permission Granting Process

Figure 14-1 Process for granting permissions
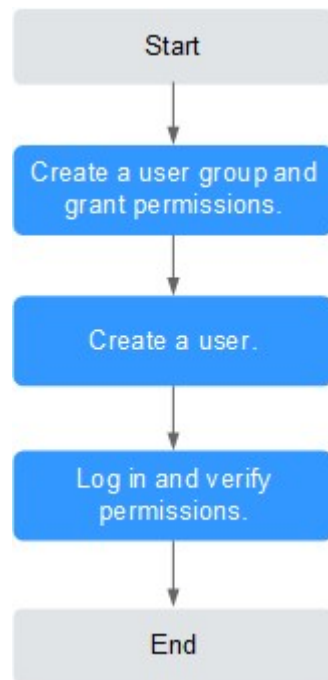
1. **Create a user group and assign permissions**.

   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"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "hss:vuls:set",
                "hss:vuls:list"
            ]
        }
```

```
        ]
    }
```

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.

Table 15-1 SecMaster operations recorded by 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

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	uploadAttachment
Creating a Plug-in Template	component	createComponentTemplate

Operation	Resource Type	Trace Name
Updating a Plug-in Template	component	updateComponentTemplate
Deleting a Plug-in Template	component	deleteComponentTemplate
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 Viewing CTS Traces in the Trace List

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 Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

NOTE

These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

This section describes how to query or 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 longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.

- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.

- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

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.

   – **Enterprise Project ID**: Enter an enterprise project ID.

   – **Access Key**: Enter a temporary or permanent access key ID.

   – Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.

5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.

   – Enter any keyword in the search box and press **Enter** to filter desired traces.

   – Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.

   – Click ↻ 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: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.

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 5,000 records.
   - Click ↻ to view the latest information about traces.

8. Click ⌄ on the left of a trace to expand its details.

9. Click **View Trace** in the **Operation** column. The trace details are displayed.

View Trace   ✕

```
{
    "request": "",
    "trace_id": "                              ",
    "code": "200",
    "trace_name": "createDockerConfig",
    "resource_type": "dockerlogincmd",
    "trace_rating": "normal",
    "api_version": "",
    "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
    "source_ip": "              ",
    "domain_id": "                         ",
    "trace_type": "ApiCall",
    "service_type": "SWR",
    "event_type": "system",
    "project_id": "                         ",
    "response": "",
    "resource_id": "",
    "tracker_name": "system",
    "time": "Nov 16, 2023 10:54:04 GMT+08:00",
    "resource_name": "dockerlogincmd",
    "user": {
        "domain": {
            "name": "        ",
            "id": "                         "
```

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.