SecMaster

User Guide

Issue 10

Date 2024-03-28

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Contents

1 Authorizing SecMaster

Scenario

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

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

Table 1-1 Agency permissions

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

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

Permission	Description	Assign To	When to Use
OBS 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 execute alert playbooks and obtain OBS asset details for baseline checks.
ELB ReadOnlyAccess	Read-only permissions for ELB.	SecMaster_Agency	Used to obtain ELB asset details for baseline checks.
CFW FullAccess	All permissions for CFW.	SecMaster_Agency	Used to execute preventive playbooks.
RMS ReadOnlyAccess	Read-only permissions for RMS.	SecMaster_Agency	Used by the playbooks of notifying of critical O&M operations.

Prerequisites

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

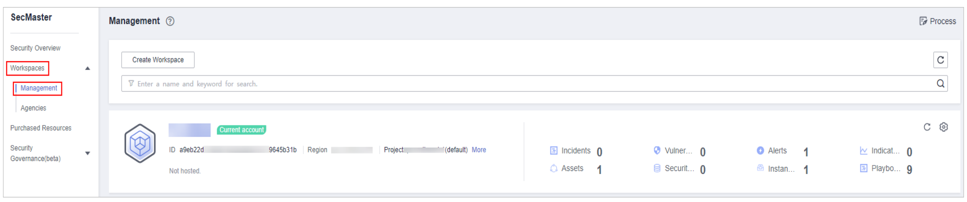
Procedure

Step 1 Log in to the management console.

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

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

Figure 1-1 Workspace page



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

Figure 1-2 Authorizing for SecMaster

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

----End

2 Buying SecMaster

2.1 Buying the Standard Edition

Scenario

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

NOTE

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

Edition Description

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

Table 2-1 SecMaster editions

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

Procedure

Step 1 Log in to the management console.

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

Step 3 On the **Security Overview** page, click **Buy SecMaster** in the upper right corner.

Step 4 (Optional) You need to perform access authorization before you purchase SecMaster for the first time. On the **Access Authorization** panel displayed, select **Consent to Authorization** and click **Submit**.

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

Figure 2-1 Buying the standard edition

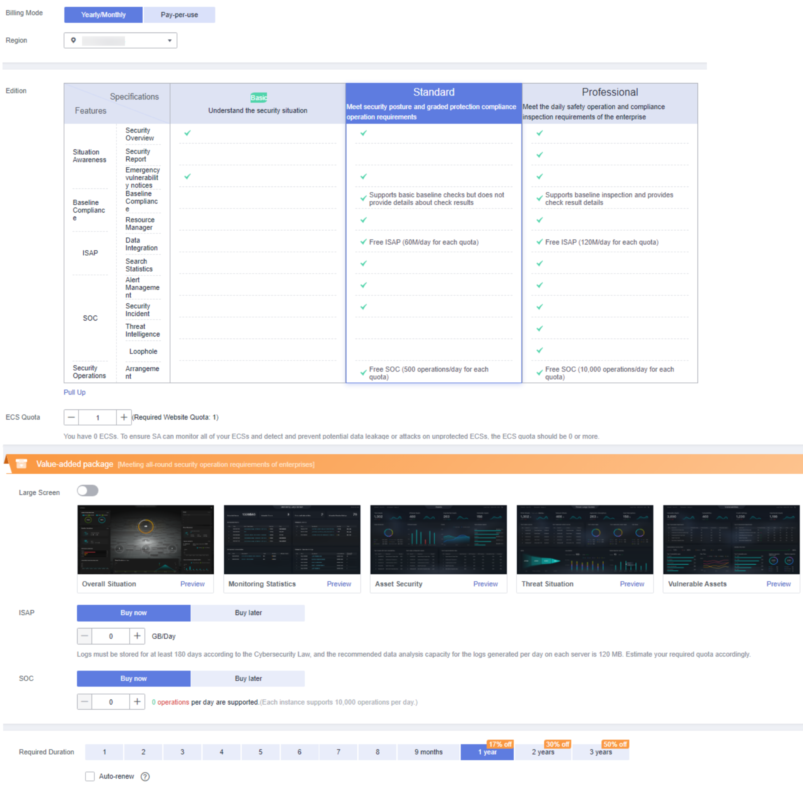


Table 2-2 Parameters for purchasing the standard edition

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

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

Step 6 Confirm the product details and click **Next**.

Step 7 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

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

----End

Verification

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

Related Operations

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

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

2.2 Buying the Professional Edition

Scenario

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

NOTE

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

Edition Description

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

Table 2-3 SecMaster editions

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

Yearly/Monthly Billing

Step 1 Log in to the management console.

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

Step 3 On the **Security Overview** page, click **Buy SecMaster** in the upper right corner.

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

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

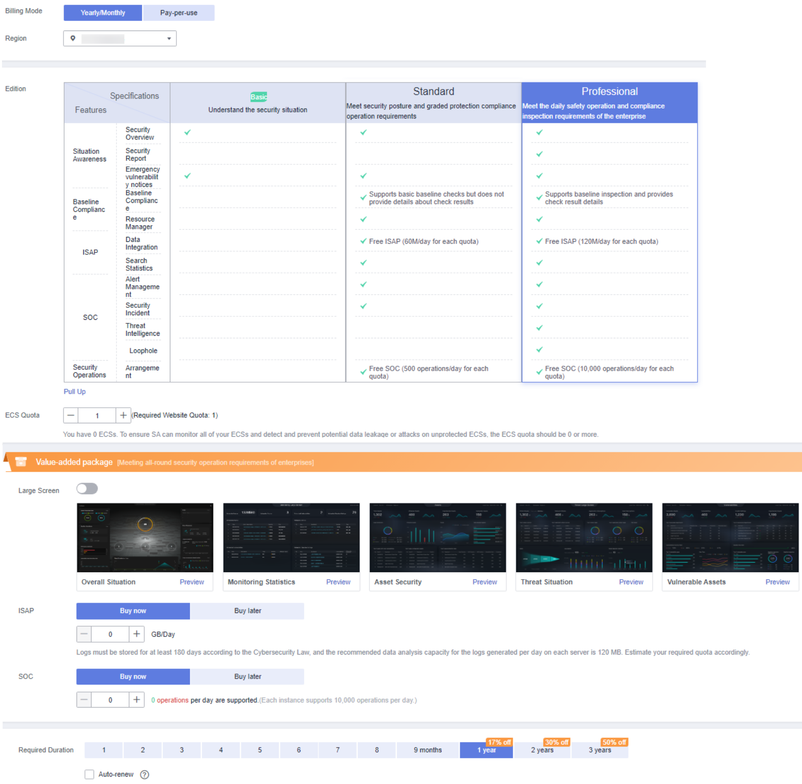


Figure 2-2 Purchasing SecMaster professional edition in yearly/monthly mode

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

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

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

Step 6 Confirm the product details and click **Next**.

Step 7 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

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

----End

Pay-per-Use Billing

Step 1 Log in to the management console.

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

Step 3 On the **Security Overview** page, click **Buy SecMaster** in the upper right corner.

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

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

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

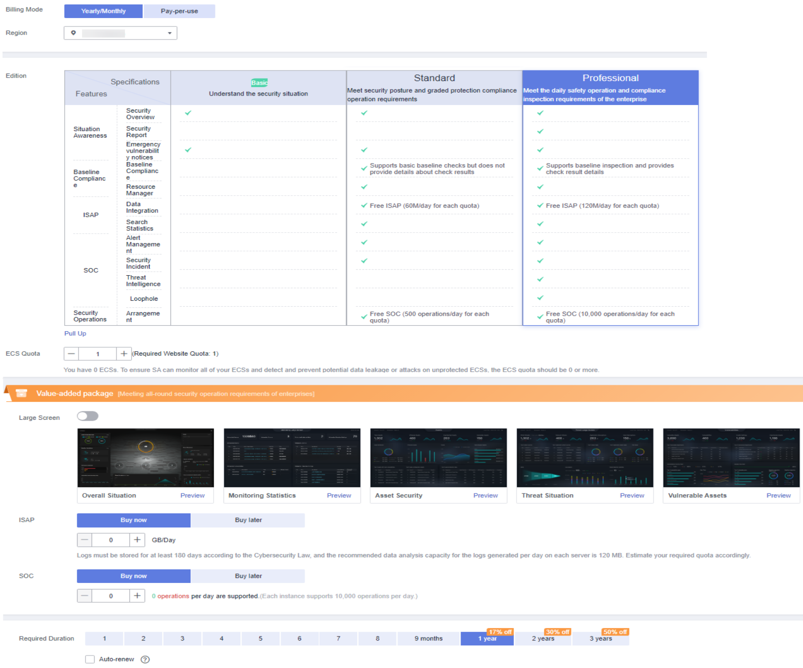


Table 2-5 Parameters for purchasing the SecMaster professional edition in pay-per-use mode

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

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

Step 6 Confirm the product details and click **Next**.

Step 7 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

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

----End

Effective Conditions

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

Related Operations

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

2.3 Upgrading the Service Edition

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

Table 2-6 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.

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

NOTE

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

Edition Description

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

Table 2-7 SecMaster editions

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

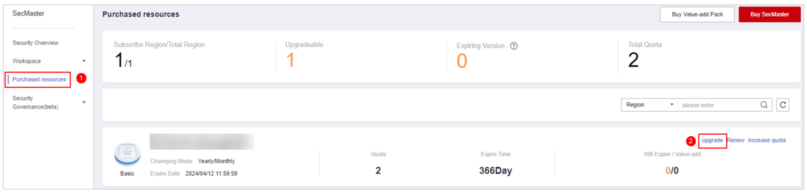
Upgrading Basic to Standard or Professional

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Purchased Resources**. Locate the target region and click **Upgrade**.

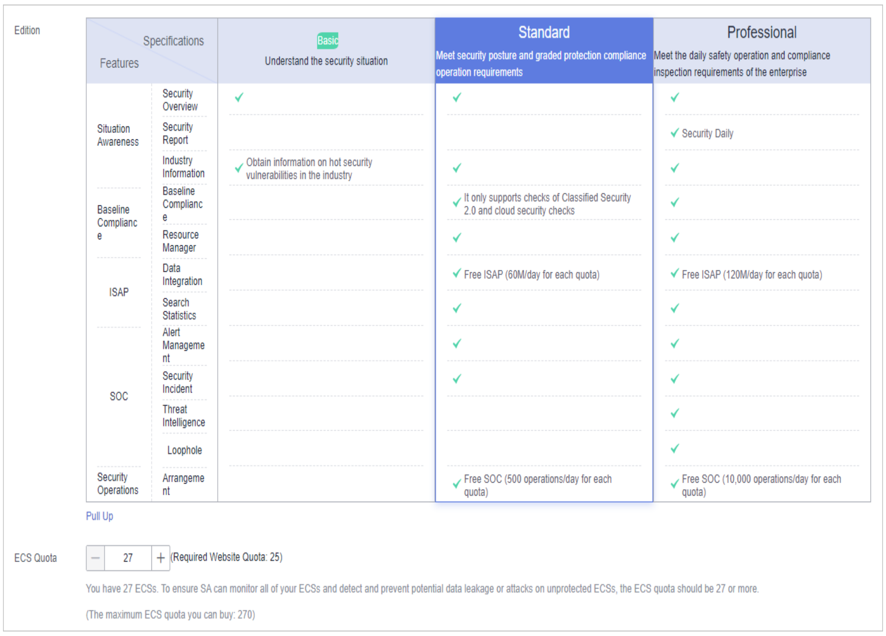
Figure 2-4 Upgrading the basic edition



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

1. **Current Configuration**: configuration information of the purchased SecMaster version
2. **Upgrade Method**: By default, **Version Upgrade** is selected.
3. **Edition**: Select **Standard** or **Professional**.

Figure 2-5 Selecting an edition



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

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

Step 6 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

Step 7 On the payment page, select a payment method and complete the payment.

----End

Upgrading Standard to Professional

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, locate the region where you want to upgrade and click **Upgrade**.

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

1. **Current Configuration**: version information of the current SecMaster before you increase the quota.
2. **Upgrade Method**: Select **Version Upgrade**. You can also select **Increase Quota**.
3. **Optional Version**: Select **Professional** to upgrade to the professional edition.

Figure 2-6 Selecting the professional edition

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

Table 2-8 ECS quota description

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

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

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

Step 6 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

Step 7 On the payment page, select a payment method and complete the payment.

----End

Effective Conditions

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

Related Operations

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

2.4 Purchasing Value-Added Packages

Scenario

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

NOTE

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

Limitations and Constraints

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

Prerequisites

You have purchased the SecMaster standard edition or professional edition.

Purchasing a Yearly/Monthly Value-added Package

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, click **Buy Value-added Pack** in the upper right corner.

Step 4 On the purchase page, configure required parameters.

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

Figure 2-7 Purchasing a value-added package

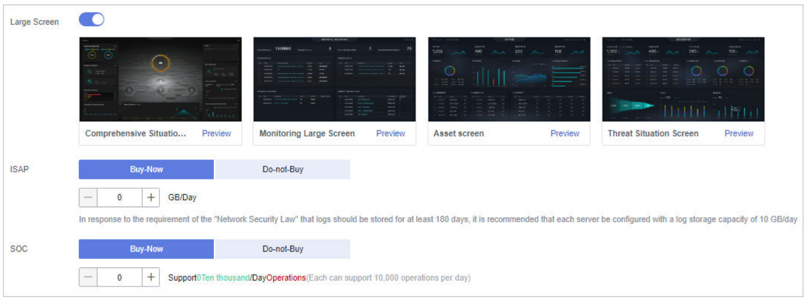


Table 2-9 Purchasing a value-added package

Feature	Buy Now	Do Not Buy
Large Screen	Toggle on the button next to **Large Screen** to buy the large screen function.	Retain the toggle-off status ( ).
ISAP	1. Select **Buy now**. 2. Set the amount of log volume you want to store daily.	Select **Buy later**.
SOC	1. Select **Buy now**. 2. Set the number of daily operations allowed.	Select **Buy later**.

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

Step 5 Set **Required Duration**. You can select the required duration from one month to three years.

NOTE

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

Step 6 Confirm the product details and click **Next**.

Step 7 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

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

----End

Purchasing a Pay-per-Use Value-added Package

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, click **Buy Value-added Package** in the upper right corner.

Step 4 On the purchase page, configure required parameters.

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

Figure 2-8 Purchasing a value-added package

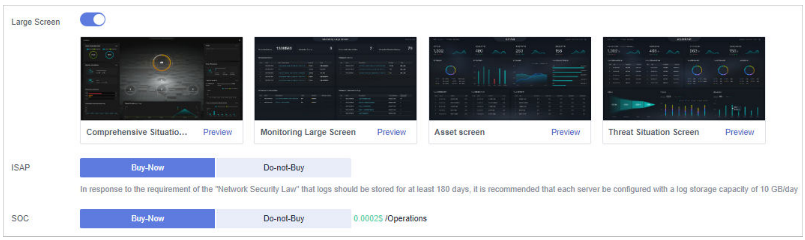


Table 2-10 Purchasing a value-added package

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

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

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

Step 6 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

Step 7 On the payment page, select a payment method and complete the payment.

----End

Follow-up Operations

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

2.5 Increasing the Quota

Scenario

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

NOTE

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

Limitations and Constraints

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

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, locate the region where you want to add quotas and click **Increase Quota**.

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

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

Figure 2-9 Increasing the quota

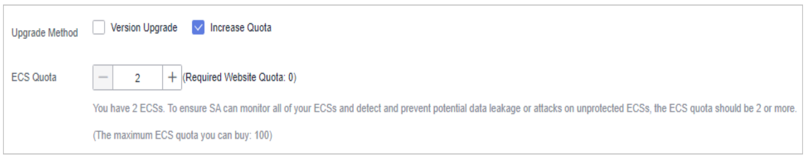


Table 2-11 ECS quota description

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

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

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

Step 6 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

Step 7 On the payment page, select a payment method and complete the payment.

----End

2.6 Unsubscribing from SecMaster

Scenario

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

- Yearly/Monthly billing mode: a prepaid mode. You can unsubscribe from a purchased cloud service and apply for a full refund unconditionally within five days of the purchase. Each account can request five-day unconditional full refund for 10 times in a year. Handling fees are required if you unsubscribe from a service over 5 days after it is purchased.

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

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

NOTE

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

Limitations and Constraints

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

  After all asset quotas (professional edition or standard edition) are unsubscribed from and the current edition is the basic edition, you can unsubscribe from value-added packages.
- In the **pay-per-use** professional edition, when you unsubscribe from or cancel the asset quota of the professional edition, the value-added package is also unsubscribed or canceled.
- The value-added packages cannot be used independently.

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

Unsubscribing from Yearly/Monthly Resources

Step 1 Log in to the management console.

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

Step 3 Click **Standard** or **Professional** in the upper right corner. A window for you to manage SecMaster assets will be displayed.

Step 4 In the row of the ECS quota or value-added package billed on a yearly/monthly basis, click **Unsubscribe**.

Step 5 Locate the row that contains the target instance, and click **Unsubscribe** in the **Operation** column.

Step 6 Confirm the information about the resource to be unsubscribed, select the unsubscription reason, and select **I understand a handling fee will be charged for this unsubscription.**

Step 7 Click **Confirm**.

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

----End

Canceling Pay-per-Use SecMaster Resources

Step 1 Log in to the management console.

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

Step 3 Click **Professional** in the upper right corner. The edition management window is displayed.

Step 4 In the row of the SecMaster edition purchased in pay-per-use billing mode, click **Cancel** to release the purchased SecMaster resources.

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

----End

Unsubscribing from a Plus Features

Step 1 Log in to the management console.

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

Step 3 Click **Standard** or **Professional** in the upper right corner. A window for you to manage SecMaster assets will be displayed.

Step 4 Unsubscribe a Plus Feature

- For a pay-per-use value-added package:

  Click **Cancel** to release the pay-per-use asset quota. Go to the edition management window and verify that the subscription to resources billed on a pay-per-use basis is canceled.
- For yearly/monthly billed value-added packages:
  a. Click **Unsubscribe**. The **Unsubscriptions** page is displayed.
  b. Locate the row that contains the target instance, and click **Unsubscribe** in the **Operation** column.
  c. Confirm the information about the resource to be unsubscribed, select the unsubscription reason, and select **I understand a handling fee will be charged for this unsubscription.**
  d. Click **Confirm**.

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

----End

3 Security Overview

3.1 Overview

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

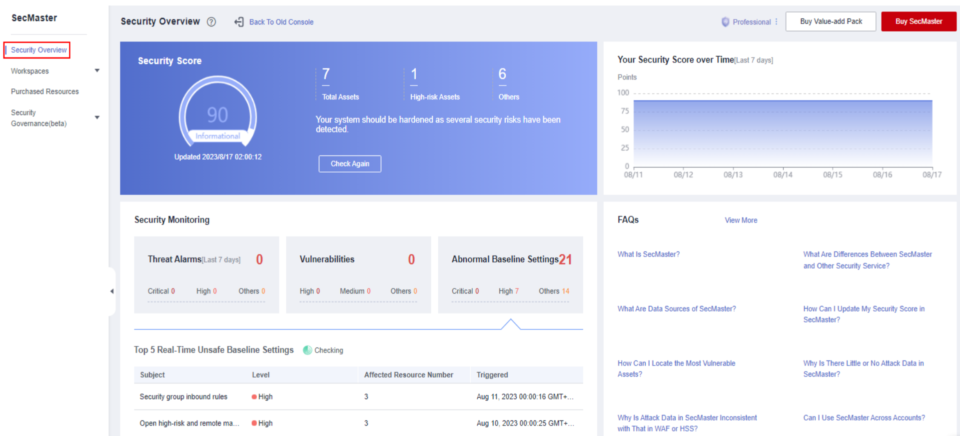
Procedure

Step 1 Log in to the management console.

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

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

Figure 3-1 Security Overview



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

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

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

Table 3-1 Security Overview

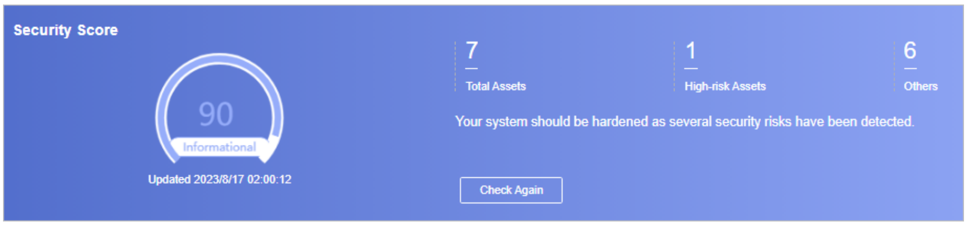
Parameter	Statistical Period	Update Frequency	Description
Security Score	Real-time	• Automatic update at 02:00 every day • Updated every time you click **Check Again**	The score is calculated based on what security services are enabled, and the levels and numbers of unhandled configuration issues, vulnerabilities, and threats. For 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 of your workloads on the cloud based on the SecMaster edition you are using. You can quickly understand the unprocessed risks and their threats to your assets. **Figure 3-2** shows an example.

Figure 3-2 Security Score



- The security score is automatically updated at 02:00 every day. You can also click **Check Again** to update it immediately.
- The score ranges from 0 to 100. The higher the security score, the more secure your assets. For details, see **Security Score**.
- Different color blocks in the security score ring chart indicate different severity levels. For example, yellow indicates that your security is medium.
- The security score is updated when you refresh status of the alert incident after risk handling. After you fix the risks, you can click **Check Again** so that SecMaster can check and score your system again.

  NOTE

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

Security Monitoring

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

Figure 3-3 Security Monitoring

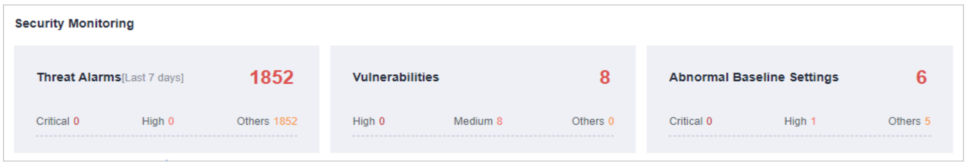


Table 3-2 Security Monitoring parameters

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. **Figure 3-4** Viewing real-time alerts 

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Vulnerabilities</td><td>
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 top 5 vulnerability types.

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.

Figure 3-5 Top 5 Vulnerability Types


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.

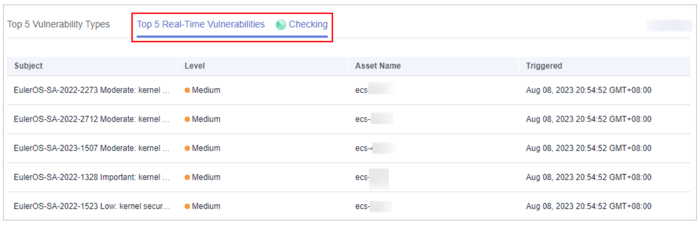
You can view details such as the vulnerability name, severity, asset name, and discovery time.

</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>

– If no data is available here, no vulnerabilities are detected on the current day.

Figure 3-6 Viewing real-time vulnerabilities

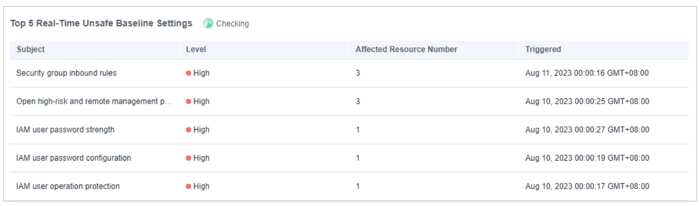


</td></tr>
<tr><td>Abnormal Baseline Settings</td><td>

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, click the **Abnormal Baseline Settings** panel.
  - You can view details of the top compliance risks discovered in the latest check, such as check item name, severity, asset name, and discovery time.
  - If no data is available, no violations are detected for the last 30 days.

Figure 3-7 Viewing compliance risks

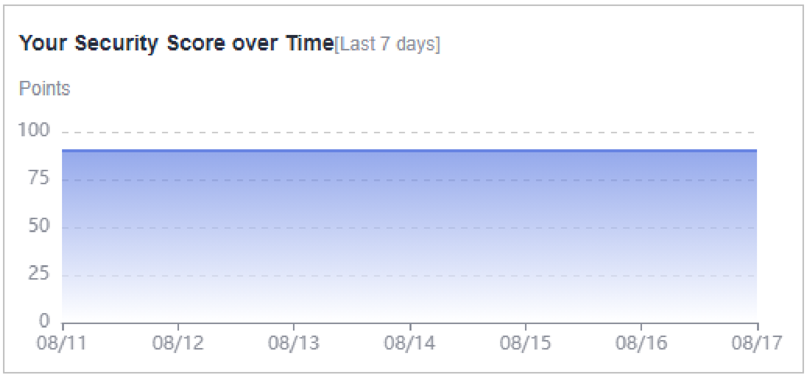


</td></tr>
</table>

Your Security Score over Time

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

Figure 3-8 Your Security Score over Time



3.2 Security Score

Scenario

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

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

This topic describes how your security score is calculated.

Security Score

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

- There are six risk severity levels, **Secure**, **Informational**, **Low**, **Medium**, **High**, and **Critical**.
- The score ranges from 0 to 100. The higher the security score, the lower the risk severity level.
- The security score starts from **0** and the risk severity level is escalated up from **Secure** to the next level every 20 points. For example, for scores ranging from **40** to **60**, the risk severity is **Medium**.
- The color keys listed on the right of the chart show the names of donut slices. Different color represents different risk severity levels. For example, the yellow slice indicates that your asset risk severity is **Medium**.
- If you have fixed asset risks and refreshed the alert status, you can click **Check Again** to update the security score.

NOTE

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

Table 3-3 Security score table

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

Unscored Check Items

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

Table 3-4 Unscored check items

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

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

4 Workspaces

4.1 Workspace Overview

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

What Is a Workspace?

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

- Workspace management:

  A single workspace can be bound to common projects and regions to support workspace operation modes in different scenarios.
- Workspace agencies:
  - Workspace data hosting: All workspaces of a single account can be aggregated to a workspace for cross-account centralized security operations.
  - Workspace hosting: You can create agencies to let a user centrally view the asset risks, alerts, and incidents of multiple workspaces.

What Is a Data Space?

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

What Is a Data Pipeline?

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

General Rules for Workspaces

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

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

4.2 Creating a Workspace

Scenario

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

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

This section describes how to create a workspace.

Limitations and Constraints

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

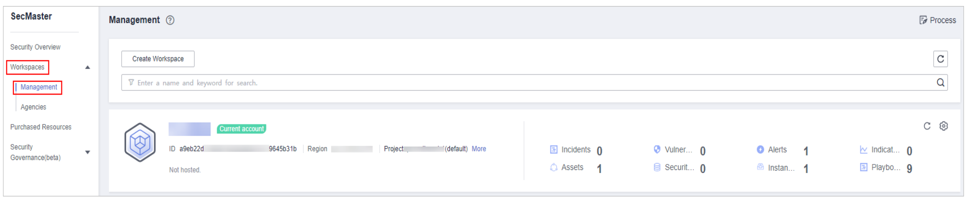
Procedure

Step 1 Log in to the management console.

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

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

Figure 4-1 Workspace page



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

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

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. If you select **Enterprise Project**, you need to select an enterprise project from the drop-down list. This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. To learn more, see **Enabling the Enterprise Center**. You can use enterprise projects to more efficiently manage cloud resources and project members. **NOTE** Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.
Workspace Name	Create a name for your workspace. The name must meet the following requirements: ● Only letters (A to Z and a to z), numbers (0 to 9), and the following special characters are allowed: -_() ● A maximum of 64 characters are allowed.
Tag	(Optional) Tag of the workspace, which is used to identify the workspace and help you classify and track your workspaces.
Description	(Optional) User remarks

Step 6 Click **OK**.

----End

4.3 Managing Workspaces

4.3.1 Viewing Workspace Details

Scenario

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

NOTE

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

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

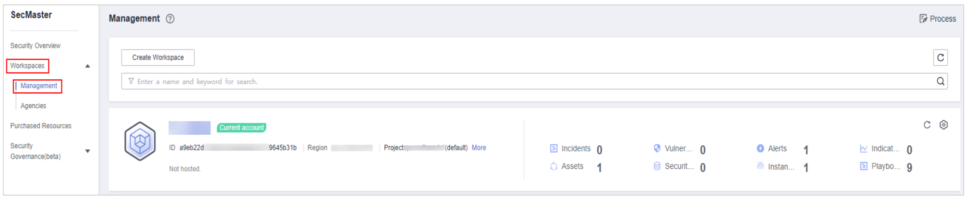
Procedure

Step 1 Log in to the management console.

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

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

Figure 4-2 Workspace page



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

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

Figure 4-3 Workspace details

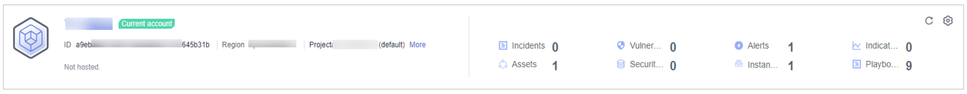


Table 4-2 Workspace parameters

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

Parameter	Description
Hosting Status	Whether the workspace is hosted
Incidents	Number of incidents in the workspace
Vulnerabilities	Number of vulnerabilities in the workspace
Alerts	Number of alerts in the workspace
Indicators	Number of indicators in the workspace
Assets	Number of assets in the workspace
Security Analysis	Number of existing data spaces in the workspace
Instances	Number of instances in the workspace
Playbooks	Number of playbooks in the workspace

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

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

----End

4.3.2 Editing a Workspace

Scenario

After a workspace is added, you can modify the workspace basic settings, including name, tag, and description.

This section describes how to edit a workspace.

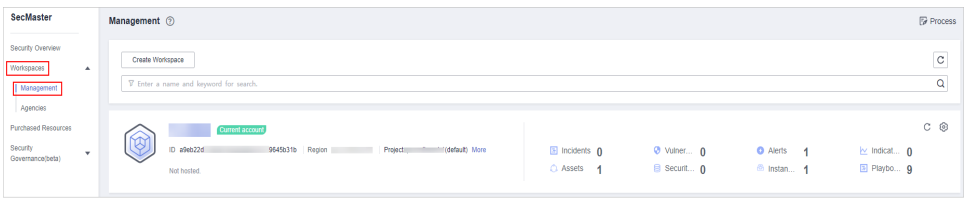
Procedure

Step 1 Log in to the management console.

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

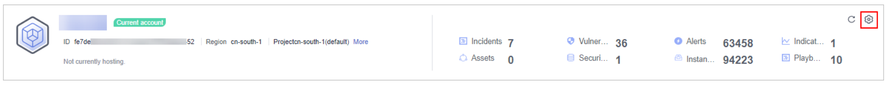
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-4 Workspace page



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

Figure 4-5 Workspace details page



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

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

----End

4.3.3 Managing Workspace Tags

Scenario

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

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

This topic describes how to manage tags.

Limitations and Constraints

A maximum of 10 tags can be added for a workspace.

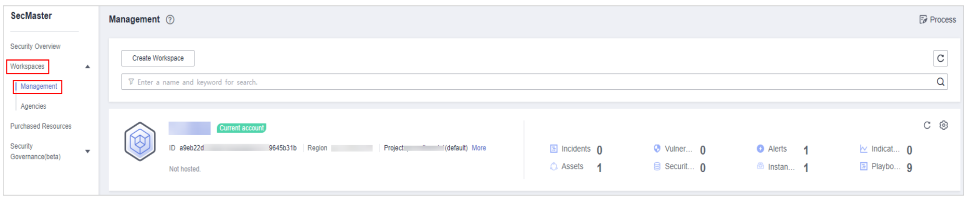
Procedure

Step 1 Log in to the management console.

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

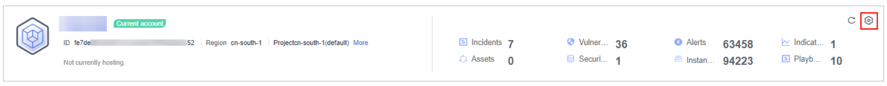
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-6 Workspace page



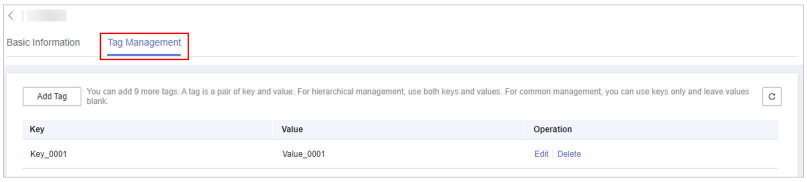
Step 4 Click on the right of the target workspace to go to the details page.

Figure 4-7 Workspace details page



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

Figure 4-8 Tag Management



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

Table 4-3 Managing tags

Operation	Description
Adding a tag	1. On the **Tag Management** tab, click **Add Tag**. 2. In the displayed **Add Tag** tab, configure the tag key and value. 3. Click **OK**.
Editing a tag	1. On the **Tag Management** tab, locate the row that contains the target tag and click **Edit** in the **Operation** column. 2. In the displayed **Edit Tag** dialog box, change the tag value. 3. Click **OK**.
Deleting a tag	On the **Tag Management** tab, locate the row that contains the target tag and click **Delete** in the **Operation** column. In the displayed **Delete Tag** dialog box, click **OK**.

----End

4.3.4 Deleting a Workspace

Scenario

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

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

Limitations and Constraints

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

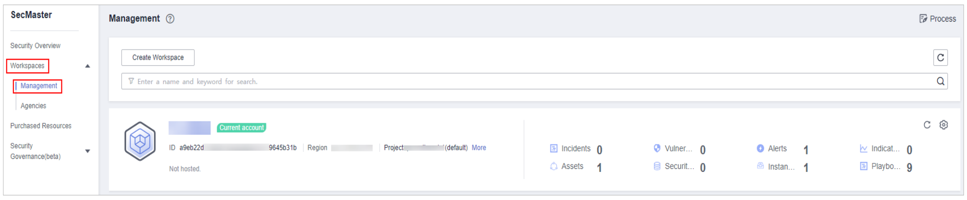
Deleting a Workspace

Step 1 Log in to the management console.

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

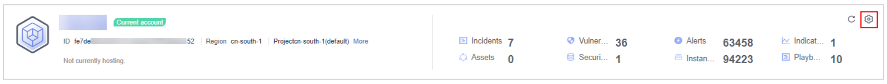
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**.

Figure 4-9 Workspace page



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

Figure 4-10 Workspace details page



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

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

CAUTION

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

----End

4.4 Workspace Agencies

4.4.1 Overview

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

Table 4-4 Process

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

Limitations and Constraints

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

4.4.2 Creating an Agency View

Scenario

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

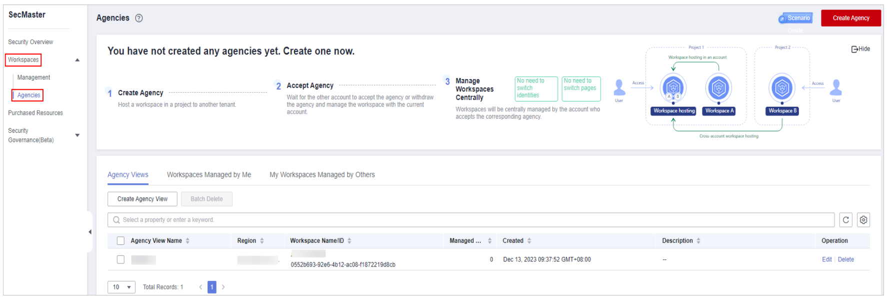
Procedure

Step 1 Log in to the management console.

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

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

Figure 4-11 Agencies



Step 4 On the **View** tab, click **Create Agency View**. The **Create Agency View** slide-out panel is displayed.

Step 5 Set parameters required for creating the agency view.

Table 4-5 Parameters for creating an agency view

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

Step 6 Click **OK**.

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

----End

Related Operations

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

4.4.3 Creating an Agency

Scenario

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

Limitations and Constraints

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

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

Prerequisites

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

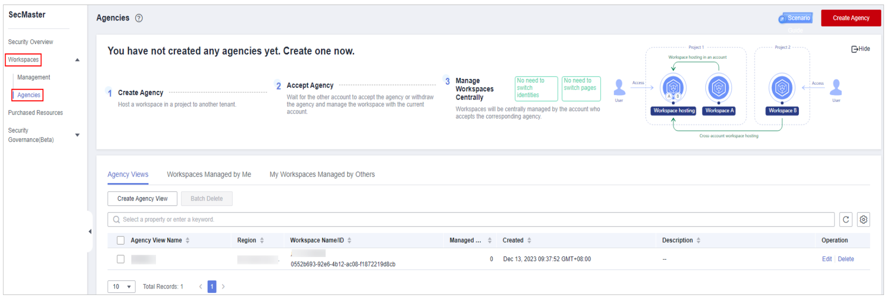
Procedure

Step 1 Log in to the management console.

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

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

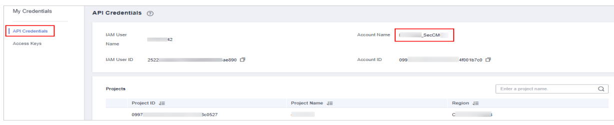
Figure 4-12 Agencies



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

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

Table 4-6 Parameters for creating an agency

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

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

Step 6 Click **Confirm**.

----End

Follow-up Operations

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

4.4.4 Authorizing an Agency

Scenario

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

Prerequisites

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

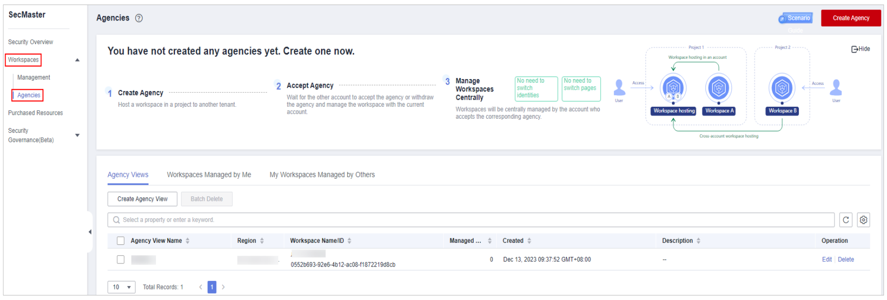
Procedure

Step 1 Log in to the management console.

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

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

Figure 4-14 Agencies



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

Step 5 In the displayed dialog box, click **Confirm**.

----End

Follow-up Operations

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

4.4.5 Managing Agencies

Scenario

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

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

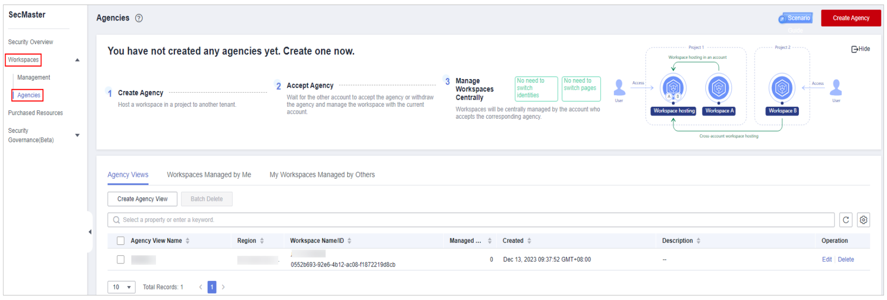
Agency Views

Step 1 Log in to the management console.

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

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

Figure 4-15 Agencies



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

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

- Viewing agency views

Table 4-7 Agency view information

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

- Editing an agency view
  a. Locate the row that contains the agency view, and click **Edit** in the **Operation** column.
  b. On the **Edit Agency View** slide-out panel, modify the parameters and click **OK**.
- Deleting an agency view
  a. Locate the row that contains the agency view, and click **Delete** in the **Operation** column.
     To delete multiple agency views, select them in the agency view list and click **Batch Delete** above the list.
  b. In the displayed dialog box, click **Confirm**.

----End

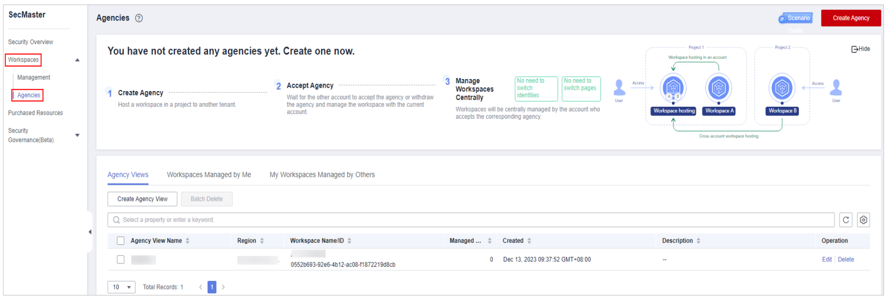
Workspaces Managed by Me

Step 1 Log in to the management console.

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

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

Figure 4-16 Agencies



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

Step 5 View and manage workspaces managed by you.

- Viewing workspaces managed by you

Table 4-8 Workspace parameters

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

- Managing workspaces managed by you

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

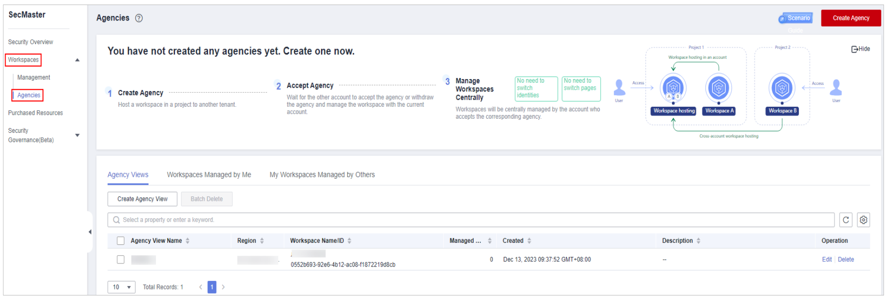
My Workspaces Managed by Others

Step 1 Log in to the management console.

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

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

Figure 4-17 Agencies



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

Step 5 On the **My Workspaces Managed by Others** tab, view and manage the workspaces that are managed by others.

- Viewing your workspaces managed by others

Table 4-10 Viewing your workspaces managed by others

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

- Managing your workspaces managed by others

Table 4-11 Viewing your workspaces managed by others

Operation	Description
Modifying an accepted workspace agency	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**.

Operation	Description
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.

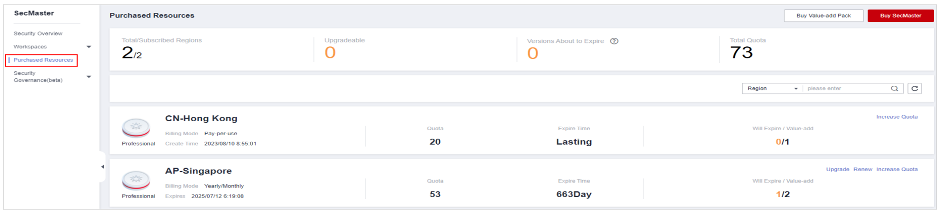
Procedure

Step 1 Log in to the management console.

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

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

Figure 5-1 Purchased Resources



Step 4 View details on the purchased resource page.

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

----End

6 Security Governance

6.1 Overview

What Is Security Governance?

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

NOTE

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

Features

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

- Compliance Pack

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

  The compliance status of cloud assets is checked periodically through 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.

6.2 Security Compliance Pack Description

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

- **Security Standard**

Security Standard

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

Table 6-1 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 Procedure

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

Figure 6-1 Procedure

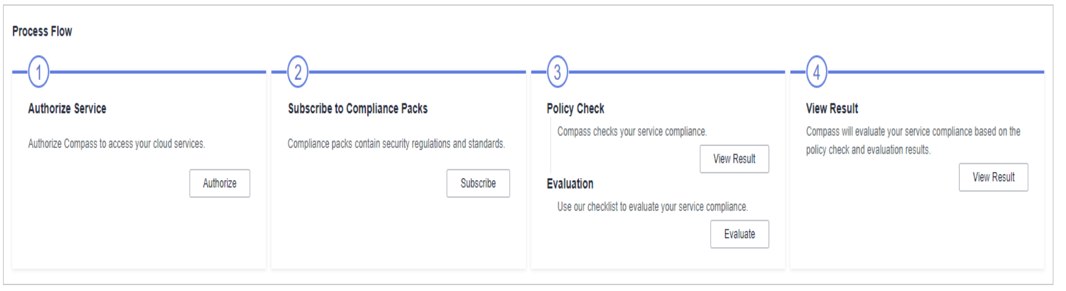


Table 6-2 Procedure

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

6.4 Authorizing Service

Scenario

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

Authorizing SecMaster to access your cloud assets.

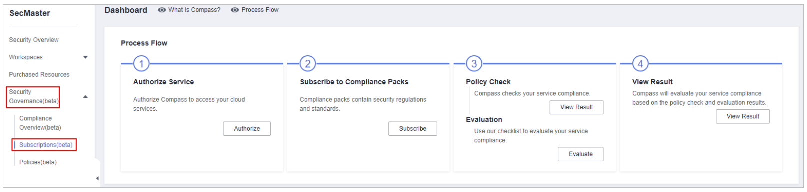
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-2 Subscriptions page



Step 4 On the **Subscriptions** page, click **Authorize** in the **Authorize Service** process. The service authorization dialog box is displayed.

Step 5 In the displayed dialog box, click **Agree to authorize**.

----End

6.5 Subscribing to Compliance Packs

Scenario

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

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

Prerequisites

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

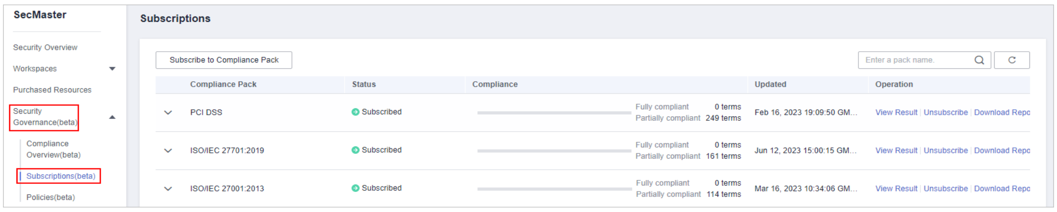
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-3 Subscriptions page



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

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

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

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

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

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

----End

6.6 User Self-Assessment

Scenario

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

Prerequisites

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

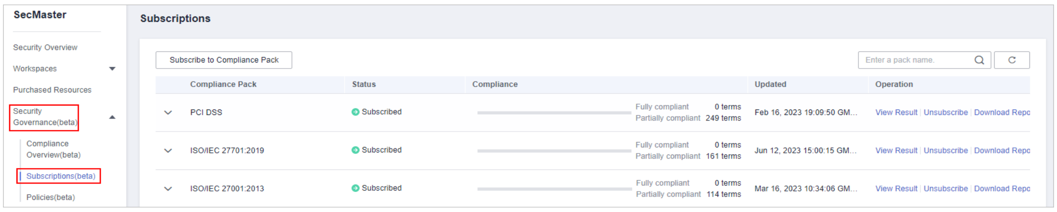
Procedure

Step 1 Log in to the management console.

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

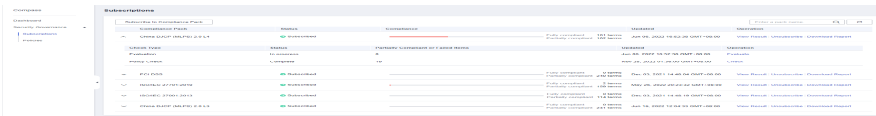
Step 3 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-4 Subscriptions page



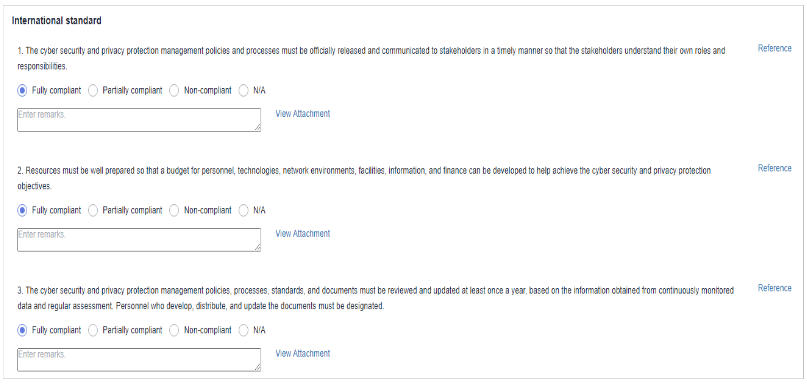
Step 4 Click on the left of the compliance pack to be self-assessed to expand the compliance pack information. In the Tenant Self-Assessment area, click **Evaluate** in the **Operation** column. The evaluation page is displayed.

Figure 6-5 Self-evaluation



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

Figure 6-6 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 6 After the evaluation is complete, click **Submit** in the lower right corner.

----End

6.7 Security Compliance Overview

Scenario

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

Prerequisites

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

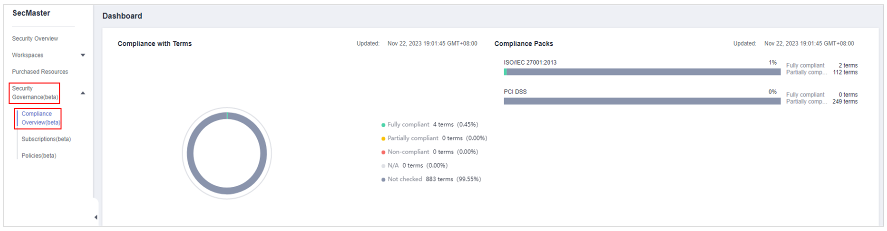
View the compliance with laws and regulations and standard clauses.

Step 1 Log in to the management console.

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

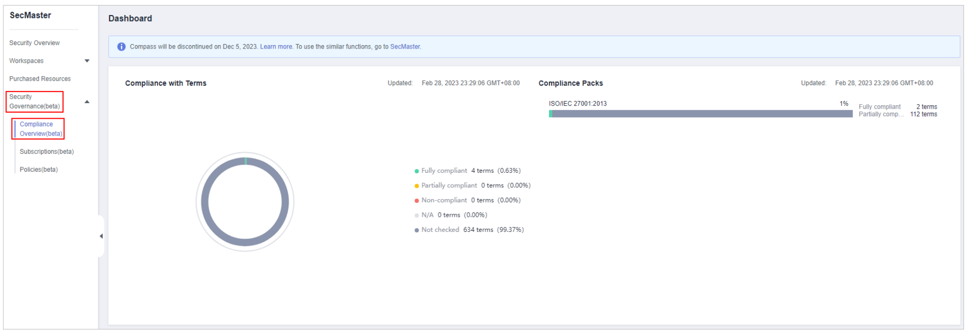
Step 3 In the navigation pane on the left, choose **Security Governance** > **Compliance Overview**. The **Compliance Overview** page is displayed.

Figure 6-7 Compliance overview page



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

Figure 6-8 Compliance with terms



----End

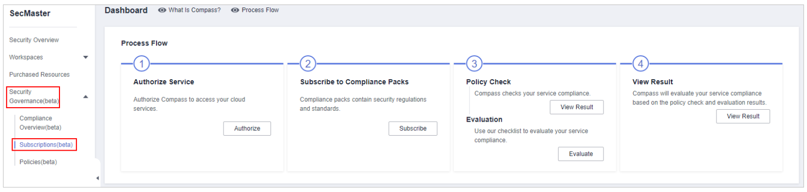
Viewing Policy Check Results

Step 1 Log in to the management console.

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

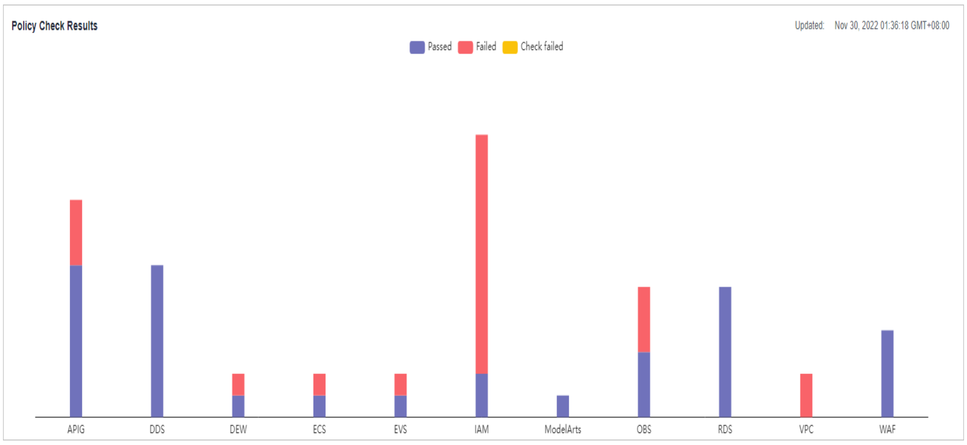
Step 3 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-9 Subscriptions page



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

Figure 6-10 Policy check results



----End

6.8 Evaluation Result

Scenario

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

Prerequisites

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

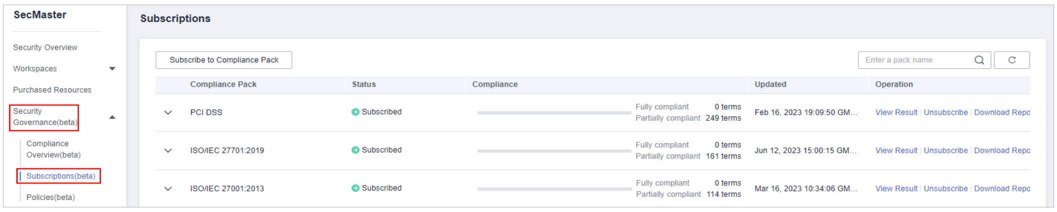
Procedure

Step 1 Log in to the management console.

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

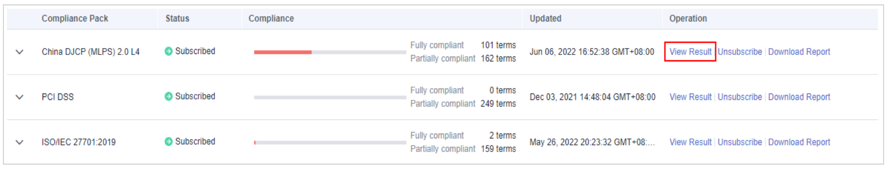
Step 3 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-11 Subscriptions page



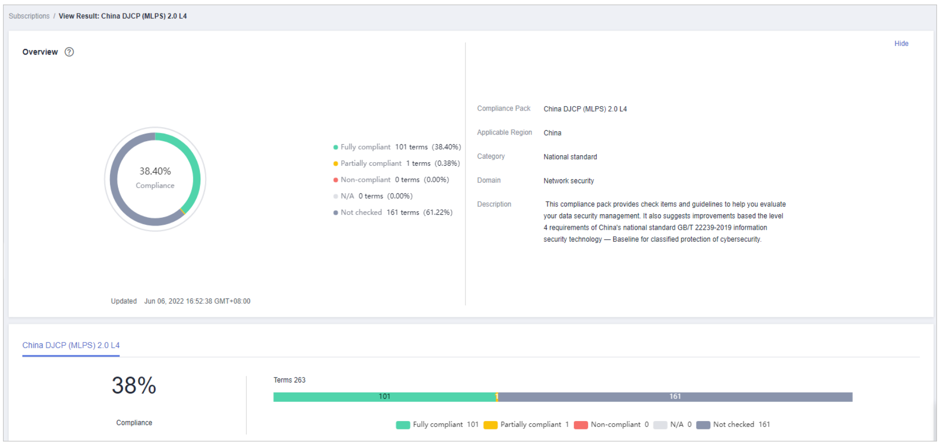
Step 4 Click **View Result** in the **Operation** column. The **Evaluation Result** page is displayed.

Figure 6-12 View result



Step 5 View the evaluation results.

Figure 6-13 Evaluation result page

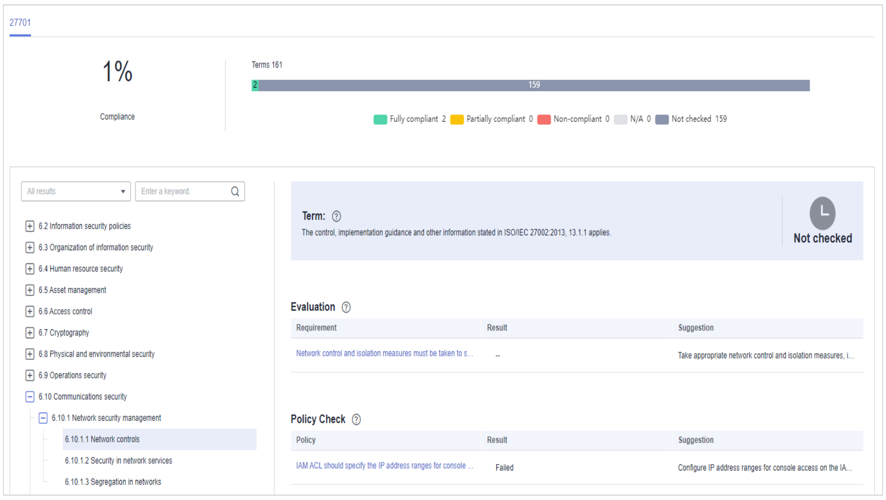


- View the overall compliance of the currently subscribed security compliance pack.
- To view the details of a term, select the clause in the navigation tree on the left. The details of the term are displayed on the right, including the term content, compliance status, and improvement suggestions.

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.

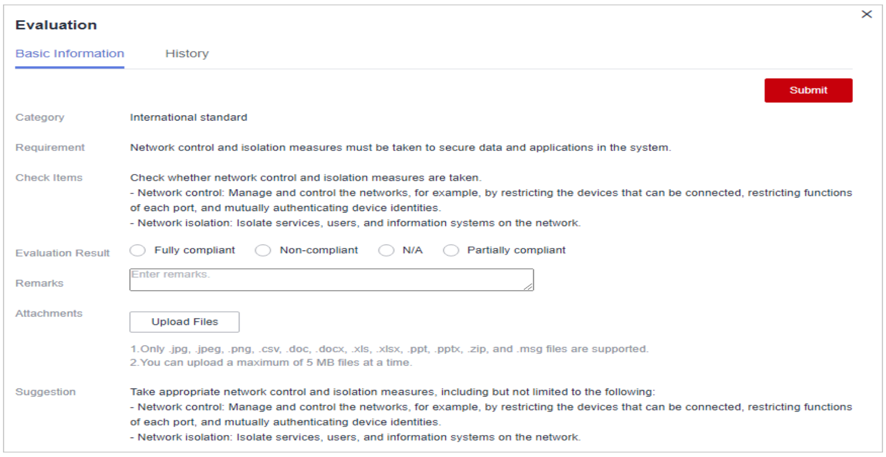
Figure 6-14 Selecting terms



  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 6-15 Self-evaluation



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

----End

6.9 Policy Check Result

Scenario

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

NOTE

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

Prerequisites

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

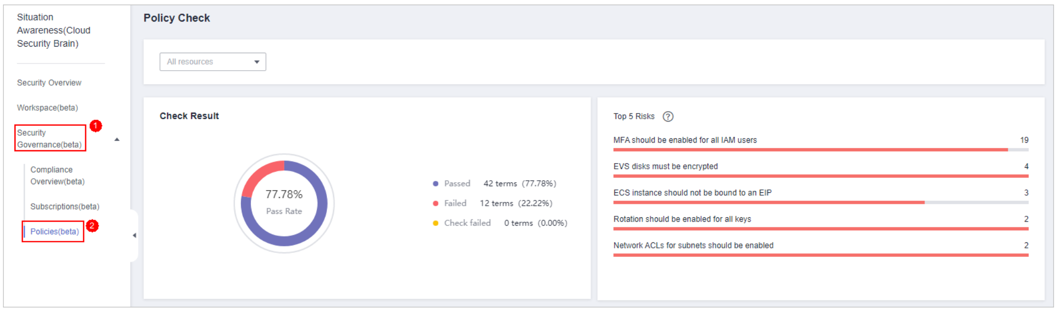
Procedure

Step 1 Log in to the management console.

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

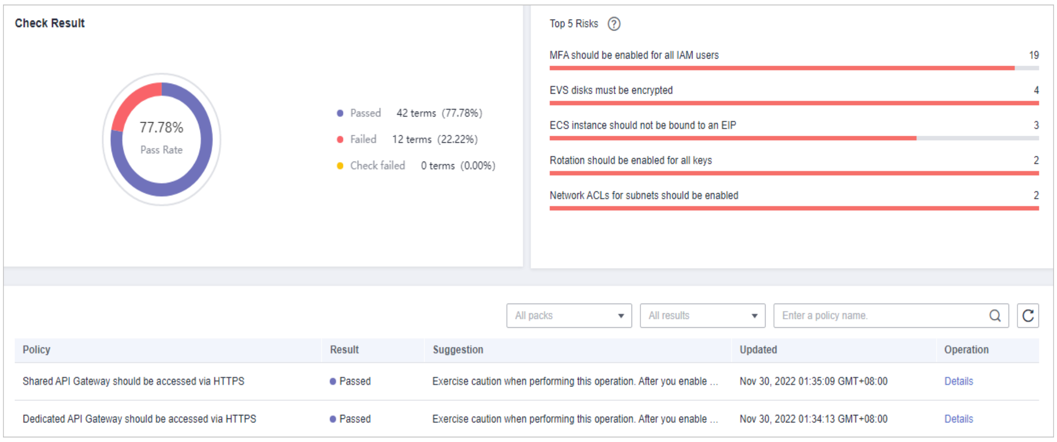
Step 3 In the navigation pane on the left, choose **Security Governance** > **Policies**. The **Policy Check** page is displayed.

Figure 6-16 Policy check page



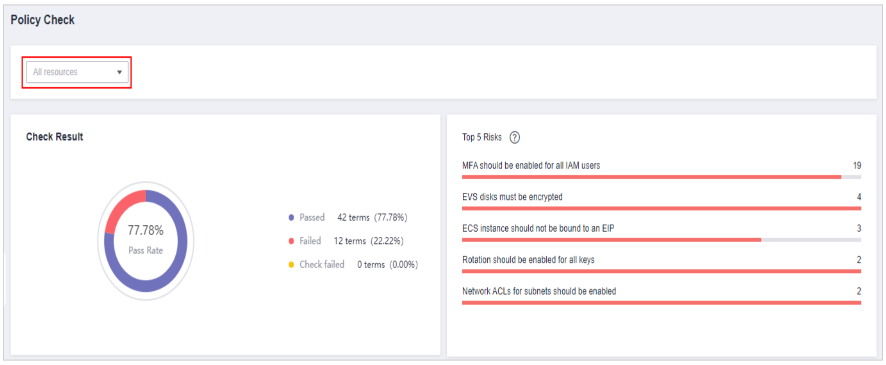
Step 4 View policy check result.

Figure 6-17 Policy check



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

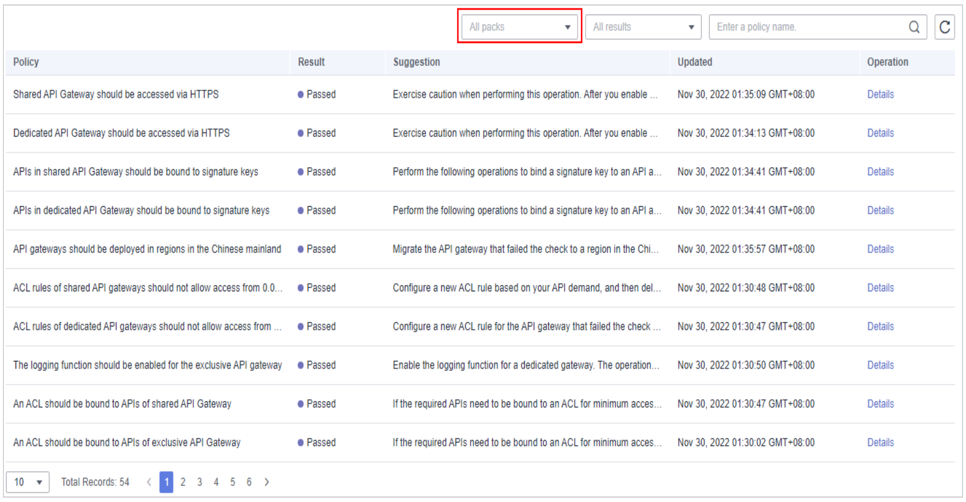
Figure 6-18 Selecting a resource



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

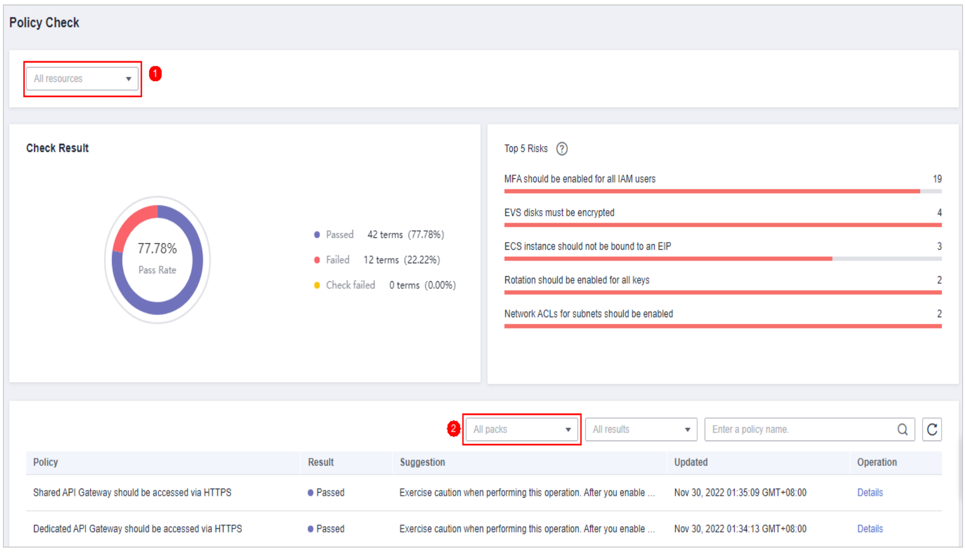
  You can also filter the results by result type or policy name.

Figure 6-19 Selecting a compliance pack



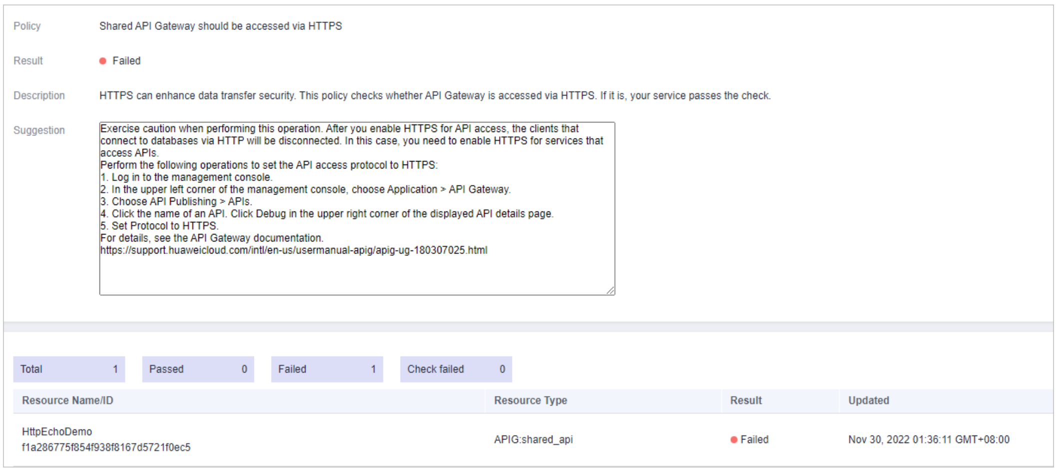
- To view the check result of a policy over a resource, select the corresponding resource from the filter box in the upper part, and then select the corresponding compliance pack in the upper part of the table.

Figure 6-20 Viewing the result of a policy over a resource



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

Figure 6-21 Details of a check



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

----End

6.10 Downloading a Compliance Report

Scenario

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

Prerequisites

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

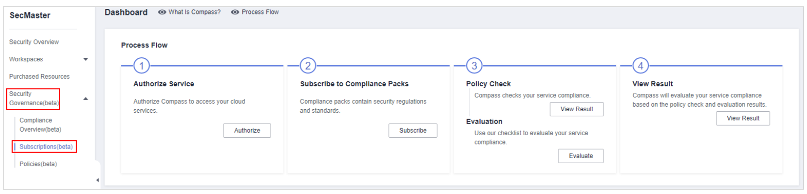
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-22 Subscriptions page



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

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

----End

6.11 Unsubscribing from a Compliance Pack

Scenario

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

Prerequisites

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

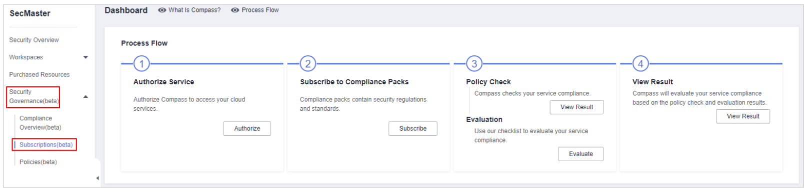
Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Governance** > **Subscriptions**. The **Subscriptions** page is displayed.

Figure 6-23 Subscriptions page



Step 4 On the **Subscriptions** page, locate the row that contains the security compliance pack to be unsubscribed from, click **Unsubscribe** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

NOTE

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

----End

7 Security Situation

7.1 Situation Overview

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

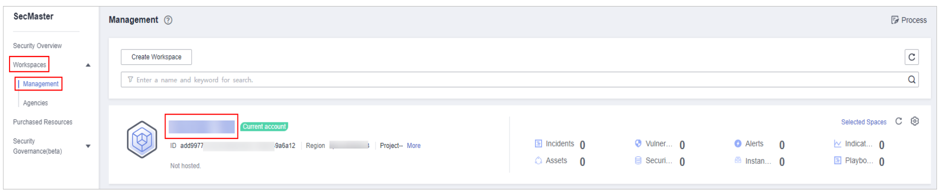
Procedure

Step 1 Log in to the management console.

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

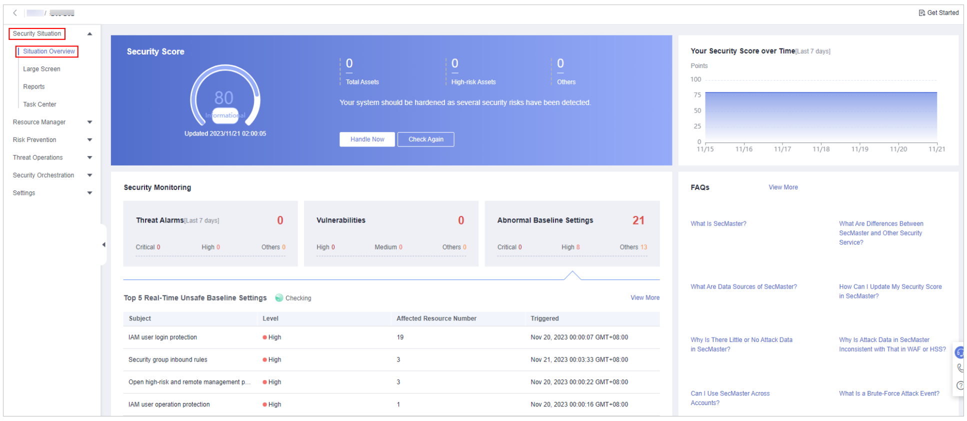
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-1 Workspace management page



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

Figure 7-2 Situation Overview



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

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

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

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

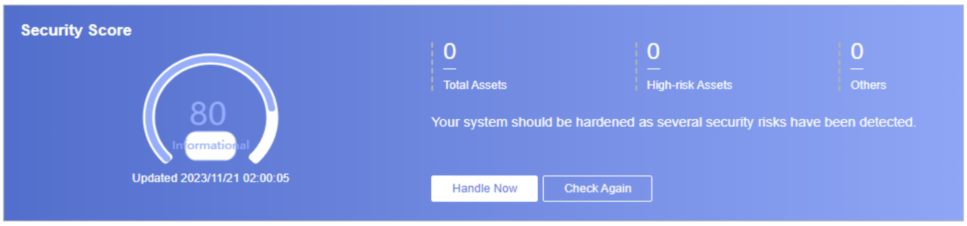
Parameter	Reference Period	Update Frequency	Description
Your Security Score over Time	Last 7 days	Every 5 minutes	Security scores in the last seven days.

----End

Security Score

The security score shows the overall health status of your workloads on the cloud based on the SecMaster edition you are using. You can quickly understand the unprocessed risks and their threats to your assets. **Figure 7-3** shows an example.

Figure 7-3 Security Score



- The security score is automatically updated at 02:00 every day. You can also click **Check Again** to update it immediately.
- The score ranges from 0 to 100. The higher the security score, the more secure your assets. For details, see **Security Scores and Unscored Items**.
- Different color blocks in the security score ring chart indicate different severity levels. For example, yellow indicates that your security is medium.
- Click **Handle Now**. The **Risks** pane is displayed on the right. You can handle risks by referring to the corresponding guidance.
  - The **Risks** slide-out panel lists all threats that you should handle in a timely manner. These threats are included in the **Threat Alarms**, **Vulnerabilities**, and **Abnormal Baseline Settings** areas.
  - The **Risks** pane displays the latest check results of the last scan. The **Alerts**, **Vulnerabilities**, and **Abnormal Baseline Settings** pages show check results of all previous scans. So, you will find the threat number on the **Risks** pane is less than that on those pages. You can click **Handle** for an alert on the **Risks** pane to go to the corresponding page quickly.
  - **Handling detected security risks:**
    i. In the **Security Score** area, click **Handle Now**.
    ii. On the **Risks** slide-out panel displayed, click **Handle**.
    iii. On the page displayed, handle risk alerts, vulnerabilities, or baseline inspection items.

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

  NOTE

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

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

Security Scores and Unscored Items

SecMaster assesses the overall security situation of your cloud assets in real time and scores your assets.

This section describes how your security score is calculated.

- Security Score

  SecMaster evaluates the overall security situation of your assets.

  – There are six risk severity levels, **Secure**, **Informational**, **Low**, **Medium**, **High**, and **Critical**.

  – The score ranges from 0 to 100. The higher the security score, the lower the risk severity level.

  – The security score starts from **0** and the risk severity level is escalated up from **Secure** to the next level every 20 points. For example, for scores ranging from **40** to **60**, the risk severity is **Medium**.

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

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

    NOTE

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

Table 7-2 Security score table

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

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

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

Table 7-3 Unscored check items

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

Category	Unscored Item	Points	Suggestion	Maximum Unscored Point
	Medium-risk vulnerabilities not fixed	2		
	Low-risk vulnerabilities not fixed	0.1		
Threat Alerts	Critical alerts not fixed	10	Fix the threats by referring to the suggestions. The security score will be updated accordingly.	30
	High-risk alerts not fixed	5		
	Medium-risk alerts not fixed	2		
	Low-risk alerts not fixed	0.1		

Security Monitoring

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

Figure 7-4 Security Monitoring

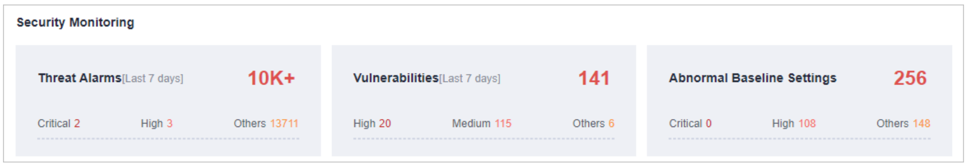


Table 7-4 Security Monitoring parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Threat Alarms</td><td>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 Alerts.

Figure 7-5 Viewing real-time alerts


</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Vulnerabilities</td><td>
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.

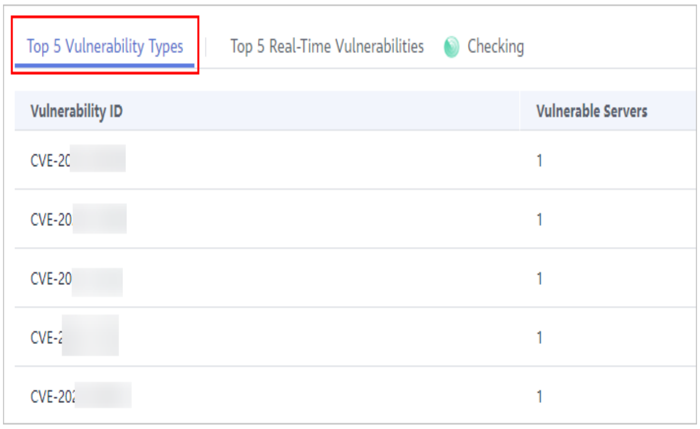
Risk severity levels:

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 top 5 vulnerability types.

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.

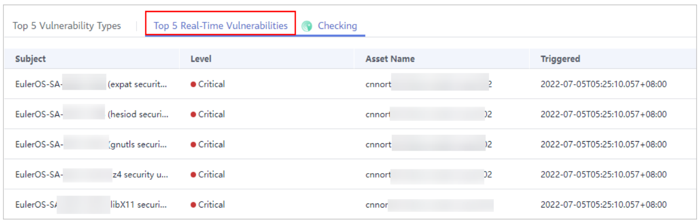
Figure 7-6 Top 5 Vulnerability Types



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.

</td></tr>
</table>

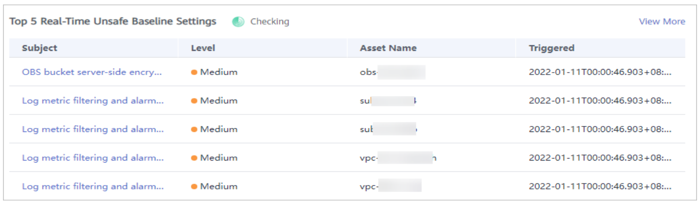
Parameter	Description
	– If no data is available here, no vulnerabilities are detected on the current day. – You can click **View More** to go to the **Vulnerabilities** page and view more vulnerabilities. You can also customize filter criteria to query vulnerability information. For details, see **Viewing Vulnerability Details**. **Figure 7-7** Viewing real-time vulnerabilities 

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Abnormal Baseline Settings</td><td>

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 for the last 30 days, click the **Abnormal Baseline Settings** panel.
  - You can view details of the top compliance risks discovered in the latest check, such as check item name, severity, asset name, and discovery time.
  - If no data is available, no compliance violations are detected for the last 30 days.
  - You can click **View More** to go to the **Baseline Inspection** page and view more compliance risks. You can also customize filter criteria to make an advanced search. For details, see **Viewing Baseline Inspection Results**.

Figure 7-8 Viewing compliance risks

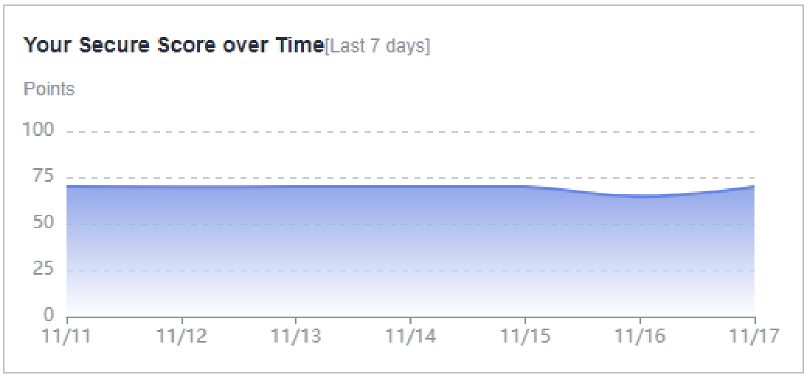


</td></tr>
</table>

Your Security Score over Time

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

Figure 7-9 Your Security Score over Time



7.2 Large Screen

7.2.1 Overall Situation Screen

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

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

Prerequisites

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

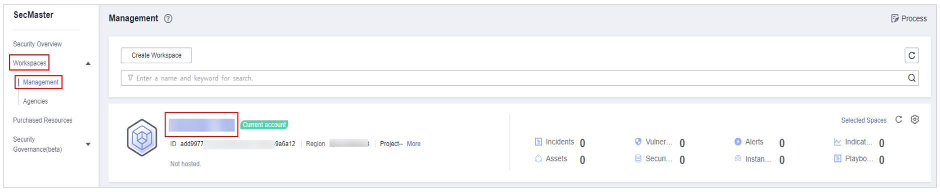
Procedure

Step 1 Log in to the management console.

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

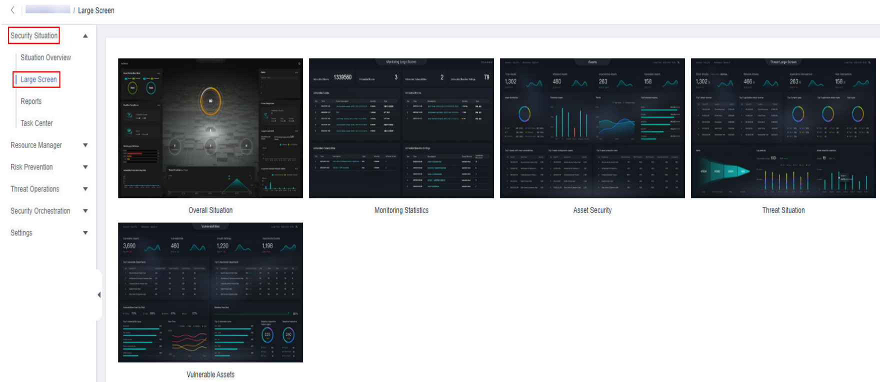
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-10 Workspace management page



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

Figure 7-11 Large Screen



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

This screen includes many graphs.

Figure 7-12 Overall Situation screen

----End

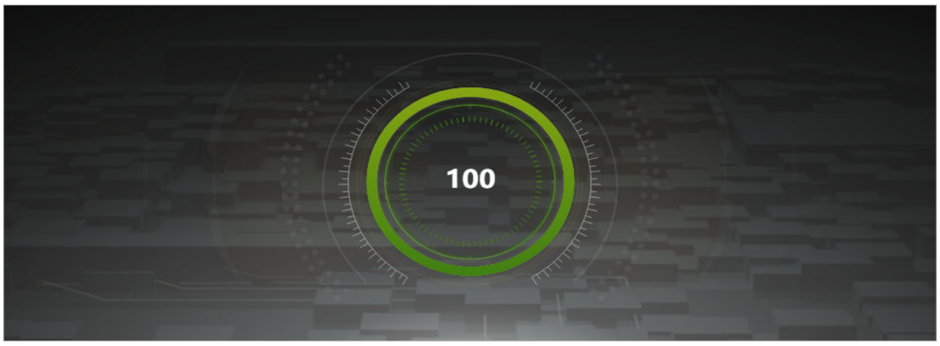
Security Score

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

Table 7-5 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 7-13 Security Score



Alert Statistics

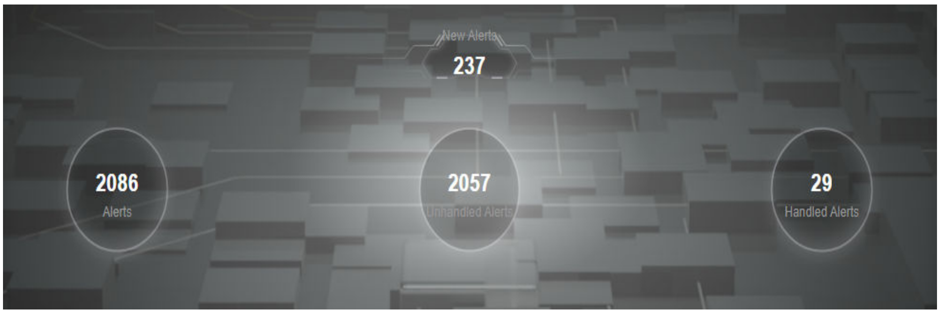
The alert statistics of interconnected services are displayed, as shown in **Figure 7-14**.

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

Table 7-6 Alert statistics

Parameter	Reference Period	Update Frequency	Description
New Alerts	Today	5 minutes	Number of new alerts generated on the current day.
Threat Alerts	Last 7 days	5 minutes	Number of new alerts generated in the last seven days.
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 7-14 Alert Statistics



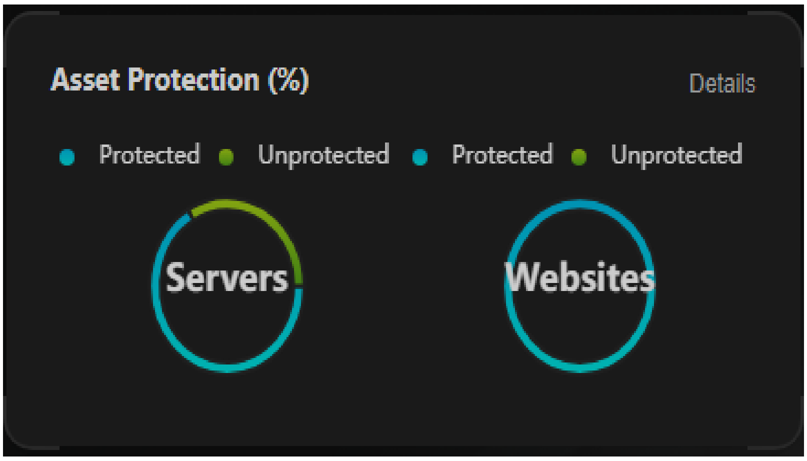
Asset Protection

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

Table 7-7 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 7-15 Asset protection rate



Baseline Inspection

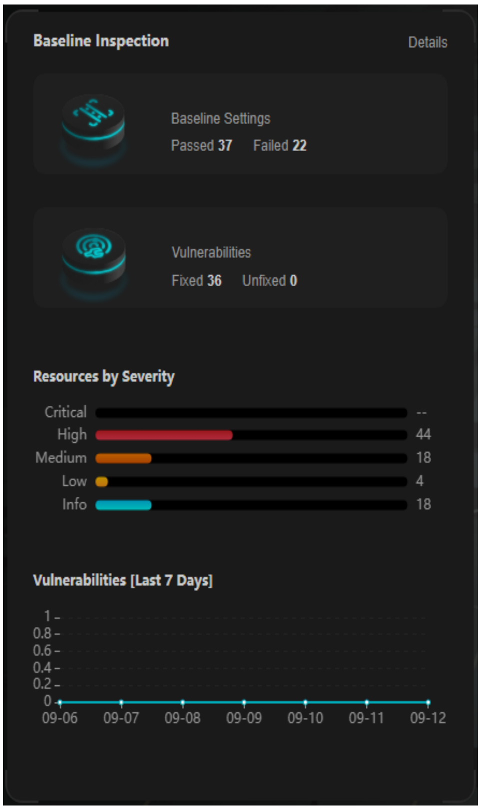
The fixing status of the baseline configuration and vulnerabilities of your assets, distribution of risky resources, and vulnerability fixing trend within seven days are displayed, as shown in **Figure 7-16**.

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

Table 7-8 Baseline inspection

Parameter	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 7-16 Baseline Inspection



Recent Threats

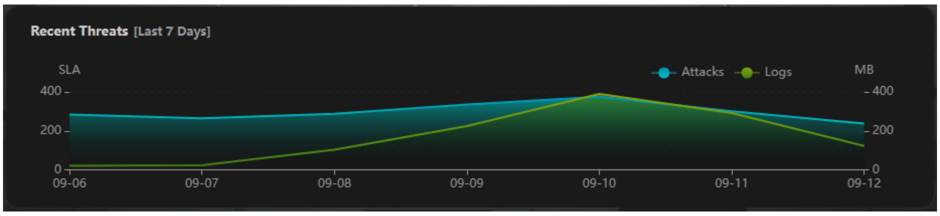
The numbers of threatened assets and security logs reported every day in the last seven days are displayed, as shown in **Figure 7-17**.

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

Table 7-9 Recent threats

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

Figure 7-17 Recent threats



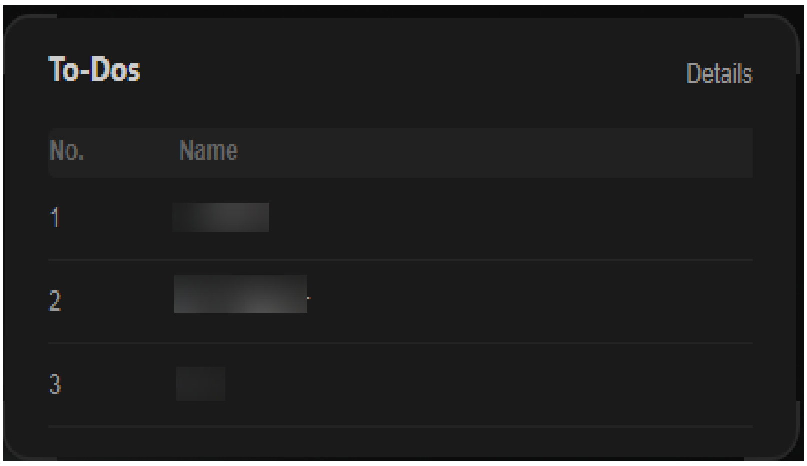
To-Dos

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

Table 7-10 To-dos

Parameter	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 7-18 To-Dos



Resolved Issues

The alert handling status, SLA and MTTR fulfillment rate in the last seven days, and automatic incident handling statistics in the last seven days are displayed, as shown in **Figure 7-19**.

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

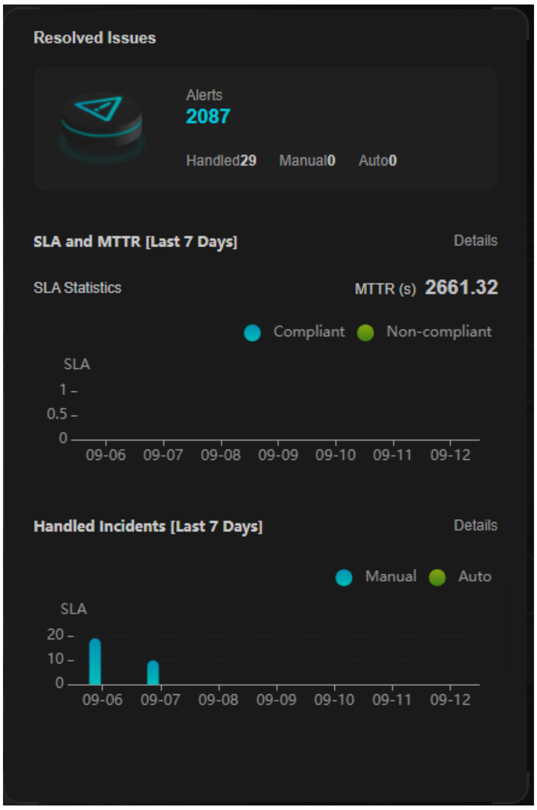
Table 7-11 Resolved issues

Parameter		Reference Period	Update Frequency	Description
Alerts	Alerts	Last 7 days	5 minutes	Number of new alerts generated in the last seven days.
	Handled			Number of alerts that have been cleared in the last seven days.
	Manual			Number of alerts that were handled within the SLA time in the last seven days. Alerts handled as planned and earlier than planned are counted.

Parameter		Reference Period	Update Frequency	Description
	Auto			Number of alerts that were automatically handled by SecMaster playbooks. To determine how an alert was handled, check whether the value of **close_comment** is **ClosedByCSB** or **ClosedBySecMaster** in the alert details. If it is, the alert was automatically handled. If it is not, the alert was manually handled.
SLA and MTTR [Last 7 Days]	SLA Statistics	Last 7 days	5 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.

Parameter	Reference Period	Update Frequency	Description
Handled Incidents [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 7-19 Resolved issues



7.2.2 Monitoring Statistics Screen

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

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

Prerequisites

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

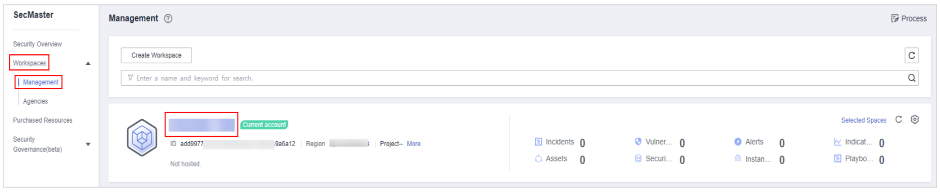
Procedure

Step 1 Log in to the management console.

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

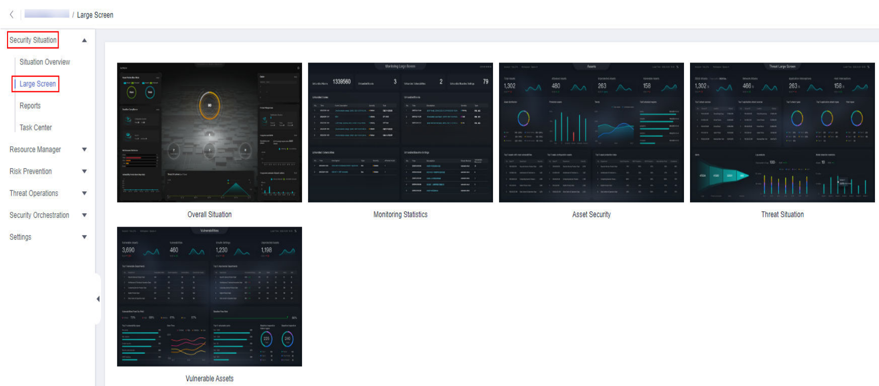
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-20 Workspace management page



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

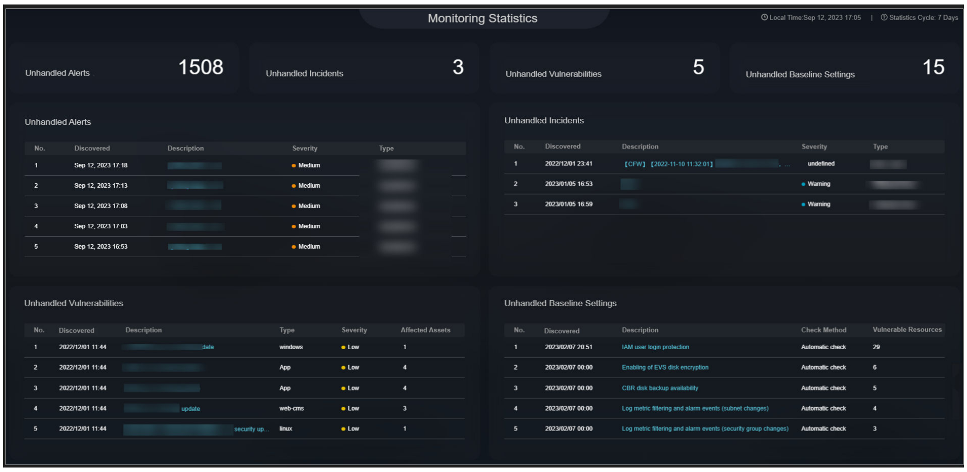
Figure 7-21 Large Screen



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

This screen includes many graphs.

Figure 7-22 Monitoring Statistics Large Screen



----End

Monitoring Statistics Overview

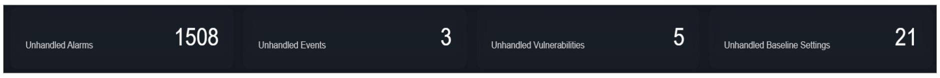
This screen displays the total number of unhandled alerts, incidents, vulnerabilities, and unsafe baseline settings.

Table 7-12 Monitoring Statistics Overview

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

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

Figure 7-23 Monitoring Statistics Overview



Unhandled Alerts

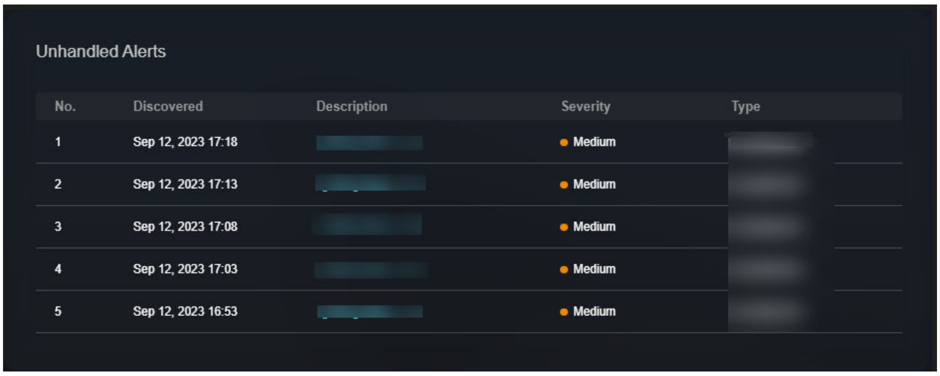
The table lists information about top 5 unhandled threat alerts, including the alert discovery time, alert description, alert severity, and alert type.

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

Table 7-13 Unhandled Alerts

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

Figure 7-24 Unhandled Alerts



Unhandled Incidents

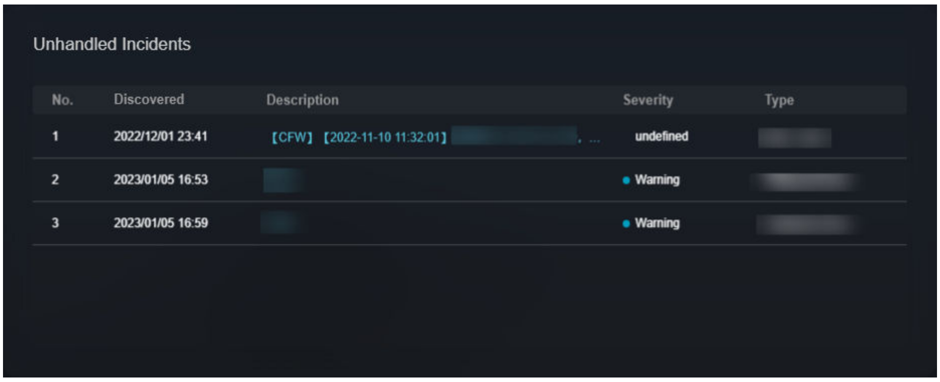
The table lists information about the top 5 unhandled incidents, including the incident discovery time, description, severity, and type.

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

Table 7-14 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. To view details about the alert statistics, choose **Threat Operations** > **Alerts** in the current workspace.

Figure 7-25 Unhandled Incidents



Unhandled Vulnerabilities

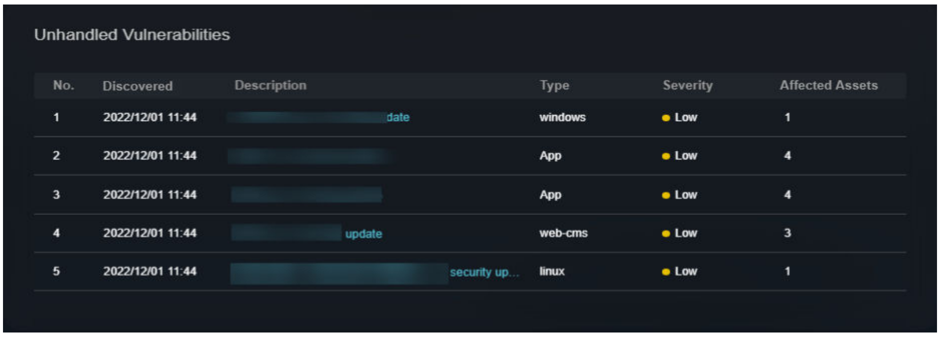
The table lists information about the top 5 unhandled vulnerabilities, including the discovery time, description, type, severity, and number of affected assets.

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

Table 7-15 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 7-26 Unhandled Vulnerabilities



Unhandled Baseline Settings

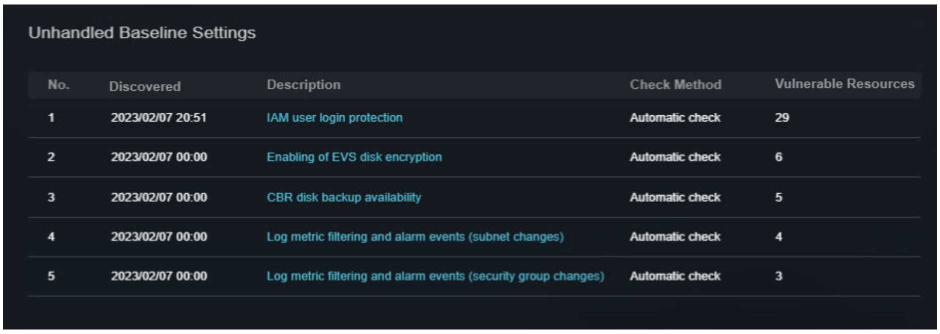
This table lists information about the top 5 unhandled unsafe baseline settings, including the discovery time, description, check method, and total number of vulnerable resources.

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

Table 7-16 Unhandled Baseline Settings

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

Figure 7-27 Unhandled Baseline Settings



Unhandled Baseline Settings

No.	Discovered	Description	Check Method	Vulnerable Resources
1	2023/02/07 20:51	IAM user login protection	Automatic check	29
2	2023/02/07 00:00	Enabling of EVS disk encryption	Automatic check	6
3	2023/02/07 00:00	CBR disk backup availability	Automatic check	5
4	2023/02/07 00:00	Log metric filtering and alarm events (subnet changes)	Automatic check	4
5	2023/02/07 00:00	Log metric filtering and alarm events (security group changes)	Automatic check	3

7.2.3 Asset Security Screen

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

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

Prerequisites

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

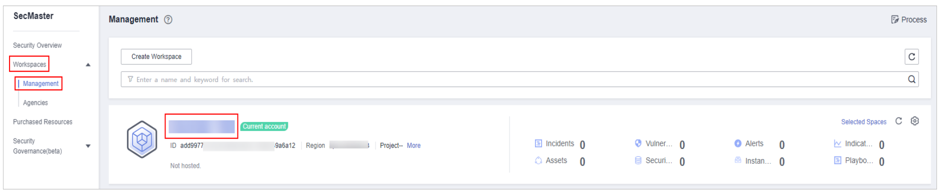
Procedure

Step 1 Log in to the management console.

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

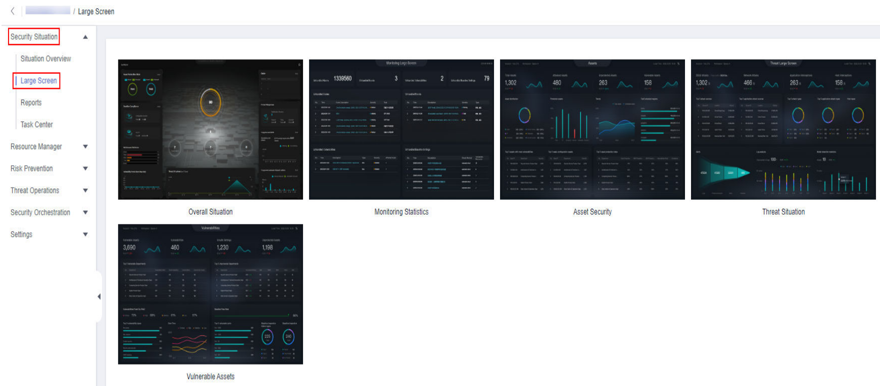
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-28 Workspace management page



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

Figure 7-29 Large Screen



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

This screen includes many graphs.

Figure 7-30 Asset Security Screen

----End

Asset Security Screen Overview

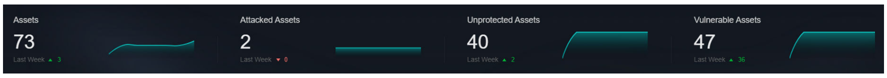
On this screen, you can view the total numbers of assets, attacked assets, unprotected assets, vulnerabilities, and assets with unsafe settings in the current workspace.

Table 7-17 Asset Security Screen

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

Parameter	Statistical Period	Update Frequency	Description
Unprotected Assets	Real-time	Hourly	Number of assets for which security protection is not enabled, for example, ECSs for which HSS is not enabled and EIPs for which DDoS is not enabled. Unprotected assets include the assets managed on the **Resource Manager** page and with no corresponding security controls enabled.
Assets with Vulnerabilities or Unsafe Settings	Real-time	Hourly	These assets include assets affected by vulnerabilities and assets have unsafe settings discovered during baseline inspection. The duplicated assets are counted only once. The vulnerability data comes from **Risk Prevention** > **Vulnerabilities**, and the baseline inspection data comes from **Risk Prevention** > **Baseline Inspection** > **Resources to Check**.

Figure 7-31 Asset Security Screen



Asset Distribution

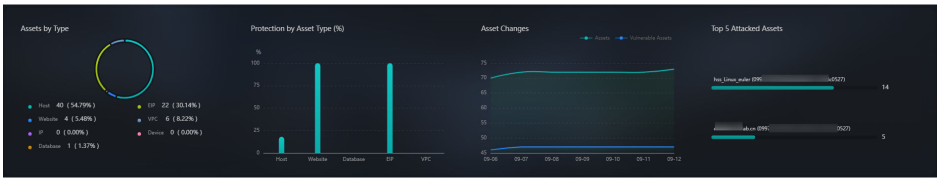
In this area, you can view assets by type, asset protection rate, asset change trend, and distribution of the five assets attacked most.

Table 7-18 Asset Distribution

Parameter	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.

Parameter	Statistical Period	Update Frequency	Description
Asset Changes	Last 7 days	Hourly	Statistics on the total number of assets, and the number of assets with vulnerabilities and unsafe settings in the last seven days.
Top 5 Attacked Assets	Last 7 days	Hourly	Top 5 attacked assets in the last seven days and the number of attacks. The data comes from **Threat Operations** > **Alerts**. You can view details on this page.

Figure 7-32 Asset Distribution



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

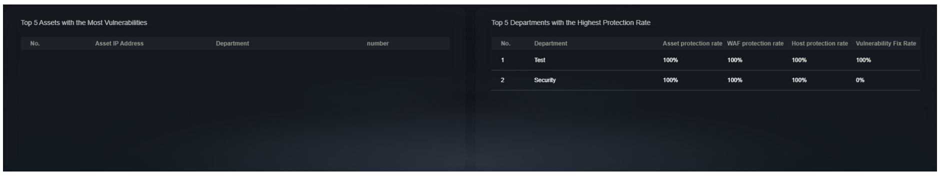
In this area, you will see the five assets with the most vulnerabilities and the five departments with the highest protection rate.

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

Parameter	Statistical Period	Update Frequency	Description
Top 5 Assets with the Most Vulnerabilities	Real-time	Hourly	Top 5 assets with the most vulnerabilities in different departments. This data is generated based on the assets affected by vulnerabilities in **Risk Prevention** > **Vulnerabilities**. Note that the assets must have department details provided, or the affected assets may fail to be counted toward this data.

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

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



7.2.4 Threat Situation Screen

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

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

Prerequisites

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

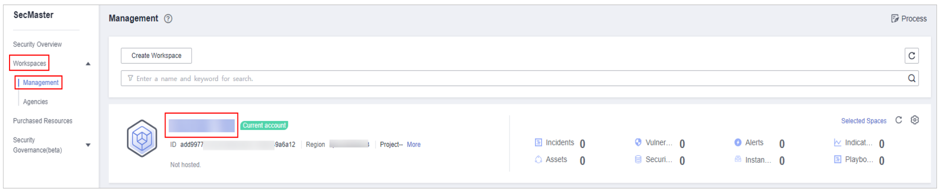
Procedure

Step 1 Log in to the management console.

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

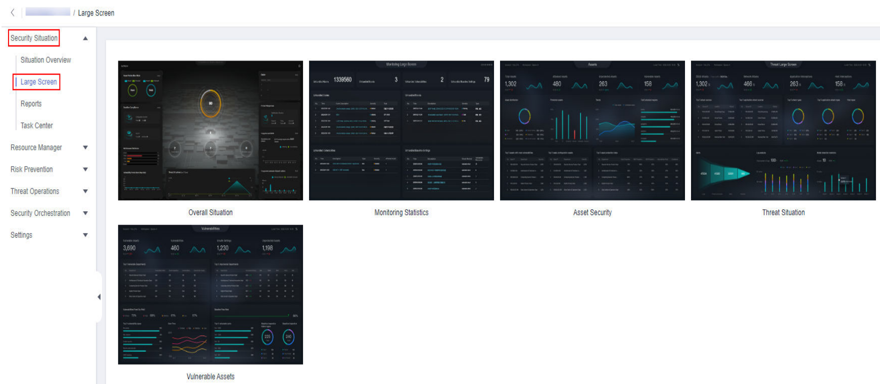
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-34 Workspace management page



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

Figure 7-35 Large Screen



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

This screen includes many graphs.

Figure 7-36 Threat Situation screen

----End

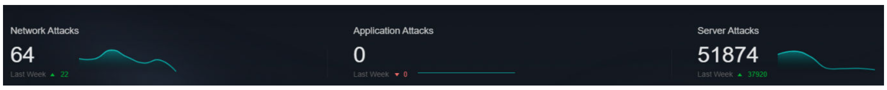
Threat Situation screen

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

Table 7-20 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 7-37 Threat Situation screen



Attack Source Distribution

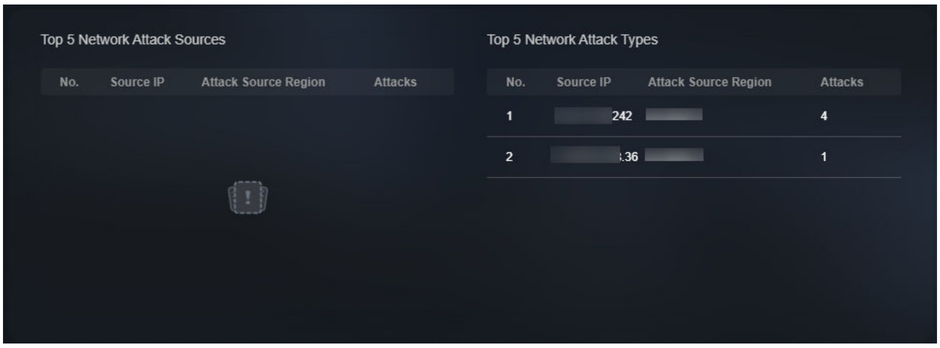
This graph displays the five attack sources who launched the most attacks against the network and application layers. You will see attacked asset details, including IP addresses, departments, and quantity.

Table 7-21 Attack source distribution

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

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

Figure 7-38 Attack source distribution



Attacks by Type

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

Table 7-22 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 **Alerts** page under **Threat Operations** in the current workspace.

Figure 7-39 Attack type distribution

Threat Situation Statistics

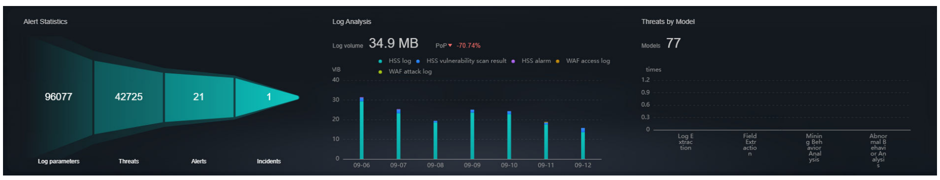
This graph shows the statistics about alerts, logs, and threat detection models in the current account.

Table 7-23 Threat Situation Statistics

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

Parameter		Statistical Period	Update Frequency	Description
	Incidents			This number reflects incidents collected in **Threat Operations** > **Incidents** for the last seven days.
Log Analysis	Log volume	Last 7 days	Hourly	Total volume 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	The number includes the models in **Threat Operations** > **Intelligent Modeling**.
	Statistical table	Last 7 days	Hourly	Number of threats detected by each type of threat detection model. If there is no threat detection model, four default types with zero threats detected are displayed.

Figure 7-40 Threat situation statistics



7.2.5 Vulnerable Assets Screen

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

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

Prerequisites

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

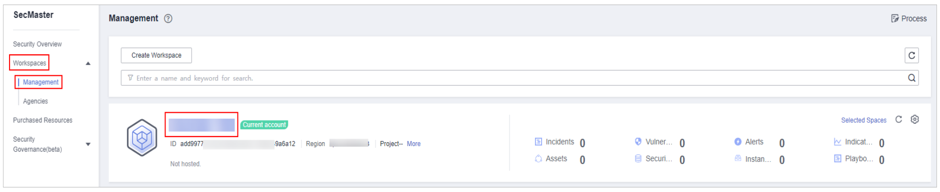
Procedure

Step 1 Log in to the management console.

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

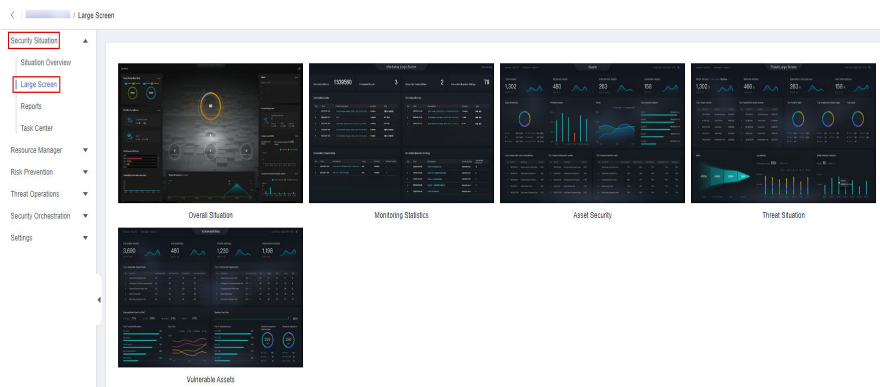
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-41 Workspace management page



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

Figure 7-42 Large Screen



Step 5 Click the **Vulnerable Assets** image to go to the information page.

This screen includes many graphs.

Figure 7-43 Vulnerable Assets Screen

----End

Vulnerable Assets Overview

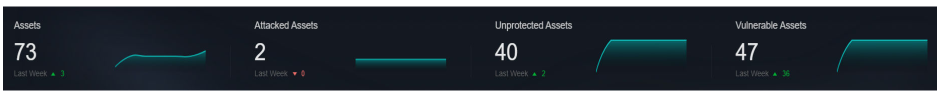
This graph displays the total numbers of vulnerable assets, vulnerabilities, unsafe baseline settings, and unprotected assets.

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

Table 7-24 Vulnerable Assets Overview

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

Figure 7-44 Vulnerable Assets Screen



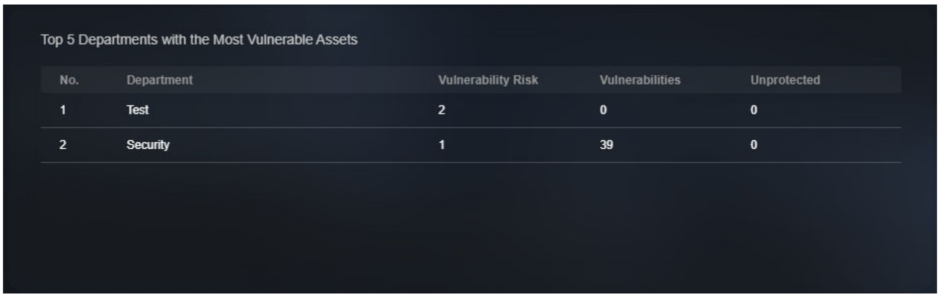
Top 5 Departments with the Most Vulnerabilities

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

Table 7-25 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 7-45 Top 5 Vulnerable Departments



Top 5 Department with the Most Unprotected Assets

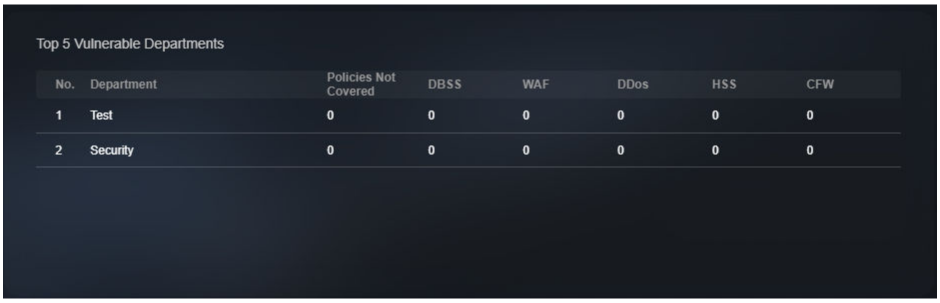
This graph displays the 5 departments with the most failed protection policies. You can view the details about these departments, including the department name and what protection policies they failed, such as DBSS, WAF, Anti-DDoS, HSS, and CFW

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

Table 7-26 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 7-46 Top 5 Department with the Most Unprotected Assets



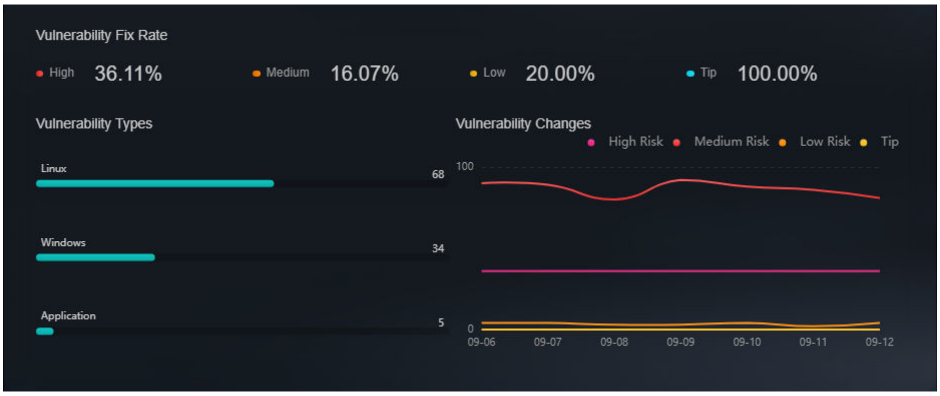
Vulnerability Fix Rate

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

Table 7-27 Vulnerability fix rate

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

Figure 7-47 Vulnerability fixing rate



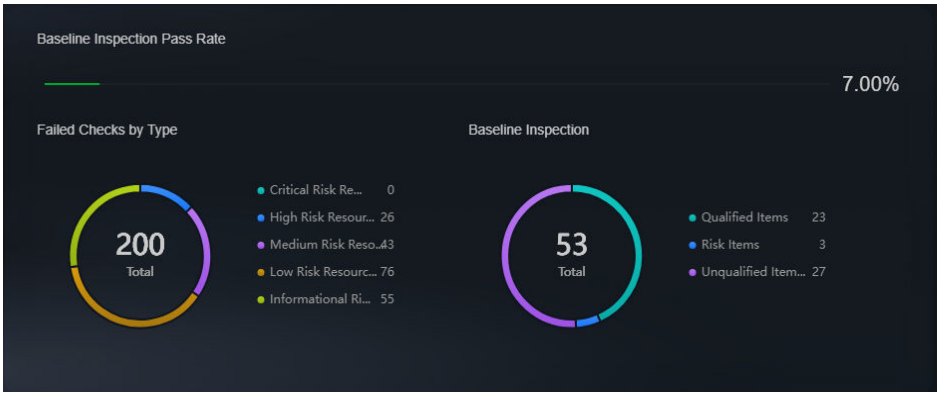
Baseline Inspection Pass Rate

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 7-28 Baseline Inspection Pass Rate

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

Figure 7-48 Baseline Inspection Pass Rate



7.3 Reports

7.3.1 Creating and Copying a Security Report

Scenario

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

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

Limitations and Constraints

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

Prerequisites

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

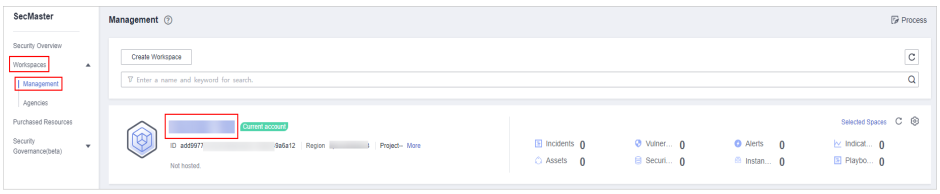
Creating a Report

Step 1 Log in to the management console.

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

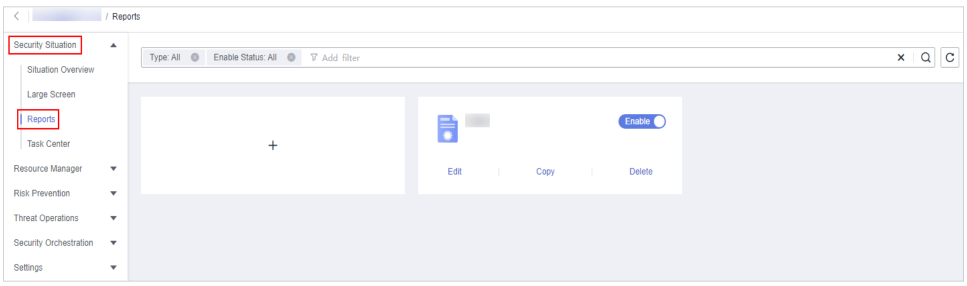
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-49 Workspace management page



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

Figure 7-50 Reports



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

Step 6 Configure basic information of the report.

Table 7-29 Report parameters

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

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

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

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

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

- Downloading a report
  a. Click in the upper left corner of the preview page on the right.
  b. In the displayed dialog box, select a report format, and click **OK**.
     The system automatically downloads the report to the local PC.
- Viewing a report in full screen: Click in the upper left corner of the preview page on the right.

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

----End

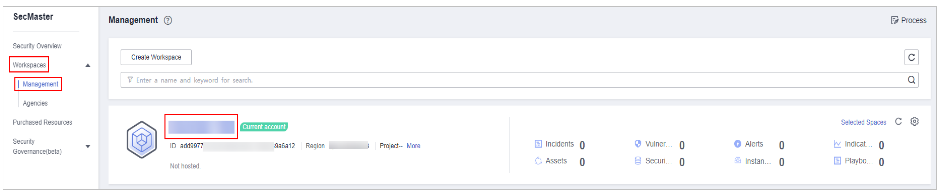
Copying a Report

Step 1 Log in to the management console.

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

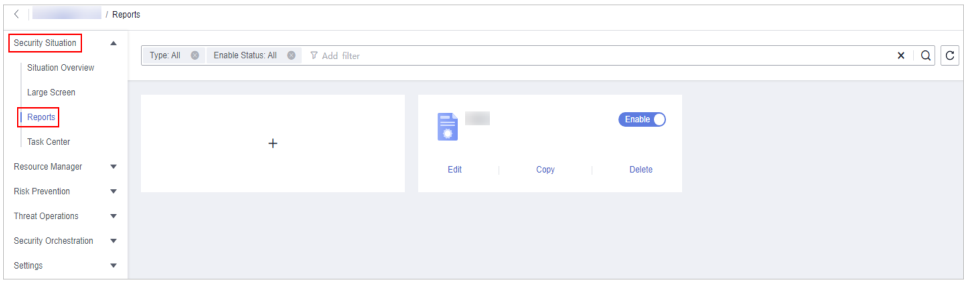
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-51 Workspace management page



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

Figure 7-52 Reports



Step 5 Select a report template and click **Copy**.

Step 6 Edit basic information of the report.

Step 7 Click **Next: Report Choose**. The report configuration page is displayed.

- Downloading a report
  a. Click in the upper left corner of the preview page on the right.
  b. In the displayed dialog box, select a report format, and click **OK**.
     The system automatically downloads the report to the local PC.
- Viewing a report in full screen: Click in the upper left corner of the preview page on the right.

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

----End

7.3.2 Viewing a Security Report

Scenario

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

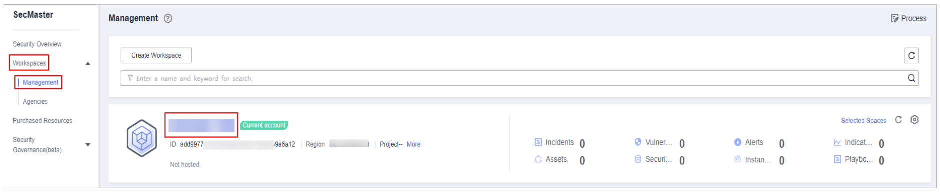
Procedure

Step 1 Log in to the management console.

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

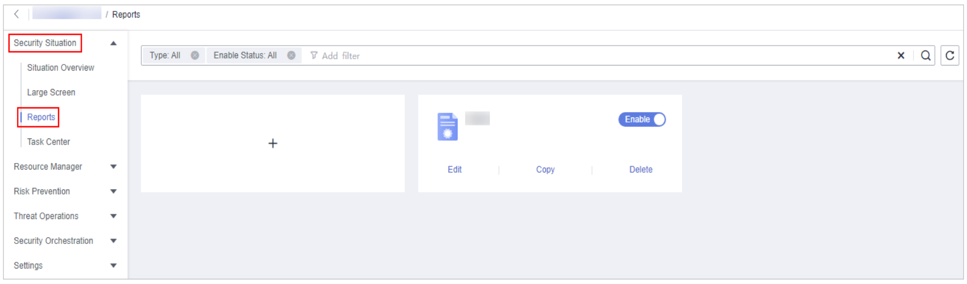
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-53 Workspace management page



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

Figure 7-54 Reports



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

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

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

----End

Content in the Daily Report Template

Table 7-30 Content in the daily report template

Parameter	Description
Data Scope	The default data scope of a daily report is from 00:00:00 to 23:59:59 on the previous day.
Security Score	SecMaster evaluates and scores your asset security for the previous day (from 00:00:00 to 23:59:59) so that you can quickly learn of the overall security posture of assets. This score varies depending on the SecMaster edition you are using.

Parameter	Description
Baseline Inspection	Displays the statistics of the latest baseline check, including the following information: ● The number of baseline check items ● Number of compliance check items in the latest baseline check ● Non-compliant check items in the latest baseline check
Security Vulnerabilities	Displays the vulnerability statistics of the accessed cloud services **on the previous day**, including the following information: ● Number of vulnerabilities ● Number of unfixed vulnerabilities
Policy Coverage	Displays the coverage of current security products, including the following information: ● Number of instances protected by security products (= Number of protected ECSs + Number of websites protected with WAF instances) ● HSS coverage (= Number of protected ECSs/Total number of ECSs) ● Number of protected cloud servers ● Protected websites
Asset Security	Displays the current asset security status, including the following information: ● Total number of current assets ● Number of vulnerable assets
Security Analysis	Displays the security analysis statistics of **the previous day**, including the following information: ● Total traffic of security logs on the previous day ● Number of security log models
Security Response (Overview)	Displays the security response statistics for **the previous day**, including the following information: ● Number of security alerts handled ● Number of confirmed intrusion incidents ● Number of executed automatic response playbooks ● Percentage of alerts handled by automatic playbooks ● Average MTTR ● Number of confirmed high-risk intrusion incidents

Parameter	Description
Asset risks	Displays the asset security status for **the previous day**, including the following information: • Number of attacked assets • Number of unprotected assets • Number of vulnerable assets • Asset change trend over the last seven days as of the previous day • Asset protection rate
Threat posture	Displays the threat posture of assets **on the previous day**, including the following information: • Number of DDoS attacks • Number of network attacks • Number of application attacks • Number of server attacks • DDoS inspection findings • Network and server attack changes • WAF inspection findings • Top 5 network attack types • Top 5 application attack type statistics • Top 5 server attack type statistics • Top 5 application attack sources distribution • Top 5 attacked application distribution • Top 5 server alert distribution • Top 5 network attack sources distribution • HSS inspection findings
Log analysis	Displays the log analysis results for **the previous day**, including the following information: • Number of log sources on the previous day • Number of log indexes on the previous day • Total number of logs received on the previous day • Log volume stored on the previous day • Log change trend over the last seven days as of the previous day • Access traffic statistics of top 5 log sources over the last seven days as of the previous day • Number of alerts generated by top 10 models on the previous day

Parameter	Description
Security Response (Details)	Displays the security response information for **the previous day**, including the following information: ● Number of alerts handled on the previous day ● Number of incidents handled on the previous day ● Number of vulnerabilities fixed on the previous day ● Number of unsafe baseline settings fixed on the previous day ● Threat alert distribution and quantity on the previous day ● Top 5 intrusion incidents by type on the previous day ● Top 5 emergency responses on the previous day ● Top 20 threat alerts handled on the previous day
External Security Info	Displays information about external security hotspots for **the previous day**.

Content in the Weekly Report Template

Table 7-31 Content in the **Weekly** Report Template

Parameter	Description
Data Scope	SecMaster collects security information from 00:00 on Monday to 24:00 on Sunday of the previous week.
Security Score	SecMaster evaluates and scores your asset security for the last day of the previous week so that you can quickly learn of the overall security posture of assets. This score varies depending on the SecMaster edition you are using.
Baseline Inspection	Displays the statistics of the latest baseline check in the previous week, including the following information: ● The number of baseline check items ● Number of compliance check items in the latest baseline check ● Non-compliant check items in the latest baseline check
Security vulnerabilities	Displays the vulnerability statistics of the accessed cloud services **for the last week**, including the following information: ● Number of vulnerabilities. ● Number of unfixed vulnerabilities

Parameter	Description
Policy Coverage	Displays the latest asset security information on the last day of the previous week, including the following information: • Number of instances protected by security products (= Number of protected ECSs + Number of websites protected with WAF instances) • HSS coverage (= Number of protected ECSs/Total number of ECSs) • Number of protected cloud servers • Protected websites
Asset security	Displays the latest asset security information on the last day in the last week, including the following information: • Total number of assets • Number of vulnerable assets
Security analysis	Displays the security analysis statistics, including the following information: • Total security log traffic of last week • Number of security log models on the last day of the last week
Security Response (Overview)	Displays the security response information for the previous week, including the following information: • Number of security alerts handled over the previous week • Number of confirmed intrusion incidents over the previous week • Number of executed automatic response playbooks • Percentage of alerts handled by automatic playbooks • Average MTTR • Number of confirmed high-risk intrusion incidents
Asset risks	Displays the latest asset security information on the last day of the previous week, including the following information: • Week-over-week changes on attacked asset quantity in monthly reports • Week-over-week changes on unprotected asset quantity in monthly reports • Week-over-week changes on vulnerable asset quantity in monthly reports • Asset changes over the previous week • Asset protection (%)

Parameter	Description
Threat posture	Displays the latest threat posture n on the last day of the previous week, including the following information: ● Number of DDoS attacks ● Number of network attacks ● Number of application attacks ● Number of server attacks ● DDoS inspection findings ● Network attack changes ● WAF inspection findings ● Top 5 network attack types ● Top 5 application attack types ● Top 5 server attack types ● Top 5 application attack sources distribution ● Top 5 attacked application distribution ● Top HSS alert distribution ● Top 5 network attack sources distribution ● HSS inspection findings
Log analysis	Displays the log analysis results for **the previous week**, including the following information: ● Number of log sources ● Number of log indexes ● Total number of received logs ● Log storage ● Log volume changes ● Top 5 log source access statistics ● Number of alerts generated by top 10 models on the previous day
Security Response (Details)	Displays the security response information for **the previous week**, including the following information: ● Number of handled alerts ● Number of handled incidents ● Number of fixed vulnerabilities ● Number of fixed baseline settings ● Threat alert distribution and quantity ● Top 5 intrusion incidents by type ● Top 5 emergency responses ● Top 20 threat alert handling
External Security Info	This part includes information about external security hotspots.

Content in the Monthly Report Template

Table 7-32 Content in the monthly report template

Parameter	Description
Data Scope	By default, a monthly report includes security information for the previous month.
Security Score	SecMaster evaluates and scores your asset security for the last day of the previous month so that you can quickly learn of the overall security posture of assets. This score varies depending on the SecMaster edition you are using.
Baseline Inspection	Displays the statistics of the latest baseline check in the previous month, including the following information: ● The number of baseline check items ● Number of compliance check items in the latest baseline check ● Non-compliant check items in the latest baseline check
Security Vulnerabilities	Displays the vulnerability statistics of the accessed cloud services on the 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 ● Average MTTR ● Number of confirmed high-risk intrusion incidents
Asset risks	Displays the latest asset security information on the last day of the last month, including the following information: ● Attacked asset quantity changes compared to the previous month ● Unprotected asset quantity changes compared to the previous month ● Vulnerable asset quantity changes compared to the previous month ● Asset changes over the previous month ● Asset protection (%)

Parameter	Description
Threat posture	Displays the latest threat posture n on the last day of the previous month, including the following information: ● Number of DDoS attacks ● Number of network attacks ● Number of application attacks ● Number of server attacks ● DDoS inspection findings ● Network attack changes ● WAF inspection findings ● Top 5 network attack types ● Top 5 application attack types ● Top 5 server attack types ● Top 5 application attack sources distribution ● Top 5 attacked application distribution ● Top HSS alert distribution ● Top 5 network attack sources distribution ● HSS inspection findings
Log analysis	Displays the log analysis results for the previous month, including the following information: ● Number of log sources ● Number of log indexes ● Total number of received logs ● Log storage ● Log volume changes ● Top 5 log source access statistics ● Number of alerts generated by top 10 models on the previous day
Security Response (Details)	Displays the security response information for the previous month, including the following information: ● Number of handled alerts ● Number of handled incidents ● Fixed vulnerabilities ● Number of fixed baseline settings ● Threat alerts by severity ● Top 5 intrusion incidents by type ● Top 5 emergency responses ● Top 20 threat alert handling

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

7.3.3 Downloading a Security Report

Scenario

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

This topic describes how to download a report.

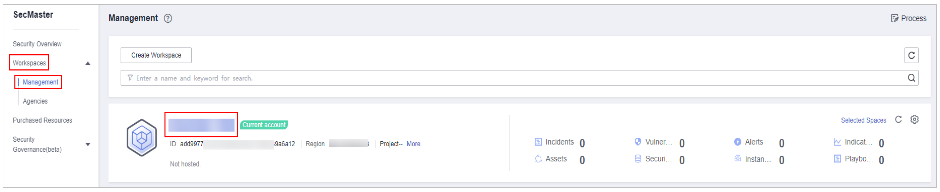
Procedure

Step 1 Log in to the management console.

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

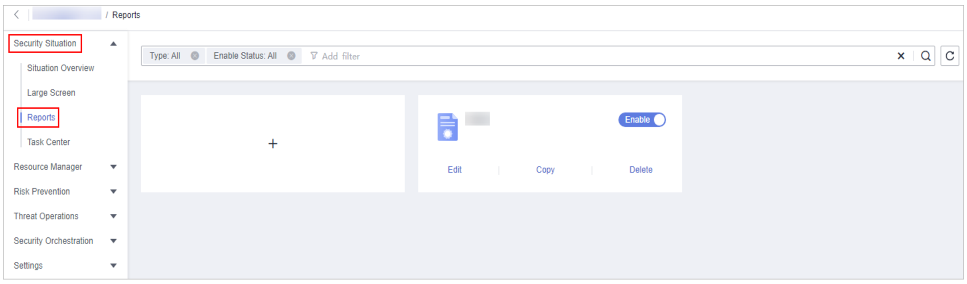
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-55 Workspace management page



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

Figure 7-56 Reports



Step 5 Locate a report template and click **Edit**.

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

Step 6 Click **Next: Report Choose** in the upper right corner. The **Report Selection** page is displayed.

Step 7 On the report selection page, click in the upper left corner of the preview page on the right.

To change the report schedule, edit it in the upper right corner of the preview page on the right.

Step 8 In the displayed dialog box, select a report format, and click **OK**.

The system automatically downloads the report to the local PC.

----End

7.3.4 Managing Security Reports

Scenario

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

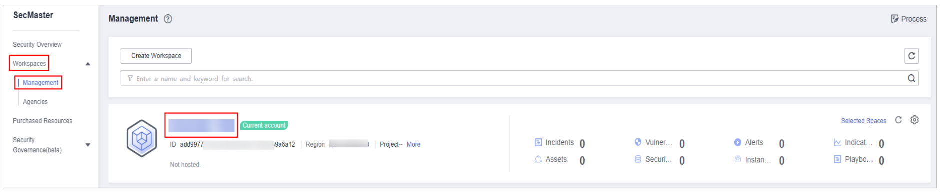
Procedure

Step 1 Log in to the management console.

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

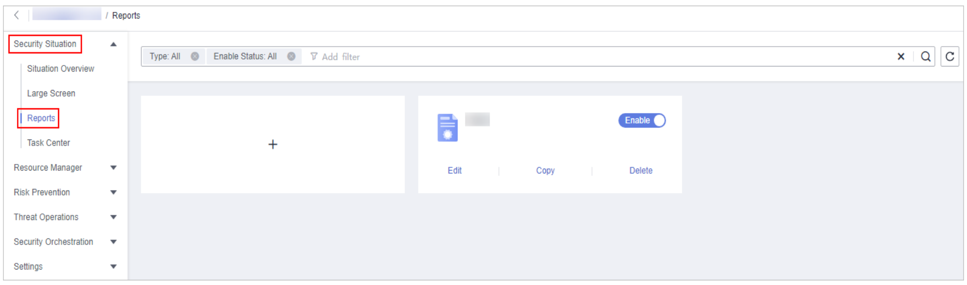
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-57 Workspace management page



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

Figure 7-58 Reports



Step 5 Manage security reports.

Table 7-33 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 **Complete** in the lower right corner.
Deleting a Security Report	1. On the **Reports** page, locate the desired report and click **Delete**. 2. In the **Warning** dialog box displayed, click **OK**.

----End

7.4 Task Center

7.4.1 Viewing To-Do Tasks

Scenario

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

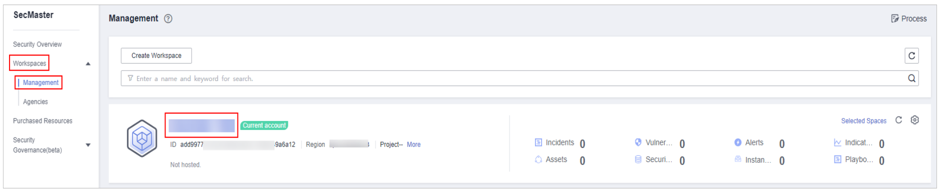
Procedure

Step 1 Log in to the management console.

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

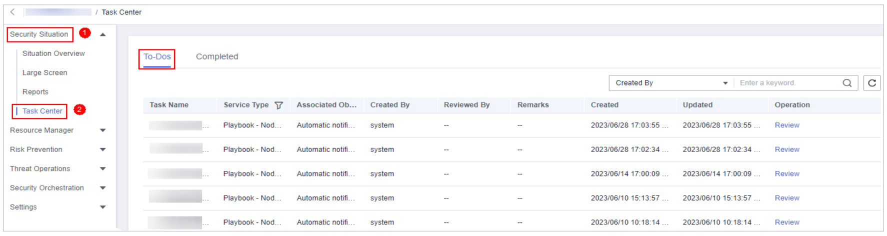
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-59 Workspace management page



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

Figure 7-60 To-Dos



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

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

Table 7-34 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.

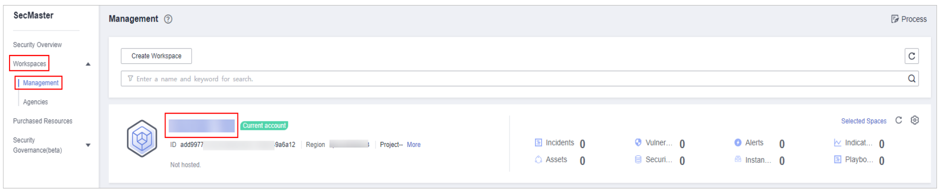
Procedure

Step 1 Log in to the management console.

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

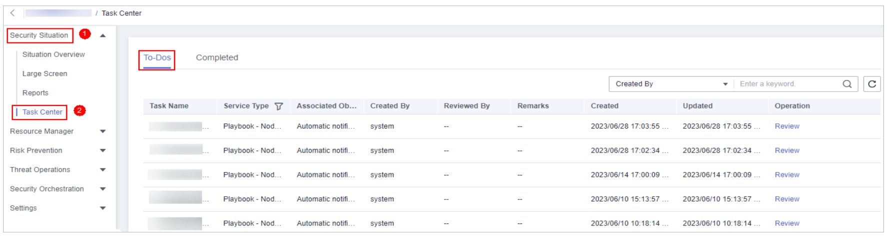
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-61 Workspace management page



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

Figure 7-62 To-Dos



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

The approval mode varies according to the service type.

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

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

----End

7.4.3 Viewing Completed Tasks

Scenario

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

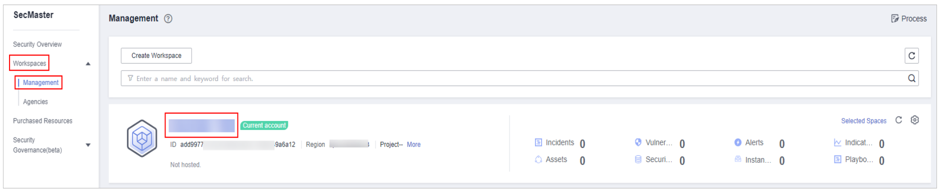
Procedure

Step 1 Log in to the management console.

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

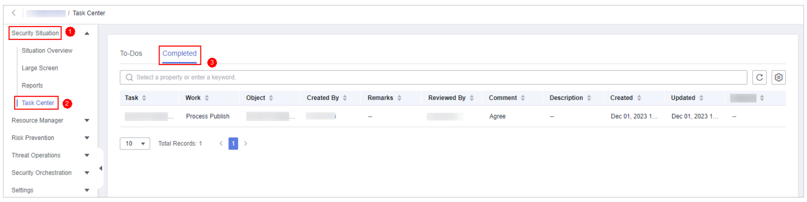
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 7-63 Workspace management page



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

Figure 7-64 Completed



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

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

Table 7-35 Completed task parameters

Parameter	Description
Task	Name of a task.

Parameter	Description
Work	Type of a task. ● Workflow release ● Playbook release ● Playbook - Node review
Object	Name of the corresponding playbook or workflow.
Created By	User who creates the task.
Remarks	Remarks of the task.
Reviewed By	Reviewer of the playbook/workflow
Comment	Review comment of the task.
Description	Description of the task.
Created	Time when the playbook or workflow was created.
Updated	Last time the playbook or workflow was updated.
Expired	Time the task expires.

----End

8 Resource Manager

8.1 Overview

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

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

Asset Source and Corresponding Security Products

Table 8-1 Asset source and corresponding security products

Parameter	Source	Security Product
Servers	Elastic Cloud Server (ECS)	Host Security Service (HSS)
Website	Web Application Firewall (WAF)	Web Application Firewall (WAF)
Database	Relational Database Service (RDS)	Database Security Service (DBSS)
VPC	Virtual Private Cloud (VPC)	Cloud Firewall (CFW)
EIP	Elastic IP (EIP)	CNAD Basic (Anti-DDoS)
Device	On-premises devices	--
Note: If the protection status of an asset on the SecMaster console is **Unprotected**, the corresponding security product is not enabled. If the protection status is **-**, the corresponding security product cannot be used in the region where the asset locates.		

8.2 Configuring Resource Subscription

Scenario

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

This section describes how to make a subscription to resources.

NOTE

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

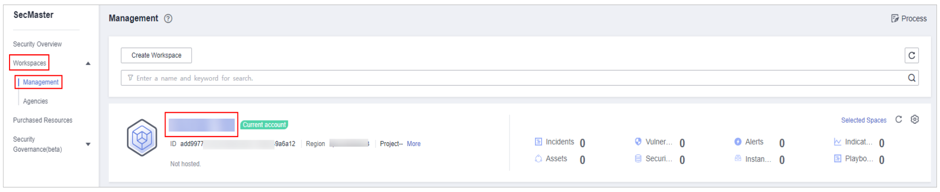
Procedure

Step 1 Log in to the management console.

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

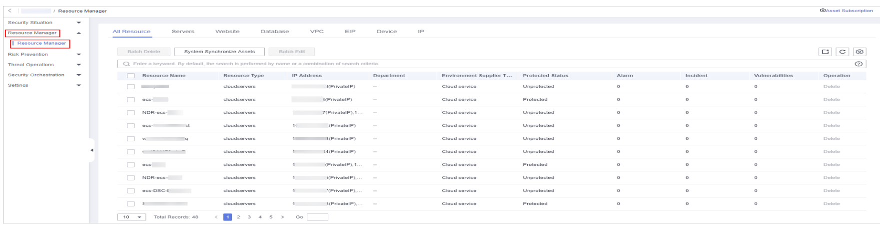
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-1 Workspace management page



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

Figure 8-2 Resource Manager



Step 5 On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.

Step 6 On the **Asset Subscription** page sliding from the right, locate the row that contains the region where the target resource is located, and enable subscription.

Step 7 Click **OK**.

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

----End

8.3 Viewing Resource Information

Scenario

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

Prerequisites

You have purchased the SecMaster standard or professional edition.

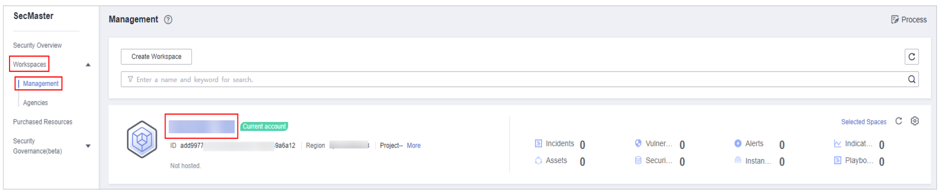
Procedure

Step 1 Log in to the management console.

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

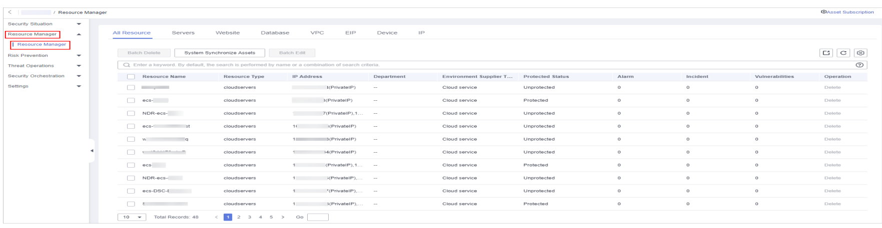
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-3 Workspace management page



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

Figure 8-4 Resource Manager



Step 5 On the displayed page, view the resource details.

- You can view resource information by resource type. For example, you can select the **Servers** tab to view details about servers you have.
- If there are a large number of resources on this page, you can select **Resource Type** and click to search for a specific resource.

- You can view the total number of assets below the asset list. You can view a maximum of 10,000 asset records page by page. To view more than 10,000 asset records, optimize the filter criteria.
- To view more details about a resource, click its name to go to the details page. On the details page, you can:
  - View the basic information, environment information, and managed resources.
  - Edit the owner, service system, and department of the resource. You can also bind the resources to or unbind the resources from an owner, service system, or department.

Table 8-2 Asset source and corresponding security products

Parameter	Source	Security Product
Servers	Elastic Cloud Server (ECS)	Host Security Service (HSS)
Website	Web Application Firewall (WAF)	Web Application Firewall (WAF)
Database	Relational Database Service (RDS)	Database Security Service (DBSS)
VPC	Virtual Private Cloud (VPC)	Cloud Firewall (CFW)
EIP	Elastic IP (EIP)	CNAD Basic (Anti-DDoS)
Device	On-premises devices	--
Note: If the protection status of an asset on the SecMaster console is **Unprotected**, the corresponding security product is not enabled. If the protection status is **-**, the corresponding security product cannot be used in the region where the asset locates.		

----End

Related Operations

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

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

8.4 Importing and Exporting Assets

Scenario

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

This section describes how to import and export assets.

Prerequisites

You have purchased the SecMaster standard or professional edition.

Limitations and Constraints

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

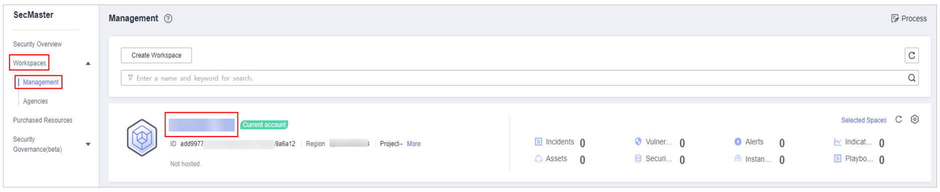
Importing Assets

Step 1 Log in to the management console.

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

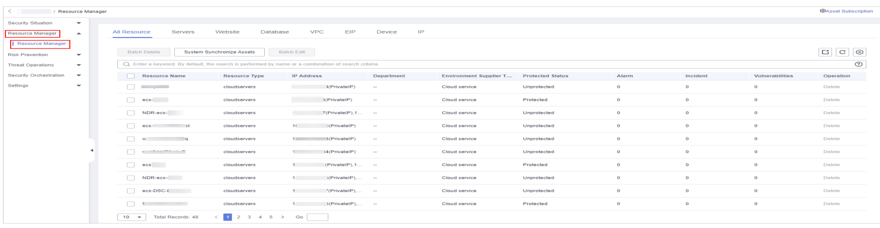
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-5 Workspace management page



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

Figure 8-6 Resource Manager



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

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

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

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

Step 9 Click **OK**.

----End

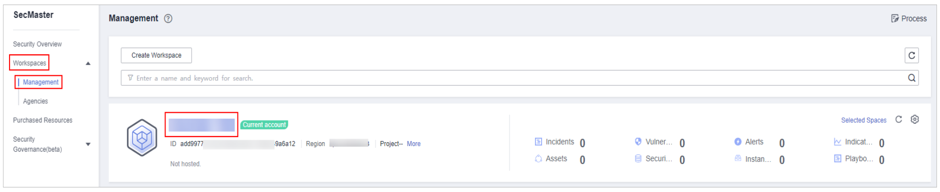
Exporting Assets

Step 1 Log in to the management console.

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

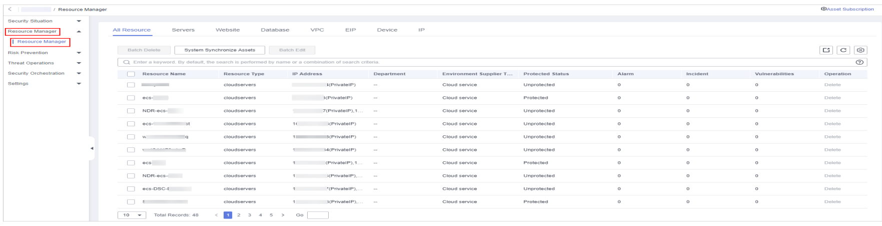
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-7 Workspace management page



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

Figure 8-8 Resource Manager



Step 5 On the asset management page, click the corresponding asset tab. For example, if you want to export servers, click the **Servers** tab.

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

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

Table 8-3 Exporting assets

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

Step 8 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

8.5 Editing and Deleting Resources

Scenario

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

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

Prerequisites

You have purchased the SecMaster standard or professional edition.

Limitations and Constraints

Only assets imported outside the cloud can be deleted.

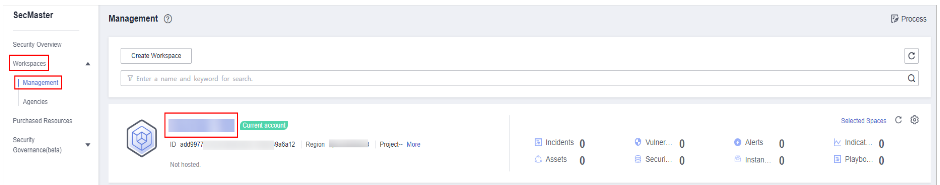
Procedure

Step 1 Log in to the management console.

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

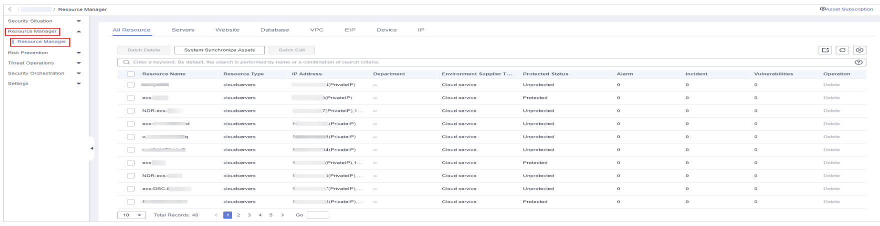
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 8-9 Workspace management page



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

Figure 8-10 Resource Manager



Step 5 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.

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

Limitations and Constraints

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

Baseline Check Methods

- Automated baseline checks

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

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

- Manual baseline checks

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

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

Process

Table 9-1 Process

No.	Operation	Description
1	(Optional) **Creating a Custom Baseline Check Plan**	SecMaster uses the default check plan to check all assets. ● Default plan: SecMaster checks your assets under your account in the current region every three days from 00:00 to 06:00. ● Custom plans: SecMaster performs baseline inspections based on the standards and time you specify in the custom check plans.
2	(Optional) **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, 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 Creating a Custom Baseline Check Plan

Scenario

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

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

Limitations and Constraints

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

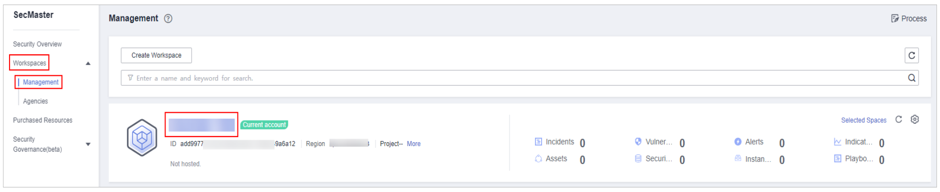
Procedure

Step 1 Log in to the management console.

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

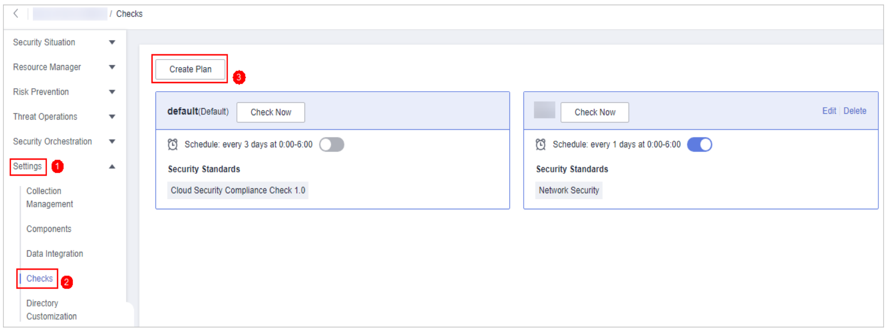
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-1 Workspace management page



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

Figure 9-2 Creating a check plan



Step 5 Configure the check plan.

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

Table 9-2 Basic information about a check plan

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

2. Select a security standard for the plan.

   Select the baseline check items to be checked.

Step 6 Click **OK**.

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

----End

Related Operations

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

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

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

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

9.1.3 Starting an Immediate Baseline Check

Scenario

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

- Periodic check: SecMaster periodically executes the default check plan or the check plans you configure.
- Immediate check: You can start check items in all security standards or a specific check plan anytime.

This topic describes how to start an immediate baseline check plan.

Limitations and Constraints

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

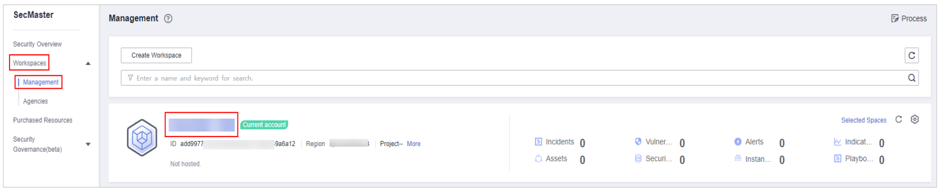
Starting a Check Based on Selected Standards

Step 1 Log in to the management console.

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

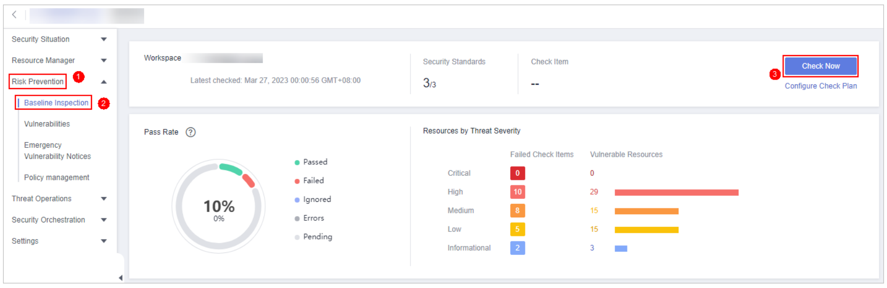
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-3 Workspace management page



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

Figure 9-4 Check Now



Step 5 In the displayed dialog box, click **OK**.

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

----End

Starting a Check Based on a Check Plan

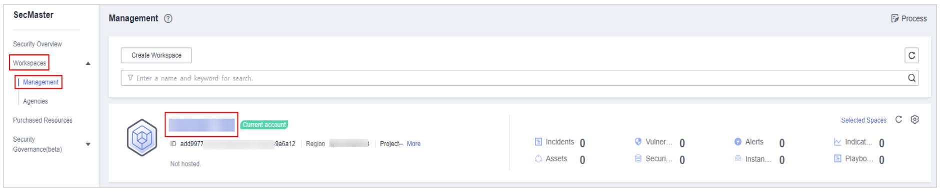
The following describes how to manually execute a check plan immediately.

Step 1 Log in to the management console.

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

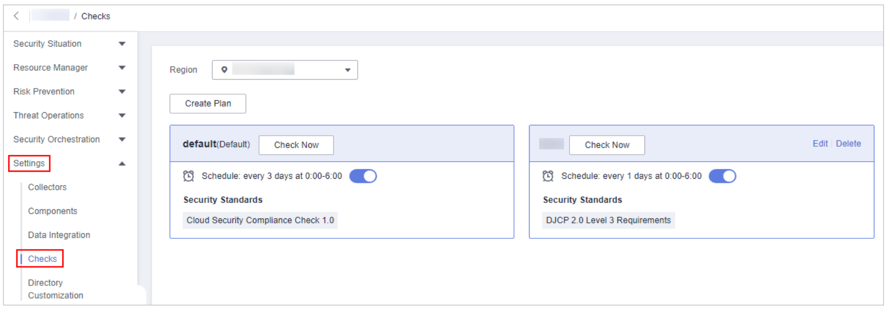
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-5 Workspace management page



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

Figure 9-6 Checks page



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

SecMaster immediately executes the selected baseline check plan.

----End

9.1.4 Handling Manual Check Items

Scenario

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

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

Prerequisites

- You have completed the check offline.

Constraints and Limitations

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

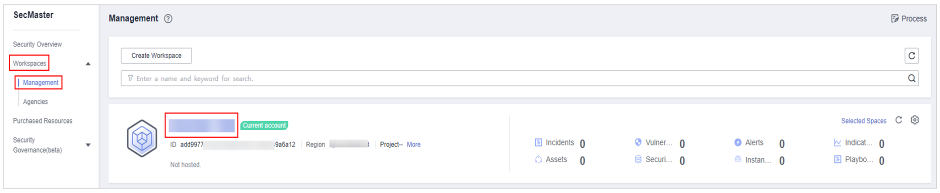
Procedure

Step 1 Log in to the management console.

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

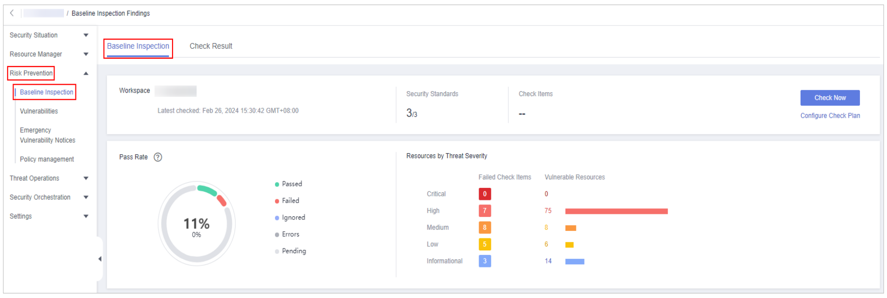
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-7 Workspace management page



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

Figure 9-8 Accessing the baseline inspection page



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

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

NOTE

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

----End

9.1.5 Viewing Baseline Inspection Results

Scenario

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

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

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

Prerequisites

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

Viewing Check Results on the Baseline Inspection Tab

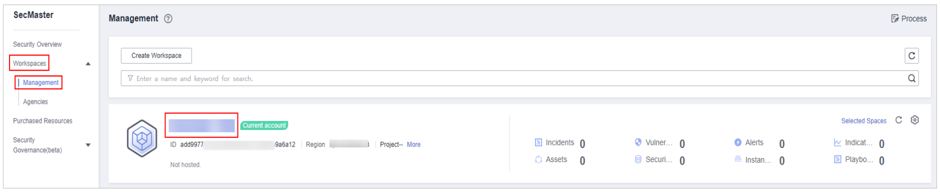
View the check results of all check items in a region.

Step 1 Log in to the management console.

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

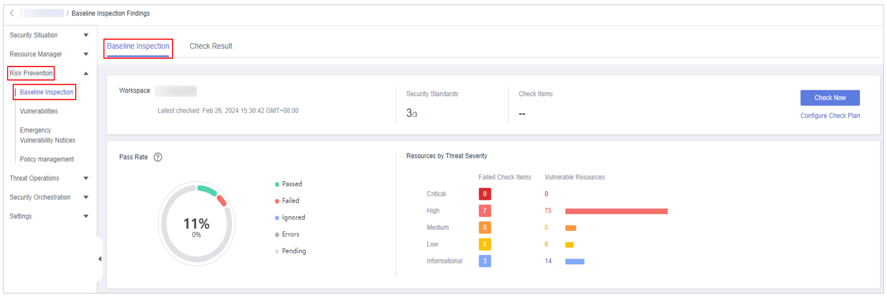
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-9 Workspace management page



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

Figure 9-10 Accessing the baseline inspection page



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

Figure 9-11 Viewing Baseline Inspection Results

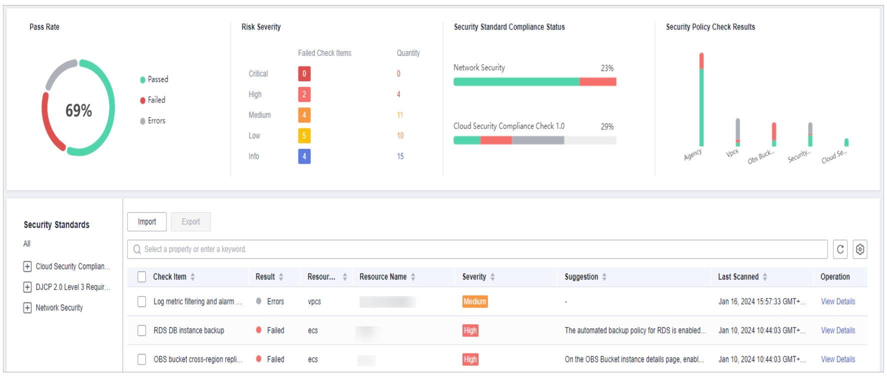


Table 9-3 Baseline inspection results

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

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

----End

Viewing Check Results on the Result Tab

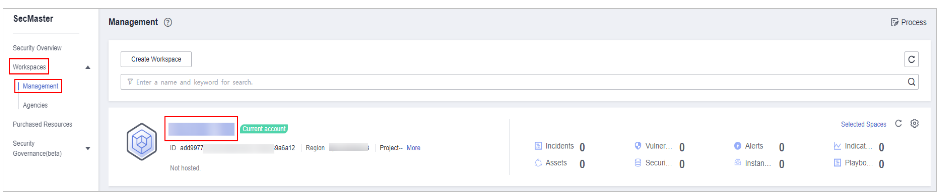
SecMaster allows you to view the check results of automatic check items by checked resource.

Step 1 Log in to the management console.

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

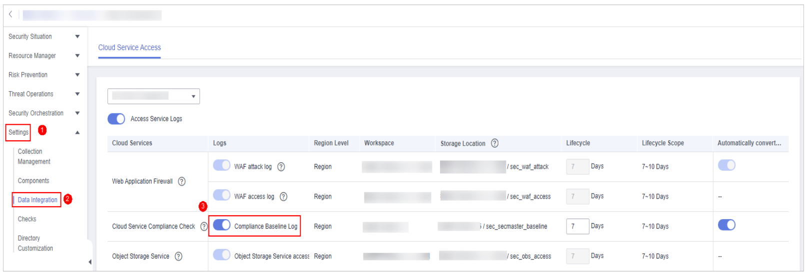
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-12 Workspace management page



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

Figure 9-13 Compliance baseline log

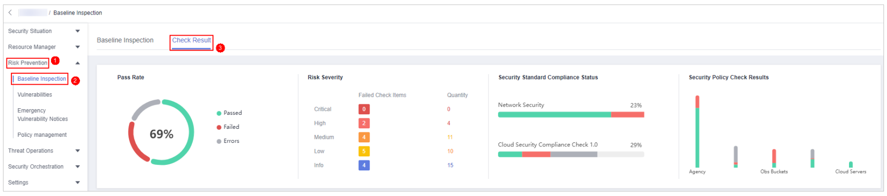


After the setting is complete, you can perform an immediate check on the **Baseline Inspection** page. You can view check results on the **Check Result** page 10 minutes later. For details about operations related to immediate check, see **Starting an Immediate Baseline Check**.

If no immediate checks are performed, the system performs the check at the specified time according to the preset check plan. You can view the check results on the **Check Result** page.

Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. On the displayed page, click the **Result** tab.

Figure 9-14 Check result tab



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

Figure 9-15 Viewing check results

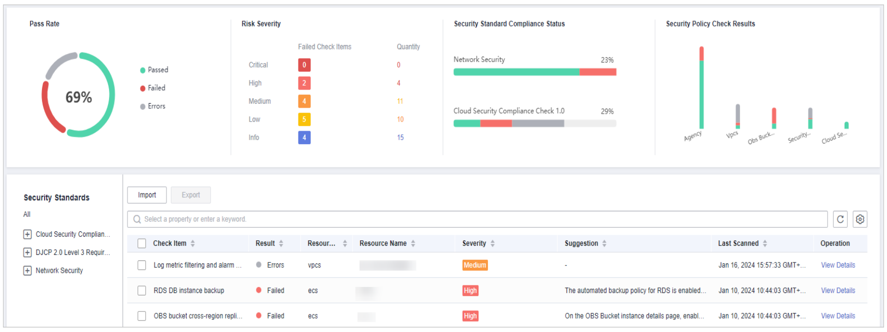


Table 9-4 Check result parameters

Parameter	Description
Pass Rate	Rate of the passed check items in the latest baseline check. Overall pass rate = Passed check items/Total check items All check items in security standards used for the check plan executed are considered when the pass rate is calculated. The check result can be **Passed**, **Failed**, or **Errors**.
Risk Severity	Risks found in the last baseline check are listed by severity as well as the corresponding resource quantity. **Severity**: **Critical**, **High**, **Medium**, **Low**, and **Informational**.
Security Standard Compliance Status	This part shows how well your workloads comply with each security standard. You will see a percentage of passed check items in total check items for each standard.
Security Policy Check Results	This graph shows how many failed and passed check items your cloud services have in the last baseline check.
Security Standards and the check result list	All security standards and check results are displayed. ● To view the check results of a security standard, click the security standard on the left. The check result details will be displayed on the right. ● To view details about a baseline check item, click **View Details** in the **Operation** column. On the **Baseline inspection issues** page, view the detailed description, check result, and suggestions of the check item. **NOTE** SecMaster **basic edition** does not support viewing of cloud service baseline inspection details. After **Buying the Professional Edition**, you can view details about unsafe resources and hardening suggestions.

----End

9.1.6 Handling Baseline Inspection Results

Scenario

To handle the check result, perform the following operations:

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

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

Limitations and Constraints

When you import check results, note the following restrictions:

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

Prerequisites

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

Handling Unsafe Settings

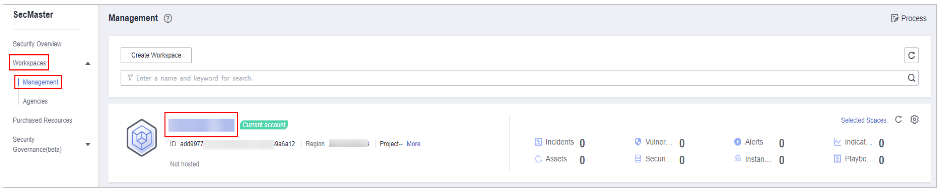
The following describes how to fix unsafe settings discovered by check item **IAM user login protection**.

Step 1 Log in to the management console.

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

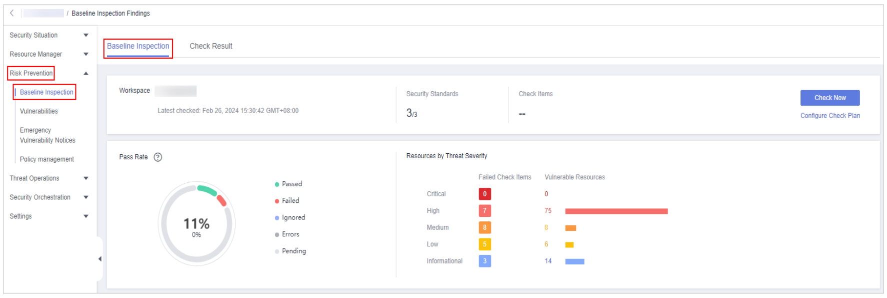
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-16 Workspace management page



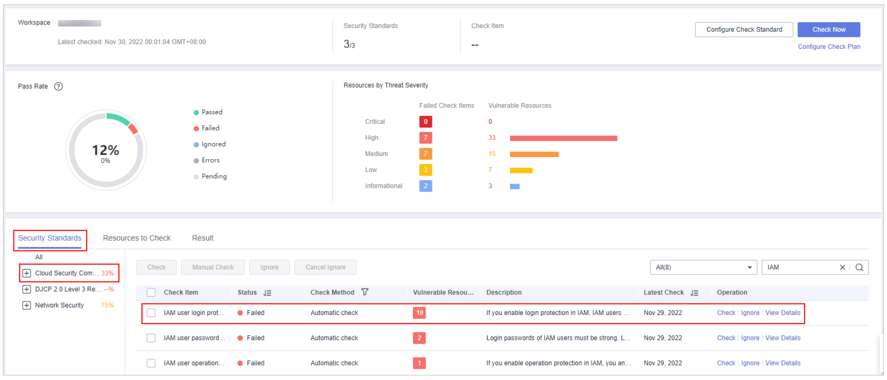
Step 4 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**.

Figure 9-17 Accessing the baseline inspection page



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

Figure 9-18 Check item status



- If the icon of a check item status is green, the configuration is correct and no unsafe settings found.
- If the icon of a check item status is red, there may be inappropriate configurations and the assets may have potential risks.

Step 6 In the **IAM user login protection** row, click **View Details** in the **Operation** column to go to the details page.

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

Table 9-5 Check items

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

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

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

----End

Reporting Manual Check Results to SecMaster

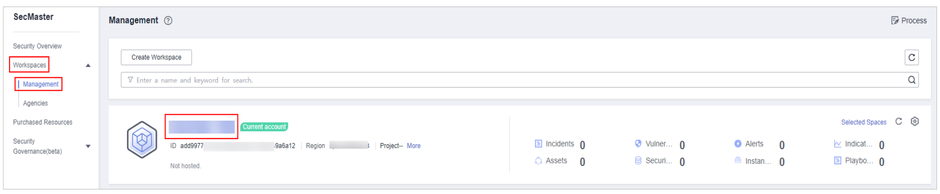
For manual check items, after you finish each check, report the check result to SecMaster. The pass rate is calculated based on results from both manual and automatic checks.

Step 1 Log in to the management console.

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

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

Figure 9-19 Workspace management page



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

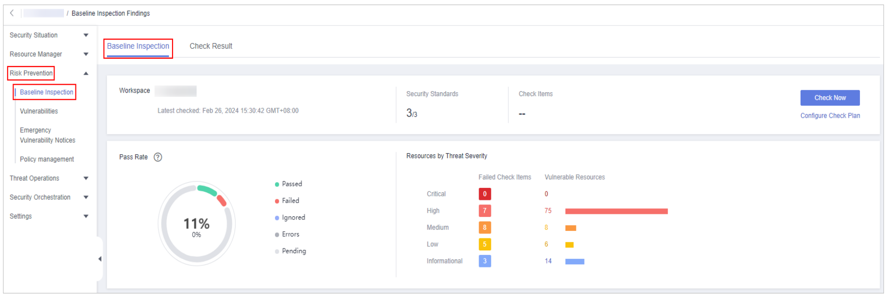


Figure 9-20 Accessing the baseline inspection page

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

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

NOTE

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

----End

Ignoring a Check Item

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

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

Step 1 Log in to the management console.

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

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

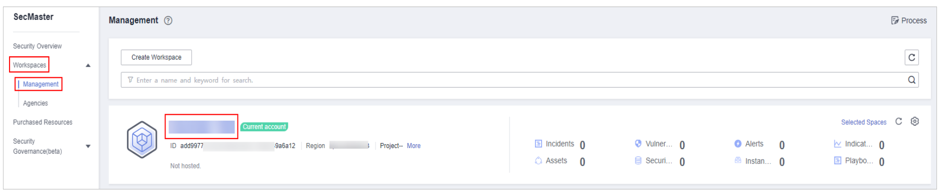
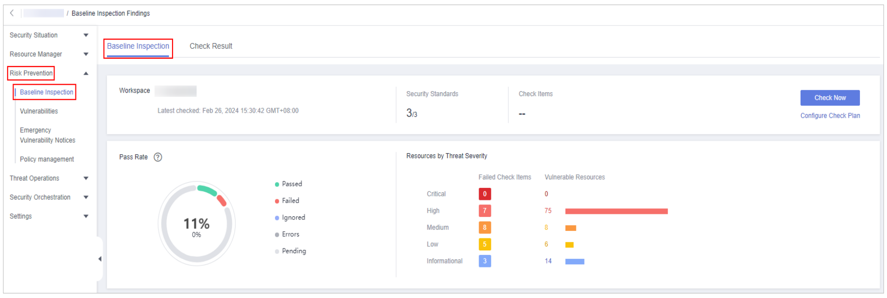


Figure 9-21 Workspace management page

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

Figure 9-22 Accessing the baseline inspection page



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

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

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

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

----End

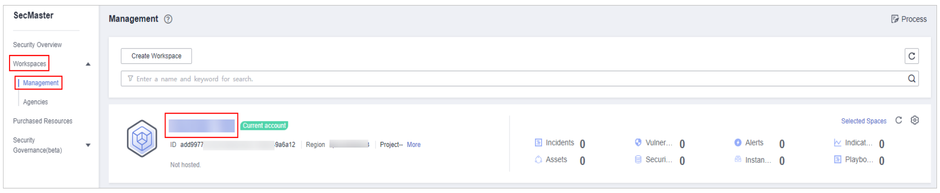
Importing and Exporting Check Results

Step 1 Log in to the management console.

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

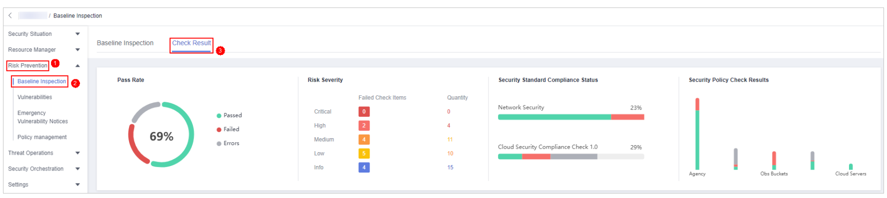
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-23 Workspace management page



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

Figure 9-24 Check result tab



Step 5 Import or export the check result.

- Import:

  NOTE

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

  a. In the upper left corner above the check result list, click **Import**.
  b. In the dialog box displayed, click **Download Template** and complete the template.
  c. In the displayed dialog box, click **Add File** and upload the completed template file.
  d. Click **OK**.

- Export:

  a. Select target check items from the result list and click **Export** in the upper left corner above the check result list.
  b. In the displayed dialog box, select the format and data columns you want.
  c. Click **OK**.

----End

9.2 Vulnerability Management

9.2.1 Overview

Background

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

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

ECS Vulnerabilities

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

The following host vulnerabilities can be detected:

Table 9-6 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 where to view details about Linux, Windows, Web-CMS, and application vulnerabilities.

Prerequisites

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

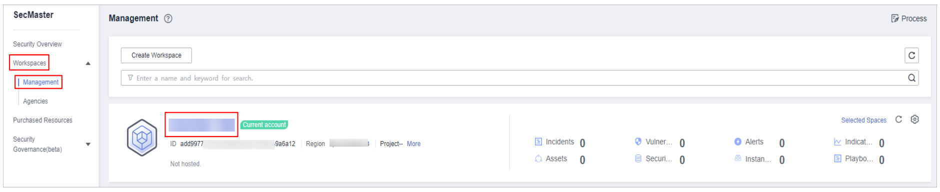
Procedure

Step 1 Log in to the management console.

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

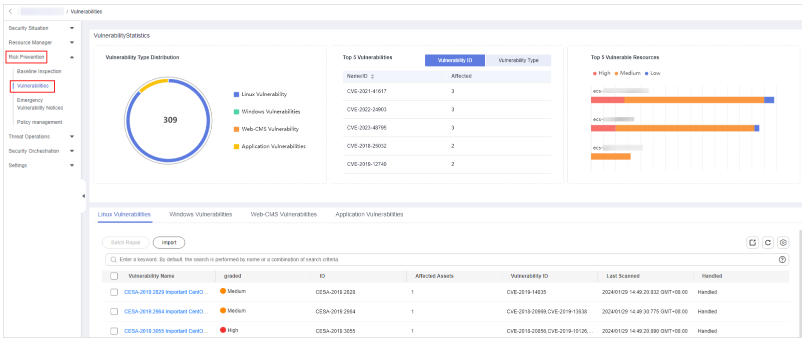
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-25 Workspace management page



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

Figure 9-26 Accessing the vulnerability management page



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

Table 9-7 Viewing vulnerability information

Parameter	Description
Vulnerability Type Distribution	This graph displays the total number of vulnerabilities and the distribution of vulnerabilities by type.
Top 5 Vulnerabilities	• The **Top 5 Vulnerabilities** area lists the five vulnerabilities with the most affected assets. The more affected assets, the higher the vulnerability ranking is. • The **Vulnerability ID** tab displays the IDs and the affected asset quantity for the five vulnerabilities. • The **Vulnerability Type** tab displays the names, severity levels, and affected asset quantity for the five vulnerabilities.

Parameter	Description
Top 5 Vulnerable Resources	This graph displays the five resources with the most vulnerabilities.
Vulnerability List	● The vulnerable list area includes **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Web-CMS Vulnerabilities**, and **Application Vulnerabilities** tabs. **Table 9-8** lists parameters for these vulnerability tabs. ● To quickly search for a specific vulnerability, use filters in your search. Specifically, you can specify the vulnerability name, vulnerability ID, severity, and handling status, enter a keyword in the search box, and click . ● To view details about a vulnerability, click the vulnerability name and view the details on the page displayed on the right. ● You can view the total number of vulnerabilities below the vulnerability list. You can view a maximum of 10,000 vulnerability records page by page. To view more than 10,000 records, optimize the filter criteria.

Table 9-8 Vulnerability parameters

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

----End

9.2.3 Fixing Vulnerabilities

Scenario

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

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

Table 9-9 Recommended fixing methods

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

CAUTION

- Vulnerability fixing operations cannot be rolled back. If a vulnerability fails to be fixed, services will probably be interrupted, and incompatibility issues will probably occur in middleware or upper layer applications. To prevent unexpected consequences, you are advised to use CBR to back up ECSs. For details, see **Purchasing a Server Backup Vault**. Then, use idle servers to simulate the production environment and test-fix the vulnerability. If the test-fix succeeds, fix the vulnerability on servers running in the production environment.
- Servers need to access the Internet and use external image sources to fix vulnerabilities. If the server cannot access the Internet or the services provided by the external image source are unstable, you can use the image source provided by Huawei Cloud to fix vulnerabilities. To ensure that the vulnerability is successfully fixed, ensure that the image source . For details, see **Configuring the Image Source**.

Constraints

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

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

Fixing Vulnerabilities on the Console

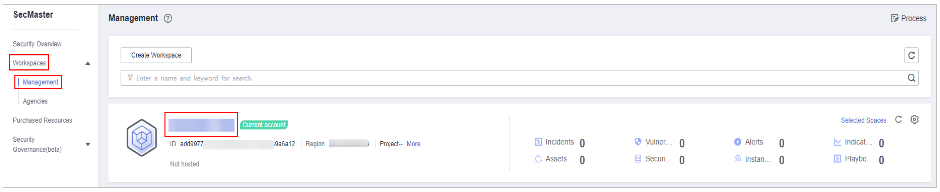
Only Linux vulnerabilities and Windows vulnerabilities can be fixed using the repair function on the console.

Step 1 Log in to the management console.

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

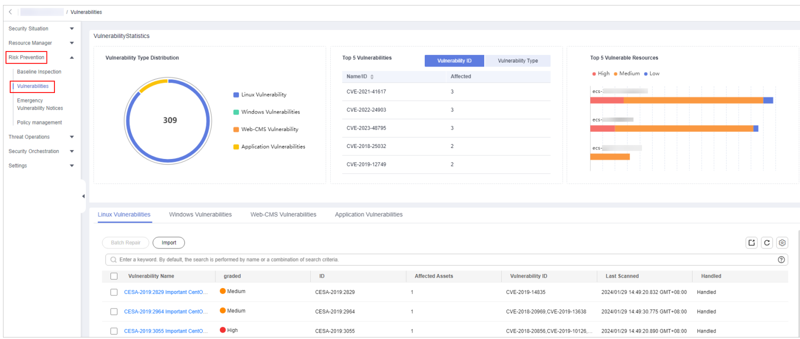
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-27 Workspace management page



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

Figure 9-28 Accessing the vulnerability management page



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

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

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

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

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

NOTE

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

----End

Manually Fixing Software Vulnerabilities

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

- **Vulnerability Fixing Commands**

  On the basic information page of vulnerabilities, you can fix a detected vulnerability based on the provided suggestions. For details about the vulnerability fixing commands, see **Table 9-10**.

  NOTE

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

  Table 9-10 Vulnerability fix 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 9-11 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 Importing and Exporting Vulnerabilities

Scenario

This section describes how to import and export vulnerabilities.

- **Importing Vulnerabilities**
- **Exporting Vulnerabilities**

Constraints

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

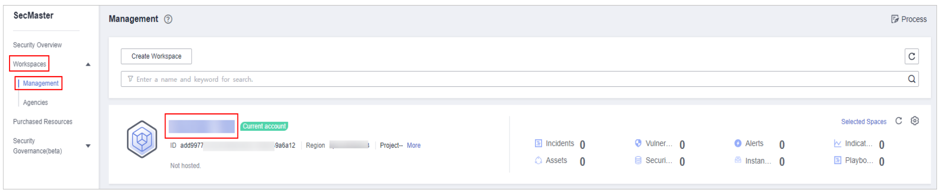
Importing Vulnerabilities

Step 1 Log in to the management console.

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

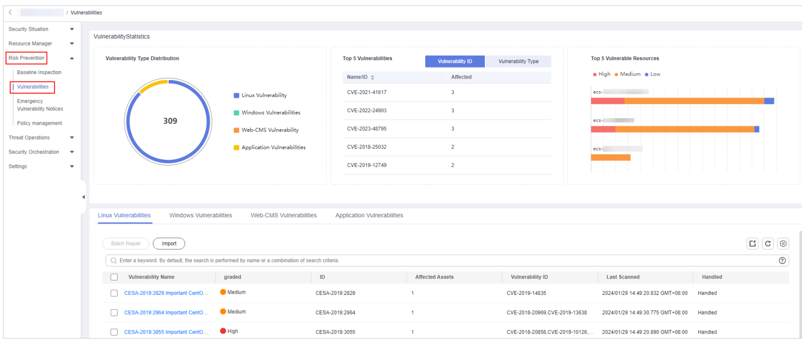
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-29 Workspace management page



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

Figure 9-30 Accessing the vulnerability management page



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

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

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

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

Step 9 Click **OK**.

----End

Exporting Vulnerabilities

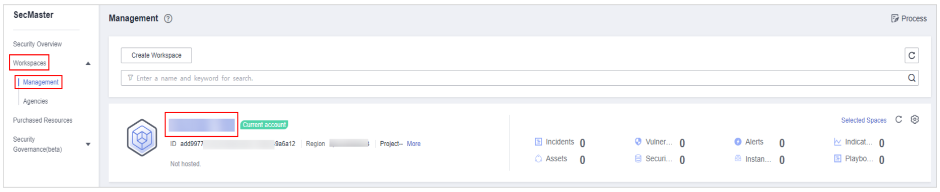
A maximum of 9,999 vulnerability records can be exported.

Step 1 Log in to the management console.

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

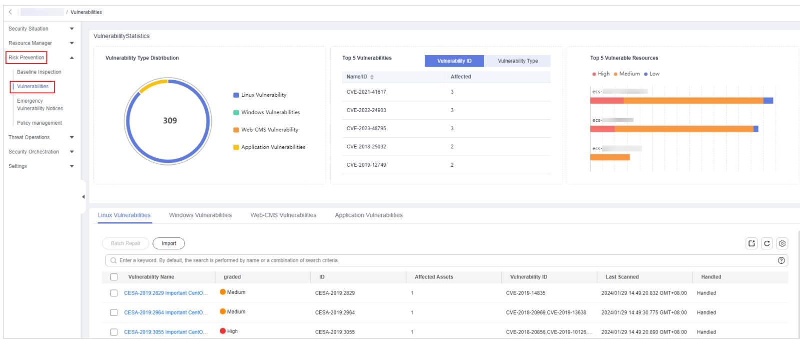
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-31 Workspace management page



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

Figure 9-32 Accessing the vulnerability management page



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

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

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

Table 9-12 Exporting vulnerabilities

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

Step 8 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

9.2.5 Ignoring and Unignoring a Vulnerability

Scenario

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

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

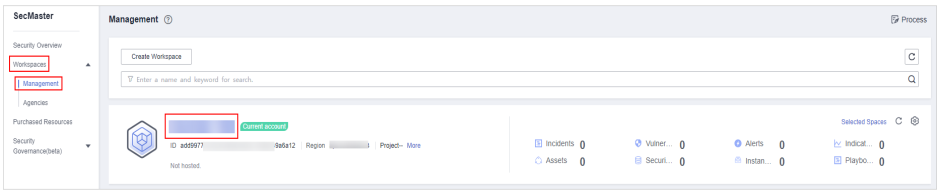
Procedure

Step 1 Log in to the management console.

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

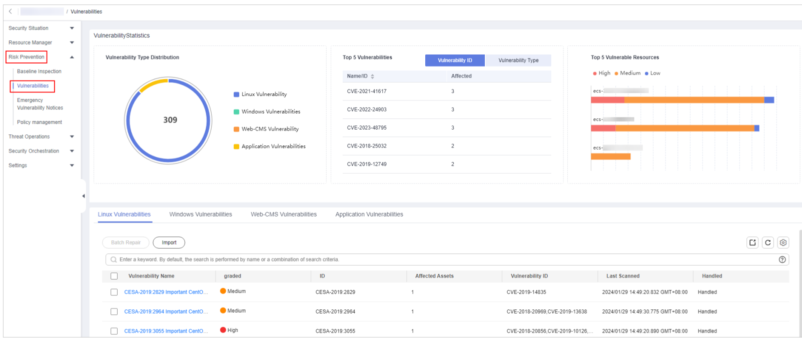
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-33 Workspace management page



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

Figure 9-34 Accessing the vulnerability management page



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

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

Step 7 Ignore or unignore the target vulnerability.

- Ignore

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

- Unignore

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

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

----End

9.3 Viewing/Exporting Emergency Vulnerability Notices

Background

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

With the emergency vulnerability notices, you can easily:

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

Scenario

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

Limitations and Constraints

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

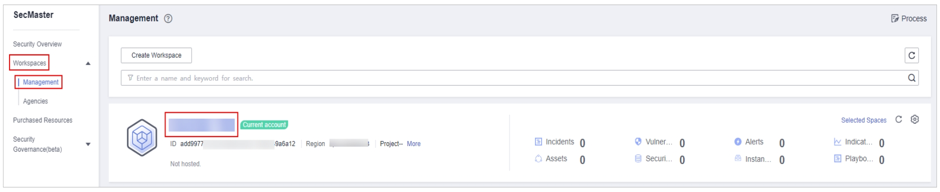
Viewing Emergency Vulnerability Notices

Step 1 Log in to the management console.

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

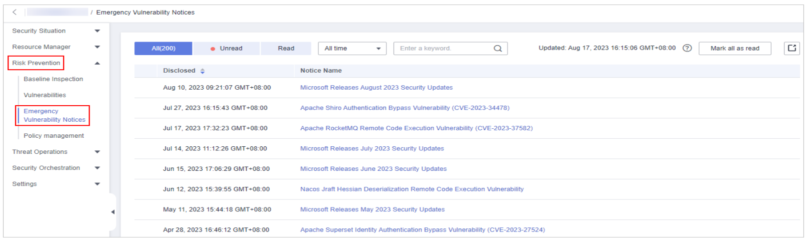
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-35 Workspace management page



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

Figure 9-36 Accessing the emergency vulnerability notices page



Step 5 View the update time of emergency vulnerability notices.

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

Step 6 View details of an emergency vulnerability notice.

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

Step 7 View emergency vulnerability notices by time range.

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

Step 8 Search for historical emergency vulnerability notices.

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

----End

Exporting Emergency Vulnerability Notices

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

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

9.4 Policy Management

9.4.1 Overview

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

In the policy management module, you can view all policies centrally, manage policies for seven defense lines manually, and query manual and automatic block records quickly.

Limitations and Constraints

- Currently, the emergency policies include only the blacklist policies of CFW/WAF/VPC security groups/IAM.
- A maximum of 300 emergency policies that support block aging can be added for a single workspace you have. A maximum of 1,300 emergency policies can be added for a single workspace you have. A maximum of 50 IP addresses or IAM users can be selected as blocked objects for an emergency policy.
- If an IP address or IP address range or an IAM user is added to the blacklist, CFW/WAF/VPC/IAM will block requests from that IP address without checking whether the requests are malicious.

9.4.2 Viewing Defense Policies

Scenario

This section describes how to view defense policies.

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

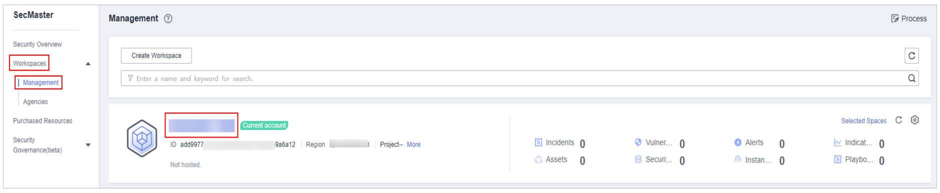
Procedure

Step 1 Log in to the management console.

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

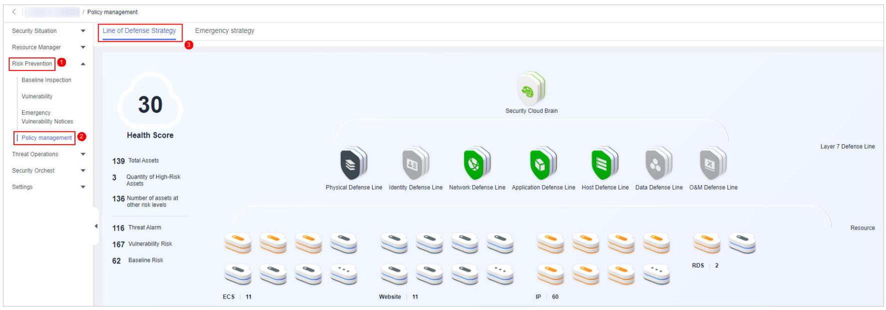
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-37 Workspace management page



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

Figure 9-38 Line of Defense Strategy



Step 5 View defense policy statistics.

- **Health Score**: indicates the current health status of resources.

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

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

----End

9.4.3 Configuring Defense Policies

Scenario

This section describes how to configure protection policies.

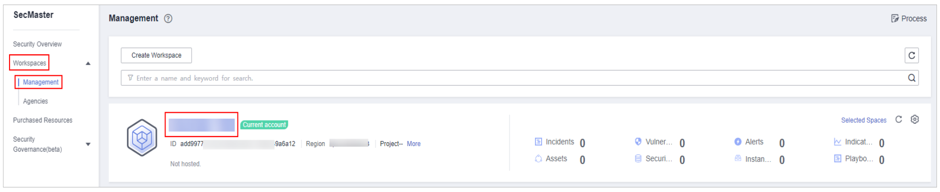
Procedure

Step 1 Log in to the management console.

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

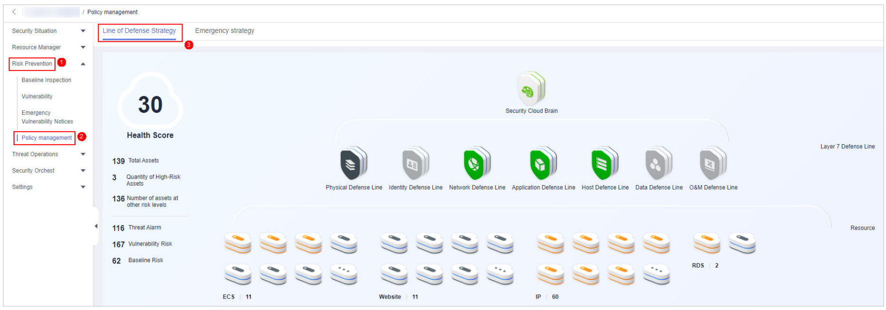
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-39 Workspace management page



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

Figure 9-40 Line of Defense Strategy



Step 5 Click the name of the defense line to which the security service belongs. The cloud service information corresponding to the defense line slides out from the right.

Step 6 On the tab page of the corresponding cloud service, click **Protection Policy** to go to the configuration page.

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

Step 7 On the policy configuration page, configure policies of the corresponding cloud service.

- Anti-DDoS policy configuration:
  - Configuring a Protection Policy

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

----End

9.4.4 Adding or Editing an Emergency Policy

Scenario

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

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

Table 9-13 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 or edit an emergency policy.

Limitations and Constraints

- A maximum of 300 emergency policies that support block aging can be added for a single workspace you have. A maximum of 1,300 emergency policies can be added for a single workspace you have. A maximum of 50 IP addresses or IAM users can be selected as blocked objects for an emergency policy.

- If an IP address or IP address range or an IAM user is added to the blacklist, CFW/WAF/VPC/IAM will block requests from that IP address without checking whether the requests are malicious.
- Once an emergency policy is added, its blocked object type and blocked objects, such as IP addresses, IP address ranges, or IAM user names, cannot be modified.

Prerequisites

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

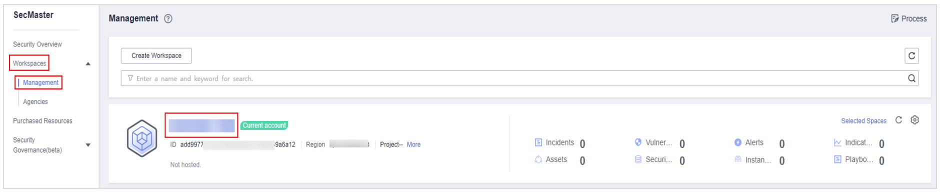
Adding an Emergency Policy

Step 1 Log in to the management console.

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

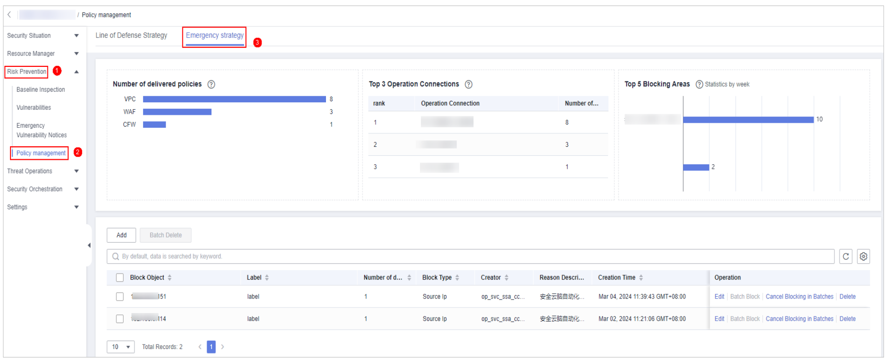
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-41 Workspace management page



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

Figure 9-42 Emergency strategy page



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

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

Table 9-14 Emergency policy parameters

Parameter	Description
Blocked Object Type	Type of the object to be blocked. You can select **IP** or **IAM**.
Block Object	● If you select **IP** for **Blocked Object Type**, enter one or more IP addresses or IP address ranges you want to block. If there are multiple IP addresses or IP address ranges, separate them with commas (,). Example: – Single IP address: 192.168.0.0 – IP address range: 192.168.0.0/12 ● If you select **IAM** for **Blocked Object Type**, enter IAM user names. ● A maximum of 50 IP addresses, IP address ranges, or IAM users can be blocked by an emergency policy once.
Label	Label of a custom emergency policy.
Operation Connection	Select the operation connection for the policy.
Block Aging	Check whether the policy needs to be stopped. ● If you select **Yes**, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address or IP address range will not be blocked. ● If you select **No**, the policy is always valid and blocks the specified IP address or IP address range.
Reason Description	Description of the custom policy.

Step 7 Click **OK**.

----End

Editing an Emergency Policy

NOTE

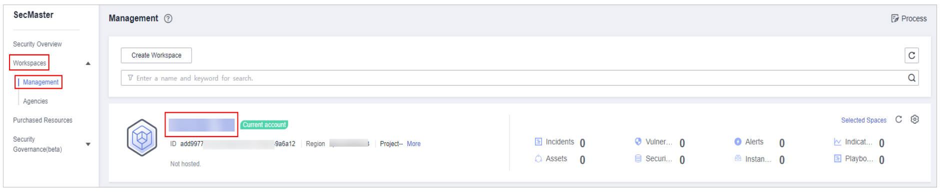
Once an emergency policy is added, its blocked object type and blocked objects, such as IP addresses, IP address ranges, or IAM user names, cannot be modified.

Step 1 Log in to the management console.

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

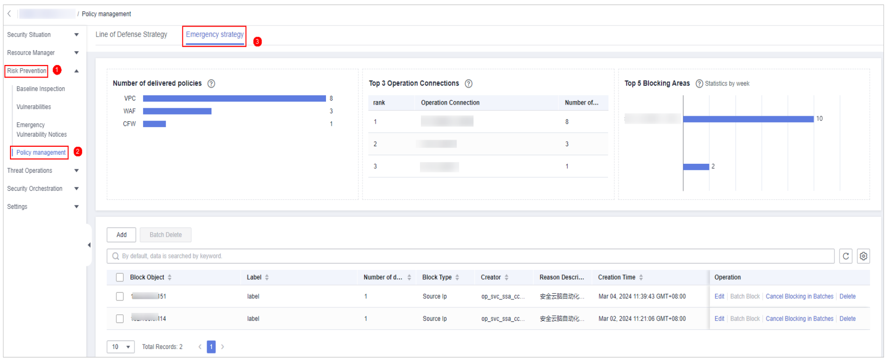
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-43 Workspace management page



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

Figure 9-44 Emergency strategy page



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

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

Table 9-15 Emergency policy parameters

Parameter	Description
Blocked Object Type	After an emergency policy is added, its blocked object cannot be modified.
Blocked Object	After an emergency policy is added, its blocked object cannot be modified.
Label	Label of a custom emergency policy.
Operation Connection	Select the operation connection for the policy.
Block Aging	Check whether the policy needs to be stopped. ● If you select **Yes**, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address or IP address range will not be blocked. ● If you select **No**, the policy is always valid and blocks the specified IP address or IP address range.

Parameter	Description
Reason Description	Description of the custom policy.

Step 7 Click **OK**.

----End

Creating a SecMaster Agency

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

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity and Access Management**.

Step 3 Add a custom policy.

1. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.
2. Configure a policy.
   - **Policy Name**: Enter a policy name.
   - **Policy View**: Select **JSON**.
   - **Policy Content**: Copy the following content and paste it in the text box.

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

   a. Click **OK**.

Step 4 Create an agency.

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

----End

9.4.5 Viewing Emergency Policies

Scenario

This section describes how to view emergency policies.

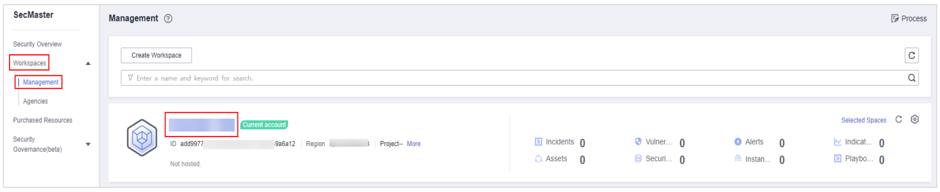
Procedure

Step 1 Log in to the management console.

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

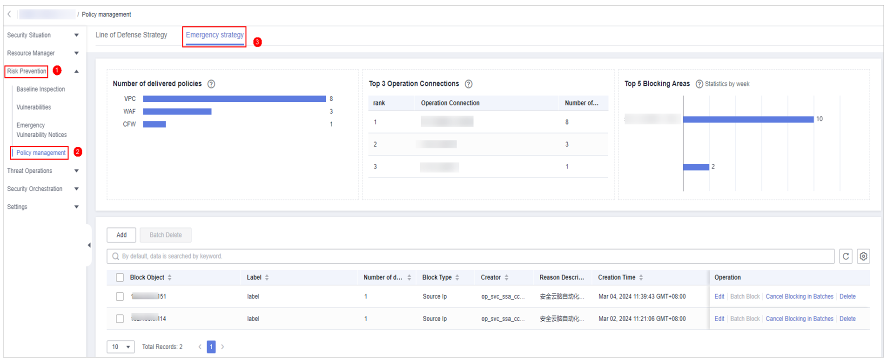
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-45 Workspace management page



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

Figure 9-46 Emergency strategy page



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

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

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

Table 9-16 Emergency policy parameters

Parameter	Description
Block Object	IP addresses, IAM usernames, or IP address ranges to be blocked.
Label	Label information of the policy.
Number of delivered policies	Number of policies delivered to corresponding product.
Block Type	Block type configured for the policy.
Creator	Creator of the policy.
Reason Description	Policy description.
Creation Time	Time when the policy was created.
Operation	You can edit or delete a policy.

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

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

----End

9.4.6 Deleting an Emergency Policy

Scenario

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

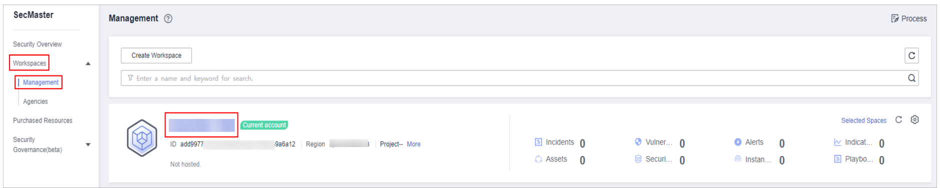
Procedure

Step 1 Log in to the management console.

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

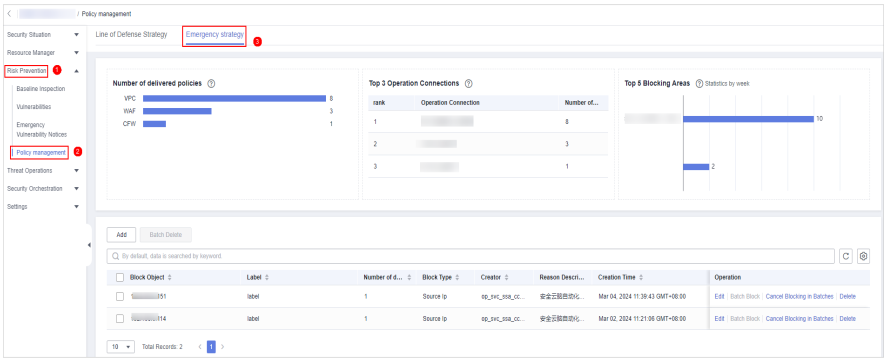
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-47 Workspace management page



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

Figure 9-48 Emergency strategy page



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

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

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

----End

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

Scenario

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

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

Limitations and Constraints

If an IP address or IP address range or an IAM user is added to the blacklist, CFW/WAF/VPC/IAM will block requests from that IP address without checking whether the requests are malicious.

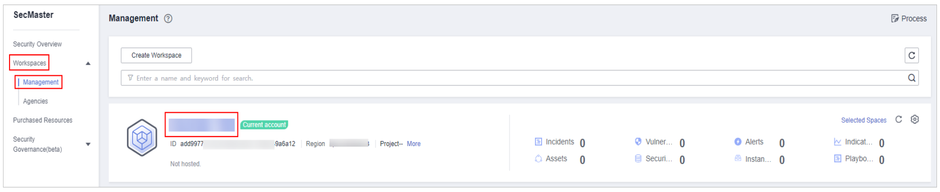
Enabling an IP Address Blocklist for Multiple Connections

Step 1 Log in to the management console.

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

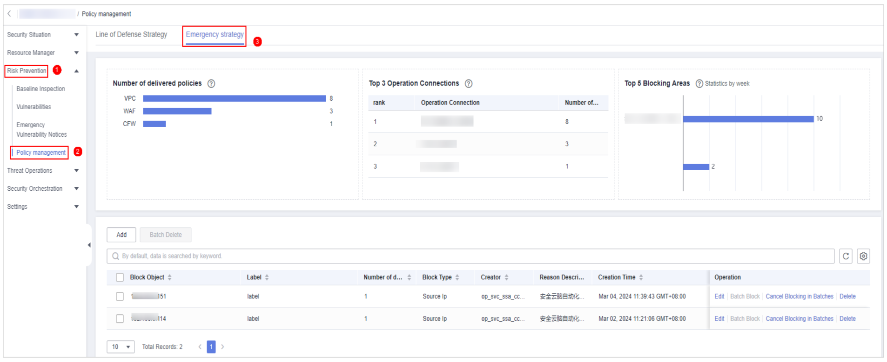
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-49 Workspace management page



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

Figure 9-50 Emergency strategy page



Step 5 On the emergency policy page, locate the row that contains the policy you want to enable batch block and click **Batch Block** in the **Operation** column.

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

----End

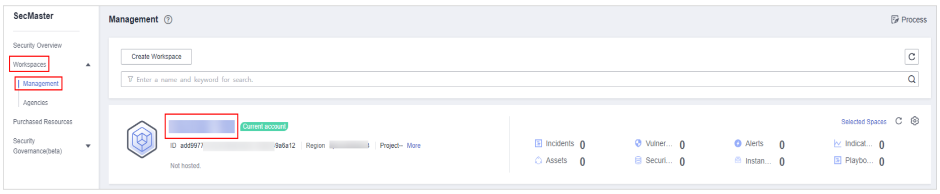
Canceling Batch Block

Step 1 Log in to the management console.

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

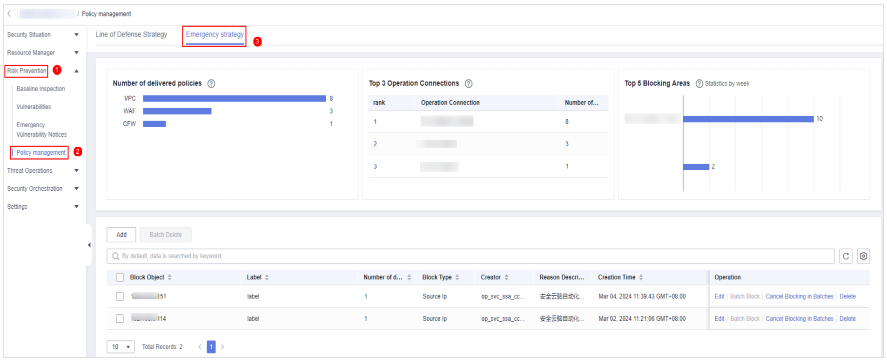
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 9-51 Workspace management page



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

Figure 9-52 Emergency strategy page



Step 5 On the emergency policy page, locate the row that contains the target policy, click **Cancel Blocking in Batches** in the **Operation** column.

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

----End

10 Threat Operations

10.1 Incident Management

10.1.1 Viewing Incidents

Scenario

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

This topic describes how to view incident information.

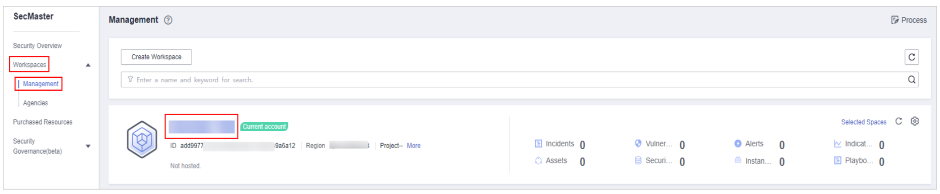
Procedure

Step 1 Log in to the management console.

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

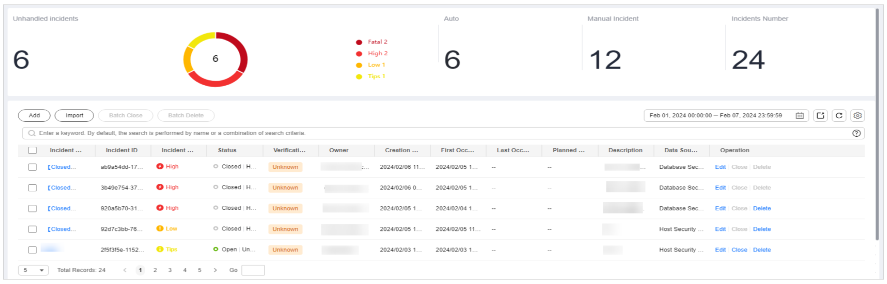
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-1 Workspace management page



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

Figure 10-2 Incidents



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

Figure 10-3 Viewing an Incident

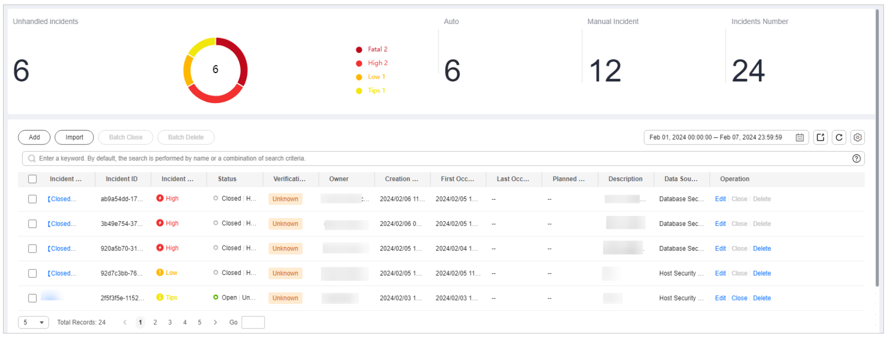


Table 10-1 Viewing an Incident

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.
Incidents Number (Incidents)	This area displays how many incidents that are reported within the specified time range in the current workspace.

Parameter	Description
Incident list	The list displays more details about each incident. You can view the total number of incidents below the incident list. You can view a maximum of 10,000 incident records page by page. To view more than 10,000 records, optimize the filter criteria. In the incident list, you can view the incident name, severity, source, and status. To obtain overview of an incident, click the incident name. The **incident overview** panel is displayed on the right. ● On the **Incident Overview** panel, you can view incident handling suggestions, basic information, and associated information (including associated threat indicators, alerts, incidents, and attack information). ● To view incident details, click **Incident Details** in the lower right corner of the incident overview panel. The incident details page is displayed. On the details page, you can view the incident timeline and attack information in addition to the information on the overview page. For example, you can view the first occurrence time of an incident, detection time, and attack process ID. ● On the incident overview or details page, you can change the incident severity and status in the corresponding drop-down list boxes. ● On the incident overview or details page, you can associate or disassociate alerts, incidents, and indicators and view information about affected resources.

----End

10.1.2 Adding or Editing an Incident

Scenario

This section describes how to add or edit an incident.

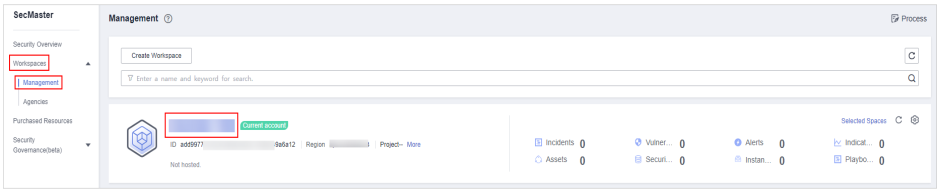
Adding an Incident

Step 1 Log in to the management console.

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

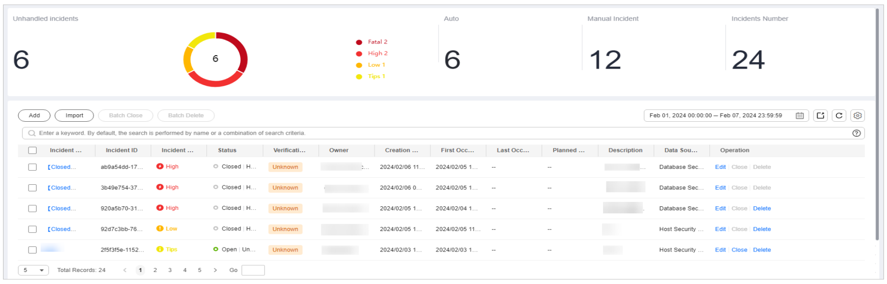
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-4 Workspace management page



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

Figure 10-5 Incidents



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

Table 10-2 Parameters for adding an incident

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

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

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

----End

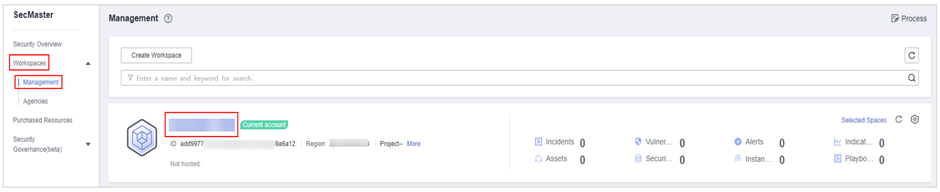
Editing an Incident

Step 1 Log in to the management console.

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

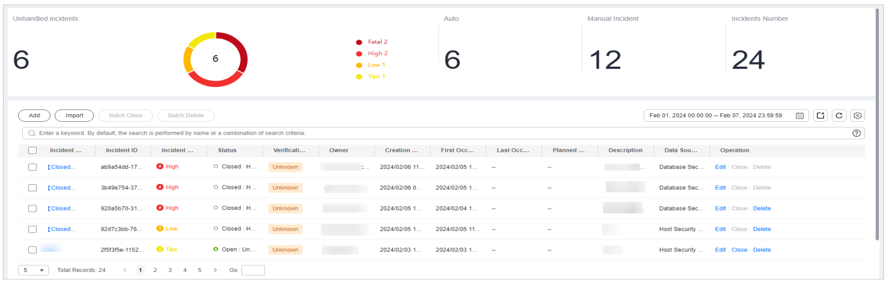
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-6 Workspace management page



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

Figure 10-7 Incidents



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

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

Table 10-3 Parameters for editing an incident

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

Parameter		Description
	(Optional) Owner	Primary owner of the incident.
Timeline	First Occurrence Time	Time when the incident occurred first time.
	(Optional) Last Occurrence Time	Time when the incident occurred last time.
	(Optional) Planned Closure Time	Time to close the incident.
Other	(Optional) Verification Status	Verification status of the incident to identify the accuracy of the incident. The options are **Unknown**, **Positive**, and **False positive**.
	(Optional) Phase	Incident phase. ● **Preparation**: Prepare resources to process incidents. ● **Detection and analysis**: Detect and analyze the cause of an incident. ● **Contain, extradition, and recovery**: Handle an incident. ● **Post Incident Activity**: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging. This parameter **cannot be modified** once configured.
	(Optional) Label	Label of the incident.
	Description	Incident description. The value can contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 1,024 characters.

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

----End

10.1.3 Importing and Exporting Incidents

Scenario

This section describes how to import and export incidents.

Limitations and Constraints

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

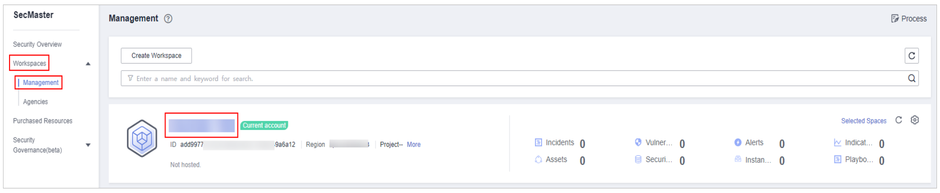
Importing Incidents

Step 1 Log in to the management console.

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

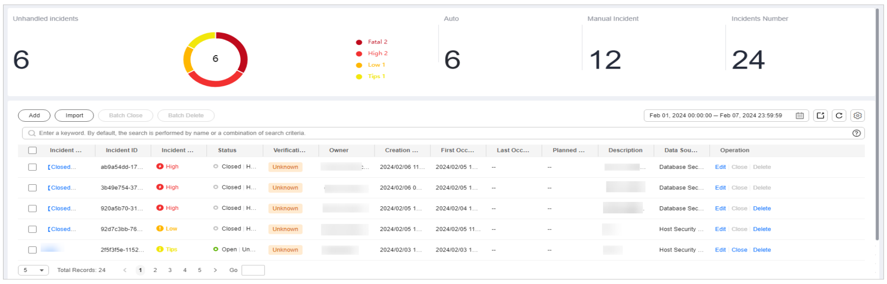
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-8 Workspace management page



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

Figure 10-9 Incidents



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

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

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

Step 8 Click **OK**.

----End

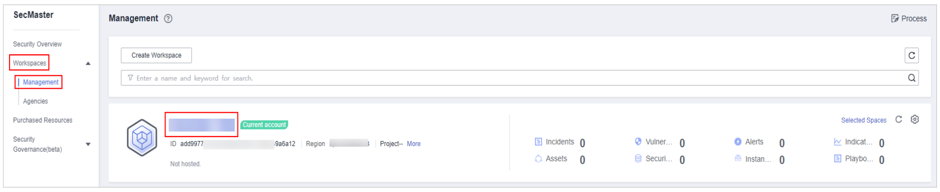
Exporting Incidents

Step 1 Log in to the management console.

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

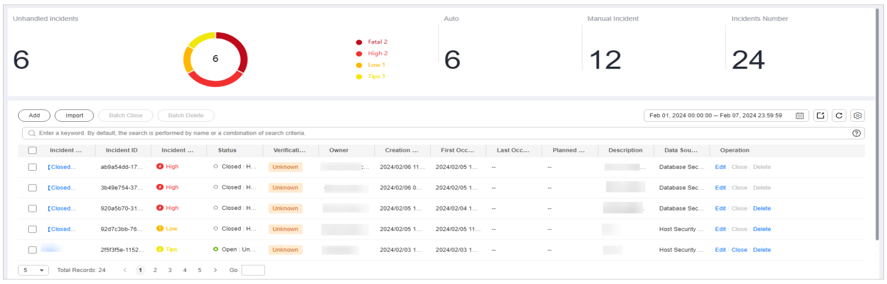
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-10 Workspace management page



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

Figure 10-11 Incidents



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

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

Table 10-4 Exporting incidents

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

Step 7 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

10.1.4 Closing or Deleting Incidents

Scenario

This topic describes how to close and delete an incident.

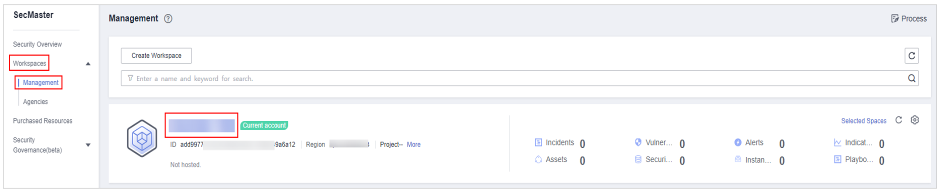
Procedure

Step 1 Log in to the management console.

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

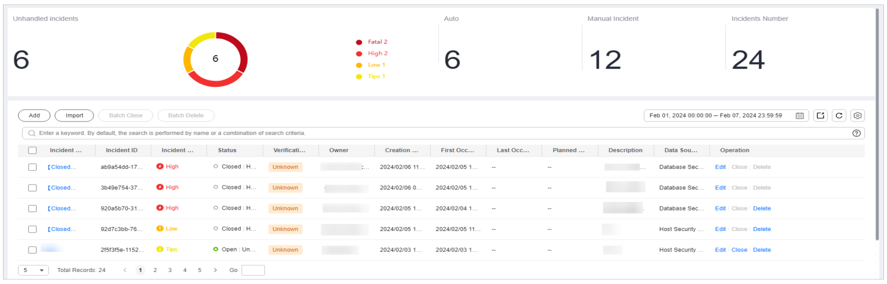
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-12 Workspace management page



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

Figure 10-13 Incidents



Step 5 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 Viewing Alerts

Scenario

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

This section describes how to view alert information.

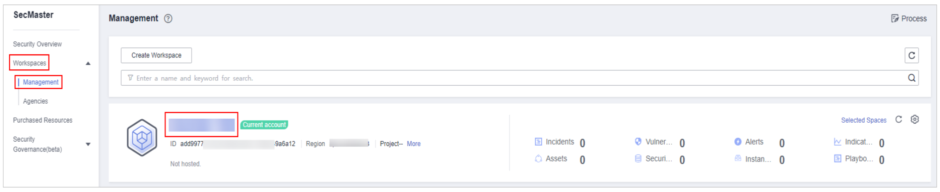
Procedure

Step 1 Log in to the management console.

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

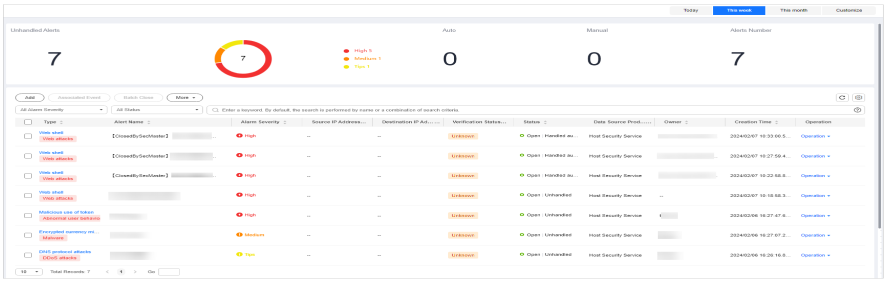
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-14 Workspace management page



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

Figure 10-15 Alerts



Step 5 View alert information.

Figure 10-16 Viewing Alerts

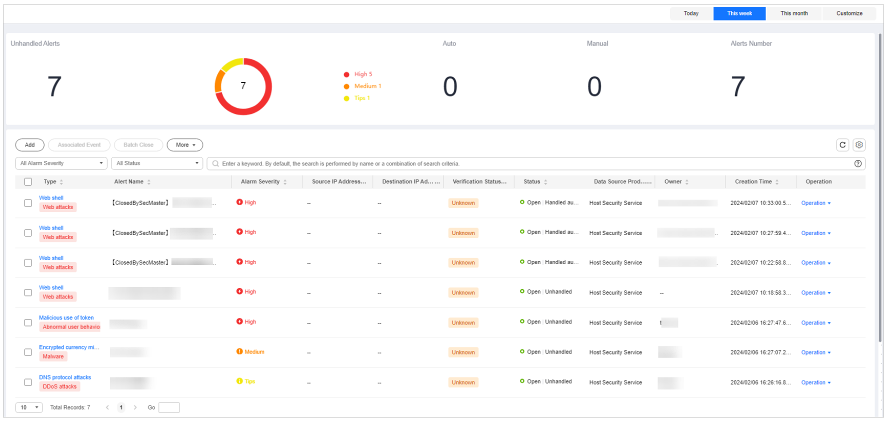


Table 10-6 Viewing Alerts

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 to an incident, and refresh the alert status. ● You can view the security overview, context, relationship, and comments about the alert. – **Security Overview**: On this tab, you can view the summary, handling suggestions, basic information, and request details of the alert. – **Context**: On this tab, you can view the key and full context information of the alert in JSON format or in a table. – **Relationship**: On this tab, you can view associated information, such as associated alerts, incidents, indicator, and affected assets, about the alert. – **Comment**: On this tab, you can view historical comments on the alert and make your comments.

----End

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

Scenario

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

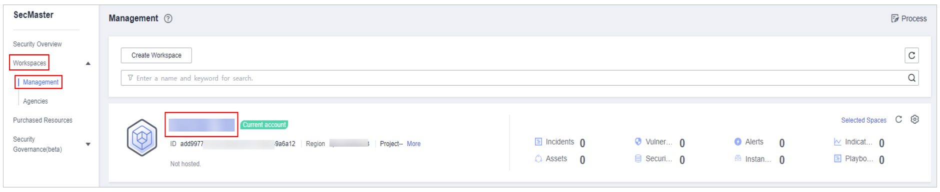
Converting an Alert to an Incident

Step 1 Log in to the management console.

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

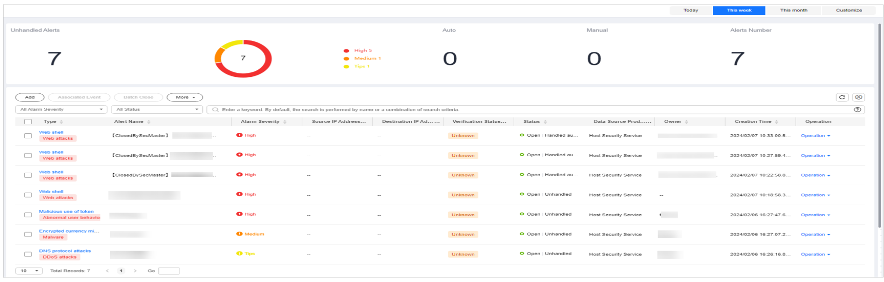
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-17 Workspace management page



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

Figure 10-18 Alerts



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

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

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

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

Step 7 Click **OK**.

----End

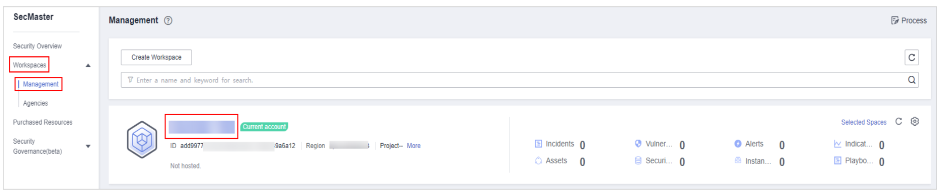
Associating an Alert with an Incident

Step 1 Log in to the management console.

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

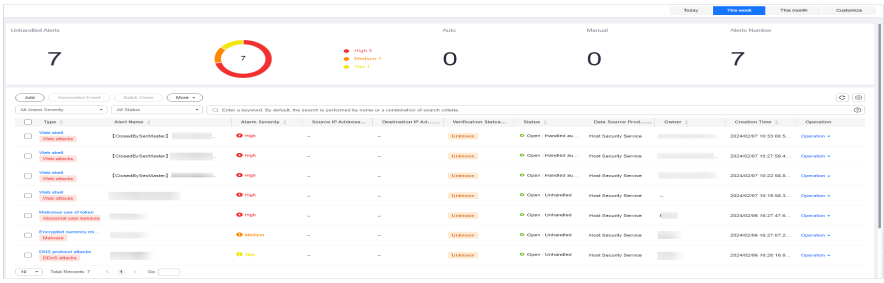
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-19 Workspace management page



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

Figure 10-20 Alerts



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

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

----End

10.2.3 Adding or Editing an Alert

Scenario

This section describes how to add or edit an alert.

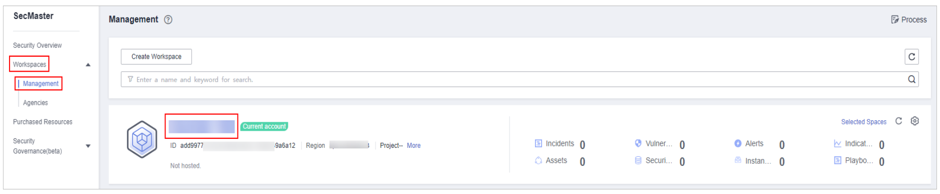
Adding an Alert

Step 1 Log in to the management console.

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

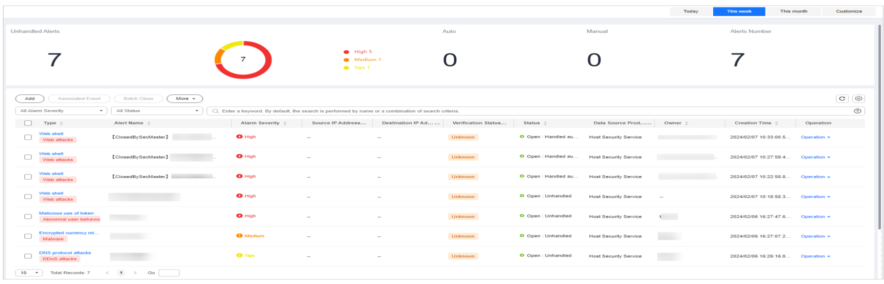
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-21 Workspace management page



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

Figure 10-22 Alerts



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

Table 10-7 Alert parameters

Parameter		Description
Basic information	Alert Name	User-defined alert name. The value must contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 255 characters
	Alert Type	Alert type
	Alert Severity	Alert severity. The options are **Tips**, **Low**, **Medium**, **High**, and **Fatal**.
	Status	Alert status. The options are **Open**, **Blocked**, and **Closed**.
	(Optional) Owner	Primary owner of the alert.
	Data Source Product Name	Data source name
	Data Source Type	Type of the data source. The options are **Huawei**, **Third-party**, and **Tenant**.
Timeline	First Occurrence Time	Time when an alert is generated for the first time.
	(Optional) Last Occurrence Time	Last time when an alert was generated
	(Optional) Planned Closure Time	Time when the alert plan is disabled.
Other	(Optional) Labels	Alert labels.
	(Optional) Debugging data	Whether to enable simulated debugging.
	(Optional) Verification Status	Verification status of the alert to identify the accuracy of the incident. The options are **Unknown**, **Positive**, and **False positive**.
	(Optional) Stage	Alert phase. ● **Preparation**: Prepare resources to process alert. ● **Detection and analysis**: Detect and analyze the cause of an alert. ● **Contain, extradition, and recovery**: Handle an alert. ● **Post Incident Activity**: Follow-up activities.

Parameter		Description
	Description	Alert description. The value can contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 1,024 characters.

Step 6 Click **OK**.

----End

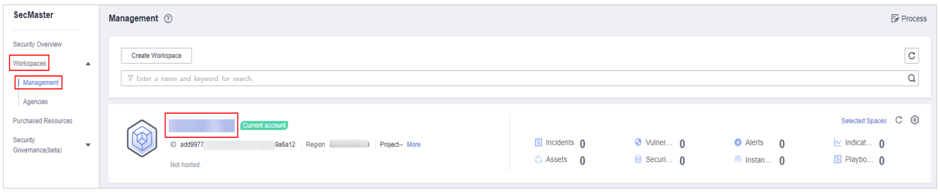
Editing an Alert

Step 1 Log in to the management console.

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

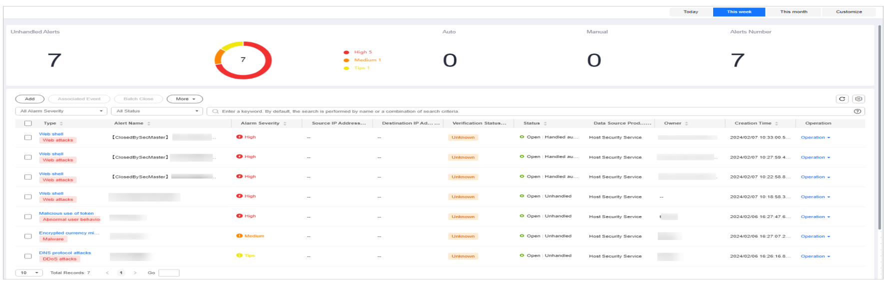
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-23 Workspace management page



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

Figure 10-24 Alerts



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

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

Table 10-8 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 255 characters
	Alert Type	Alert type
	Alert Severity	Alert severity. The options are **Tips**, **Low**, **Medium**, **High**, and **Fatal**.
	Status	Alert status. The options are **Open**, **Blocked**, and **Closed**.
	(Optional) Owner	Primary owner of the alert.
	Data Source Product Name	Name of the data source, which **cannot be changed**
	Data Source Type	Type of the data source, which **cannot be changed**
Timeline	First Occurrence Time	Time when an alert is generated for the first time.
	Last Occurrence Time	Last time when an alert was generated
	Planned Closure Time	Time when the alert plan is disabled.
Other	Labels	Alert labels.
	Debugging data	Whether to enable simulated debugging. This parameter **cannot be modified** once configured.
	Verification Status	Verification status of the alert to identify the accuracy of the incident. The options are **Unknown**, **Positive**, and **False positive**.
	Stage	Alert phase. ● **Preparation**: Prepare resources to process alert. ● **Detection and analysis**: Detect and analyze the cause of an alert. ● **Contain, extradition, and recovery**: Handle an alert. ● **Post Incident Activity**: Follow-up activities.

Parameter		Description
	Description	Alert description. The value can contain: ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 1,024 characters.

Step 7 Click **OK**.

----End

10.2.4 Importing and Exporting Alerts

Scenario

This section describes how to import and export alerts.

Limitations and Constraints

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

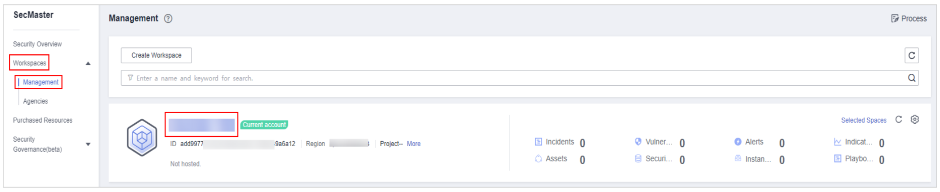
Importing Alerts

Step 1 Log in to the management console.

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

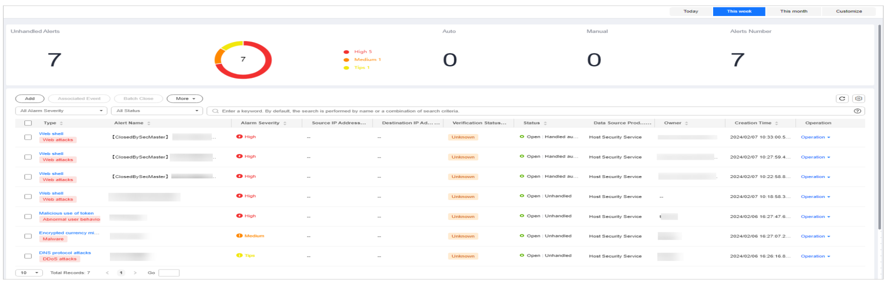
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-25 Workspace management page



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

Figure 10-26 Alerts



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

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

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

Step 8 Click **OK**.

----End

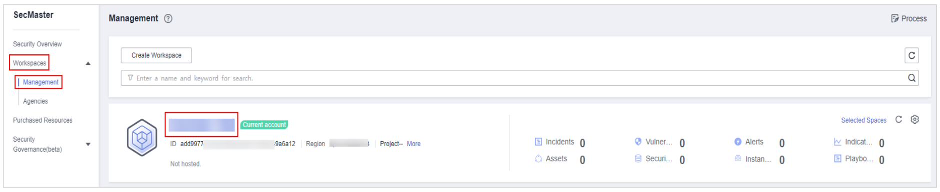
Exporting Alerts

Step 1 Log in to the management console.

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

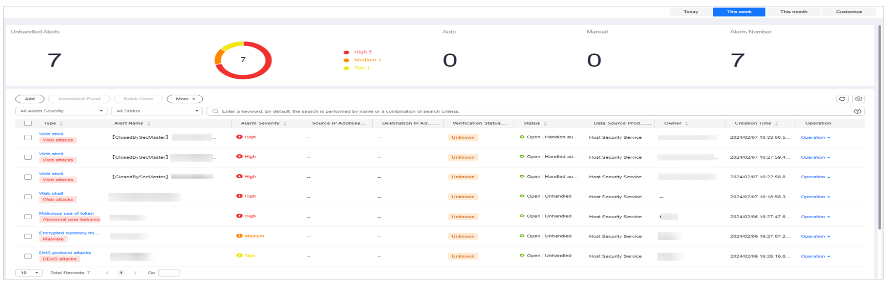
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-27 Workspace management page



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

Figure 10-28 Alerts



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

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

Table 10-9 Exporting alerts

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

Step 7 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

10.2.5 Closing or Deleting an Alert

Scenario

This topic describes how to close and delete an alert.

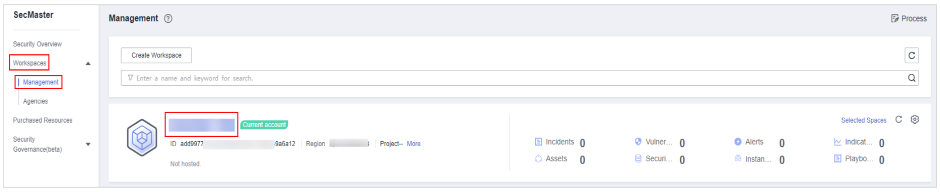
Procedure

Step 1 Log in to the management console.

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

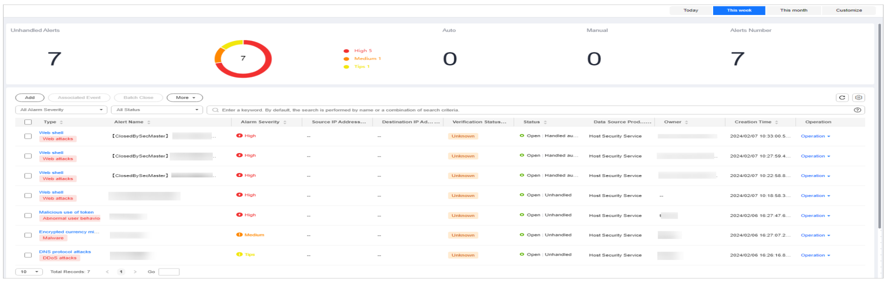
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-29 Workspace management page



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

Figure 10-30 Alerts



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

Table 10-10 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

10.2.6 Handling Alerts based on Suggestions

During data integration, SecMaster can automatically convert cloud service logs to alerts. SecMaster provides the following suggestions for handling such concerted alerts.

Abnormal System Behavior/High-risk Command Execution

Table 10-11 High-Risk Command Execution

Data Source	HSS alert logs
Alert Presentation	[dangercmd] [HSS] Host: {{ipList}} Run dangercmd, {{__time}}
Monitoring Scenario	High-Risk commands executed on servers
Alert Field	To view corresponding high-risk command alerts in SecMaster, take the following steps: 1. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**. 2. 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**.

<table>
<tr><td>Investigation Guideline and Handling Suggestion</td><td>1. Go to the Threat Operations > Security Analysis page in SecMaster, expand the target data space, and click pipeline sec-hss-alarm. The query and analysis page of ssec-hss-alarm is displayed on the right.
2. Search for the log details for the current alert based on the values of the appendInfo.event_type, __time, and ipList fields to confirm the meaning and purpose of the command.
● Use the appendInfo.process_info field to check whether the current high-risk command (process_cmdline) and its parent process command (parent_process_cmdline) are suspicious.
● You can use sec-hss-log to query the host (ipList) behavior in a similar period of time, and use appendInfo.pid_link (sec-hss-log) and appendInfo.process_info.parent_process_pid(sec-hss-alarm) to sort the process sequence. Then, you can make informative decisions to find out suspicious processes and commands. For those processes and commands, you can scan for further hacking behavior, such as viewing sensitive data, viewing network environments, privilege escalation, network proving, and PoC execution.
● If it is confirmed that the fault is triggered by attacks, contact the resource owner immediately.</td></tr>
<tr><td>High-Risk Command</td><td>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.</td></tr>
</table>

Web Attacks (SQL Injection)

- **Corresponding Alert Field**

  To view corresponding SQL inject alerts in SecMaster, take the following steps:

  a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.

  b. Click the name of the **WAF Alert Categorization and Re-Mapping** to go to the details page.

     The **msg.attack** for SQL injection is **sqli**.

- **Troubleshooting Methods and Handling Suggestions**
  a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-waf-attack**. The query and analysis page of sec-waf-attack is displayed on the right.
  b. Search for the log details for the current alert based on the values of the **attack**, **__time**, and **sip** fields. The key parameters are as follows:
     - **hit_data**: attack packet or link.
     - **uri**: request URL.
     - **action**: processing action
     - **cookie**: request cookie information.
  c. Check attack packets to see how the SQL injection is made and check whether there is any vulnerability in the application.
     If there is, rectify the fault in time by using parameterized query, input verification, and software update and patching.

Web Attacks/Vulnerability Exploits

- **Corresponding Alert Field**
  To view corresponding vulnerability exploit alerts in SecMaster, take the following steps:
  a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.
  b. Click the name of the **WAF Alert Categorization and Re-Mapping** to go to the details page.
     The **msg.attack** value for vulnerability exploits is **vuln**.
- **Troubleshooting Methods and Handling Suggestions**
  a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-waf-attack**. The query and analysis page of sec-waf-attack is displayed on the right.
  b. Search for the log details for the current alert based on the values of the **attack**, **__time**, and **sip** fields. The key parameters are as follows:
     - **hit_data**: attack packet or link.
     - **uri**: request URL.
     - **action**: processing action
     - **cookie**: request cookie information.
     - **header**: request header information.
  c. Confirm the vulnerability exploit type based on the attack packet and detect vulnerabilities in attacked assets.
     If there is a vulnerability, fix it in a timely manner to prevent attackers from exploiting this vulnerability to attack the system or applications.

Web Attacks/Command Injection

- **Corresponding Alert Field**

  To view corresponding command injection alerts in SecMaster, take the following steps:

  In SecMaster, choose **Security Orchestration** > **Objects** > **Classify&Mapping**. Click **WAF Alert Categorization and Re-Mapping** to go to the details page. The **msg.attack** value for command injection attacks is **cmdi**.

- **Troubleshooting Methods and Handling Suggestions**

  a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-waf-attack**. The query and analysis page of sec-waf-attack is displayed on the right.

  b. Search for the log details for the current alert based on the values of the **attack**, **__time**, and **sip** fields. The key parameters are as follows:

     - **hit_data**: attack packet or link.
     - **uri**: request URL.
     - **action**: processing action
     - **cookie**: request cookie information.
     - **header**: request header information.

  c. Check attack packets to see how the command injection is made and check whether there is any vulnerability in the application.

     - If there is any vulnerability, fix it as soon as possible and update the related software or database version.
     - Perform a comprehensive check on the system to see if there are other vulnerabilities or backdoors.
     - Restrict system access permissions. For example, you can disable the root account and restrict access from some IP addresses to reduce possible intrusion paths.

Abnormal System/Process Behavior

Locate the affected assets, services, and workloads based on the corresponding alerts.

- **Corresponding Alert Field**

  To view corresponding abnormal system or process behavior alerts in SecMaster, take the following steps:

  a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.

  b. Click the name of the **HSS Alert Categorization and Re-Mapping** to go to the details page.

     Abnormal process behavior: **msg.appendInfo.event_type=3007**

- **Troubleshooting Methods and Handling Suggestions**

a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-hss-alarm**. The query and analysis page of sec-hss-alarm is displayed on the right.
   i. Search for the log details for the current alert based on the values of the **appendInfo.event_type**, **__time**, and **ipList** fields.
b. Check the information about the current process and parent process in **appendInfo. process_info** to determine whether the process is abnormal. If the process is abnormal, contact the corresponding resource owner.
   - Immediately stop affected processes or services to avoid further attacks or other damage.
   - Investigate the causes and sources of abnormal behavior by all means, for example, viewing logs, monitoring the system, and analyzing the process memory, to determine the specific symptoms and possible root causes of exceptions.
   - Based on the nature and severity of the abnormal behavior, take proper measures, such as restarting processes, rectifying software errors, rectifying system faults, and replacing hardware devices.
   - Comprehensively check the affected system to see if there are other vulnerabilities or backdoors.

Abnormal System Behavior/Key File Directory Modifications

Locate the affected assets, services, and workloads based on the corresponding alerts.

- **Corresponding Alert Field**

  To view corresponding key file directory modification alerts in SecMaster, take the following steps:

  a. Go to the **Security Orchestration** page of the target workspace. Then, choose **Objects** > **Classify&Mapping**.
  b. Click the name of the **HSS Alert Categorization and Re-Mapping** to go to the details page.

     Key file directory modification: **msg.appendInfo.event_type=3005**
- **Troubleshooting Methods and Handling Suggestions**
  a. Go to the **Threat Operations** > **Security Analysis** page in SecMaster, expand the target data space, and click pipeline **sec-hss-alarm**. The query and analysis page of sec-hss-alarm is displayed on the right.
  b. Search for the log details for the current alert based on the values of the **appendInfo.event_type**, **__time**, and **ipList** fields.

     In the preceding information, **appendInfo.file_info** indicates the file directory information. Check whether the file directory information is normal. If the file directory information is abnormal, contact the corresponding resource owner.
     - Determine the impact scope of the change. First, determine the files that are affected by the directory change and the impact of the files on services. If the impact scope is large, immediate measures must be taken to prevent further losses.

- Restore key files: If directories or files are changed abnormally, restore them in a timely manner. If a file is deleted or damaged, you need to restore it from a backup. If the files are not backed up, stop related operations immediately and take data restoration measures to restore the files to the status before the change.
- Update related configurations: For some programs and systems that require configuration file paths, update related configurations in a timely manner to ensure that these programs and systems can correctly access key files.
- Review the change reason: Review and check the reason for the directory change. If the change was caused by human misoperations, correct the fault and strengthen management in a timely manner. If the change was made by the system, evaluate the necessity and impact of the change and ensure that the change is reasonable and secure.
- Enhance security measures: For security management of key files, measures must be enhanced to ensure that files cannot be mistakenly deleted, maliciously tampered with, or disclosed. Measures such as encryption, backup, and access control can be taken to ensure file integrity and availability.

10.2.7 One-click Blocking or Unblocking

Scenario

An emergency policy is used to quickly prevent attacks. You can select a block type based on the alert source to block attackers. **Table 10-12** lists recommended settings. You can also block a single attack source based on the comprehensive investigation of multiple alerts.

Table 10-12 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.

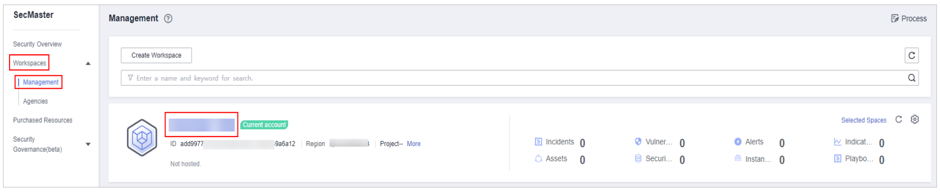
One-click Blocking

Step 1 Log in to the management console.

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

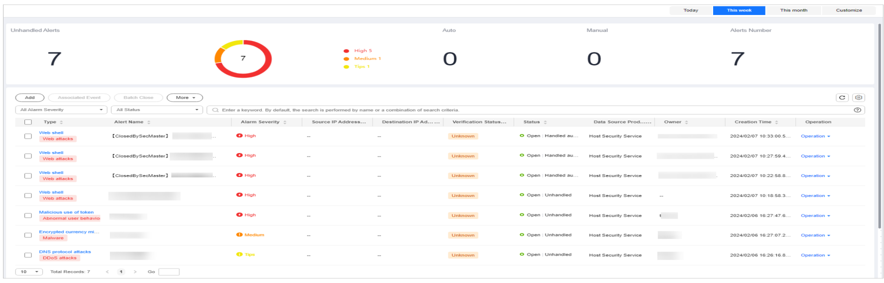
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-31 Workspace management page



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

Figure 10-32 Alerts



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

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

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

Table 10-13 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 (,). Example: – Single IP address: 192.168.0.0 – IP address range: 192.168.0.0/12 ● If you select **IAM** for **Blocked Object Type**, enter IAM user names. ● A maximum of 50 IP addresses, IP address ranges, or IAM users can be blocked by an emergency policy once.
Label	Label of the custom emergency policy.
Operation Connection	Select the operation connections for the policy.
Block Aging	Check whether the policy needs to be stopped. ● If you select **Yes**, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address or IP address range will not be blocked. ● If you select **No**, the policy is always valid and blocks the specified IP address or IP address range.
Reason Description	Description of the custom policy.

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

----End

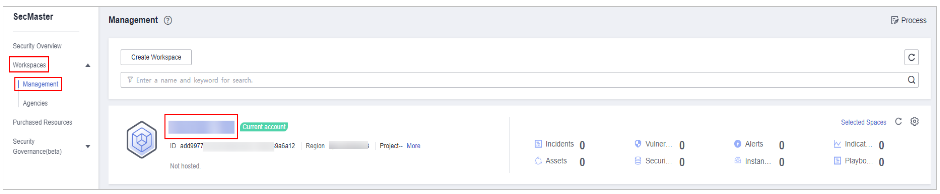
One-click Unblocking

Step 1 Log in to the management console.

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

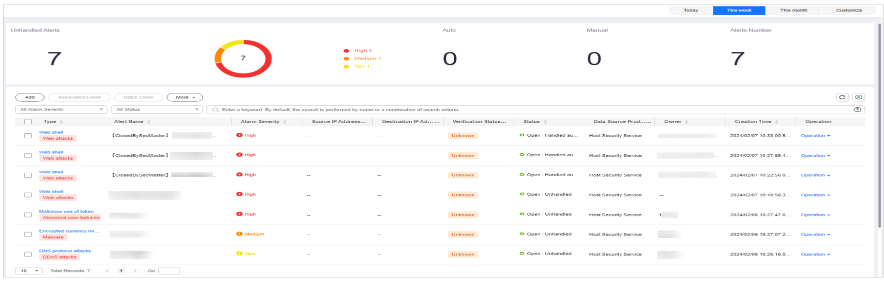
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-33 Workspace management page



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

Figure 10-34 Alerts



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

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

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

----End

10.3 Indicator Management

10.3.1 Adding and Editing an Indicator

Scenario

The indicator library list displays information about all your indicators.

This section describes how to create and edit an indicator.

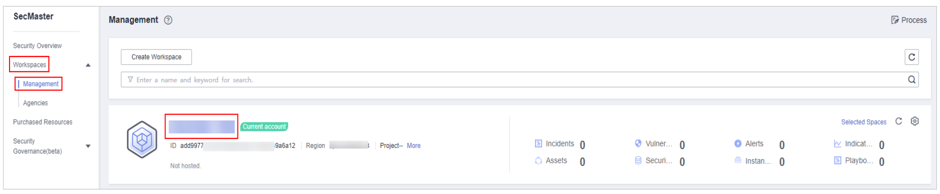
Adding an Indicator

Step 1 Log in to the management console.

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

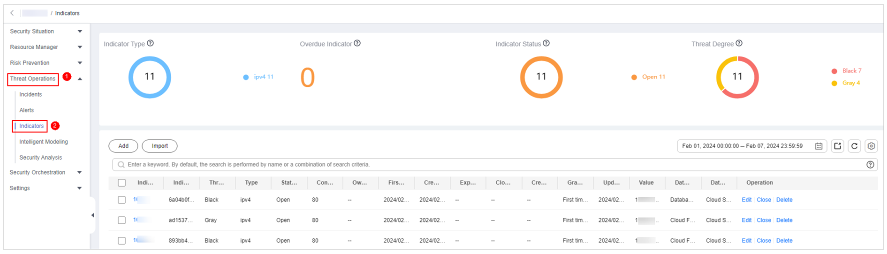
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-35 Workspace management page



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

Figure 10-36 Indicators



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

Table 10-14 Indicator parameters

Parameter	Description
Indicator Name	Name of a user-defined threat indicator. The value can contain: Only uppercase letters, lowercase letters, digits, and the special characters: -_ ()
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 **Huawei**, **Third-party**, and **Tenant**.
Status	Indicator status. Possible values are **Open**, **Closed**, and **Revoked**.
(Optional) Confidence	Reliability of the selected indicator. The value ranges from 80 to 100.
(Optional) Owner	Primary owner of the indicator.
(Optional) Labels	Label of a user-defined counter.
First Occurrence Time	First occurrence time of the indicator.
Last Occurrence Time	Latest occurrence time of the indicator.
(Optional) Expiration Time	Expiration time of the indicator.
Invalid or not	Whether to invalidate the indicator. The default value is **No**.

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

Step 6 Click **OK**.

----End

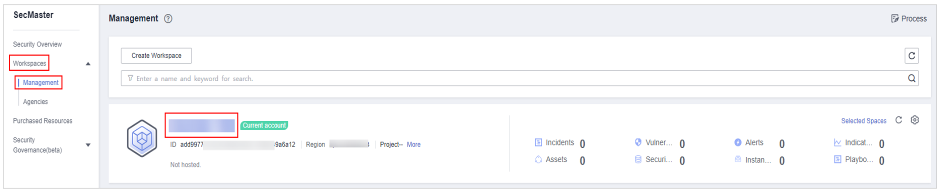
Editing an Indicator

Step 1 Log in to the management console.

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

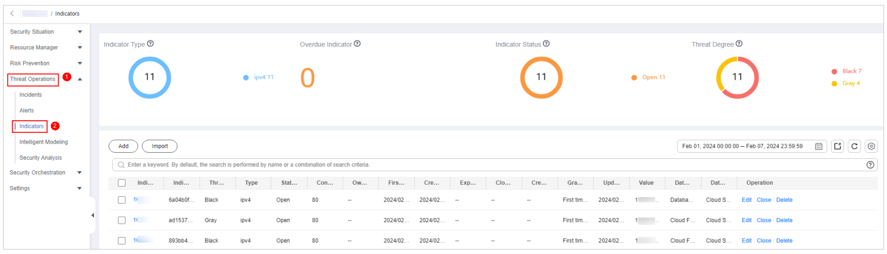
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-37 Workspace management page



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

Figure 10-38 Indicators



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

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

Table 10-15 Indicator parameters

Parameter	Description
Indicator Name	Name of a user-defined threat indicator. The value can contain: Only 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	Name of the data source, which **cannot be changed**
Data Source Type	Type of the data source, which **cannot be changed**
Status	Indicator status. Possible values are **Open**, **Closed**, and **Revoked**.
Confidence	Reliability of the selected indicator. The value ranges from 80 to 100.
Owner	Primary owner of the indicator.
Labels	Label of a user-defined indicator.
First Occurrence Time	First occurrence time of the indicator.
Last Occurrence Time	Latest occurrence time of the indicator.
Expiration Time	Expiration time of the indicator.
Invalid or not	Whether to invalidate the indicator. The default value is **No**.
Granularity	Granularity of the indicator. The options are **First time observed**, **Self-produced data**, **To be purchased**, and **Query from external network**.
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

10.3.2 Disabling and Deleting an Indicator

Scenario

This topic describes how to disable or delete an indicator.

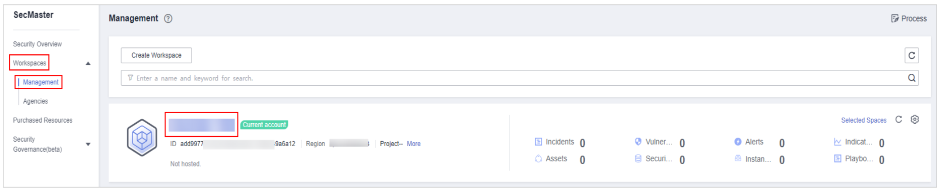
Procedure

Step 1 Log in to the management console.

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

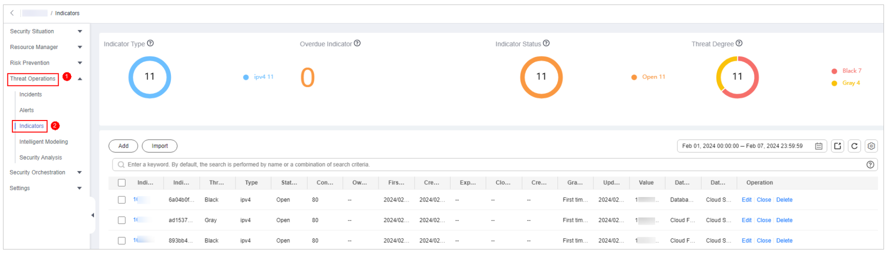
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-39 Workspace management page



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

Figure 10-40 Indicators



Step 5 On the **Indicators** page, close or delete an indicator.

Table 10-16 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**.

Operation	Description
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 Intelligence Indicators

Scenario

This section describes how to import and export intelligence indicators.

Constraints

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

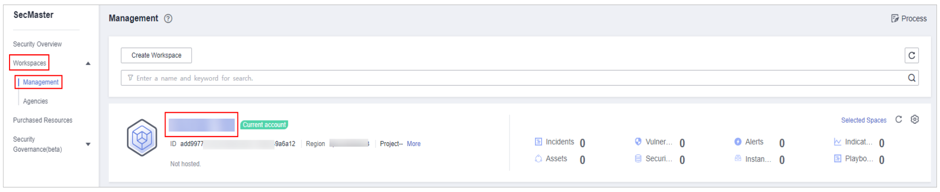
Importing an Indicator

Step 1 Log in to the management console.

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

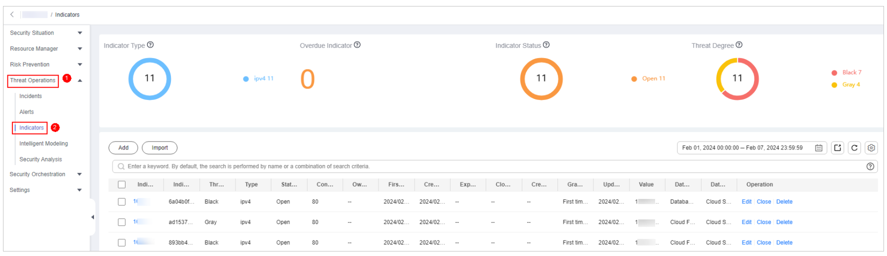
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-41 Workspace management page



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

Figure 10-42 Indicators



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

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

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

Step 8 Click **OK**.

----End

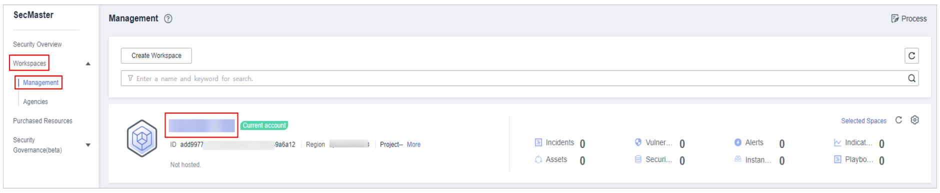
Exporting Indicators

Step 1 Log in to the management console.

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

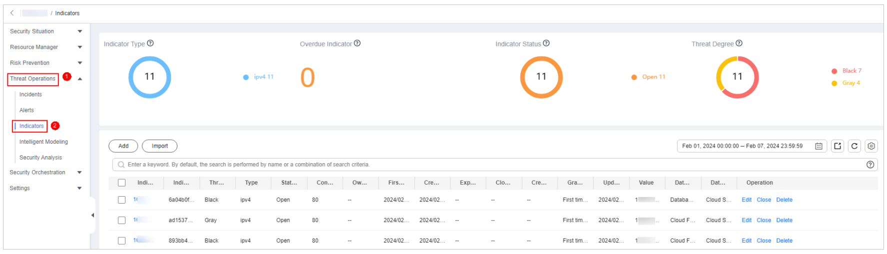
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-43 Workspace management page



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

Figure 10-44 Indicators



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

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

Table 10-17 Exporting indicators

Parameter	Description
Format	By default, the indicator list is exported into an Excel.

Parameter	Description
Columns	Select the indicator parameters to be exported.

Step 7 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

10.3.4 Viewing Indicators

Scenario

This topic describes where to view existing intelligence indicators.

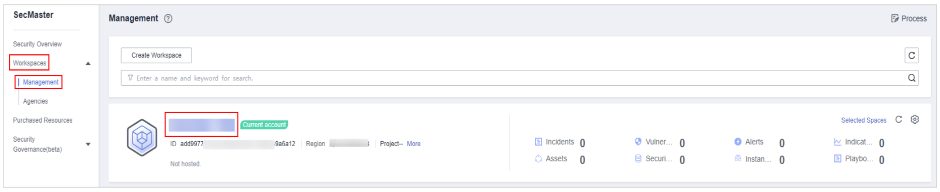
Procedure

Step 1 Log in to the management console.

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

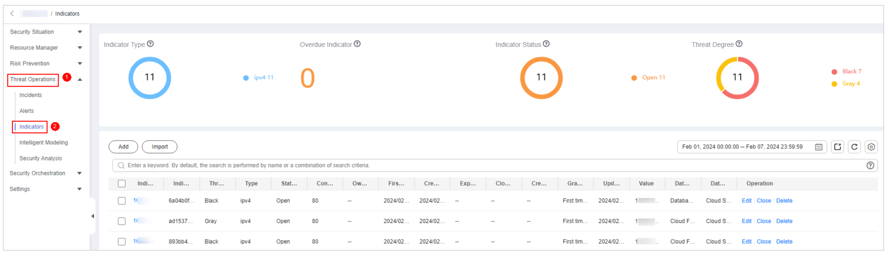
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-45 Workspace management page



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

Figure 10-46 Indicators



Step 5 On the **Indicators** page, view details about the indicator.

Figure 10-47 Viewing an Indicator

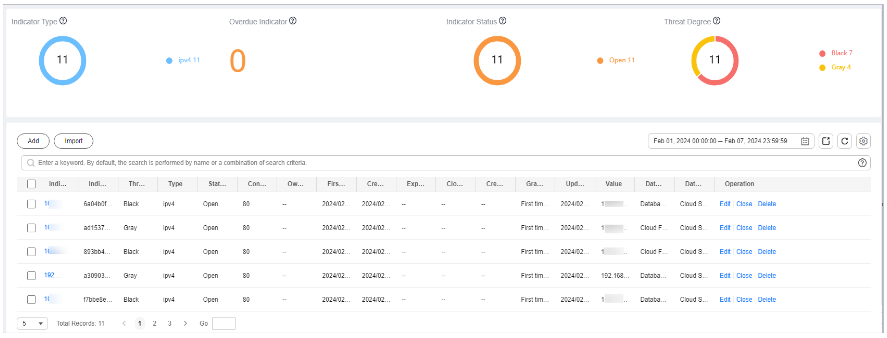


Table 10-18 Indicator parameters

Parameter	Description
Indicator Type	**Indicator Type** displays the total number of indicators of all types and the number of indicators of the corresponding type.
Overdue Indicator	**Overdue Indicator** displays the total number of threat indicators that have expired and have not been closed.
Indicator Status	**Indicator Status** displays the total number of indicators in different states and the number of indicators in the corresponding state.
Threat Degree	**Threat Degree** displays the number of indicators of different threat levels.
Indicator list	Displays detailed information about each indicator. You can view the total number of indicators below the indicator list. You can view a maximum of 10,000 indicator records page by page. To view more than 10,000 records, optimize the filter criteria. You can view the threat degree, discovery time, and status of indicators. To view details about an indicator, click the indicator name. The indicator details are displayed on the right of the page. ● On the **Indicator Overview** page, you can view basic information of an indicator as well as its association information, such as associated indicators, alerts, and incidents. ● In the **Associated Information** area, you can bind or unbind an indicator to or from other indicators, alerts, and incidents.

----End

10.4 Intelligent Modeling

10.4.1 Viewing Available Model Templates

Scenario

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

This section describes how to view available model templates.

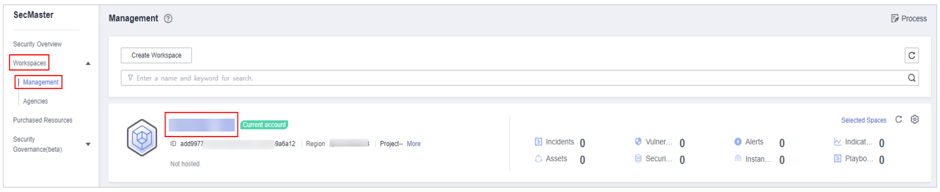
Procedure

Step 1 Log in to the management console.

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

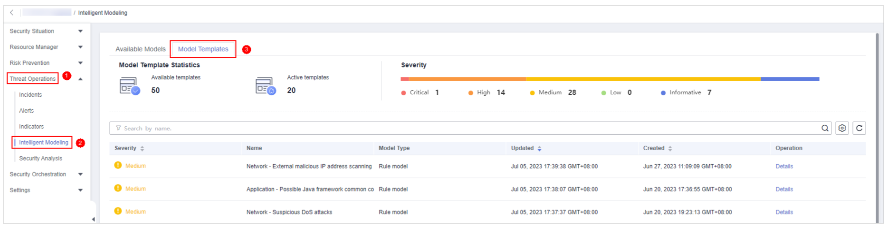
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-48 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**. On the displayed page, click the **Model Templates** tab.

Figure 10-49 Model Templates tab



Step 5 On the **Model Templates** tab, view available model templates.

Table 10-19 Template information

Parameter	Description
Model Template Statistics	This area displays how many **Available templates** and how many **Active templates** you have.
Severity	This bar displays the number of available templates by severity levels, including **Critical**, **High**, **Medium**, **Low**, and **Informative**.

Parameter	Description
Template list	● The template list displays the severity, name, and model type of each template as well as when the template is created and upgraded. ● To view details about a model template, locate the row that contains the template, click **Details** in the **Operation** column. The template details page is displayed on the right. On the details page, you can view the description, query rules, triggering conditions, and query plans of the current model template.

----End

10.4.2 Creating and Editing a Model

Scenario

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

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

- Creating an Alert Model Using a Template
- Creating a Custom Alert Model
- Editing a Model

Limitations and Constraints

- A maximum of 100 alert models can be created in a single workspace under a single account in a single region.
- The running interval of an alert model must be greater than or equal to 5 minutes, and the time range for querying data must be less than or equal to 14 days.

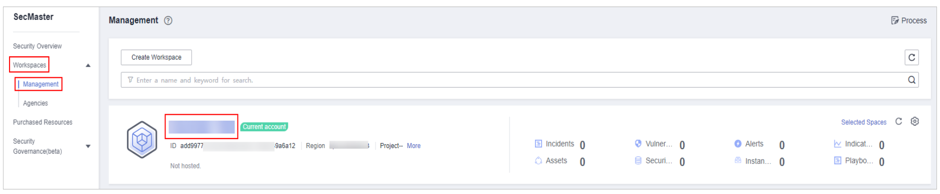
Creating an Alert Model Using a Template

Step 1 Log in to the management console.

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

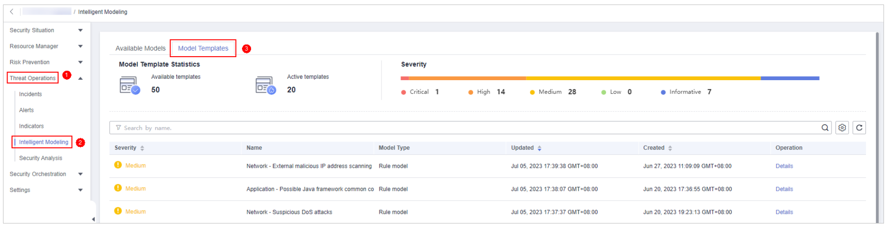
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-50 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**. On the displayed page, click the **Model Templates** tab.

Figure 10-51 Model Templates tab



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

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

Step 7 On the **Create Threat Model** page, configure basic information about the model by referring to **Table 10-20**.

Table 10-20 Basic alert model parameters

Parameter	Description
Pipeline Name	Select the execution pipeline of the alert model.
Model Name	Name of the alert model.
Severity	Severity of the alert model. You can set the severity to **Critical**, **High**, **Medium Low**, or **Informative**.
Alarm Type	Alarm type displayed after the alert model is triggered.
Model Type	The default value is **Rule model**.
Description	Description of the alert model
Status	Indicates whether to enable the alert model. • : indicates that the model is enabled. This is the default status. • : indicates that the model is disabled. 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 10-21**.

Table 10-21 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result.
Query Plan	Set an alert query plan. ● Running query interval: xx minutes/hour/day. If the running query interval is minute, set this parameter to a value ranging from 5 to 59 minutes. If the running query interval is hour, set this parameter to a value ranging from 1 to 23 hours. If the running query interval is day, set this parameter to a value ranging from 1 to 14 days. ● Time window: xx minutes/hour/day. If the time window is minute, the value ranges from 5 minutes to 59 minutes. If the time window is hour, the value ranges from 1 hour to 23 hours. If the time window is day, the value ranges from 1 day to 14 days. ● Execution Delay: xx minutes. The value ranges from 0 to 5 minutes.
Advanced Alarm Settings	● **Custom Information**: Customize extended alert information. Click **Add**, and set the **key** and **value** information. ● **Alarm Details**: Enter the alarm name, description, and handling suggestions.
Trigger Condition	Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx. If there are multiple triggers, click **Add**.
Alarm Trigger	The way to trigger alerts for queried results. The options are as follows: ● One alert for all query results ● One alert for each query result
Debugging	Sets whether to generate debugging alarms.
Suppression	Specifies whether to stop the query after an alert is generated. ● : indicates that the query stops after an alert is generated. ● : indicates that the query is not stopped after an alert is generated.

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

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

----End

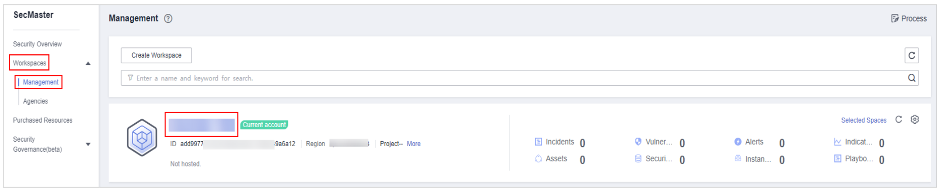
Creating a Custom Alert Model

Step 1 Log in to the management console.

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

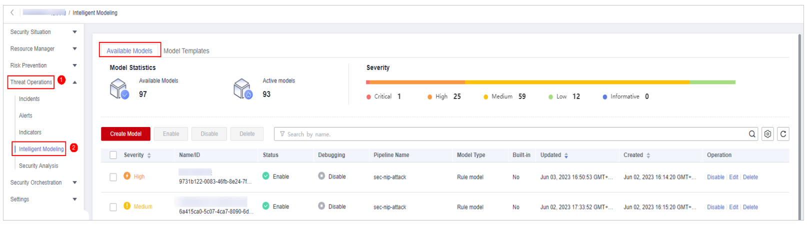
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-52 Workspace management page



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

Figure 10-53 Available Models



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

Step 6 On the **Create Model** slide-out panel displayed, configure basic information about the alert model. For details about the parameters, see **Table 10-22**.

Table 10-22 Basic alert model parameters

Parameter	Description
Pipeline Name	Select the execution pipeline of the alert model.
Model Name	Name of the alert model.
Severity	Severity of the alert model. You can set the severity to Critical, High Risk, Medium Risk, Low Risk, or Warning.

Parameter	Description
Alarm Type	Alarm type displayed after the alert model is triggered.
Model Type	The default value is **Rule model**.
Description	Description of the alert model
Status	Indicates whether to enable the alert model. • : indicates that the model is enabled. This is the default status. • : indicates that the model is disabled. The status set here can be changed after the entire alert model is set successfully.

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

Step 8 Set the model logic. For details about the parameters, see **Table 10-23**.

Table 10-23 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result. For details about the syntax, see **Query and Analysis Statements - SQL Syntax**.
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.
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. ● : indicates that the query stops after an alert is generated. ● : indicates that the query is not stopped after an alert is generated.

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

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

----End

Editing a Model

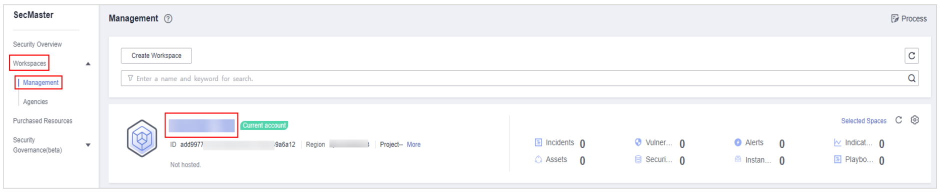
Only custom models can be edited.

Step 1 Log in to the management console.

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

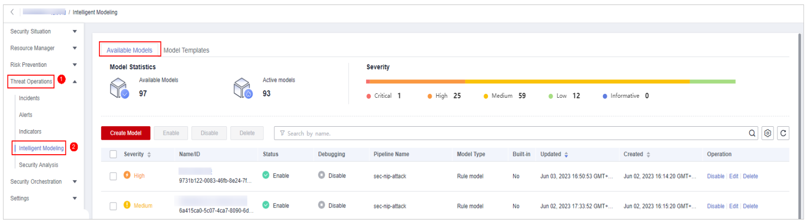
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-54 Workspace management page



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

Figure 10-55 Available Models



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

Step 6 On the **Edit Model** slide-out panel, configure basic information about the alert model. For details about the parameters, see **Table 10-24**.

Table 10-24 Basic alert model parameters

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

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

Step 8 Set the model logic. For details about the parameters, see **Table 10-25**.

Table 10-25 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result.
Query Plan	Set an alert query plan. ● Running query interval: xx minutes/hour/day. If the running query interval is minute, set this parameter to a value ranging from 5 to 59 minutes. If the running query interval is hour, set this parameter to a value ranging from 1 to 23 hours. If the running query interval is day, set this parameter to a value ranging from 1 to 14 days. ● Time window: xx minutes/hour/day. If the time window is minute, the value ranges from 5 minutes to 59 minutes. If the time window is hour, the value ranges from 1 hour to 23 hours. If the time window is day, the value ranges from 1 day to 14 days. ● Execution Delay: xx minutes. The value ranges from 0 to 5 minutes.
Advanced Alarm Settings	● **Custom Information**: Customize extended alert information. Click **Add**, and set the **key** and **value** information. ● **Alarm Details**: Enter the alarm name, description, and handling suggestions.
Trigger Condition	Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx. If there are multiple triggers, click **Add**.
Alarm Trigger	The way to trigger alerts for queried results. The options are as follows: ● One alert for all query results ● One alert for each query result
Debugging	Sets whether to generate debugging alarms.
Suppression	Specifies whether to stop the query after an alert is generated. ● : indicates that the query stops after an alert is generated. ● : indicates that the query is not stopped after an alert is generated.

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

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

----End

10.4.3 Viewing Available Models

Scenario

This topic describes how to view available models.

Prerequisites

A model has been created. For details, see **Creating and Editing a Model**.

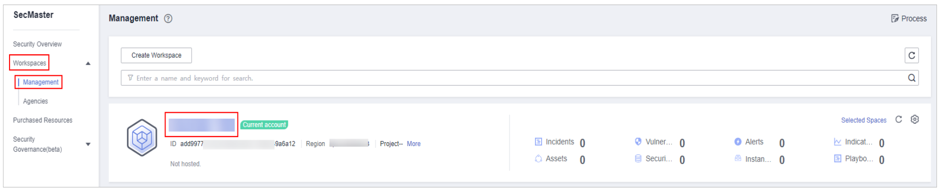
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

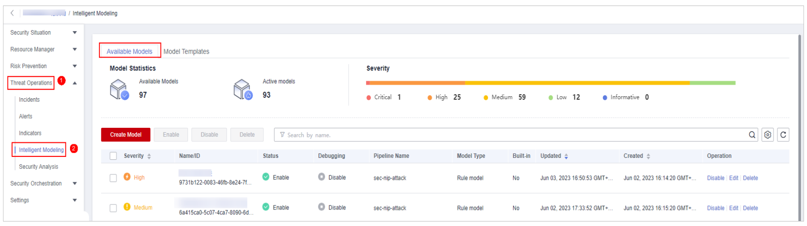
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-56 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**.

Figure 10-57 Available Models



Step 5 On the **Available Models** tab, view available models.

Table 10-26 Viewing available models

Parameter	Description
Model Statistics	This area displays how many **Available Models** and how many **Active models** you have.
Severity	This bar displays the number of available models by severity levels, including **Critical**, **High**, **Medium**, **Low**, and **Informative**.
Model list	The model list displays the severity, name/ID, pipeline name, model type of each model as well as when the model is created and upgraded.

----End

10.4.4 Managing Models

Scenario

This topic walks you through how to manage models, such as enabling, disabling, and deleting a model.

Limitations and Constraints

Only custom models can be enabled, disabled, and deleted.

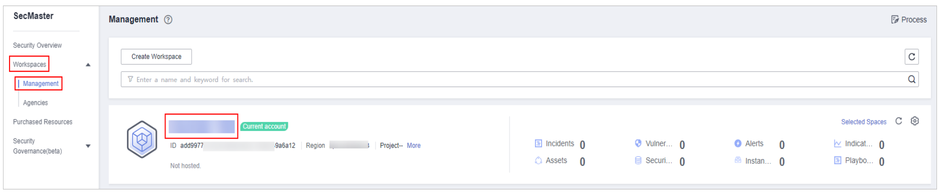
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

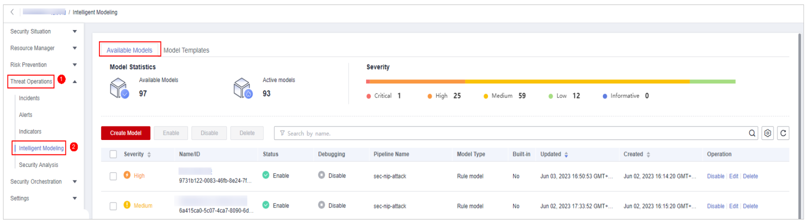
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-58 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**.

Figure 10-59 Available Models



Step 5 On the **Available Models** tab, manage models.

Table 10-27 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.
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 **Log Access Supported by SecMaster**.

Limitations and Constraints

- A maximum of 500 results can be returned for a single analysis query.
- A maximum of 50 shortcut queries can be created in a pipeline. That is, a maximum of 50 query analysis criteria can be saved as shortcut queries.
- If there are over 50,000 results for a single query, the accuracy may decrease. In this case, you can select a short time range or apply more filter criteria to reduce the number of query results.
- In aggregation queries (for example, GROUP BY statement) based on several fields, the default number of buckets for the second field is 10. If more than 10 buckets are generated, part of qualified data will be lost. In this case, the query results are not accurate.

10.5.2 How to Use Security Analysis

Table 10-28 shows the process of using the security analysis function.

Table 10-28 Process

Step	Description
Adding a Workspace	Add a workspace for resource isolation and control.
Integrating Data	Configure the data to be accessed. SecMaster can integrate log data of multiple Huawei Cloud products, such as storage, management and supervision, and security. After the integration, you can search for and analyze all collected logs.
(Optional) **Adding a Data Space**	Create a data space for storing collected log data. For data accessed through the console, the system creates a default data space. You do not need to create a data space.
(Optional) **Creating a Pipeline**	Create pipelines for collecting, storing, and querying log data. For data accessed through the console, the system creates a default data pipeline. You do not need to create a pipeline.

Step	Description
Configuring Indexes	Configure indexes to narrow down the query scope. By default, indexes have been configured for some reserved fields in the accessed cloud service logs. For details, see **Log Fields**.
Querying and Analyzing Data	Query and analyze the accessed data.
Downloading Logs	Allows you to download raw logs or queried and analyzed logs.
Querying Analysis Results in Charts and Tables	After you run query and analysis statements, SecMaster can display the query and analysis results in charts and tables. Currently, data can be displayed in tables, line charts, bar charts, and pie charts.

10.5.3 Log Fields

If you access WAF, HSS, CFW, CTS, and IPS logs through the console, SecMaster adds information such as log sources and timestamps to these logs in the form of key-value pairs.

This section describes the meaning of each field.

- **Common Fields**: describes common fields.
- **sec-waf-attack**: describes the fields in WAF attack logs.
- **sec-waf-access**: describes the fields in WAF access logs.
- **sec-obs-access**: describes the fields in OBS access logs.
- **sec-nip-attack**: describes the fields in IPS attack logs.
- **sec-iam-audit**: describes the fields in IAM audit logs.
- **sec-hss-vul**: describes the fields in the HSS host vulnerability scan result.
- **sec-hss-alarm**: describes the fields in the HSS host security alerts.
- **sec-hss-log**: describes the fields in the HSS host security logs.
- **sec-ddos-attack**: describes the fields in the DDoS attack logs.
- **sec-cts-audit**: describes the fields in the CTS logs.
- **sec-cfw-risk**: describes the fields in the CFW attack incident logs.
- **sec-cfw-flow**: describes the fields in the CFW traffic logs.
- **sec-cfw-block**: describes the fields in the CFW access control logs.
- **sec-apig-access**: describes the fields in the API Gateway access logs.
- **sec-dbss-alarm**: describes the fields in the DBSS alert logs.
- **sec-dsc-alarm**: describes the fields in the DSC alert logs.

Common Fields

Table 10-29 Common fields

Parameter	Field Type	Description
__time	Date	Time when a log is generated
__raw	String	Raw log
ops.source	String	Data source
ops.rgn	String	Site
ops.csvc	String	Data source (cloud service)
ops.ver	String	Data warehouse version
ops.hash	String	Integrity verification of **extend hash value of original**
[src_/dest_]asset.domain.id	String	Domain ID
[src_/dest_]asset.domain.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
[src_/dest_]geo.isp	String	Carrier
[src_/dest_]geo.loc.lat	Float	Latitude
[src_/dest_]geo.loc.lon	Float	Longitude
[src_/dest_]geo.tz	Integer	Time zone
[src_/dest_]geo.utc_off	Integer	Time zone
[src_/dest_]geo.cac	String	Time zone

Parameter	Field Type	Description
[src_/dest_]geo.iddc	String	International call prefix code
[src_/dest_]geo.cc	String	Country code (ISO)
[src_/dest_]geo.contc	String	Continental code (ISO)
[src_/dest_]geo.idc	String	Data center (equipment room)
[src_/dest_]geo.bs	String	Mobile base station
[src_/dest_]geo.cc3	String	Country code (3 digits)
[src_/dest_]geo.euro	String	EU member states

sec-waf-attack

Fields in WAF attack logs

Table 10-30 sec-waf-attack

Field	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 10-31 describes the fields in WAF access logs.

Table 10-31 sec-waf-access

Field	Type	Description
requestid	String	Random ID
time	Date	Log time
eng_ip	String	Engine IP address
hostid	String	ID of a protected domain name
tenantid	String	Tenant ID of the protected domain name
projectid	String	Project ID of the protected domain name
remote_ip	String	IP address of the client that sends the request
scheme	String	Request protocol type
response_code	String	Response code of a request
method	String	Request method
http_host	String	Domain name of the requested server
url	String	Request URL
request_length	String	Request length
bytes_send	String	Total number of bytes sent to the client
body_bytes_sent	String	Total number of bytes of the response body sent to the client
upstream_addr	String	IP address of the selected backend server
request_time	String	Request processing time, which starts from the first byte sent from the client
upstream_response_time	String	Response time of the backend server
upstream_status	String	Response code of the backend server
upstream_connect_time	String	Duration for connecting to the backend server

Field	Type	Description
upstream_header_time	String	Time used by the backend server to receive the first byte of the response header
bind_ip	String	Retrieval IP address of the engine
engine_id	String	Unique ID of the engine
time_iso8601	Date	ISO 8601 time of the log
sni	String	Domain name requested through the SNI
tls_version	String	Version of the protocol used to establish an SSL connection
ssl_curves	String	List of curves supported by the client
ssl_session_reused	String	Whether an SSL session is reused ● **r**: It is reused. ● **.**: It is not used.
process_time	String	Detection duration of the engine
x_forwarded_for	String	Content of **X-Forwarded-For** in the request header
cdn_src_ip	String	Content of **Cdn-Src-Ip** in the request header
x_real_ip	String	Content of **X-Real-Ip** in the request header

sec-obs-access

Fields in OBS access logs

Table 10-32 sec-obs-access

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 10-33 sec-nip-attack

Field	Type	Description
SyslogId	String	Log serial number (SN).
Vsys	String	Virtual system name.
Policy	String	Name of a security policy.
SrcIp	String	Source IP address of a packet.
DstIp	String	Destination IP address of a packet.
SrcPort	String	Source port of a packet. For an ICMP packet, the value of this field is **0**.
DstPort	String	Destination port of a packet. For an ICMP packet, the value of this field is **0**.
SrcZone	String	Source security zone of a packet.
DstZone	String	Destination security zone of a packet.
User	String	Username.
Protocol	String	Protocol of the packet detected by a signature.
Application	String	Application that the packet detected by a signature belongs to.
Profile	String	Name of a configuration file.
SignName	String	Name of a signature.
SignId	String	ID of a signature.
EventNum	String	The field is used for log mergence. Whether logs are merged is determined by the mergence frequency and conditions. The value is **1** if logs are not merged.

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 10-34 sec-iam-audit

Field	Type	Description
uid	String	User ID
un	String	Username
did	String	Domain ID
dn	String	Domain name
src	String	Request domain name
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 10-35 sec-hss-vul

Field	Type	Description
agentUuid	String	Agent UUID.
alarmCsn	String	Alert UUID, which is randomly generated when the master generates an alert.
alarmKey	String	Alert keyword. For an alert, it is the **msg_id** reported by the transparent transmission agent. For a vulnerability, it is generated by the master.
alarmVersion	String	Agent version.

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 10-36 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_direction	String	Flow direction.
	app_info	sql	String	Executed SQL statement.
		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.

Field			Type	Description
		process_euid	Integer	Effective process user ID.
		parent_process_name	String	Parent process name.
		parent_process_path	String	Parent process file path.
		parent_process_pid	Integer	Parent process ID.
		parent_process_uid	Integer	Parent process user ID.
		parent_process_cmdline	String	Parent process file command line.
		parent_process_filename	String	Parent process file name.
		parent_process_start_time	Long	Parent process start time.
		parent_process_gid	Integer	Parent process group ID.
		parent_process_egid	Integer	Effective parent process group ID.
		parent_process_euid	Integer	Effective parent process user ID.
		child_process_name	String	Subprocess name.
		child_process_path	String	Subprocess file path.
		child_process_pid	Integer	Subprocess ID.
		child_process_uid	Integer	Subprocess user ID.
		child_process_cmdline	String	Subprocess file command line.

Field			Type	Description
		child_process_filename	String	Subprocess file name.
		child_process_start_time	Long	Subprocess start time.
		child_process_gid	Integer	Subprocess group ID.
		child_process_egid	Integer	Effective subprocess group ID.
		child_process_euid	Integer	Effective subprocess user ID.
		virt_cmd	String	Virtualization command.
		virt_process_name	String	Virtualization process name.
		escape mode	String	Escape mode.
		escape cmd	String	Command executed after the escape.
	user_info	user_id	Integer	User ID.
		user_gid	Integer	User GID.
		user_name	String	Username.
		user_group_name	String	User group name.
		user_home_dir	String	User home directory.
		login_ip	String	User login IP address.
		service_type	String	Login service type.
		service_port	Integer	Login service port.
		login_mode	String	Login mode.
		login_last time	Long	Last login time of a user.

Field			Type	Description
		login_fail_count	Integer	Failed login attempts.
		pwd_hash	String	Password hash.
		pwd_with_fuzzing	String	Anonymized password.
		pwd_used_days	Integer	Password age (days).
		pwd_min_days	Integer	Minimum password validity period.
		pwd_max_days	Integer	Maximum password validity period.
		pwd_warn_left_days	Integer	Advance warning of password expiration (days).
	file_info	file_path	String	File path/name.
		file_alias	String	File alias.
		file_size	Integer	File size.
		file_mtime	Long	Time when the file is last modified.
		file_atime	Long	Time when the file is last accessed.
		file_ctime	Long	Time when the file status last changes.
		file_hash	String	File hash value.
		file_md5	String	File MD5 value.
		file_sha256	String	File SHA256 value.
		file_type	String	File type.
		file_content	String	File content.
		file_attr	String	File attribute.
		file_operation	String	File operation type.
		file_change_attr	String	Old/New attribute.

Field			Type	Description
		file_new_path	String	New file path.
		file_desc	String	File description.
		file_key_word	String	File keyword.
		is_dir	Boolean	Whether the file is a directory.
		fd_info	String	File handle information.
		fd_count	Integer	Number of file handles.
	forensic_info	monitor_process	String	Monitoring process.
		escape_mode	String	Escape mode.
		abnormal_port	String	Abnormal port.
	geo_info	src_country	String	Source country/region.
		src_city	String	Source city.
		src_latitude	Long	Source latitude.
		src_longitude	Long	Source longitude.
		dest_country	String	Destination country/region.
		dest_city	String	Destination city.
		dest_latitude	Long	Destination latitude.
		dest_longitude	Long	Destination longitude.
	malware_info	malware_family	String	Malware family.
		malware_class	String	Malware classification.
	system_info	pwd_valid	Boolean	Whether the password is valid.
		pwd_min_len	Integer	Password length.

Field			Type	Description
		pwd_digit_credit	Integer	Digits contained in the password.
		pwd_uppercase_letter	Integer	Uppercase letters contained in the password.
		pwd_lowercase_letter	Integer	Lowercase letters contained in the password.
		pwd_special_characters	Integer	Special characters contained in the password.
	extend_info	hit_rule	String	Hit rule.
		rule_name	String	Rule name.
		rulesetname	String	Rule set name.
		report_type	String	Reported data type.
	ti_info	ti_source	String	Intelligence source.
		ti_class	String	Intelligence classification.
		ti_threat_type	String	Intelligence threat type.
		ti_first_time	Long	First detection time.
		ti_last_time	Long	Last detection time.

sec-hss-log

Fields in HSS security logs

Table 10-37 sec-hss-log

Field	Type	Description
agentUuid	String	Agent UUID.
alarmCsn	String	Alert UUID.

Field		Type	Description
alarmKey		String	Alert keyword. For an alert, it is the **msg_id** reported by the transparent transmission agent. For a vulnerability, it is generated by the master.
alarmVersion		String	Agent version.
occurTime		Long	Incident occurrence time (accurate to millisecond).
severity		Long	Severity.
hostUuid		String	UUID of the affected host.
hostName		String	Name of the affected host.
hostIp		String	Communication IP address of the affected host.
ipList		String	List of IP addresses of affected hosts.
cloudId		String	Cloud agent SN.
region		String	Region where the affected host is located.
projectId		String	ID of the affected tenant.
enterpriseProjectId		String	ID of the affected enterprise tenant.
appendInfo		Object	Alert details.
appendInfo	agent_id	String	Agent ID.
	version	String	Incident version.
	container_name	String	Container ID (in container security scenarios).
	image_name	String	Image name (in container security scenarios).
	event_id	String	Incident ID (GUID).
	event_name	String	Incident name.
	event_classid	String	Unique incident ID.
	occur_time	Long	Occurrence time (accurate to second).
	recent_time	Long	Last occurrence time (accurate to second).

Field			Type	Description
	event_category		Integer	Incident category.
	event_type		Integer	Incident type.
	event_count		Integer	Number of incidents.
	severity		Integer	Severity.
	attack_phase		Integer	Attack phase.
	attack_tag		Integer	Attack tag.
	confidence		Integer	Confidence.
	action		Integer	Action.
	detect_module		String	Detection module.
	report_source		String	Report source.
	related_events		String	Related incident ID.
	resource_info		Object	Resource information.
	network_info		Object	Network information.
	app_info		Object	Application information.
	system_info		Object	System information.
	process_info		list	Process information.
	user_info		list	User information.
	file_info		list	File information.
	geo_info		Object	Geographic information.
	malware_info		Object	Malware information.
	forensic_info		String	Evidence collection field.
	recommendation		String	Handling suggestions.
	extend_info		String	Extended incident information.
	resource_info	project_id	String	Project ID.
		region_name	String	Region name.
		vpc_id	String	VPC ID.
		host_name	String	Host name.
		host_ip	String	Host IP address.
		host_id	String	Host ID (ECS ID).

Field			Type	Description
		cloud_id	String	Cloud agent SN.
		vm_name	String	VM name.
		vm_uuid	String	VM UUID.
		container_id	String	Container ID.
		image_id	String	Image ID.
		sys_arch	String	System CPU architecture.
		os_bit	String	OS bit version.
		os_type	String	OS type.
		os_name	String	OS name.
		os_version	String	OS version.
	network_info	local_address	String	Local address.
		local_port	Integer	Local port.
		remote_address	String	Remote address.
		remote_port	Integer	Remote port.
		src_ip	String	Source IP address.
		src_port	Integer	Source port.
		src_domain	String	Source domain.
		dest_ip	String	Destination IP address.
		dest_port	Integer	Destination port.
		dest_domain	String	Destination domain.
		protocol	String	Protocol.
		app_protocol	String	Application layer protocol.
		flow_direction	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_process_filename	String	Subprocess file name.
		child_process_start_time	Long	Subprocess start time.
		child_process_gid	Integer	Subprocess group ID.
		child_process_egid	Integer	Effective subprocess group ID.
		child_process_euid	Integer	Effective subprocess user ID.
		virt_cmd	String	Virtualization command.
		virt_process_name	String	Virtualization process name.
		escape mode	String	Escape mode.
		escape cmd	String	Command executed after the escape.
	user_info	user_id	Integer	User ID.
		user_gid	Integer	User GID.
		user_name	String	Username.
		user_group_name	String	User group name.
		user_home_dir	String	User home directory.
		login_ip	String	User login IP address.
		service_type	String	Login service type.
		service_port	Integer	Login service port.
		login_mode	String	Login mode.
		login_last time	Long	Last login time of a user.

Field			Type	Description
		login_fail_count	Integer	Failed login attempts.
		pwd_hash	String	Password hash.
		pwd_with_fuzzing	String	Anonymized password.
		pwd_used_days	Integer	Password age (days).
		pwd_min_days	Integer	Minimum password validity period.
		pwd_max_days	Integer	Maximum password validity period.
		pwd_warn_left_days	Integer	Advance warning of password expiration (days).
	file_info	file_path	String	File path/name.
		file_alias	String	File alias.
		file_size	Integer	File size.
		file_mtime	Long	Time when the file is last modified.
		file_atime	Long	Time when the file is last accessed.
		file_ctime	Long	Time when the file status last changes.
		file_hash	String	File hash value.
		file_md5	String	File MD5 value.
		file_sha256	String	File SHA256 value.
		file_type	String	File type.
		file_content	String	File content.
		file_attr	String	File attribute.
		file_operation	String	File operation type.
		file_change_attr	String	Old/New attribute.

Field			Type	Description
		file_new_path	String	New file path.
		file_desc	String	File description.
		file_key_word	String	File keyword.
		is_dir	Boolean	Whether the file is a directory.
		fd_info	String	File handle information.
		fd_count	Integer	Number of file handles.
	forensic_info	monitor_process	String	Monitoring process.
		escape_mode	String	Escape mode.
		abnormal_port	String	Abnormal port.
	geo_info	src_country	String	Source country/region.
		src_city	String	Source city.
		src_latitude	Long	Source latitude.
		src_longitude	Long	Source longitude.
		dest_country	String	Destination country/region.
		dest_city	String	Destination city.
		dest_latitude	Long	Destination latitude.
		dest_longitude	Long	Destination longitude.
	malware_info	malware_family	String	Malware family.
		malware_class	String	Malware classification.
	system_info	pwd_valid	Boolean	Whether the password is valid.
		pwd_min_len	Integer	Password length.

Field			Type	Description
		pwd_digit_credit	Integer	Digits contained in the password.
		pwd_uppercase_letter	Integer	Uppercase letters contained in the password.
		pwd_lowercase_letter	Integer	Lowercase letters contained in the password.
		pwd_special_characters	Integer	Special characters contained in the password.
	extend_info	hit_rule	String	Hit rule.
		rule_name	String	Rule name.
		rulesetname	String	Rule set name.
		report_type	String	Reported data type.
	ti_info	ti_source	String	Intelligence source.
		ti_class	String	Intelligence classification.
		ti_threat_type	String	Intelligence threat type.
		ti_first_time	Long	First detection time.
		ti_last_time	Long	Last detection time.

sec-ddos-attack

Fields in Anti-DDoS attack logs

Table 10-38 sec-ddos-attack

Field	Type	Description
log_type	String	Log type
time	Date	local time
device_ip	String	Device IP address

Field	Type	Description
device_type	String	Device type (**CLEAN**: cleaning device; **DETECT**: detecting device)
direction	String	Log direction (**inbound**, **outbound**)
zone_id	String	Protected object ID
zone_name	String	Protected object name
zone_ip	String	IP address
biz_id	String	Business ID
is_deszone	String	Whether the traffic is network segment traffic (**true**, **false**)
is_ipLocation	String	Whether the traffic is geographical location traffic (**true**, **false**)
ipLocation_id	String	Geographical location ID
total_pps	String	Total pps
total_kbps	String	Total rate in kbps
tcp_pps	String	Rate of TCP packets to the target (in pps)
tcp_kbps	String	Rate of TCP traffic to the target (in kbps)
tcpfrag_pps	String	Rate of TCP fragments to the target (in pps)
tcpfrag_kbps	String	Rate of TCP fragment traffic to the target (in kbps)
udp_pps	String	Rate of UDP packets to the target (in pps)
udp_kbps	String	Rate of UDP traffic to the target (in kbps)
udpfrag_pps	String	Rate of UDP fragments to the target (in pps)
udpfrag_kbps	String	Rate of UDP fragment traffic to the target (in kbps)
icmp_pps	String	Rate of ICMP packets to the target (in pps)
icmp_kbps	String	Total ICMP traffic to the target (in kbps)
other_pps	String	Rate of OTHER packets to the target (in pps)

Field	Type	Description
other_kbps	String	Total OTHER traffic to the target (in kbps)
syn_pps	String	Number of SYN packets to the target (in pps)
synack_pps	String	Number of SYN/ACK packets to the target (in pps)
ack_pps	String	Rate of ACK packets to the target (in pps)
finrst_pps	String	Rate of FIN/Rst packets to the target (in pps)
http_pps	String	Rate of HTTP packets to the target (in pps)
http_kbps	String	Rate of HTTP traffic to the target (in kbps)
http_get_pps	String	Total packet rate of HTTP requests to the target (in pps)
https_pps	String	Rate of HTTPS packets to the target (in pps)
https_kbps	String	Rate of HTTPS traffic to the target (in kbps)
dns_request_pps	String	Rate of DNS Query packets to the target (in pps)
dns_request_kbps	String	Rate of DNS Query traffic to the target (in kbps)
dns_reply_pps	String	Rate of DNS Reply packets to the target (in pps)
dns_reply_kbps	String	Rate of DNS Reply traffic to the target (in kbps)
sip_invite_pps	String	Rate of SIP packets to the target (in pps)
sip_invite_kbps	String	Rate of SIP traffic to the target (in kbps)
tcp_increase_con	String	Number of new TCP connections to the target per second
udp_increase_con	String	Number of new UDP connections to the target per second
icmp_increase_con	String	Number of new ICMP connections to the target per second

Field	Type	Description
other_increase_con	String	Number of OTHER connections to the target per second
tcp_concur_con	String	Number of concurrent TCP connections to the target
udp_concur_con	String	Number of concurrent UDP connections to the target
icmp_concur_con	String	Number of concurrent ICMP connections to the target
other_concur_con	String	Number of concurrent OTHER connections to the target
total_average_pps	String	Average pps of all traffic to the target
total_average_kbps	String	Average Kbps of all traffic to the target

sec-cts-audit

Fields in CTS logs

Table 10-39 sec-cts-audit

Field	Type	Description
time	Date	Time when an incident occurs. The value is the local standard time (GMT +local time zone), for example, 2022/11/08 11:24:04 GMT+08:00.
user	Object	Cloud account used to perform the recorded operation.
request	Object	Requested operation.
response	Object	Response to the request.
service_type	String	Operation source.
resource_type	String	Resource type.
resource_name	String	Resource name.
resource_id	String	Unique resource ID.
source_ip	String	IP address of the user who performs an operation. The value of this parameter is empty if the operation is triggered by the system.

Field	Type	Description
trace_name	String	Operation name.
trace_rating	String	Level of an operation incident. The options are as follows: ● **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 10-40 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 10-41 sec-cfw-flow

Field	Type	Description
app	String	Application type
dst_ip	String	Destination IP address
dst_port	String	Destination port number
end_time	Date	Flow end time
protocol	String	Protocol type
to_c_bytes	String	Number of bytes sent from the server to the client
to_c_pkts	String	Number of packets sent from the server to the client
to_s_bytes	String	Number of bytes sent from the client to the server
to_s_pkts	String	Number of packets sent from the server to the client
src_ip	String	Source IP address
src_port	String	Source port number
start_time	Date	Flow start time

sec-cfw-block

Fields in CFW access control logs

Table 10-42 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 10-43 sec-apig-access

Field	Type	Description
region_id	String	Site.
api_id	String	API ID.
body_bytes_sent	String	Response body size.
bytes_sent	String	Size of the entire response.
domain	String	Public network domain name.
errorType	String	Status of request throttling. Value **1** indicates that request throttling is enabled.
http_user_agent	String	User agent ID.
http_x_forwarded_for	String	**X-Forwarded-For** header.
opsuba_api_url	String	Request URI.
out_times	String	Time required for interaction between the gateway and peripheral components.
remote_addr	String	Remote IP address.
request_id	String	Request ID.

Field	Type	Description
request_length	String	Size of the entire request.
request_method	String	HTTP request method.
request_time	String	Time required for access.
scheme	String	Protocol.
server_protocol	String	Request protocol.
status	String	Status.
time_local	Date	Time.
upstream_addr	String	Remote IP address.
upstream_connect_time	String	Time required for a remote connection.
upstream_header_time	String	Time required for receiving the header at the remote end.
upstream_response_time	String	Time required for returning a response from the remote end.
upstream_status	String	Remote status.
upstream_uri	String	Request backend URI.
user_name	String	Project ID or app ID of the user.

sec-dbss-alarm

Fields in DBSS alert logs

Table 10-44 dbss-alarm

Field	Type	Description
domain_id	String	Account ID.
project_id	String	Project ID
region	String	Region
tenant_vpc_id	String	VPC ID of the tenant
tenant_subnet_id	String	Subnet ID of the tenant
instance_id	String	Instance ID
instance_name	String	Instance name
alarm	Object	Alert object

Field		Type	Description
source_type		String	DBSS
alarm	alarm_risk	String	Severity
	client_ip	String	Connection IP address
	database_ip	String	IP address for accessing the database
	count	Long	Number of alerts
	user_name	String	Database username
	schema	String	Oracle schema
	rule_name	String	Rule name
	rule_id	String	Rule ID
	sql_type	String	SQL execution type
	sql_result	String	SQL execution result
	db_type	String	Database type

sec-dsc-alarm

The reserved fields in DSC alert logs vary depending on the log types.

Table 10-45 AK SK leakage (aksk_leakage)

Field	Type	Description
log_type	String	Alert type
region_id	String	Region
domain_id	String	Account ID.
project_id	String	Project ID
leakage_ak	String	AK
source	String	Leakage source
find_time	String	Discovery time
account	String	Account name.
file_name	String	File name
file_suffix	String	File name extension
leakage_user_id	String	Sub-user ID of the leakage

Field	Type	Description
leakage_user_name	String	Sub-username of the leakage
leakage_domain_id	String	Leaked account ID.
leakage_domain_name	String	Leaked account name.
url	String	Website URL of the leakage

Table 10-46 Risky OBS bucket files (obs_risk)

Field	Type	Description
log_type	String	Alert type
region_id	String	Region
domain_id	String	Account ID.
project_id	String	Project ID
bucket_policy	String	Public bucket/Private bucket
bucket_domain_id	String	ID of the account that the bucket belongs to.
bucket_project_id	String	ID of the project to which the bucket belongs
bucket_name	String	Bucket name
file_name	String	File name
file_path	String	File path
risk_level	Integer	Sensitive risk level
sensitive_data_type	String[]	Sensitive data type
privacy_detail	String	Personal privacy data details
file_type	String	File type
mimetypes	String	File type
rule_list	List<Map<String,String>>	List of matched rules
keyword	String	Keyword for matching sensitive data rules
available_zone	String	AZ
encrypted	String	Whether to encrypt data

Table 10-47 Sensitive data fields (db_risk)

Field	Type	Description
log_type	String	Alert type
region_id	String	Region
domain_id	String	Account ID.
project_id	String	Project ID
vpc_id	String	VPC ID
db_instance_type	String	RDS PUB
db_instance_id	String	Database instance ID
db_instance_type	String	Database instance type
db_instance_ip	String	IP address of the database instance
db_instance_domain_id	String	ID of the account that the database instance belongs to.
db_instance_project_id	String	ID of the project to which the database instance belongs
db_instance_name	String	Database instance name
db_name	String	Database name
table_name	String	Table name
field_name	String	Field name
data_type	String	Field data type
risk_level	Integer	Sensitive risk level
sensitive_data_type	String[]	Sensitive data type
privacy_detail	String	Personal privacy data details
rule_list	List<Map<String,String>>	List of matched rules
keyword	String	Keyword for matching sensitive data rules

10.5.4 Configuring Indexes

An index in security analysis is a storage structure used to sort one or more columns in log data. Different index configurations generate different query and analysis results. Configure indexes based on your requirements.

If you want to use the analysis function, you must configure field indexes. After configuring a field index, you can specify field keys and field values to narrow down the query scope. For example, the query statement **level:error** is to query logs whose **level** field contains the value **error**.

Limitations and Constraints

Custom index can be configured only for new custom pipelines. For details, see **Creating a Pipeline**.

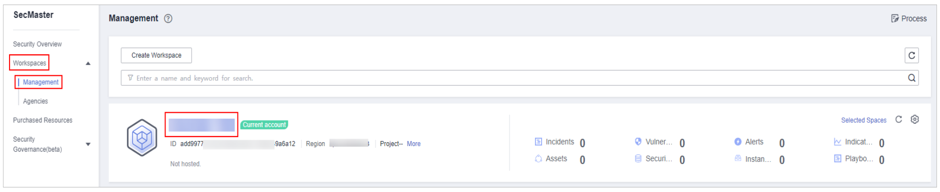
Configuring Field Indexes

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

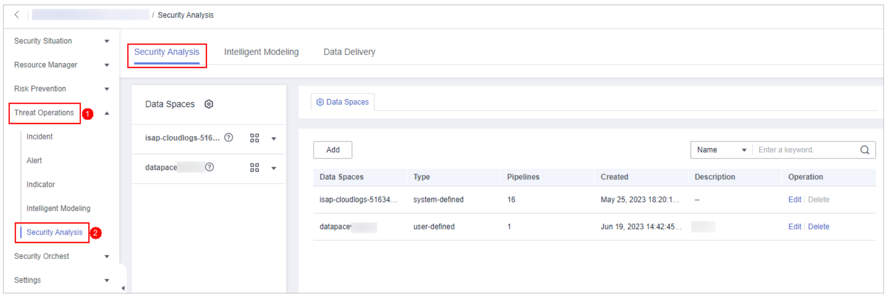
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-60 Workspace management page



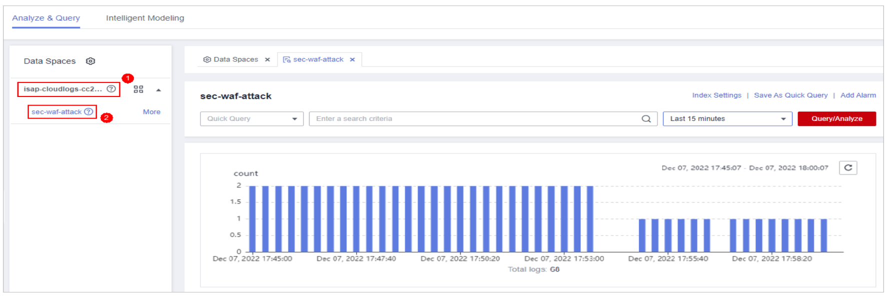
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-61 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-62 Pipeline data page



Step 6 On the pipeline page, click **Index Settings** in the upper right corner.

Step 7 On the **Index Settings** page, configure index parameters.

1. Enable the index status.

   The index status is enabled by default. When the index status is disabled, collected logs cannot be queried using indexes.

2. Configure index parameters. For details about the parameters, see **Table 10-48**.

Table 10-48 Parameters for index settings

Parameter	Description
Field	Log field (key)
Type	Data type of the log field value. The options are text, keyword, long, integer, double, float, date, and json.
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 8 Click **OK**.

----End

10.5.5 Querying and Analyzing Data

Scenario

You can query and analyze collected log data in real time on the **Analyze & Query** tab.

This topic walks you through how to query and analyze log data.

- Entering Query Criteria for Query and Analysis
- Using Existing Fields for Query and Analysis
- Managing Query Analysis Results

Prerequisites

Data access has been completed. For details, see **Data Integration**.

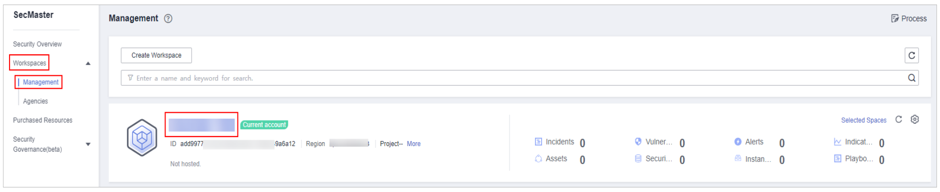
Entering Query Criteria for Query and Analysis

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

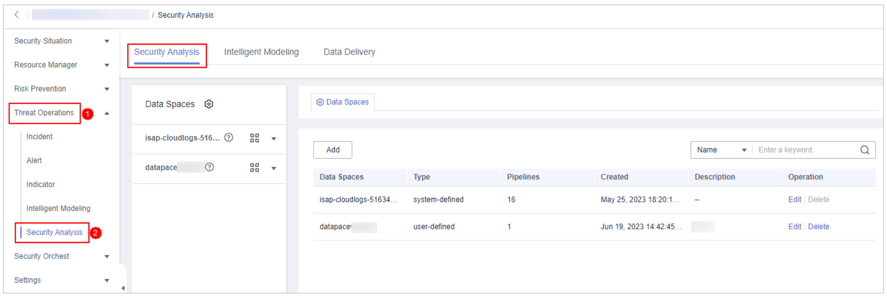
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-63 Workspace management page



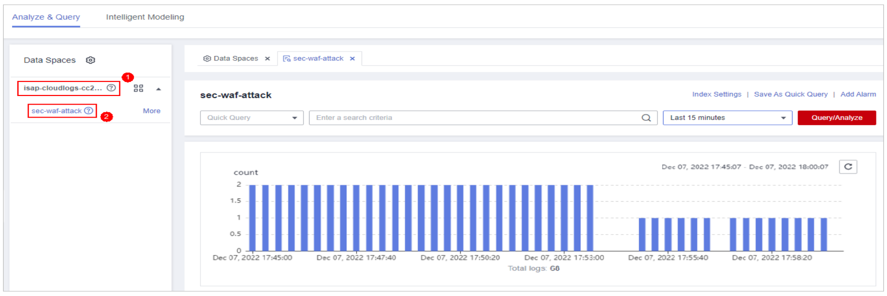
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-64 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-65 Pipeline data page



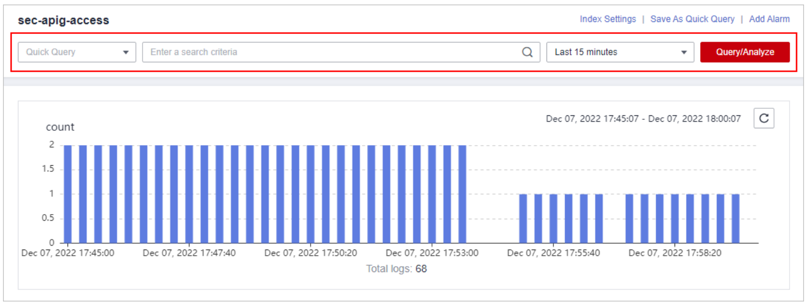
Step 6 On the pipeline data retrieval page, enter the query analysis statement.

A query analysis statement consists of a query statement and an analysis statement. The format is **Query Statement|Analysis Statement**. For details about the syntax of query analysis statements, see **Query and Analysis Statements - SQL Syntax**.

NOTE

If the reserved field is of the text type, **MATCH_QUERY** is used for word segmentation query by default.

Figure 10-66 Query/Analyze



Step 7 Select **Last 15 minutes** as the time range.

You can select **Last 15 minutes**, **Last hour**, or **Last 24 hours** or customize a time range for the query.

Step 8 Click **Query/Analyze** and view the results.

----End

Using Existing Fields for Query and Analysis

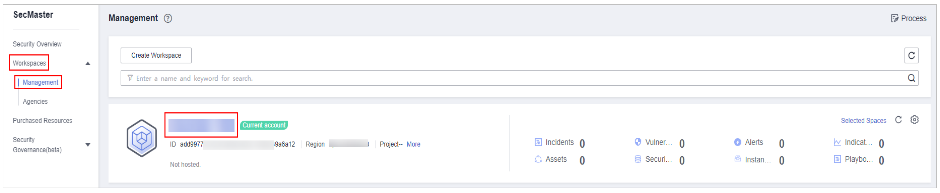
The following part describes how to use existing fields to query and analyze logs.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

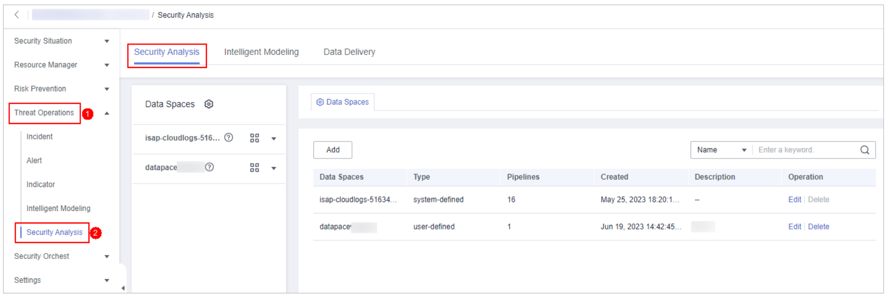
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-67 Workspace management page



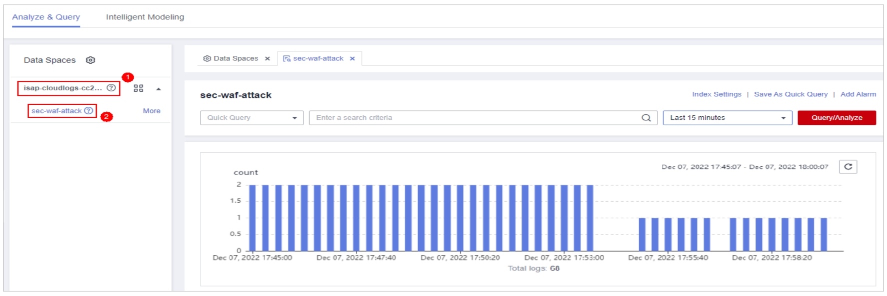
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-68 Accessing the Security Analysis tab page



Step 5 In the **Data Spaces** tree on the left, click a data space name to show the pipeline list. Then, click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-69 Pipeline data page



Step 6 Set search criteria.

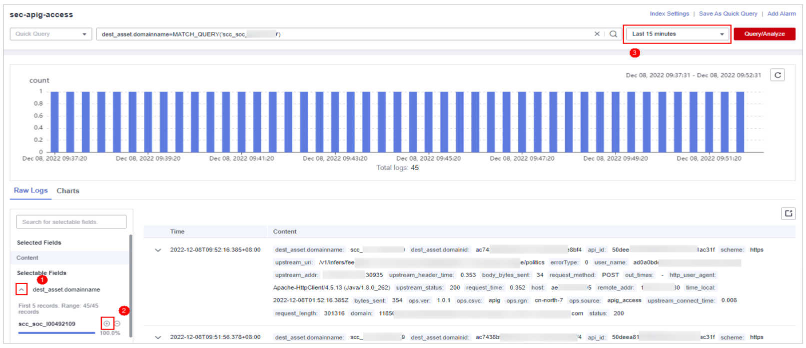
For details about the existing fields in the access data, see **Log Fields**.

NOTE

If the reserved field is of the text type, **MATCH_QUERY** is used for word segmentation query by default.

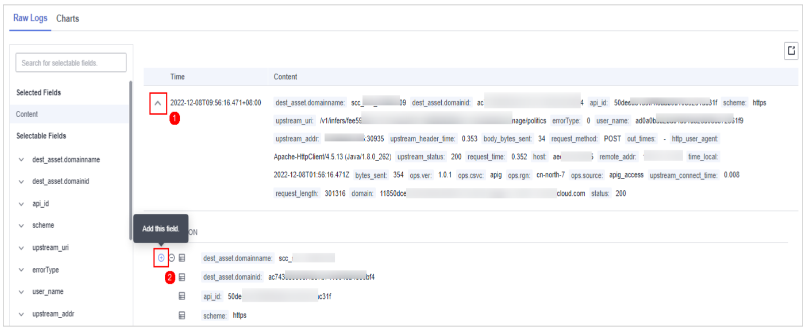
- Click before an optional field on the left and click (adding a field value) or (removing a field value) next to the target field. The matched fields are displayed in the query box.

Figure 10-70 Filtering a Field Value (1)



- If you have expanded the log data at a specific time point and need to filter some fields, click ⊕ (adding a field value) or ⊖ (removing a field value) in front of the field name. The query box displays the matched fields.

Figure 10-71 Filtering a Field Value (2)



Step 7 By default, data in the last 15 minutes is queried and displayed. If you want to query log data in other time ranges, set the query time and click **Query/Analyze**.

----End

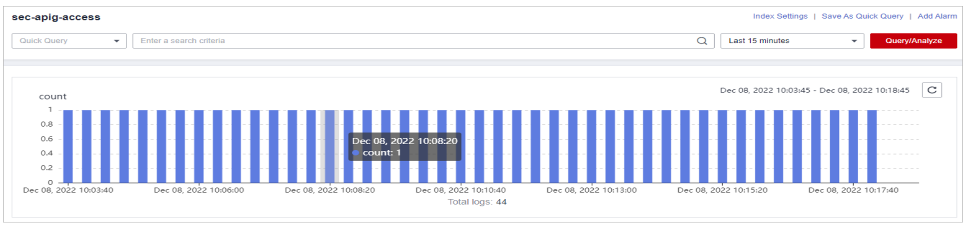
Managing Query Analysis Results

SecMaster displays query and analysis results in the form of log distribution bar charts, **Raw Logs**, and **Charts**.

- Log distribution bar chart

  A bar chart is used to display queried logs over time. You can move the cursor to a certain bar to view the number of logs hit at the time the bar represents.

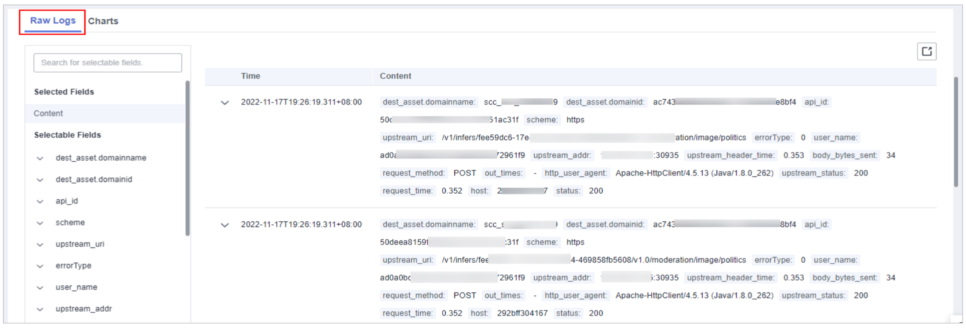
Figure 10-72 Log distribution bar chart



- **Raw Logs**

  The **Raw Logs** tab displays the results of the current query.

Figure 10-73 Raw Logs



– To display log data over time:

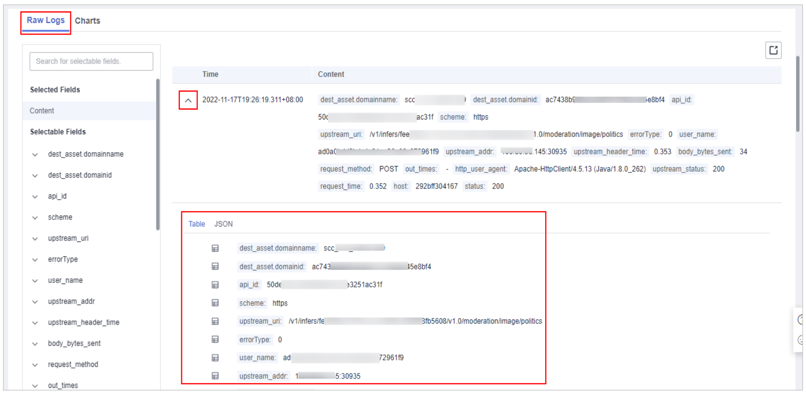
- By default, log data in the last 15 minutes is displayed. To display data in other time, select the time range in the upper right corner.

Figure 10-74 Selecting the 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.

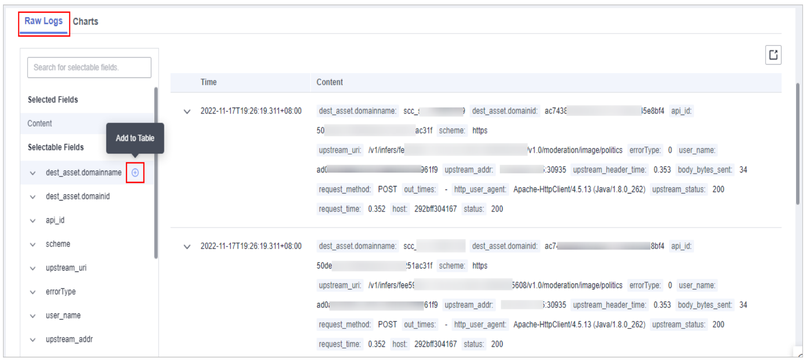
  To view data in JSON format, click the **JSON** tab. Data in JSON format is displayed on the page.

Figure 10-75 Expand to display data



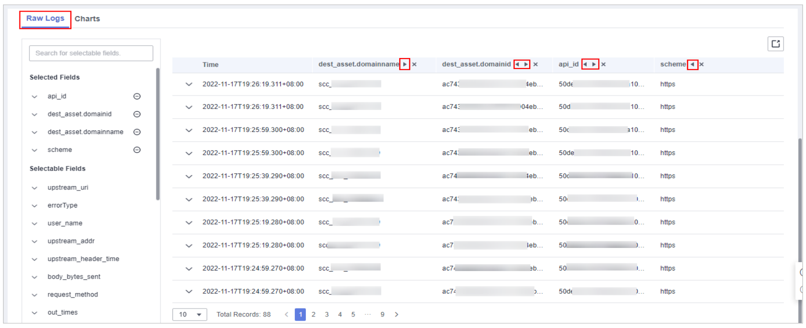
- To display or filter some fields in the list, select the fields to be displayed in the Available Fields area on the right and click next to the field name. The fields are displayed in the log data list on the right.

Figure 10-76 Selected fields to be displayed



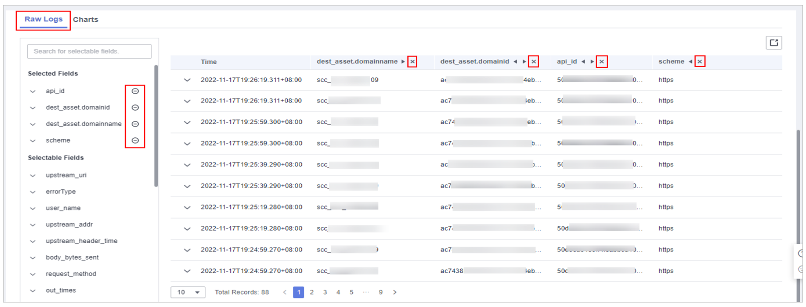
- ○ To adjust the field sequence: In the heading columns of the log data list on the right, select a field and then click or next to the field name to move the field left or right by one column with each click.

Figure 10-77 Adjusting field display sequence



- ○ To cancel the display: In the table header column of the log data list on the right, select the target field, and click next to the field name, or click next to the field name on the left.

Figure 10-78 Cancel



– To export logs: On the **Raw Logs** tab page, click in the upper right corner of the page. The system automatically downloads raw logs to the local PC.

- **Charts**

  After a query statement is executed, you can view visualized query analysis results on the **Charts** tab.

On the **Charts** tab, SecMaster provides query and analysis results in multiple chart types, such as tables, line charts, bar charts, and pie charts. For details, see **Overview**.

- **Alarm**

  In the upper right corner of the **Analyze & Query** tab, click **Add Alarm** to add alert models. You can set alert rules for generating alerts for query and analysis results hit the rules. For details, see **Quickly Adding a Log Alarm Model**.

- **Quick Query**

  In the upper right corner of the query analysis page, click **Save as Quick Query** to save search criteria as a quick query. For details, see **Quick Query**.

10.5.6 Downloading Logs

Scenario

SecMaster allows you to download raw logs or query and analysis logs.

Prerequisites

Data access has been completed. For details, see **Data Integration**.

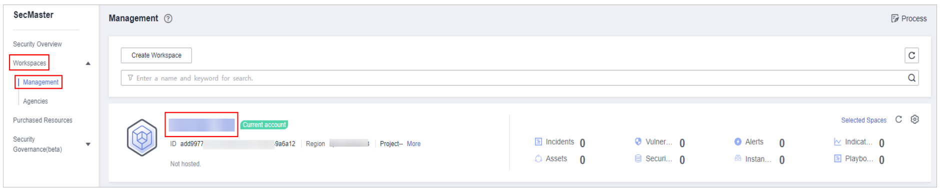
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

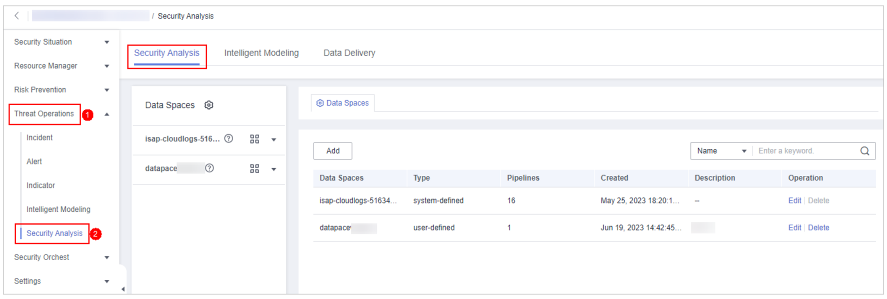
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-79 Workspace management page



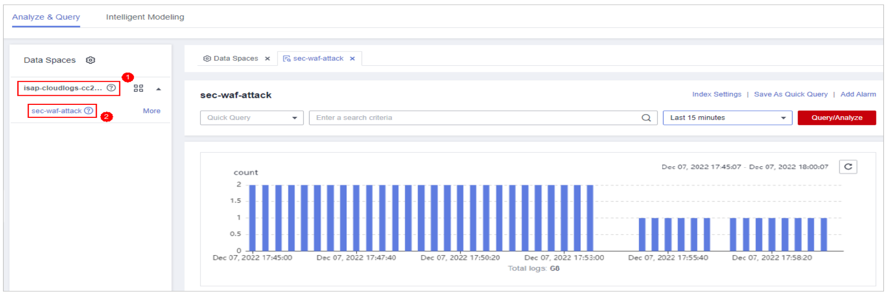
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-80 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-81 Pipeline data page



Step 6 (Optional) On the pipeline data retrieval page, enter the search criteria, select a time range, and click **Query/Analyze**.

Step 7 Download logs.

- Raw logs: On the **Raw Logs** tab page, click . The system downloads logs to the local PC.
- Chart logs: On the **Charts** tab page, click **Download**. The system downloads the logs to the local PC.

----End

10.5.7 Query and Analysis Statements - SQL Syntax

10.5.7.1 Basic Syntax

An SQL statement consists of a query statement and an analysis statement, which are separated by a vertical bar (|). Query statements can be used independently, but analysis statements must be used together with query statements.

```
Query Statement | Analysis Statement
```

Table 10-49 Basic syntax

Statement Type	Description
Query Statement	A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.
Analysis Statement	An analysis statement is used to calculate and collect statistics on query results.

10.5.7.2 Limitations and Constraints

- Query statements do not support mathematical operations, such as (age + 100) ≤ 1000.

- Aggregate functions support only fields and do not support expressions, for example, avg(log(age)).
- Multi-table association is not supported.
- Subqueries are not supported.
- A maximum of 500 records can be returned on the page.
- A maximum of 10,000 groups can be returned by GROUP BY.

10.5.7.3 Query Statements

A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.

This topic describes query statements and examples.

Syntax

A query statement can be in either of the following formats:

- If the value is only *, full data is returned without filtering.
- It consists of one or more query clauses. The clauses are connected by **NOT**, **AND**, and **OR**. **()** can be used to increase the priority of the query conditions in parentheses.

The basic structure of a query clause is as follows:

```
Field Name Operator Field Value
```

Operators lists the operators that can be used.

Operators

Table 10-50 Operator descriptions

Operator	Description
=	Queries logs in which the value of a field is equal to a certain value.
<>	Queries the logs in which the value of a field is not equal to a certain value.
>	Queries logs in which the value of a field is greater than a specified value.
<	Queries logs in which the value of a field is less than a specified value.
>=	Queries logs in which the value of a field is greater than or equal to a specified value.
<=	Queries logs in which the value of a field is less than or equal to a specified value.

Operator	Description
IN	Queries the logs whose field values are within a specified value range.
BETWEEN	Queries the logs whose field values are in the specified range.
LIKE	Searches for logs of a field value in full text.
IS NULL	Queries logs whose field value is NULL.
IS NOT NULL	Query logs whose field value is NOT NULL.

Examples

Table 10-51 Example query statements

Query Requirement	Query Statement
All logs	*
Logs about successful GET requests (status codes 200 to 299).	request_method = 'GET' AND status BETWEEN 200 AND 299
Logs of GET or POST requests	request_method = 'GET' OR request_method = 'POST'
Logs of non-GET requests	NOT request_method = 'GET'
Logs about successful GET or POST requests	(request_method = 'GET' OR request_method = 'POST') AND status BETWEEN 200 AND 299
Logs of GET or POST request failures	(request_method = 'GET' OR request_method = 'POST') NOT status BETWEEN 200 AND 299
Logs of successful GET requests (status code: 200 to 299) whose request time is greater than or equal to 60 seconds.	request_method = 'GET' AND status BETWEEN 200 AND 299 AND request_time >= 60
Logs whose request time is 60 seconds.	request_time = 60

10.5.7.4 Syntax of Analysis Statements

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
```

```
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

10.5.7.5 Analysis Statements - SELECT

Specifies the field to be queried.

Using * to query all fields.

```
SELECT *
```

Table 10-52 Using * to query all fields

account_number	firstname	gender	city	balance	employer	state	lastname	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36
13	Nanette	F	Nogal	32838	Quility	VA	Bates	28
18	Dale	M	Orick	4180	null	MD	Adams	32

Querying a Specified Field

```
SELECT firstname, lastname
```

Table 10-53 Querying a Specified Field

firstname	lastname
Amber	Duke
Hattie	Bond
Nanette	Bates
Dale	Adams

Using AS to Define Field Aliases

```
SELECT account_number AS num
```

Table 10-54 Using AS to define field aliases

num
1

num
16
13
18

Using the DISTINCT Statement

```
SELECT DISTINCT age
```

Table 10-55 Using the DISTINCT statement

age
32
36
28

Using SQL Functions

For details about functions, see **Functions**.

```
SELECT LENGTH(firstname) as len, firstname
```

Table 10-56 Using SQL functions

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

10.5.7.6 Analysis Statements - GROUP BY

Groups data by field value.

Grouping by Field Value

```
SELECT age GROUP BY age
```

Table 10-57 Grouping by field value

age
28
32
36

Grouping by Field Alias

```
SELECT account_number AS num GROUP BY num
```

Table 10-58 Grouping by field alias

num
1
16
13
18

Grouping by Multiple Fields

```
SELECT account_number AS num, age GROUP BY num, age
```

Table 10-59 Grouping by multiple fields

num	age
1	32
16	36
13	28
18	32

Using SQL Functions

For details about functions, see **Function**.

```
SELECT LENGTH(lastname) AS len, COUNT(*) AS count GROUP BY LENGTH(lastname)
```


Table 10-60 Using SQL functions

len	count
4	2
5	2

10.5.7.7 Analysis Statements - HAVING

Filters data based on grouping and **Aggregate Functions**.

```
SELECT age, MAX(balance) GROUP BY age HAVING MIN(balance) > 10000
```

Table 10-61 The HAVING function

age	MAX(balance)
28	32838
32	39225

10.5.7.8 Analysis Statements - ORDER BY

Sorts data by field value.

Sorting Data by Field Value

```
SELECT age ORDER BY age DESC
```

Table 10-62 Sorting by field value

age
28
32
32
36

10.5.7.9 Analysis Statements - LIMIT

Specifies the number of returned data records.

Specifying the Number of Returned Records

```
SELECT * LIMIT 1
```


Table 10-63 Specifying the number of returned records

account_number	firstname	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 10-64 Specifying the number of returned records and offsets

account_number	firstname	gender	city	balance	employer	state	lastname	age
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36

10.5.7.10 Analysis Statements - Functions

Mathematics Functions

Table 10-65 Mathematics Functions

Function	Purpose	Description	Example Value
abs	Absolute value	abs(number T) -> T	SELECT abs(0.5) LIMIT 1
add	Addition	add(number T, number) -> T	SELECT add(1, 5) LIMIT 1
cbrt	Cubic root	cbrt(number T) -> T	SELECT cbrt(0.5) LIMIT 1
ceil	Rounded up	ceil(number T) -> T	SELECT ceil(0.5) LIMIT 1
divide	Division	divide(number T, number) -> T	SELECT divide(1, 0.5) LIMIT 1
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

Function	Purpose	Description	Example Value
expm1	Subtract one from the power of the natural base number e.	expm1(number T) -> T	SELECT expm1(0.5) LIMIT 1
floor	Rounded down	floor(number T) -> T	SELECT floor(0.5) AS Rounded_Down LIMIT 1
ln	Returns the natural logarithm.	ln(number T) -> double	SELECT ln(10) LIMIT 1
log	Logarithm with T as the base	log(number T, number) -> double	SELECT log(10) LIMIT 1
log2	Logarithm with 2 as the base	log2(number T) -> double	SELECT log2(10) LIMIT 1
log10	Logarithm to base 10	log10(number T) -> double	SELECT log10(10) LIMIT 1
mod	Remainder	mod(number T, number) -> T	SELECT modulus(2, 3) LIMIT 1
multiply	Multiplication	multiply(number T, number) -> number	SELECT multiply(2, 3) LIMIT 1
pi	π	pi() -> double	SELECT pi() LIMIT 1
pow	T power of	pow(number T, number) -> T	SELECT pow(2, 3) LIMIT 1
power	T power of	power(number T) -> T, power(number T, number) -> T	SELECT power(2, 3) LIMIT 1
rand	Random number.	rand() -> number, rand(number T) -> T	SELECT rand(5) LIMIT 1
rint	Discard decimals.	rint(number T) -> T	SELECT rint(1.5) LIMIT 1
round	Round off	round(number T) -> T	SELECT round(1.5) LIMIT 1
sign	Symbol	sign(number T) -> T	SELECT sign(1.5) LIMIT 1
signum	Symbol	signum(number T) -> T	SELECT signum(0.5) LIMIT 1
sqrt	Square root	sqrt(number T) -> T	SELECT sqrt(0.5) LIMIT 1
subtract	Subtraction	subtract(number T, number) -> T	SELECT subtract(3, 2) LIMIT 1

Function	Purpose	Description	Example Value
/	Division	number / number -> number	SELECT 1 / 100 LIMIT 1
%	Remainder	number % number -> number	SELECT 1 % 100 LIMIT 1

Trigonometric Functions

Table 10-66 Trigonometric functions

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 to degrees	degrees(number T) -> double	SELECT degrees(0.5) LIMIT 1
radians	Converting degrees to radians	radians(number T) -> double	SELECT radians(0.5) LIMIT 1
sin	Sine	sin(number T) -> double	SELECT sin(0.5) LIMIT 1
sinh	hyperbolic sine	sinh(number T) -> double	SELECT sinh(0.5) LIMIT 1
tan	Tangent	tan(number T) -> double	SELECT tan(0.5) LIMIT 1

Temporal Functions

Table 10-67 Temporal functions

Function	Purpose	Description	Example Value
curdate	Specifies the current date.	curdate() -> date	SELECT curdate() LIMIT 1
date	Date	date(date) -> date	SELECT date() LIMIT 1
date_format	Obtains the date value based on the format.	date_format(date, string) -> string	SELECT date_format(date, 'Y') LIMIT 1
day_of_month	Month	day_of_month(date) -> integer	SELECT day_of_month(date) LIMIT 1
day_of_week	Day of a week	day_of_week(date) -> integer	SELECT day_of_week(date) LIMIT 1
day_of_year	Number of days in the current year	day_of_year(date) -> integer	SELECT day_of_year(date) LIMIT 1
hour_of_day	Number of hours on the current day	hour_of_day(date) -> integer	SELECT hour_of_day(date) LIMIT 1
maketime	Date of Generation	maketime(integer, integer, integer) -> time	SELECT maketime(11, 30, 00) LIMIT 1
minute_of_hour	Number of minutes in the current hour	minute_of_hour(date) -> integer	SELECT minute_of_hour(date) LIMIT 1
minute_of_day	Number of minutes on the current day	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
monthname	Month Name	monthname(date) -> string	SELECT monthname(date) LIMIT 1
now	Current time.	now() -> time	SELECT now() LIMIT 1
second_of_minute	Number of seconds	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
timestamp	Date	timestamp(date) -> date	SELECT timestamp(date) LIMIT 1

Function	Purpose	Description	Example Value
year	Year	year(date) -> integer	SELECT year(date) LIMIT 1

Text Functions

Table 10-68 Text functions

Function	Purpose	Description	Example Value
ascii	ASCII value of the first character	ascii(string T) -> integer	SELECT ascii('t') LIMIT 1
concat_ws	Connection String	concat_ws(separator, string, string) -> string	SELECT concat_ws('-', 'Tutorial', 'is', 'fun!') LIMIT 1
left	Obtain a character string from left to right.	left(string T, integer) -> T	SELECT left('hello', 2) LIMIT 1
length	length	length(string) -> integer	SELECT length('hello') LIMIT 1
locate	Search for a string	locate(string, string) -> integer	SELECT locate('o', 'hello') LIMIT 1
replace	Replace strings	replace(string T, string, string) -> T	SELECT replace('hello', 'l', 'x') LIMIT 1
right	Obtain a character string from right to left.	right(string T, integer) -> T	SELECT right('hello', 1) LIMIT 1
rtrim	Remove the empty character string on the right.	rtrim(string T) -> T	SELECT rtrim('hello ') LIMIT 1
substring	Obtaining a Substring	substring(string T, integer, integer) -> T	SELECT substring('hello', 2,5) LIMIT 1
trim	Remove empty character strings on both sides.	trim(string T) -> T	SELECT trim(' hello ') LIMIT 1

Function	Purpose	Description	Example Value
upper	Convert all letters to uppercase letters.	upper(string T) -> T	SELECT upper('helloworld') LIMIT 1

Other

Table 10-69 Other

Function	Purpose	Description	Example Value
if	if condition	if(boolean, object, object) -> object	SELECT if(false, 0, 1) LIMIT 1 , SELECT if(true, 0, 1) LIMIT 1
ifnull	If the field is null, the default value is used.	ifnull(object, object) -> object	SELECT ifnull('hello', 1) LIMIT 1 , SELECT ifnull(null, 1) LIMIT 1
isnull	Indicates whether a field is null. If yes, 1 is returned. If no, 0 is returned.	isnull(object) -> integer	SELECT isnull(null) LIMIT 1 , SELECT isnull(1) LIMIT 1

10.5.7.11 Analysis Statements - Aggregate Functions

Table 10-70 Aggregate functions

Function	Purpose	Description	Example Value
avg	Average value	avg(number T) -> T	SELECT avg(age) LIMIT 1
sum	Sum	sum(number T) -> T	SELECT sum(age) LIMIT 1
min	Specifies the minimum value.	min(number T) -> T	SELECT min(age) LIMIT 1
max	Maximum value	max(number T) -> T	SELECT max(age) LIMIT 1

Function	Purpose	Description	Example Value
count	Occurrences	count(field) -> integer , count(*) -> integer , count(1) -> integer	SELECT count(age) LIMIT 1 , SELECT count(*) LIMIT 1 , SELECT count(1) LIMIT 1

10.5.8 Quick Query

Scenario

Quick Query is a function of SecMaster that provides saved query and analysis operations. You can save a common query and analysis statement as a quick query statement for future use.

This topic describes how to create a quick query.

Prerequisites

Indexes have been configured. For details, see **Configuring Indexes**.

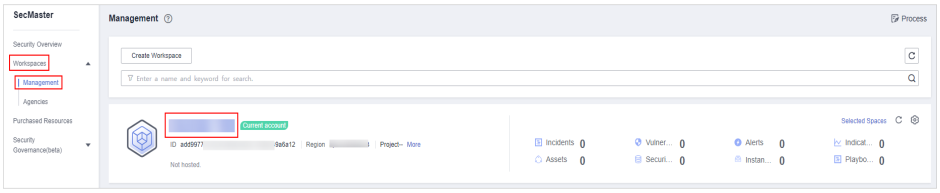
Creating a Quick Query

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

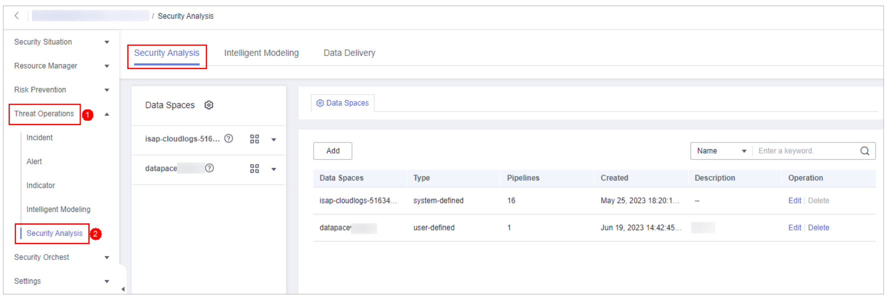
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-82 Workspace management page



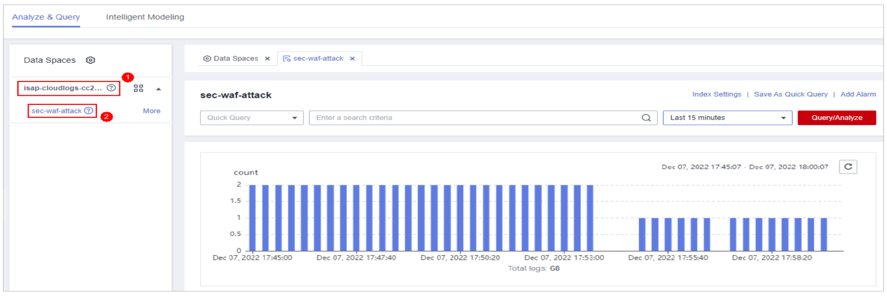
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-83 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-84 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/Analyze**.

For details, see **Querying and Analyzing Data**.

Step 7 Click **Save as Quick Query** in the upper right corner of the area, configure query parameters on the right, and click **OK**.

Table 10-71 Parameters for a quick query

Parameter	Description
Query Name	Set the name of the quick query.
Query statement	The system automatically generates the query statement entered in **Step 6**.

Step 8 Click **OK**.

After creating a quick query, you can click ▼ in the quick query search box on the pipeline data query and analysis page and select the target quick query name to use the quick query.

----End

10.5.9 Quickly Adding a Log Alarm Model

Scenario

SecMaster allows you to set alarm models for query and analysis results and trigger alarms when conditions are met.

This topic describes how to quickly configure alarm models for logs.

Prerequisites

Data access has been completed. For details, see **Data Integration**.

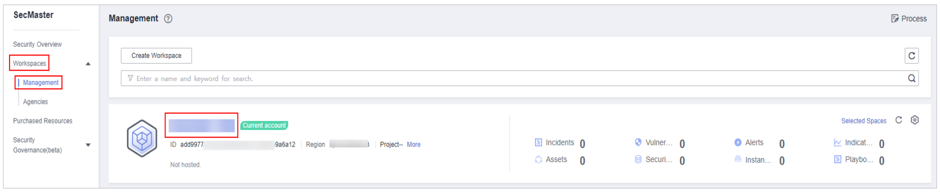
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

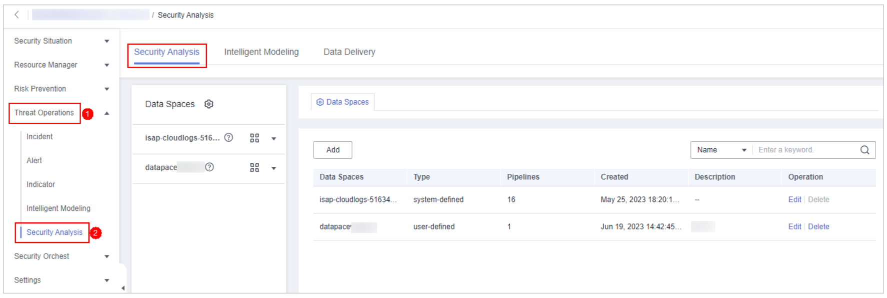
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-85 Workspace management page



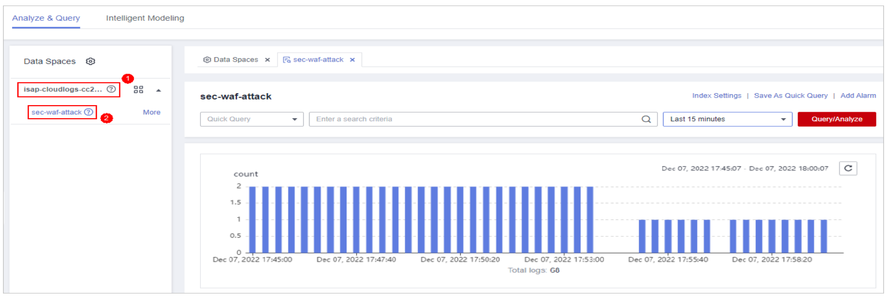
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-86 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-87 Pipeline data page

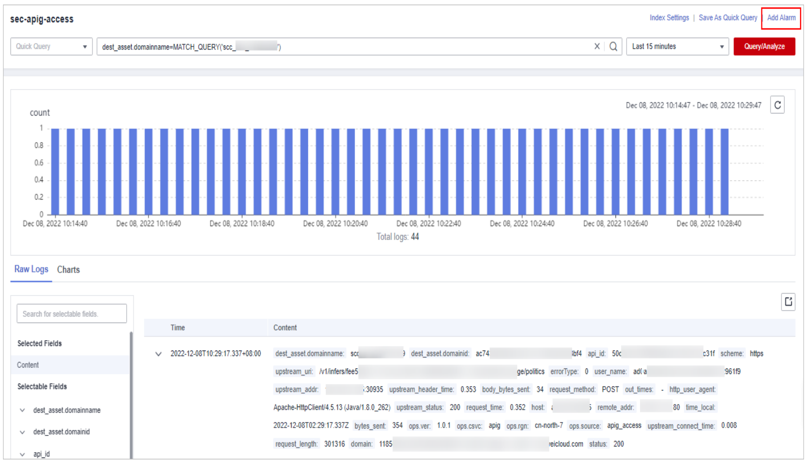


Step 6 Enter the query analysis statement, set the time range, and click **Query/Analyze**. The query analysis result is displayed.

For details, see **Querying and Analyzing Data**.

Step 7 Click **Add Alarm** in the upper right corner of the page. The **Create Alarm Model** page is displayed.

Figure 10-88 Add Alarm



Step 8 Configure basic alarm information by referring to **Table 10-72**.

Table 10-72 Basic parameters of an alarm model

Parameter	Description
Pipeline Name	The pipeline where the alert model is executed, which is generated by the system by default.
Model Name	Name of the alarm model.
Severity	Severity of alarms reported by the alarm model. You can set the severity to **Critical**, **High**, **Medium Low**, or **Informative**.
Alarm Type	Alarm type displayed after the alarm model is triggered.
Model Type	The default value is **Rule model**.
Description	Enter the description of the alarm model.
Status	The alarm model status. • : indicates that the model is enabled. This is the default status. • : indicates that the model is disabled. You can change the alarm model status after the model is configured.

Step 9 After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

Step 10 Set the model logic. For details about the parameters, see **Table 10-73**.

Table 10-73 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click **Run** and view the running result.
Query Plan	Set an alert query plan. ● Running query interval: xx minutes/hour/day. If the running query interval is minute, set this parameter to a value ranging from 5 to 59 minutes. If the running query interval is hour, set this parameter to a value ranging from 1 to 23 hours. If the running query interval is day, set this parameter to a value ranging from 1 to 14 days. ● Time window: xx minutes/hour/day. If the time window is minute, the value ranges from 5 minutes to 59 minutes. If the time window is hour, the value ranges from 1 hour to 23 hours. If the time window is day, the value ranges from 1 day to 14 days. ● Execution Delay: xx minutes. The value ranges from 0 to 5 minutes.
Advanced Alarm Settings	● **Custom Information**: Customize extended alert information. Click **Add**, and set the **key** and **value** information. ● **Alarm Details**: Enter the alarm name, description, and handling suggestions.
Trigger Condition	Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx. If there are multiple triggers, click **Add**.
Alarm Trigger	The way to trigger alerts for queried results. The options are as follows: ● One alert for all query results ● One alert for each query result
Debugging	Sets whether to generate debugging alarms.
Suppression	Specifies whether to stop the query after an alert is generated. ● : indicates that the query stops after an alert is generated. ● : indicates that the query is not stopped after an alert is generated.

Step 11 After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.

Step 12 After confirming that the preview is correct, click **OK** in the lower right corner of the page to confirm the configuration.

----End

10.5.10 Charts

10.5.10.1 Overview

SecMaster supports a wide range of chart types to display query and analysis results. You can select the one you like.

SecMaster can display query and analysis results in the following chart types:

- **Table**
- **Line Chart**
- **Bar Chart**
- **Pie Chart**

10.5.10.2 Tables

The query and analysis results can be displayed in a table.

Table is the most commonly used method to display and analyze data. In SecMaster, the data results obtained by querying and analyzing statements are displayed in tables by default.

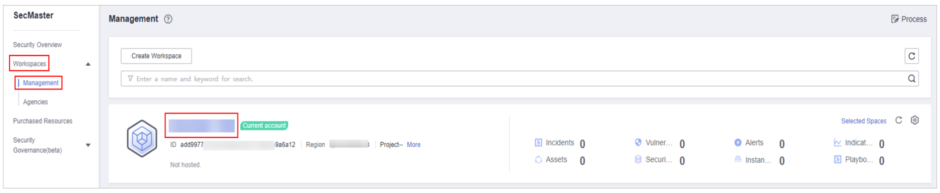
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

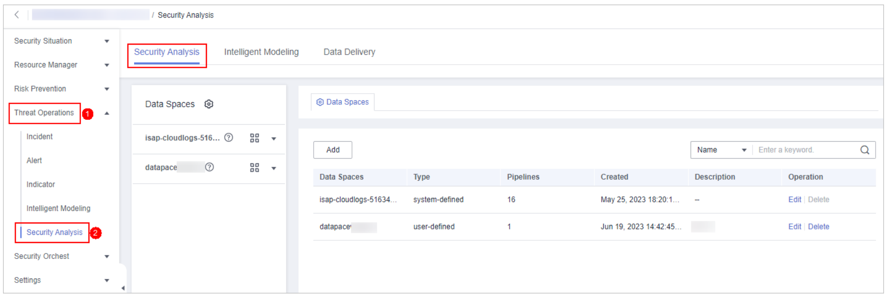
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-89 Workspace management page



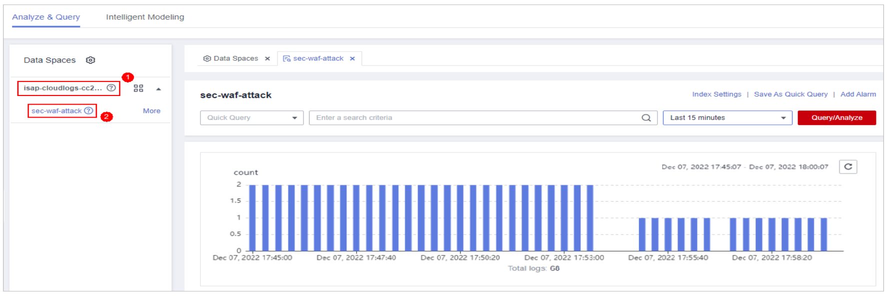
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-90 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

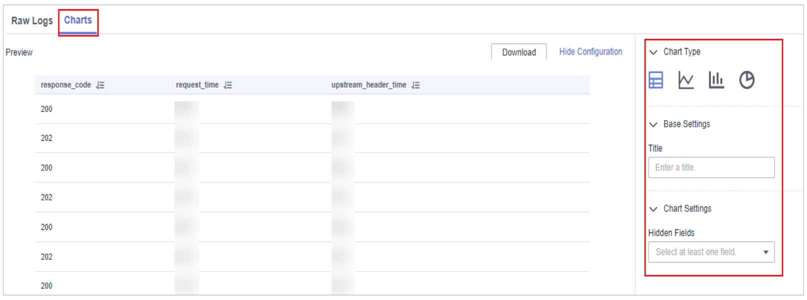
Figure 10-91 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/ Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-92 Charts



Step 8 Set parameters in the table.

Table 10-74 Table parameters

Category	Parameter	Description
Base Settings	Title	Customize the table title.
Chart Settings	Hidden Fields	Select a target field to hide it in the table.

After the chart is configured, you can preview the configured data analysis on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.10.3 Line Charts

The query and analysis results can be displayed in a line chart.

A line chart is used to display the change of a group of data in a period and show the data change trend.

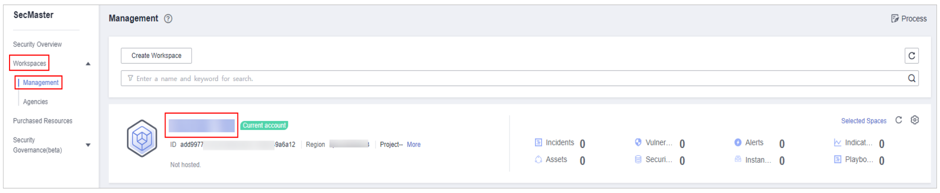
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

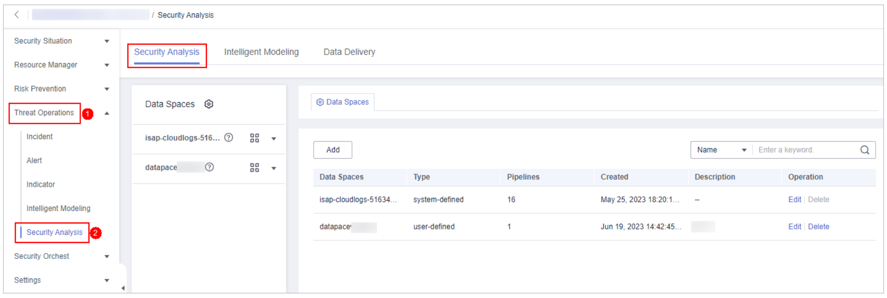
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-93 Workspace management page



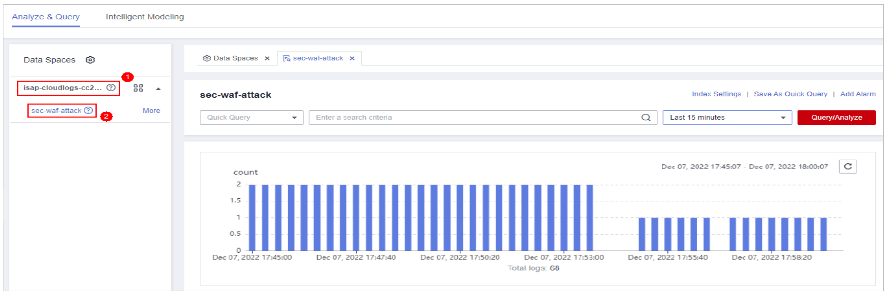
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-94 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-95 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/ Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-96 Line chart statistics

Step 8 Set line chart parameters.

Table 10-75 Line chart parameters

Category	Parameter	Description
Base Settings	Title	Customized line chart title
Chart Settings	X-Axis Title	Customized title of the X axis

Category	Parameter	Description
	Y-Axis Title	Customized title of the Y axis
	X-Axis Field	Field to be displayed on the X axis
	Y-Axis Field	Field to be displayed on the Y axis
Legend	Show Legend	Determine whether to display the legend.
	Position	This parameter is mandatory when the legend display function is enabled. Position of the legend in the chart. The options are **Top**, **Bottom**, **Left**, and **Right**.

After the chart is configured, you can preview the configured data analysis result on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.10.4 Bar Charts

The query and analysis results can be displayed in a bar chart.

A bar chart presents categorical data with rectangular bars with heights or lengths. It can be used to compare data and trends. In SecMaster, the bar chart uses vertical bars (the width is fixed and the height indicates the value) to display data by default.

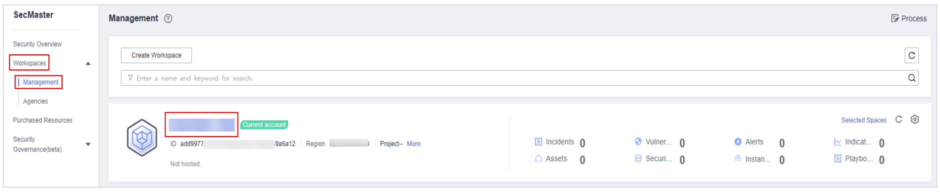
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

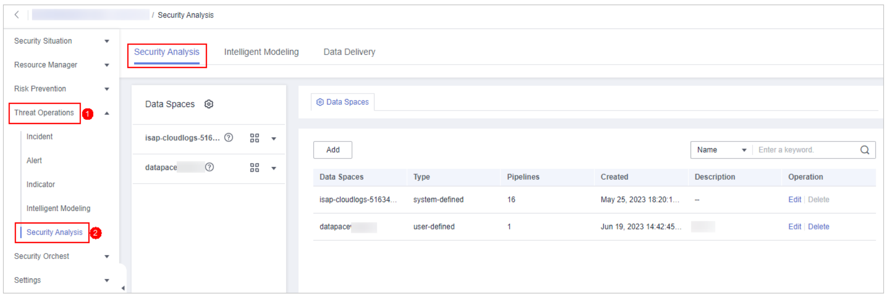
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-97 Workspace management page



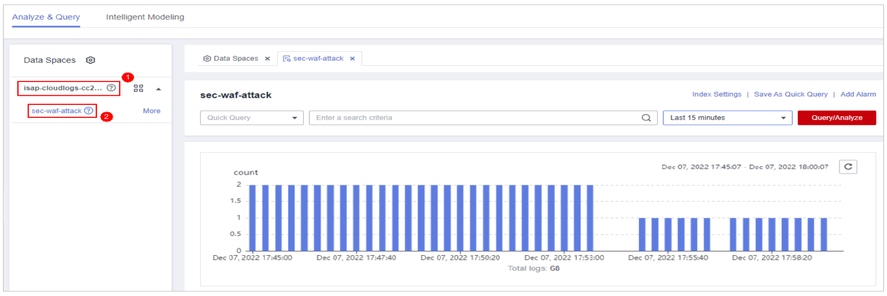
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-98 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-99 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/ Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-100 Bar chart statistics

Step 8 Set bar chart parameters.

Table 10-76 Bar chart parameters

Category	Parameter	Description
Base Settings	Title	Customized line chart title
Chart Settings	X-Axis Title	Customized title of the X axis
	Y-Axis Title	Customized title of the Y axis
	X-Axis Field	Field to be displayed on the X axis
	Y-Axis Field	Field to be displayed on the Y axis
Legend	Show Legend	Determine whether to display the legend.
	Position	This parameter is mandatory when the legend display function is enabled. Position of the legend in the chart. The options are **Top**, **Bottom**, **Left**, and **Right**.

After the chart is configured, you can preview the configured data analysis result on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.

- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.10.5 Pie Charts

The query and analysis results can be displayed in a pie chart.

The pie chart is used to show the proportion of different categories. Different categories are compared by radian.

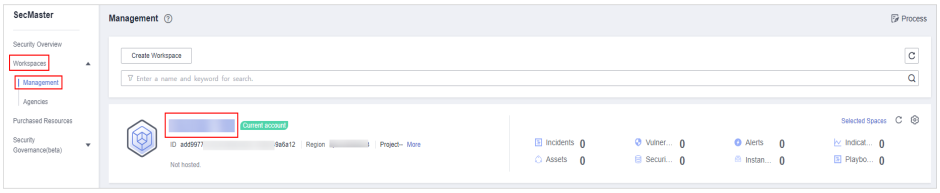
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

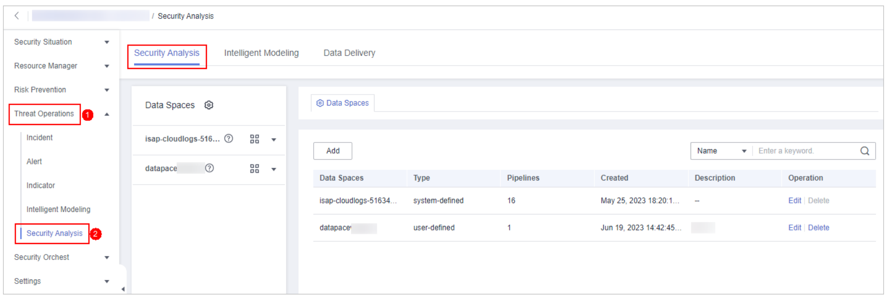
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-101 Workspace management page



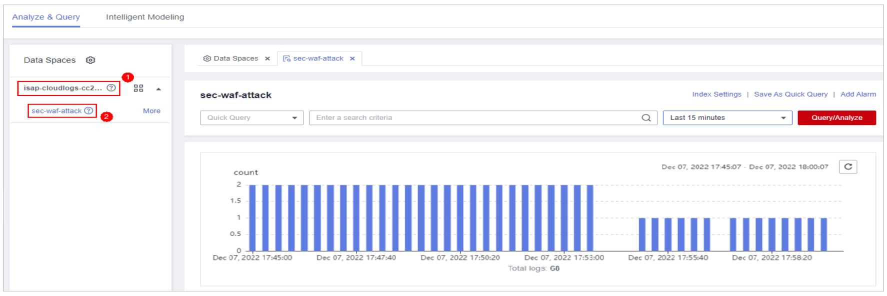
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-102 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

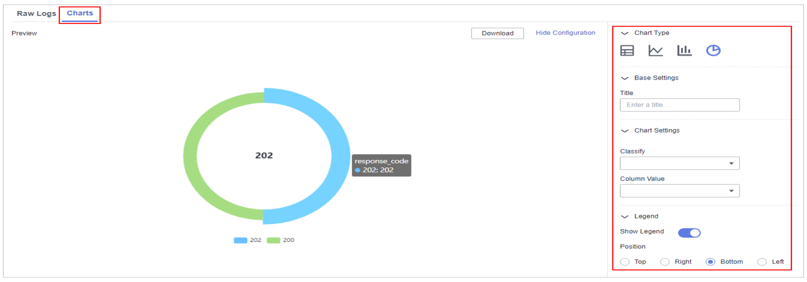
Figure 10-103 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/ Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-104 Pie chart statistics



Step 8 Set pie chart parameters.

Table 10-77 Pie chart parameters

Category	Parameter	Description
Base Settings	Title	Customized line chart title
Chart Settings	Classify	Data classification
	Column Value	Value of the data type
Legend	Show Legend	Determine whether to display the legend.
	Position	This parameter is mandatory when the legend display function is enabled. Position of the legend in the chart. The options are **Top**, **Bottom**, **Left**, and **Right**.

After the chart is configured, you can preview the configured data analysis result on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.11 Managing Data Spaces

10.5.11.1 Creating a Data Space

Scenario

A data space is a unit for data grouping, load balancing, and flow control. Data in the same data space shares the same load balancing policy.

When you need to use the security analysis, data analysis, and intelligent modeling features provided by SecMaster, you need to create a data space.

This section describes how to create a data space.

Limitations and Constraints

- A maximum of five data spaces can be created in a workspace in a region for a single account.

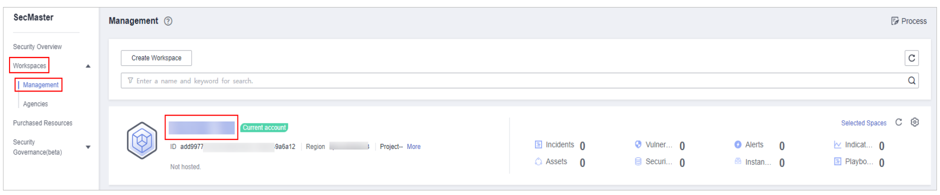
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

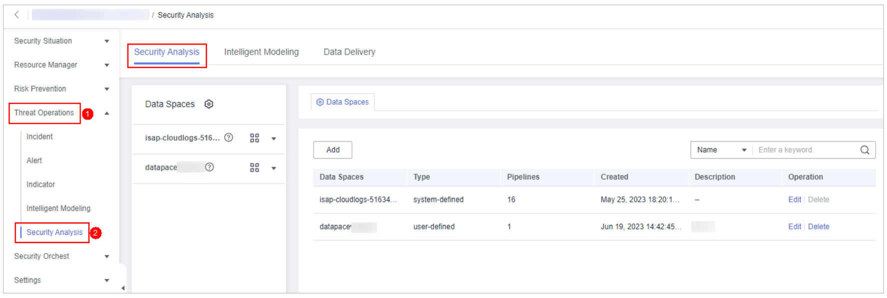
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-105 Workspace management page



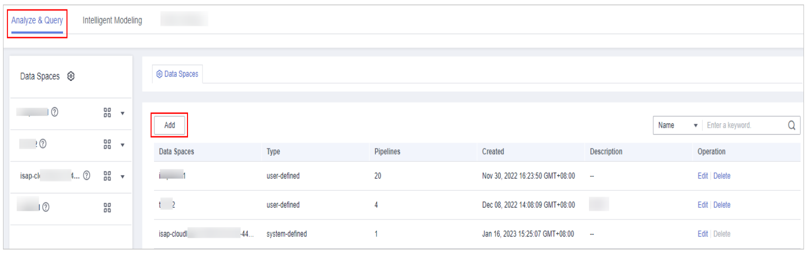
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-106 Accessing the Security Analysis tab page



Step 5 In the upper left corner of the data space list, click **Add**. The **Adding Data Spaces** page is displayed on the right.

Figure 10-107 Creating a data space



Step 6 On the **Adding Data Spaces** page, set the parameters for the new data space. For details about the parameters, see **Table 10-78**.

Table 10-78 Adding a data space

Parameter	Description
Data Space	Data space name. It must meet the following requirements: ● The name contains 5 to 63 characters. ● The value can contain letters, numbers, and hyphens (-). The hyphen (-) cannot be used at the beginning or end, or used consecutively. ● The name must be unique on Huawei Cloud and cannot be the same as any other data space name.
Description	You can make remarks on the data space. This parameter is optional.

Step 7 Click **OK**. The data space is added.

After the data space is added, you can view the new data space in the data space list.

----End

10.5.11.2 Viewing Data Space Details

Scenario

This topic describes how to view the information about a data space, including the name, type, and creation time.

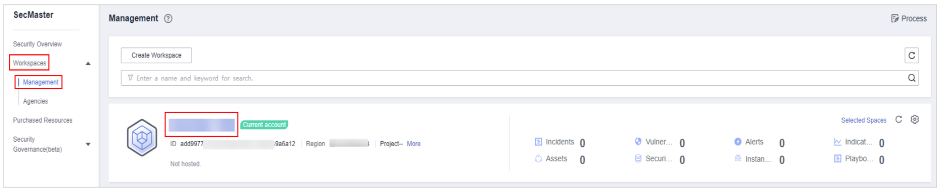
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

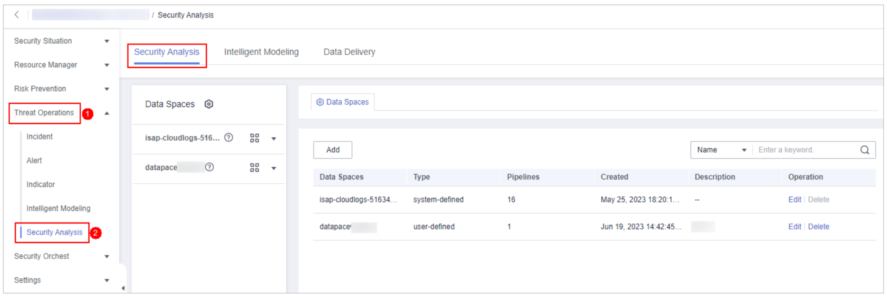
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-108 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-109 Accessing the Security Analysis tab page



Step 5 On the **Data Spaces** page, view all data space information. **Table 10-79** describes related parameters.

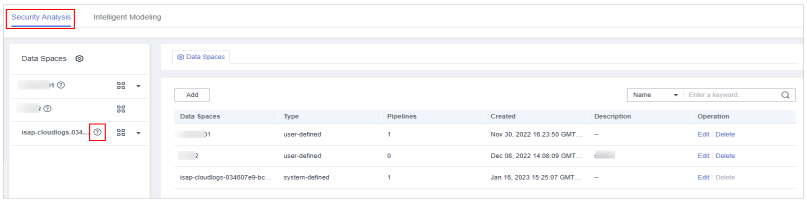
Table 10-79 Data space parameters

Parameter	Description
Data Spaces	Data space name
Type	Type of data in the data space. It may be: ● System-defined: data space created by the system by default during data access. ● User-defined: data space created by users.

Parameter	Description
Pipelines	Number of pipelines in the data space.
Created	Time when the data space is created.
Description	Description of the data space
Operation	You can perform operations such as editing and deleting in the **Operation** column.

Step 6 In the data space column on the left, click next to a data space name to view the details about the data space.

Figure 10-110 Data space details



Step 7 In the Data **Space Details** area, you can view details about a data space. For details about the parameters, see **Table 10-80**.

Table 10-80 Data space details

Parameter	Description
Data Spaces	Data space name
Pipelines	Number of pipelines in the data space.
Created	Time when the data space is created.
Description	Description of the data space

----End

10.5.11.3 Editing a Data Space

Scenario

This topic describes how to modify the information of a data space after the data space is created.

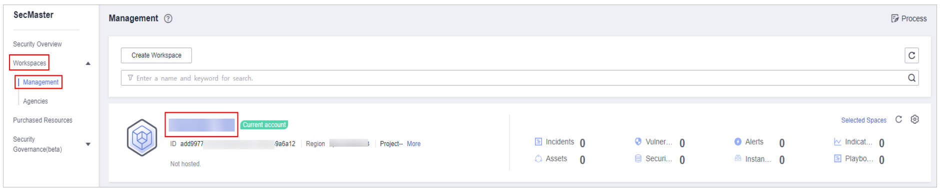
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

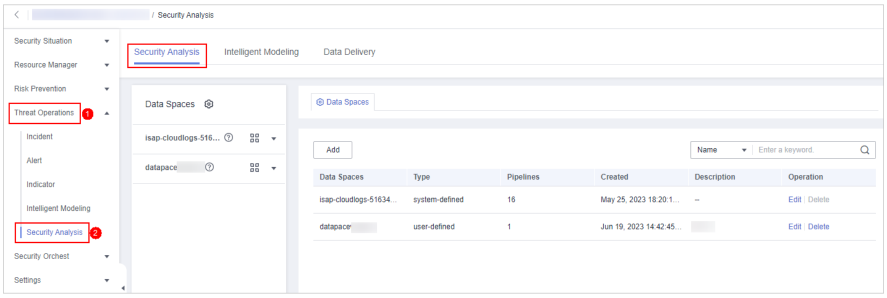
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-111 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-112 Accessing the Security Analysis tab page



Step 5 Locate the row that contains the data space to be edited, and click **Edit** in the **Operation** column.

Step 6 In the displayed **Edit Data Space** dialog box, modify the data space information.

Step 7 Click **OK**.

----End

10.5.11.4 Deleting a Data Space

Scenario

This topic describes how to delete a data space that is no longer needed.

Limitations and Constraints

- The default data space created by the system cannot be deleted.
- If a pipeline exists in the data space to be deleted, the data space cannot be deleted directly. You need to delete the pipeline before deleting the data space.

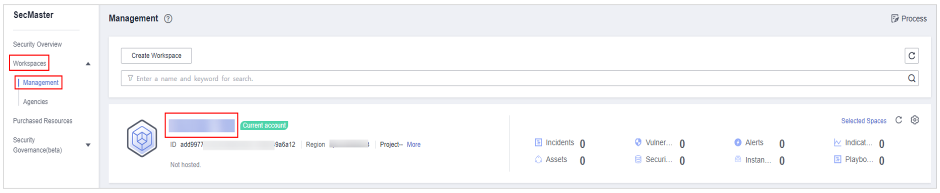
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

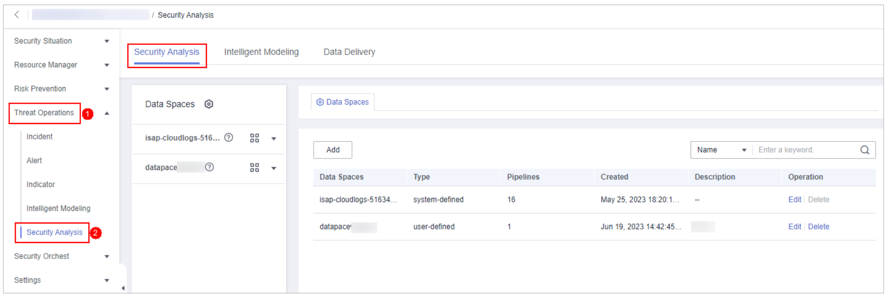
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-113 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-114 Accessing the Security Analysis tab page



Step 5 In the row containing the desired database, click **Delete** in the **Operation** column.

Step 6 In the dialog box that is displayed, click **OK**. The data space is deleted.

CAUTION

If a pipeline exists in the data space to be deleted, the data space cannot be deleted directly. You need to delete the pipeline before deleting the data space.

----End

10.5.12 Managing Pipelines

10.5.12.1 Creating a Pipeline

Scenario

A data transfer message topic and a storage index form a pipeline.

To use the security analysis, data analysis, and intelligent modeling functions provided by SecMaster, you need to create pipelines.

This section describes how to create a pipeline.

Prerequisites

- A workspace has been created. For details, see **Creating a Workspace**.
- A data space has been added. For details, see **Creating a Data Space**.

Limitations and Constraints

- A maximum of 20 pipelines can be created in a data space in a region for a single account.

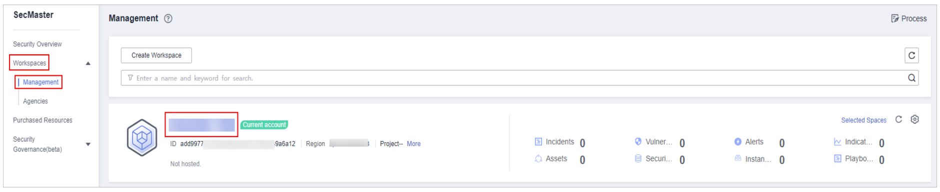
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

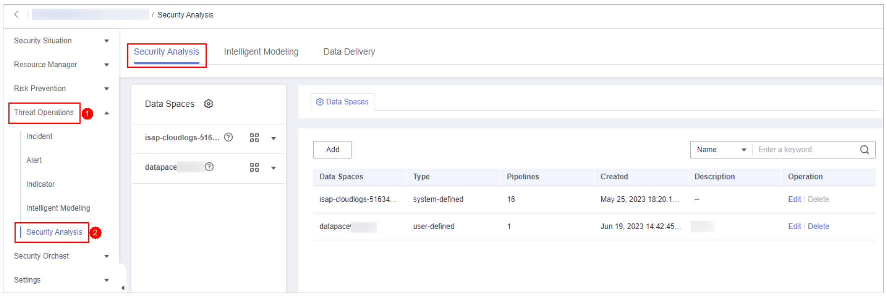
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-115 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-116 Accessing the Security Analysis tab page



Step 5 In the data space navigation pane on the left, click on the right of the data space name and select **Create Pipeline** from the drop-down list box. The **Create Pipeline** page is displayed on the right.

Figure 10-117 Creating a pipeline

Step 6 On the **Create Pipeline** page, configure pipeline parameters. For details about the parameters, see **Table 10-81**.

Table 10-81 Creating a pipeline

Parameter	Description
Data Spaces	Data space to which the pipeline belongs, which is generated by the system by default.
Pipeline Name	Name of the pipeline. It must meet the following requirements: ● The name contains 5 to 63 characters. ● The value can contain letters, numbers, and hyphens (-). The hyphen (-) cannot be used at the beginning or end, or used consecutively. ● The name must be unique in the data space.
Shards	The number of shards of the pipeline. The value range is 1 to 64.
Lifecycle	Life cycle of data in the pipeline. Value range: 7-180
Description	Remarks on the pipeline. This parameter is optional.

Step 7 Click **OK**.

After the pipeline is created, you can click the data space name or ▾ next to the data space to view the created pipeline.

----End

10.5.12.2 Viewing Pipeline Details

Scenario

This topic describes how to view the pipeline details, including the pipeline name, data space, and creation time.

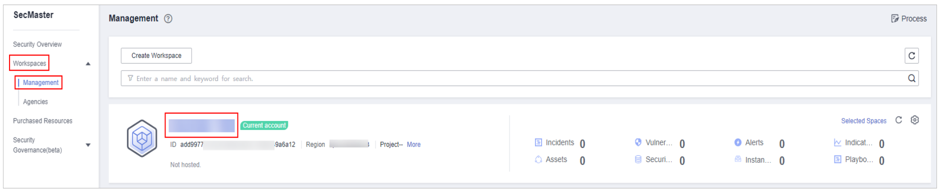
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

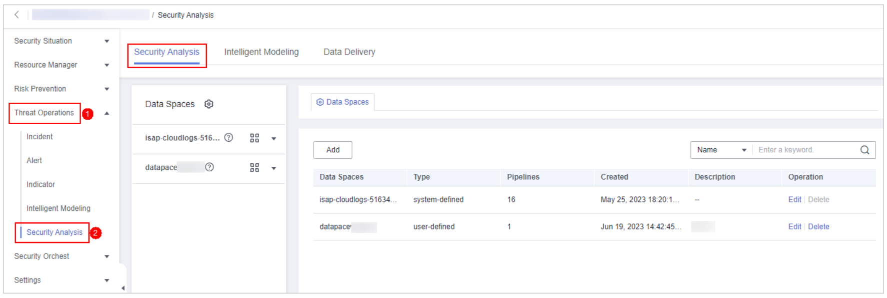
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-118 Workspace management page



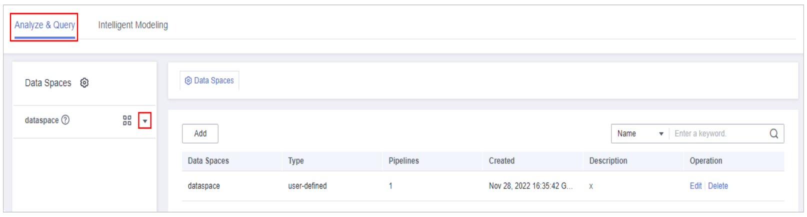
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-119 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click the data space name or to view the created pipeline.

Figure 10-120 Viewing pipeline details



Step 6 Click next to a pipeline name you want to view. The pipe details are displayed in the right pane.

Table 10-82 Pipeline parameters

Parameter	Description
Workspace Name	Name of the workspace to which the current pipe belongs.
Workspace ID	ID of the workspace to which the current pipe belongs.
Data Space Name	Name of the data space to which the current pipeline belongs.
Data Space ID	ID of the data space to which the current pipeline belongs.
Pipeline Name	Name of the current pipeline.

Parameter	Description
Pipeline ID	ID of the current pipeline.
Shards	Number of shards of the pipeline.
Lifecycle	Retention period of data in the pipeline.
Created	Time when a pipe is created
Description	Description of the pipeline

----End

10.5.12.3 Editing a Pipeline

Scenario

After a pipeline is created, you can modify the pipeline information, such as the number of shards, description, and lifecycle.

This topic describes how to modify pipeline parameters.

Limitations and Constraints

Pipelines created by the system **cannot be edited**.

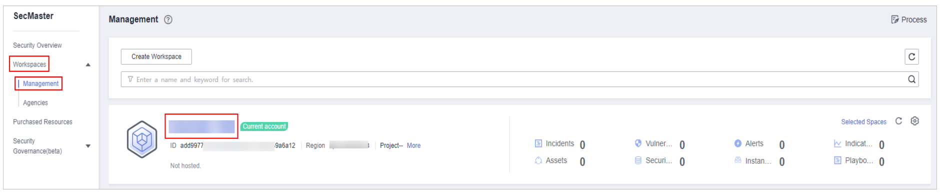
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

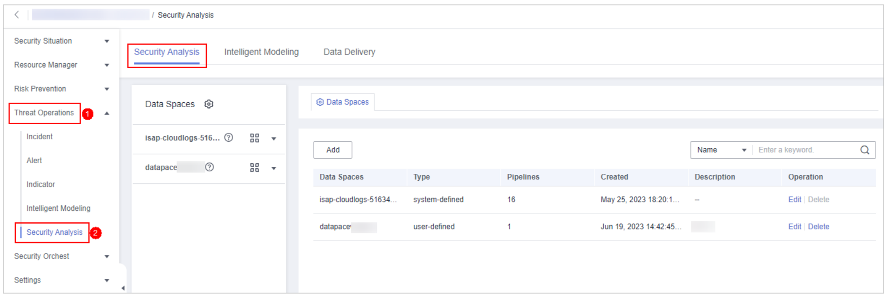
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-121 Workspace management page



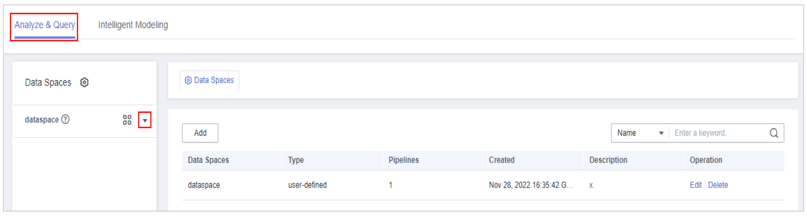
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-122 Accessing the Security Analysis tab page



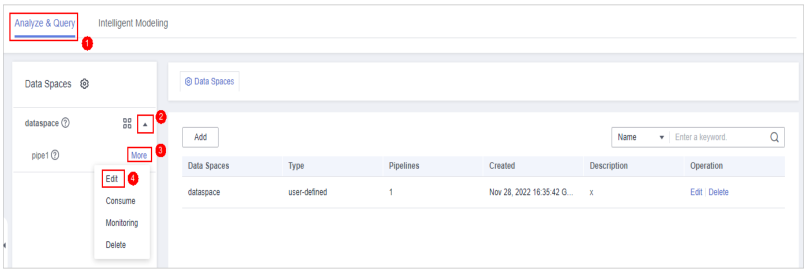
Step 5 In the data space navigation tree on the left, click the data space name or ▾ to view the created pipeline.

Figure 10-123 Viewing pipeline details



Step 6 Click **More** > **Edit** next to the pipeline name.

Figure 10-124 Entry for editing a pipeline



Step 7 On the **Edit Pipeline** page, set pipeline parameters. For details about the parameters, see **Table 10-83**.

Table 10-83 Editing a pipeline

Parameter	Description
Data Spaces	Data space to which the pipeline belongs. This parameter **cannot** be modified.
Pipeline Name	Name you specified for the pipeline. The name **cannot** be changed after the pipeline is created.
Shards	The number of shards of the pipeline. The value range is 1 to 64.
Lifecycle	Life cycle of data in the pipeline. Value range: 7-180
Description	Remarks on the pipeline. This parameter is optional.

Step 8 Click **OK**.

----End

10.5.12.4 Deleting a Pipeline

Scenario

This section describes how to delete a pipeline.

Data in the pipeline will also be deleted and cannot be restored. Exercise caution when performing this operation.

Limitations and Constraints

Pipelines created by the system cannot be deleted.

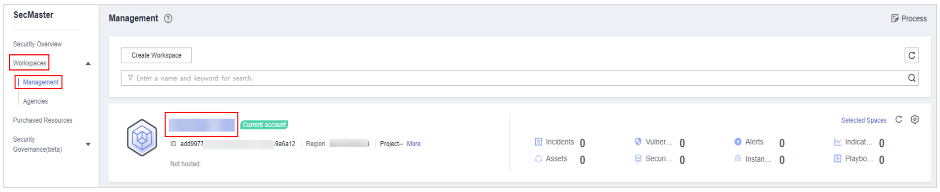
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

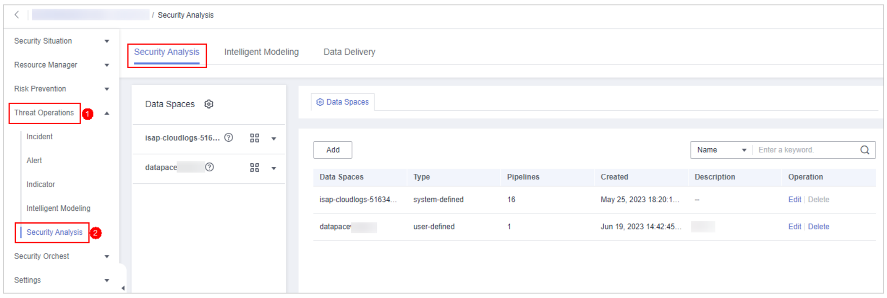
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-125 Workspace management page



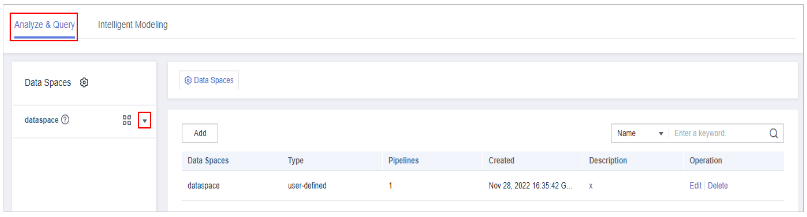
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-126 Accessing the Security Analysis tab page



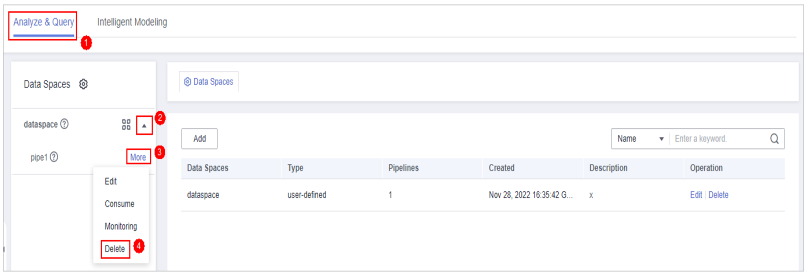
Step 5 In the data space navigation tree on the left, click the data space name or ▾ to view the created pipeline.

Figure 10-127 Viewing pipeline details



Step 6 Click **More** > **Delete** next to the pipeline name.

Figure 10-128 Deleting a pipeline



Step 7 In the dialog box that is displayed, click **OK**.

----End

10.6 Data Consumption

Data consumption refers to the process during which third-party software or cloud products consume the log data in real time through a client. It is a sequential read/write from/into full data.

SecMaster provides the data consumption function and supports real-time data consumption through the client.

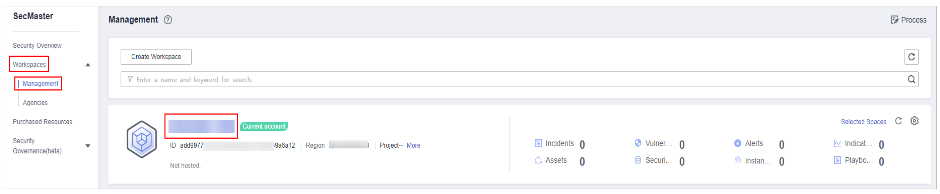
Enabling Data Consumption

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

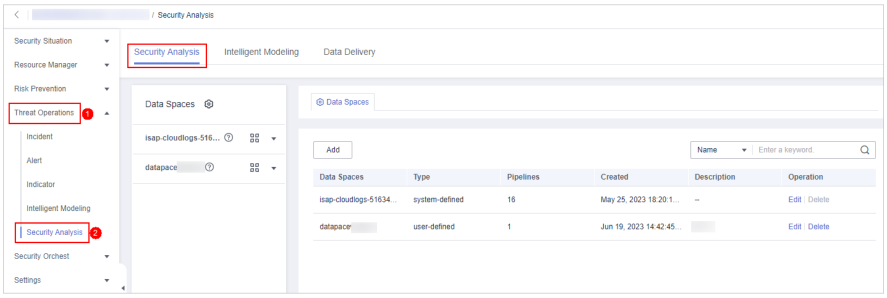
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-129 Workspace management page



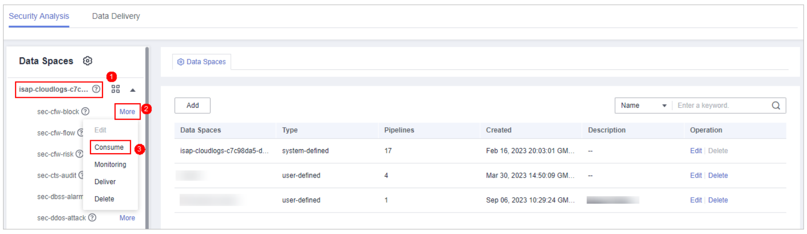
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-130 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Consume**.

Figure 10-131 Accessing the data consumption page



Step 6 On the Data Consumption page, click  next to Current Status to enable data consumption.

After the function is enabled, the consumption configuration information is displayed, as shown in **Table 10-84**.

Table 10-84 Data consumption parameters

Parameter	Description
Status	Status of the data consumption function in the current pipeline
Pipeline Name	Name of the current pipeline
Subscriber	The preset subscription mode in the system, which determines how data is transmitted to consumers.
Access Node	Access node of the current data.

----End

Related Operations

After data consumption is enabled, you can click  next to **Status** on the Data Consumption page to disable data consumption.

10.7 Data Delivery

10.7.1 Creating a Data Delivery

Scenario

SecMaster can deliver data to other pipelines or other cloud products in real time so that you can store data or consume data with other systems. After data delivery is configured, SecMaster periodically delivers the collected data to the specified pipelines or cloud products.

Currently, data can be delivered to the following cloud products: Object Storage Service (OBS) and Log Tank Service (LTS).

This section describes how to create a data delivery task.

Prerequisites

- To deliver data to OBS, ensure there is an available bucket whose bucket policy is **Public Read and Write**. For details, see **Creating an OBS Bucket**.
- To deliver data to LTS, ensure there is an available log group and log streams. For details, see **Managing Log Groups** and **Managing Log Streams**.

Limitations and Constraints

When performing cross-account delivery, the data can only be delivered to the pipelines instead of cloud services of other accounts.

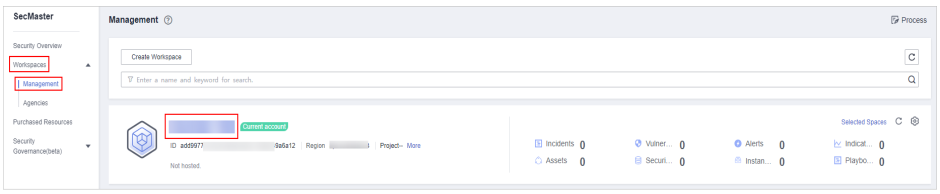
Creating a Data Delivery

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

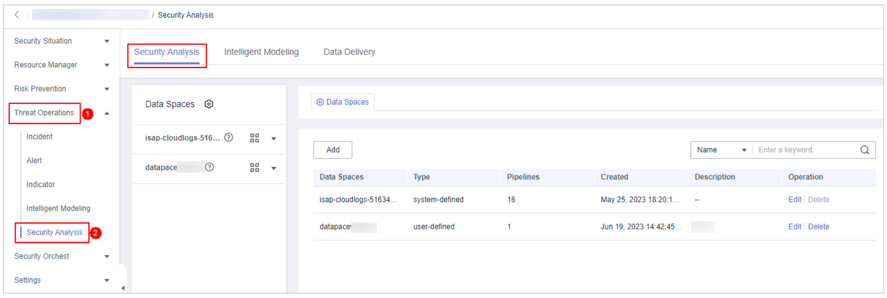
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-132 Workspace management page



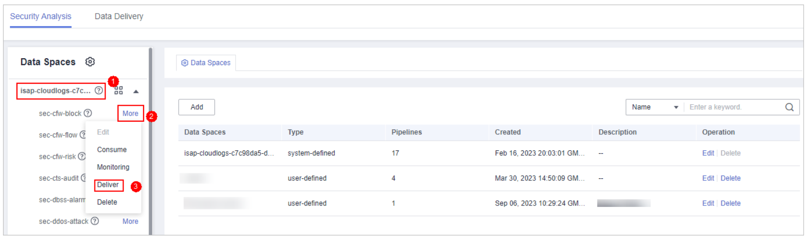
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-133 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Deliver**.

Figure 10-134 Accessing data delivery settings page



Step 6 (Optional) Authorization of the destination type is required for the first delivery. If the authorization has been performed, skip this step.

Confirm the authorization information, select **Agree to authorize** and click **OK**.

Step 7 On the **Create Delivery** page, set data delivery parameters.

1. Configure basic information.

Table 10-85 Basic information

Parameter	Description
Delivery Name	Customized delivery rule name
Resource Consumption	The value is generated by default and **does not need to be configured**.

2. Configure the data source.
   In the **Data Source Settings** area, the detailed information about the current pipeline is displayed. **You do not need to set this parameter**.

Table 10-86 Data source parameters

Parameter	Description
Delivery Type	Delivery destination type. The default value is **PIPE**.
Region	Area where the current pipeline is located
Workspace	Workspace to which the current pipeline belongs

Parameter	Description
Data Spaces	Data space to which the current pipeline belongs
Pipeline	Pipeline name
Data Read Policy	Data read policy of the current pipeline
Read By	Identity of the data source reader

3. Configure the delivery destination.
   – **PIPE**: Deliver the current pipeline data to other pipelines of the current account or pipelines of other accounts. Set this parameter as required.
     - **Current**: Deliver the current pipeline data to another pipeline of the current account. For details about the parameters, see **Table 10-87**.

Table 10-87 Destination parameters - Current account pipeline

Parameter	Description
Account Type	Account type of the data delivery destination. Select **Current**.
Delivery Type	Delivery type. Select **PIPE**.
Workspace	Workspace where the destination PIPE is located
Data Spaces	Data space where the destination PIPE is located
Pipeline	Pipeline where the destination PIPE is located
Written To	The value is generated by default and does not need to be configured.

     - Cross-account delivery: Deliver the current pipeline data to the pipeline of another account. For details about the parameters, see **Table 10-88**.

Table 10-88 Destination parameters - PIPE of Other account

Parameter	Description
Account Type	Account type of the data delivery destination. Select **Other**.
Delivery Type	Delivery type. Select **PIPE**.
Account ID	ID of the account to which the destination pipeline belongs

Parameter	Description
Workspace ID	ID of the workspace where the destination PIPE is located. For details about how to query the workspace ID, see **Step 6**.
Data Space ID	ID of the data space where the destination PIPE is located. For details about how to query the data space ID, see **Step 6**.
Pipeline ID	ID of the pipeline where the destination PIPE is located. For details about how to query the pipeline ID, see **Step 6**.
Written To	The value is generated by default and does not need to be configured.

– **LTS**: Deliver the pipeline data to LTS. For details about the parameter settings, see **Table 10-89**.

  To deliver data to LTS, ensure there is an available log group and log streams. For details, see **Managing Log Groups** and **Managing Log Streams**.

Table 10-89 Destination parameters - LTS

Parameter	Description
Account Type	Account type of the data delivery destination. When delivering data to LTS, only the **Current** account type can be selected.
Delivery Type	Delivery type. Select **LTS**.
Log Group	Destination LTS log group
Log Stream	Destination LTS log stream
Written To	The value is generated by default and does not need to be configured.

– **OBS**: Deliver the pipeline data to OBS. For details about the parameter settings, see **Table 10-90**.

  To deliver data to OBS, ensure there is an available bucket whose bucket policy is **Public Read and Write**. For details, see **Creating an OBS Bucket**.

Table 10-90 Destination parameters - OBS

Parameter	Description
Account Type	Account type of the data delivery destination. When delivering data to OBS, only the **Current** account type can be selected.

Parameter	Description
Delivery Type	Delivery type. Select **OBS**.
Bucket Name	Name of the destination OBS bucket
Written To	The value is generated by default and does not need to be configured.

4. Under **Access Authorization**, view the permissions granted in **Step 6**.

   A delivery request requires the read and write permissions to access your cloud resources. After the authorization, the delivery task can access your cloud resources.

Step 8 Click **OK**.

----End

Follow-up Operation

After a data delivery task is added, you need to grant the delivery permission. The delivery takes effect only after you accept the authorization. For details, see **Data Delivery Authorization**.

10.7.2 Data Delivery Authorization

Scenario

After a data delivery task is added, you need to grant the delivery permission. The delivery takes effect only after you accept the authorization.

This topic describes how to execute a data delivery.

Prerequisites

Data delivery has been added.

Limitations and Constraints

If the new data delivery is cross-account, you need to log in to SecMaster using the destination account and perform authorization.

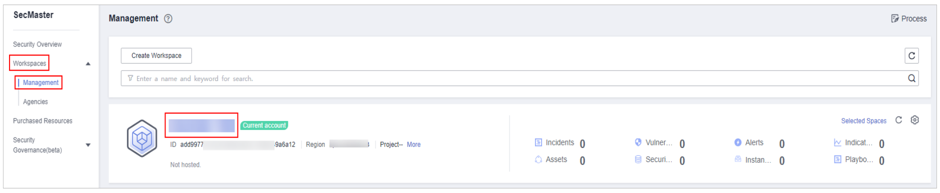
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-135 Workspace management page

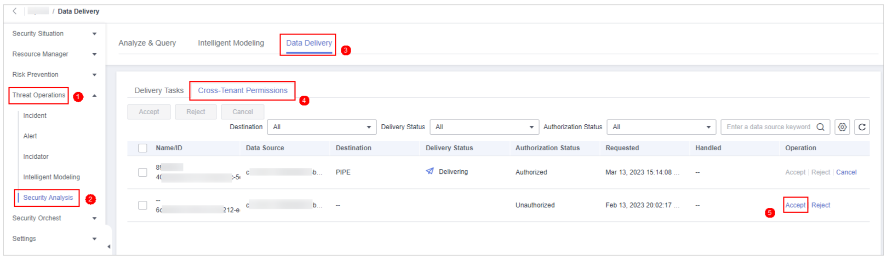


Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.

Step 5 On the **Data Delivery** page, click the **Cross-tenant Permissions** tab. On the page that is displayed, click **Accept** in the **Operation** column of the target delivery task.

To accept authorization in batches, select all tasks to be authorized and click **Accept** in the upper left corner of the list.

Figure 10-136 Data delivery authorization



After the authorization is granted, the authorization status of the target delivery task is updated to **Authorized**. You can go to the delivery destination to view the delivery details. For details, see **Checking the Data Delivery Status**.

----End

Related Operations

On the **Cross-tenant Permissions** tab page, you can select to **Reject** or **Cancel** the authorization.

Table 10-91 Cross-tenant permission authorization options

Operation	Description
Reject	In the row containing the target delivery task, click **Reject** in the **Operation** column to reject the authorization. To reject authorization in batches, select all tasks to be rejected and click **Reject** in the upper left corner of the list.

Operation	Description
Cancel	1. In the row containing the target delivery task, click **Cancel** in the **Operation** column to cancel the authorization. To cancel authorization in batches, select all tasks to be canceled and click **Cancel** in the upper left corner of the list. 2. In the displayed dialog box, click **OK**.

10.7.3 Checking the Data Delivery Status

Scenario

After the data is successfully delivered, you can view the data delivery status at the delivery destination. You can also perform the following operations:

- Delivering to Other Pipelines
- Delivering to OBS Bucket
- Delivering to LTS

Prerequisites

Data has been delivered. For details, see Creating a Data Delivery.

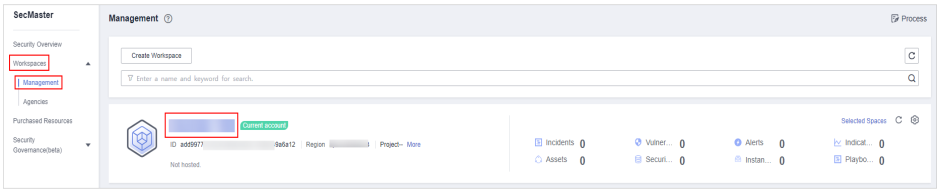
Delivering to Other Pipelines

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

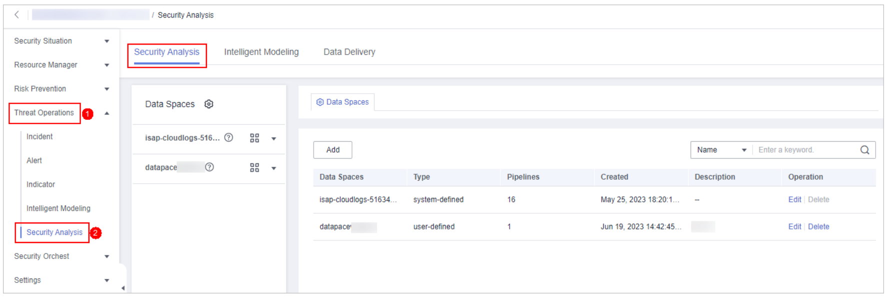
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-137 Workspace management page



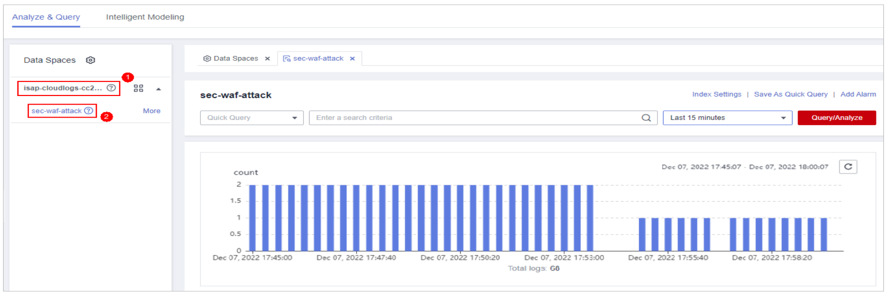
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-138 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-139 Pipeline data page



Step 6 In the target pipeline, view the delivery log information.

----End

Delivering to OBS Bucket

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Storage** > **Object Storage Service**. The bucket list page is displayed.

Step 3 On the bucket list page, click the name of the OBS bucket selected for data delivery. The details page of the target OBS bucket is displayed.

Step 4 On the OBS bucket details page, view the delivery log information.

----End

Delivering to LTS

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Log Tank Service**.

Step 3 In the log group list on the **Log Management** page, locate the log group for which you want to add data delivery and click ˅ before to the log group name.

Step 4 Click the name of the log stream selected during data delivery. The log stream details page is displayed.

Step 5 On the log stream details page, view the delivered log information.

----End

10.7.4 Managing Data Delivery

Scenario

This section describes how to manage delivery tasks.

- **Viewing a Data Delivery Task**
- **Suspending a Delivery Task**
- **Starting a Delivery Task**
- **Deleting a Delivery Task**

Prerequisites

A data delivery task has been added.

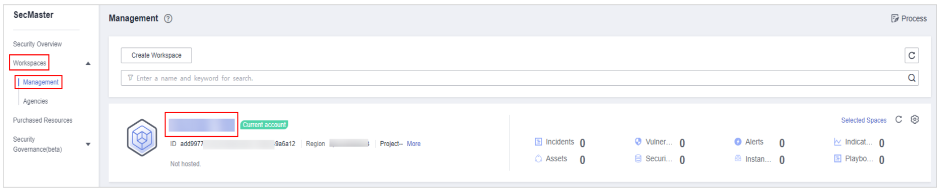
Viewing a Data Delivery Task

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

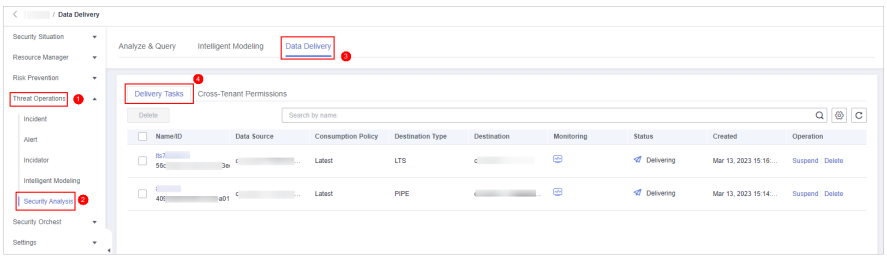
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-140 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-141 Accessing the data delivery page



Step 5 On the delivery task list page, view existing delivery tasks.

Table 10-92 Delivery task parameters

Operation	Description
Name/ID	Delivery task name and ID
Data Source	Pipeline where the data source is located
Consumption Policy	Consumption policy of a delivery task
Destination Type	Type of the data delivery destination
Destination	Data delivery destination
Monitoring	Data delivery monitoring status. You can click the monitoring icon to view the data consumption information.
Status	Status of a delivery task
Created	Time when a delivery task is created
Operation	You can delete or suspend a data delivery task.

----End

Suspending a Delivery Task

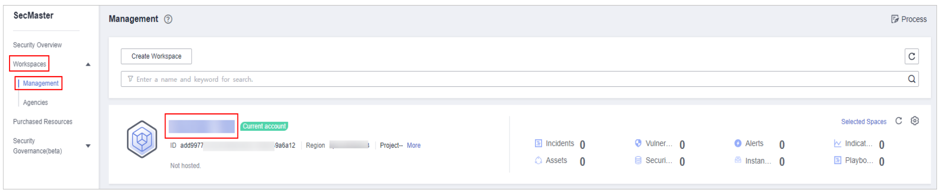
After a data delivery task is added and authorized, the delivery task status changes to **Delivering**. To stop the delivery, you can suspend the target delivery task.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

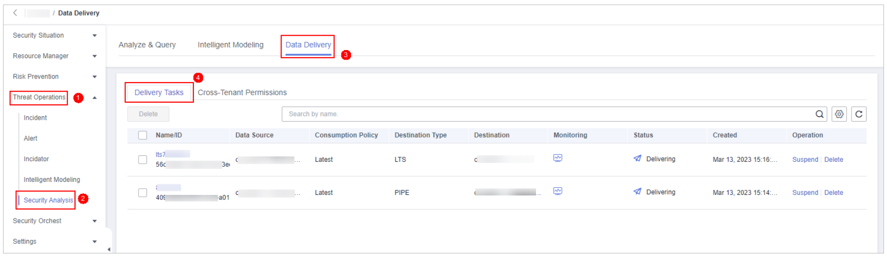
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-142 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-143 Accessing the data delivery page



Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Suspend** in the **Operation** column.

After a delivery task is suspended, the delivery task status changes to **Suspended**, indicating that the delivery task is suspended successfully.

----End

Starting a Delivery Task

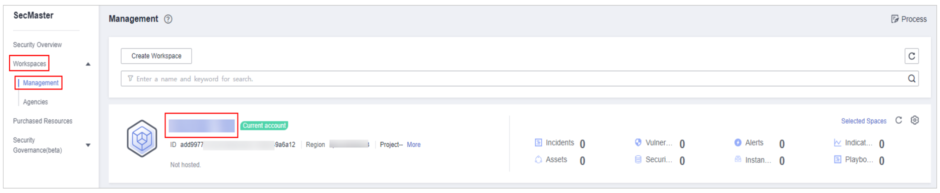
You can restart a suspended delivery task.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

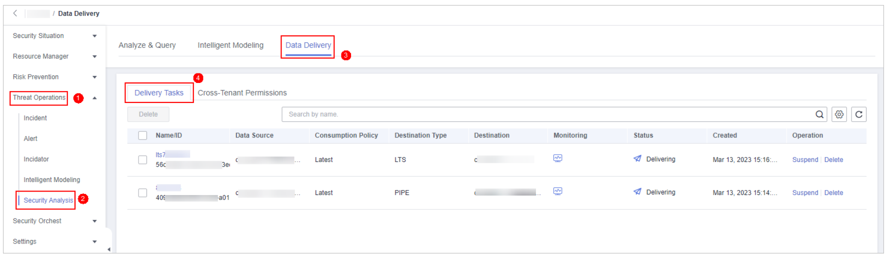
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-144 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-145 Accessing the data delivery page



Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Start** in the **Operation** column.

After a delivery task is restarted, the delivery task status changes to **Delivering**, indicating that the delivery task is successfully started.

----End

Deleting a Delivery Task

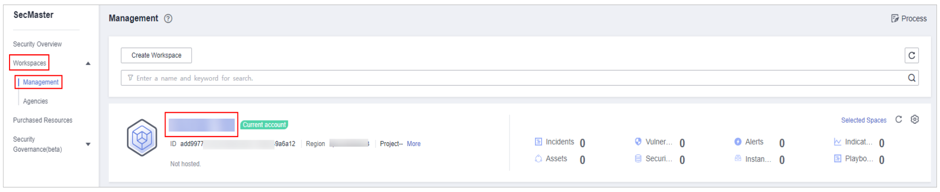
If a data delivery task is no longer needed, you can delete it.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

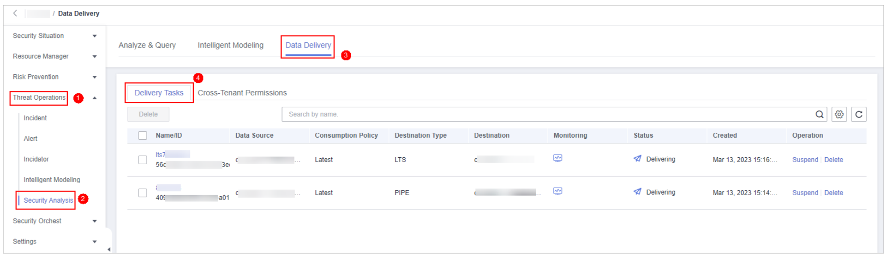
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-146 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-147 Accessing the data delivery page



Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Delete** in the **Operation** column and click **OK** in the displayed dialog box.

----End

10.7.5 Delivering Logs to LTS

Scenario

SecMaster can integrate logs of other cloud products, such as WAF, HSS, and CFW. For details about how to integrate, see **Data Integration**.

You can deliver integrated logs to Log Tank Service (LTS) for real-time decision-making and analysis, device O&M management, and service trend analysis.

This topic walks you through how to deliver integrated logs to LTS.

Prerequisites

- Logs you want to deliver have been aggregated in SecMaster. For details, see **Data Integration**.
- To deliver data to LTS, ensure there is an available log group and log streams. For details, see **Managing Log Groups** and **Managing Log Streams**.

Procedure

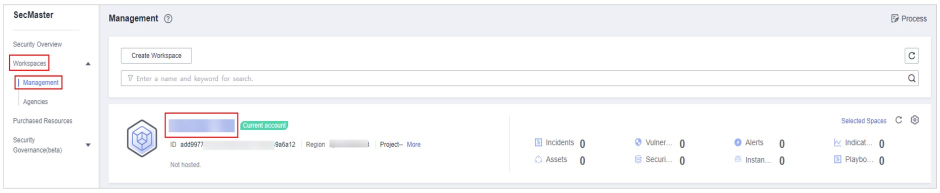
Creating a Data Delivery

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

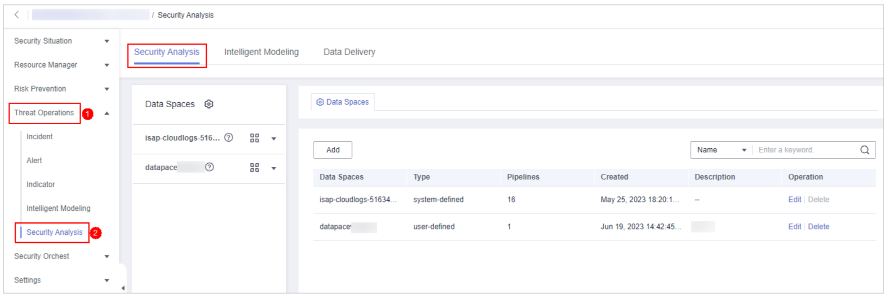
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-148 Workspace management page



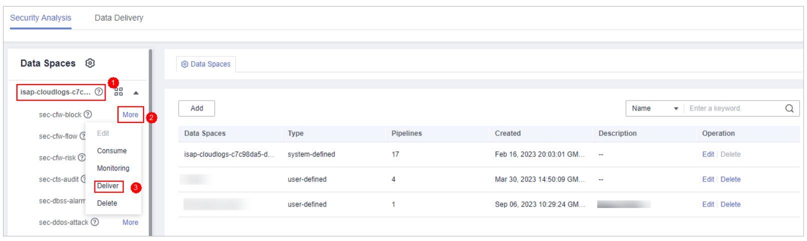
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-149 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Deliver**.

Figure 10-150 Accessing data delivery settings page



Step 6 (Optional) Authorization of the destination type is required for the first delivery. If the authorization has been performed, skip this step.

Confirm the authorization information, select **Agree to authorize** and click **OK**.

Step 7 On the **Create Delivery** page, set data delivery parameters.

- **Delivery Name**: Enter a data delivery name.
- **Account Type**: Select **Current**. Only logs of the current account can be delivered to LTS.
- **Delivery Type**: Select **LTS**.
- **Log Group**: Select an LTS log group. If no log group is available, create one. For details, see **Creating an LTS Log Group**.
- **Log Stream**: Select a destination LTS log stream. If no log stream is available, create one. For details, see **Creating an LTS Log Stream**.

Other configuration parameters are generated by the system by default and do not need to be configured.

Step 8 Under **Access Authorization**, view the permissions granted in **Step 6**.

A delivery requires the read and write permissions to access your cloud resources. A delivery task cannot access your cloud resources unless the access is authorized by you.

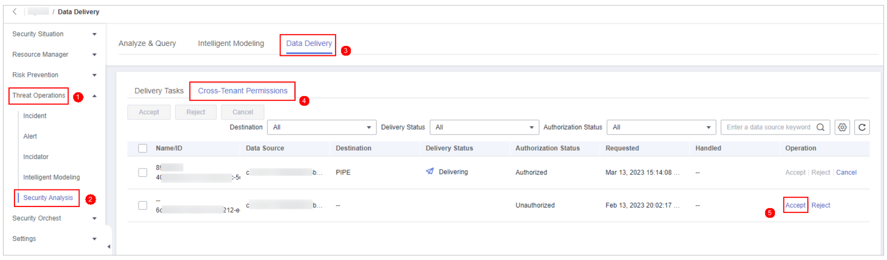
Step 9 Click **OK**.

Data Delivery Authorization

Step 10 On the **Data Delivery** page, click the **Cross-Tenant Permissions** tab. On the page displayed, click **Accept** in the **Operation** column of the target delivery task.

To accept authorization in batches, select all tasks to be authorized and click **Accept** in the upper left corner of the list.

Figure 10-151 Data delivery authorization



After the authorization is granted, the authorization status of the target delivery task is updated to **Authorized**. You can go to the delivery destination to view the delivery details.

Checking the Data Delivery Status

Step 11 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Log Tank Service**.

Step 12 In the log group list on the **Log Management** page, locate the log group for which you want to add data delivery and click ﹀ before the log group name.

Step 13 Click the name of the log stream selected during data delivery. The log stream details page is displayed.

Step 14 On the log stream details page, view the delivered log information.

----End

10.8 Data Monitoring

SecMaster can monitor metrics such as the production rate, production volume, and total consumption rate of the upstream and downstream SecMaster pipelines. You can check the service status based on the monitoring results.

Basic Concepts

- A producer is a logical object used to construct data and transmit it to the server. It stores data in message queues.
- A subscriber is used to subscribe to SecMaster pipeline messages. A pipeline can be subscribed to by multiple subscribers. SecMaster distributes messages through subscribers.
- A consumer is a running entity that receives and processes data. It consumes and processes messages in the SecMaster pipeline through subscribers.
- A message queue is the container for data storage and transmission.

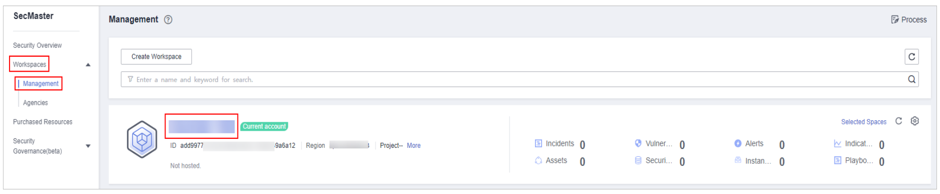
Viewing Metrics

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

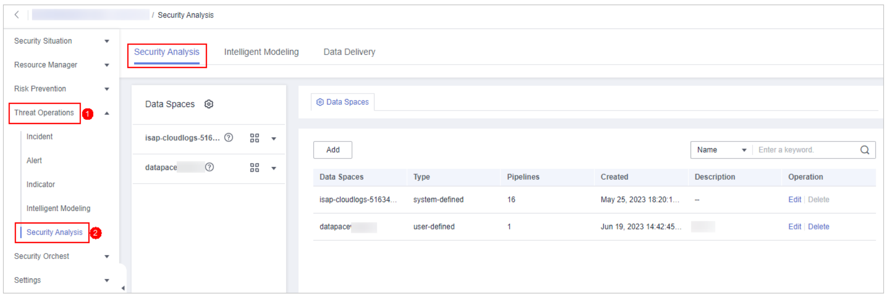
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 10-152 Workspace management page



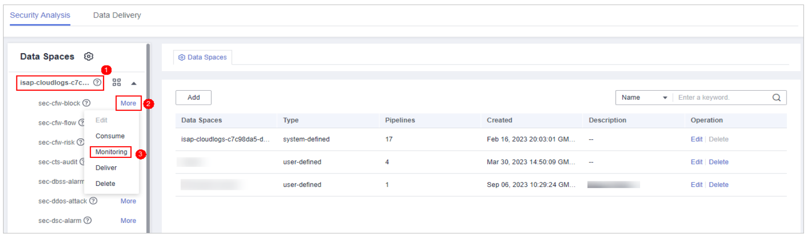
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Security Analysis**. The security analysis page is displayed.

Figure 10-153 Accessing the Security Analysis tab page



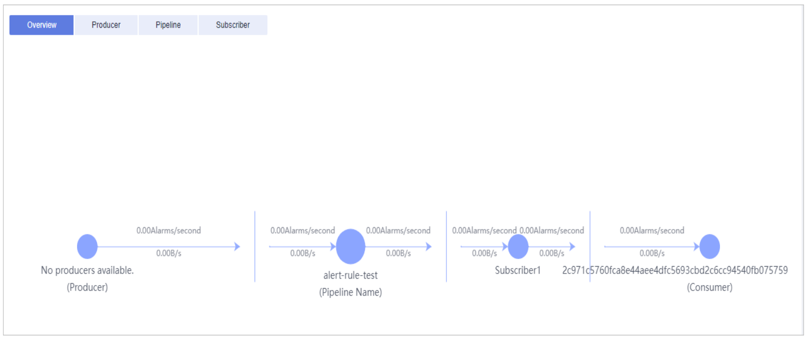
Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More** > **Monitoring**.

Figure 10-154 Accessing the data monitoring page



Step 6 On the pipeline monitoring page, view monitoring metrics.

Figure 10-155 Viewing monitored data



- **Overview**: Displays information such as the production rate between producers, pipelines, subscribers, and consumers in the current pipeline.
- **Producer**: Displays metrics of the producer, such as current production TPS, current production rate, current production volume, and current message storage size.
- **Pipeline**: Displays the pipeline message size (MB), producer-to-pipeline message size (MB), producer-to-pipeline messages, message size consumed by pipelines (MB), messages consumed by pipelines, unacknowledged message size (MB), pipeline production rate, pipeline consumption rate, average message size (KB), and offloaded message size (B) in a specified period (last 2/6/12/24 hours, last 7 days, or a customized period).

- Subscriber: displays the total consumption rate of subscribers, consumed data volume (B), consumed messages, and active consumers in a specified period (last 2/6/12/24 hours, last 7 days, or a user-defined period).

----End

11 Security Orchestration

11.1 Security Orchestration Overview

Security orchestration combines security functions of different systems or components in a system involved in security operations of enterprises and organizations based on certain logical relationships to complete a specific security operations process and procedure. It aims to help security teams of enterprises and organizations quickly and efficiently respond to network threats and implement efficient and automatic response and handling of security incidents.

It provides the following functions:

- Playbook management: you can use the built-in automatic response playbooks or customize playbooks.
- Workflow: Allows you to draw a playbook triggering flowchart.
- Instance management: allows you to monitor and manage running instances and view records.
- Security Orchestration, Automation and Response (SOAR): You can orchestrate workflows to let SecMaster automatically handle security incidents and suspicious incidents.

Limitations and Constraints

- In a single workspace of an account, the scheduling frequency of a single playbook is greater than or equal to 5 minutes.
- The maximum number of retries within a day for a single workspace of a single account is as follows:
  - Manual retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
  - API retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
- Restrictions on classification and mapping are as follows:
  - In a single workspace of a single account, a maximum of 50 classification & mapping templates can be created.

– In a single workspace of a single account, the proportion of a classification to its mappings is 1:100.
– A maximum of 100 classifications and mappings can be added to a workspace of a single account.

Basic Concepts

- Playbook

  A playbook is a formal expression of the security operation workflow in the security orchestration system and is usually executed driven by the workflow engine in the orchestrator.

  Orchestrating a playbook is to build the manual security operation workflow and software into a machine playbook.
- Workflow

  A workflow is a collaborative work mode that integrates various capabilities related to security operation, such as tools, technologies, workflows, and personnel. A workflow is the response flow when a playbook is triggered.

  It combines API-enabled security capabilities, or applications, in SecMaster and manual checkpoints based on certain logical relationships to complete a specific security operations process and procedure.

11.2 Built-in Playbooks and Workflows

In security orchestration module, SecMaster provides built-in playbooks and workflows. You can use them without extra settings.

Built-in Playbooks

The following playbooks are enabled by default:

HSS alert status synchronization, automatic notification of high-risk vulnerabilities, historical handling information associated with host defense alarms, SecMaster and WAF address group association policy, historical handling information associated with application defense alarms, historical handling information associated with network defense alarms, automatic closure of repeated alarms, and alarm IP metric marking Asset protection status statistics notification, automatic alarm statistics notification, and automatic high-risk alarm notification

Table 11-1 Built-in playbooks

Security Layer	Playbook Name	Description	Data Class
Server security	HSS alert synchronization	Automatically synchronizes HSS alerts generated for servers.	Alert
	Automatic notification of high-risk vulnerabilities	Sends email or SMS notifications to specified recipients when vulnerabilities rated as high severity are discovered.	Vulnerability

Security Layer	Playbook Name	Description	Data Class
	Attack link analysis alert notification	Analyzes attack links. If HSS generates an alert for a server, the system checks the website running on the server. If the website information and alert exist, the system sends an alert notification.	Alert
	Server vulnerability notification	Checks servers with EIPs bound on the resource manager page and notifies of discovered vulnerabilities.	CommonContext
	HSS isolation and killing of malware	Automatically isolates and kills malware.	Alert
	Mining host isolation	Isolates the server for which an alert of mining program or software was generated. The playbook also adds the server into a security group that allows no inbound or outbound traffic.	Alert
	Ransomware host isolation	Isolates the server for which an alert of ransomware was generated. The playbook also adds the server into a security group that allows no inbound or outbound traffic.	Alert
	Host Defense Alarms Are Associated With Historical Handling Information	Associates new HSS alerts with HSS alerts handled earlier and adds historical handling details to the comment area for the corresponding HSS alerts.	Alert
Application security	SecMaster WAF Address Group Association Policy	Associates an address group specified by SecMaster with WAF blacklist (IP address group blacklist) rules for all enterprise projects to block IP addresses in the address group.	CommonContext
	WAF clear Non-domain Policy	Checks WAF protection policies at 09:00 every Monday and deletes policies with no rules included.	CommonContext
	Application Defense Alarms Are Associated With Historical Handling Information	Associates new WAF alerts with WAF alerts handled earlier and adds historical handling details to the comment area for the new alerts.	Alert

Security Layer	Playbook Name	Description	Data Class
O&M security	Real-time notification of critical Organization and Management operations	Sends real-time notifications for O&M alerts generated by models. Currently, SMN notifications can be sent for three key O&M operations: attaching NICs, creating VPC peering connections, and binding EIPs to resources.	Alert
Identity security	Identity Defense Alarms Are Associated With Historical Handling Information	Associates new IAM alerts with IAM alerts handled earlier and adds historical handling details to the comment area for the new alerts.	Alert
Network security	Network Defense Alarms Are Associated With Historical Handling Information	Associates new CFW alerts with CFW alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
Others/General	Automatic notification of high-risk alerts	Sends email or SMS notifications when there are alerts rated as High or Fatal.	Alert
	Alert metric extraction	Extracts IP addresses from alerts, checks the IP addresses against the intelligence system, sets alert indicators for confirmed malicious IP addresses, and associates the indicators with the source alerts.	Alert
	Automatic disabling of repeated alerts	Associates the alerts with the same names and close the duplicated ones generated within the past seven days.	Alert
	Automatic renaming of alert names	Generates custom alert names by combining specified key fields.	Alert
	Alert IP metric labeling	Adds attack source IP address and attacked IP address labels for alerts.	Alert
	IP intelligence association	Associates alerts with SecMaster intelligence first and ThreatBook intelligence.	Alert
	Asset Protection Status Statistics Notification	Collects statistics on asset protection status every week and sends notifications to customers by email or SMS.	CommonContext

Security Layer	Playbook Name	Description	Data Class
	Alert statistics Notify	Collects statistics on alerts that are not cleared at 19:00 every day and sends notifications to customers by email or SMS.	Alert
	Automatic security blocking of high-risk alerts	If a source IP address launched more than three attacks, triggered high-risk or critical alerts, and hit the malicious label in ThreatBook, this playbook triggers the corresponding security policies in WAF, VPC, CFW, or IAM to block the IP address.	Alert

Built-in Workflows

Table 11-2 Built-in workflows

Security Layer	Workflow Name	Description	Data Class
Server security	HSS alert synchronization	Automatically synchronizes HSS alerts generated for servers.	Alert
	Automatic notification of high-risk vulnerabilities	Sends email or SMS notifications to specified recipients when vulnerabilities rated as high severity are discovered.	Vulnerability
	Vulnerability handling	Invokes the HSS Interface for fixing vulnerabilities.	Vulnerability
	Policy management – Security group blocking	Adds the target IP address to all security groups.	Policy
	Policy management – Security group blocking cancellation	Removes the target IP address from all security groups.	Policy
	One-click host isolation	Isolates all ports on the target server.	Alert
	One-click host de-isolation	Releases the target servers from the isolation security group.	Alert

Security Layer	Workflow Name	Description	Data Class
	Attack link analysis alert notification	Analyzes attack link and generates alerts when attacks found on websites running on the affected servers.	Alert
	Server vulnerability notification	Checks servers with EIPs bound on the resource manager page and notifies of discovered vulnerabilities.	CommonContext
	HSS isolation and killing of malware	Automatically isolates and kills malware.	Alert
	Host Defense Alarms Are Associated With Historical Handling Information	Parent workflow. This workflow determines which type of child workflow needs to be invoked based on HSS alerts. The workflow also associates new alerts with historical alerts and adds handling details to the comment area. The following child workflows may be invoked: Host defense alarms are associated with historical handling information - Threat Modeling - Process, Host defense alarms are associated with historical handling information - Threat Modeling - Login, and Host defense alarms are associated with historical handling information - Automatic conversion to alerts.	Alert
	Host defense alarms are associated with historical handling information - Threat Modeling - Process	A child workflow. This workflow associates process alerts constructed in threat modeling with historical handling details and adds them to the comment area for the alerts.	Alert
	Host defense alarms are associated with historical handling information - Threat Modeling - Login	A child workflow. This workflow associates login alerts constructed in threat modeling with historical handling details and adds them to the comment area for the alerts.	Alert

Security Layer	Workflow Name	Description	Data Class
	Host Defense Alarms Are Associated With Historical Handling Information - Automatic conversion to alerts.	A child workflow. This workflow associates HSS alerts that are automatically converted to SecMaster alerts with historical handling details and add them to the comment area for such SecMaster alerts.	Alert
	Host isolation - Malware	If suspicious malware (such as ransomware and mining) was detected on a server, a manual review is triggered. The malware details (such as the type, affected server, process command, and file path) are displayed for operation personnel to review. If the malware is confirmed, affected servers will be isolated automatically.	Alert
Application security	One-click WAF blocking	Blocks target IP addresses in all policies in WAF in the current account.	Alert
	One-click WAF unblocking	Unblocks the target IP addresses from a specific policy group in the WAF in the current account.	Alert
	Policy management – WAF blocking	Adds target IP addresses to a WAF blacklist.	Policy
	Policy management – Cancel WAF blocking	Removes target IP addresses from a WAF blacklist.	Policy
	WAF address group policy	Applies WAF whitelist or blacklist rules to WAF address groups specified by SecMaster.	CommonContext
	Application Defense Alarms Are Associated With Historical Handling Information	Associates WAF alerts with alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
	WAF clear Non-domain Policy	Checks WAF protection policies at 09:00 every Monday and deletes policies with no rules included.	CommonContext

Security Layer	Workflow Name	Description	Data Class
Network security	One-click CFW blocking	Adds target IP addresses to a CFW blacklist.	Alert
	One-click CFW unblocking	Removes target IP addresses from a CFW blacklist.	Alert
	Policy management – CFW blocking	Adds target IP addresses to a CFW blacklist.	Policy
	Policy management – Cancel CFW blocking	Removes target IP addresses from a CFW blacklist.	Policy
	Network Defense Alarms Are Associated With Historical Handling Information	Associates CFW alerts with alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
Identity authentication	Identity Defense Alarms Are Associated With Historical Handling Information	Associates IAM alerts with alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
	Policy Management – IAM blocking (IAM interception for policy delivery)	Triggers emergency policies and changes the status of an IAM user to Disabled.	Policy
	Policy management – Cancel IAM blocking (Policy Delivery IAM Decapsulation)	Triggers emergency policies and changes the status of an IAM user to Enabled.	Policy
Others/General	Automatic notification of high-risk alerts	Sends email or SMS notifications when there are alerts rated as High or Fatal.	Alert
	Alert metric extraction	Extracts IP addresses from alerts, verifies them the IP addresses against Threat Book, sets the confirmed malicious IP addresses as threat indicators, and associates indicators with alerts.	Alert

Security Layer	Workflow Name	Description	Data Class
	Automatic disabling of repeated alerts	Associates the alerts with the same names and close the duplicated ones generated within the past seven days.	Alert
	Automatic renaming of alert names	Generates custom alert names by combining specified key fields.	Alert
	Adding IP address to alert	Adds attack source IP address and attacked IP address labels for alerts.	Alert
	One-click unblocking	Applies unblocking workflows based on alert data source products.	Alert
	One-click blocking	Applies blocking workflows based on alert data source products.	Alert
	IP intelligence association	Associates alerts with SecMaster intelligence first and ThreatBook intelligence.	Alert
	Asset Protection Status Statistics Notification	Collects statistics on asset protection status every week and sends notifications to customers by email or SMS.	CommonContext
	Alert statistics Notify	Collects statistics on alerts that are not cleared at 19:00 every day and sends notifications to customers by email or SMS.	Alert
	Automatic security blocking of high-risk alerts	If a source IP address launched more than three attacks, triggered high-risk or critical alerts, and hit the malicious label in ThreatBook, this playbook triggers the corresponding security policies in WAF, VPC, CFW, or IAM to block the IP address.	CommonContext
	Real-time Close Alert Automatically	Clears the current alert.	CommonContext
	Real-time notification of critical Organization and Management operations	Sends real-time notifications for O&M alerts generated by models. Currently, SMN notifications can be sent for three key O&M operations: attaching NICs, creating VPC peering connections, and binding EIPs to resources.	Alert

Security Layer	Workflow Name	Description	Data Class
	Querying historical alarms	Associates an alert with the child workflow that is used to handle similar alerts before. Queries comments for historical alerts for a specified period of time and returns de-duplicated comments.	CommonContext

11.3 Security Orchestration Process

This topic describes how Security Orchestration works.

Figure 11-1 Security Orchestration process

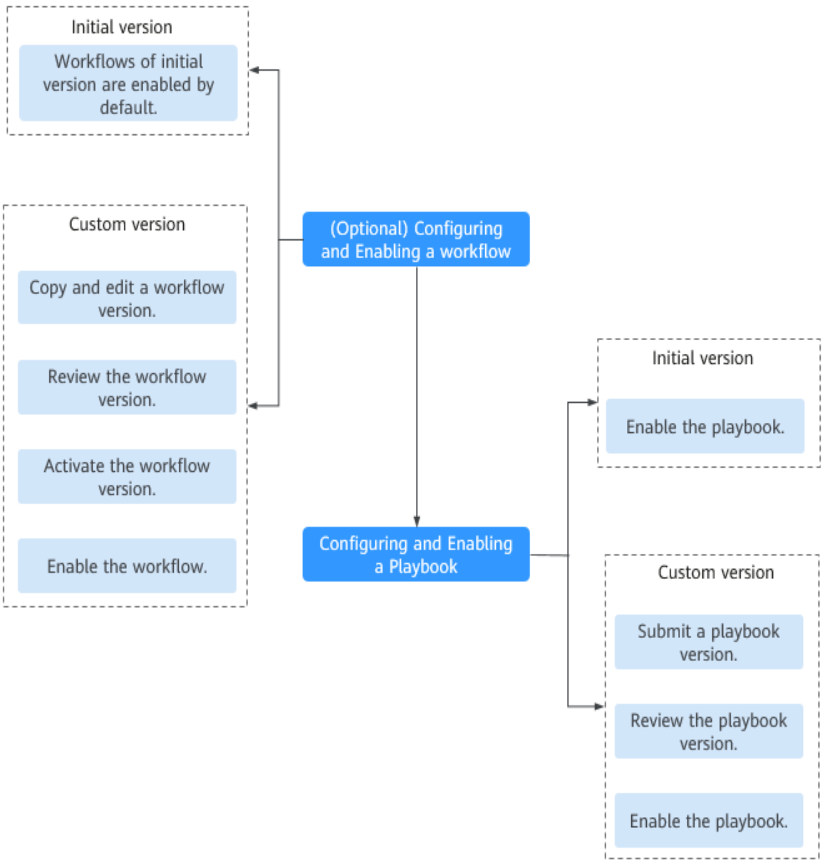


Table 11-3 Process

No.	Operation	Description
1	(Optional) **Configuring and Enabling a Workflow**	Enable the required workflows built in SecMaster. SecMaster provides some built-in workflows such as WAF uncapping, Synchronization of HSS alert status, and Fetching indicator from alert. Their initial version (V1) has been activated by default. If you need to edit a workflow, you can copy the initial version and edit it.
2	(Optional) **Configuring and Enabling a Playbook**	Enable the required playbooks built in SecMaster. By default, SecMaster provides playbooks such as **Fetching Indicator from alert**, **Synchronization of HSS alert status**, and **Automatic disabling of repeated alerts**. Most of playbooks are enabled by default. The following playbooks are enabled by default: HSS alert status synchronization, automatic notification of high-risk vulnerabilities, historical handling information associated with host defense alarms, SecMaster and WAF address group association policy, historical handling information associated with application defense alarms, historical handling information associated with network defense alarms, automatic closure of repeated alarms, and alarm IP metric marking Asset protection status statistics notification, automatic alarm statistics notification, and automatic high-risk alarm notification If you want to use a playbook that is not enabled, you can enable the initial version of the playbook (V1, activated by default), or modify the playbook and then enable it.

11.4 (Optional) Configuring and Enabling a Workflow

Scenario

SecMaster provides some built-in workflows such as WAF uncapping, Synchronization of HSS alert status, and Fetching indicator from alert. Their initial version (V1) has been activated by default.

You can customize and edit existing workflows. This topic describes how to configure and enable custom workflows.

Enabling a Workflow of a Custom Version

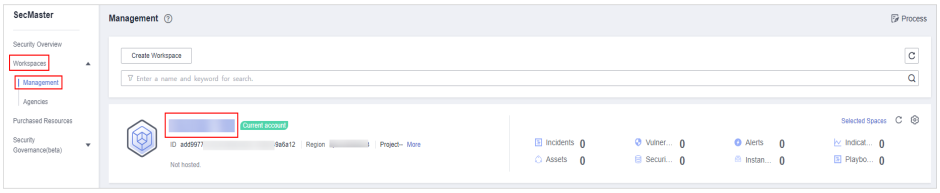
Accessing the workflow management page

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

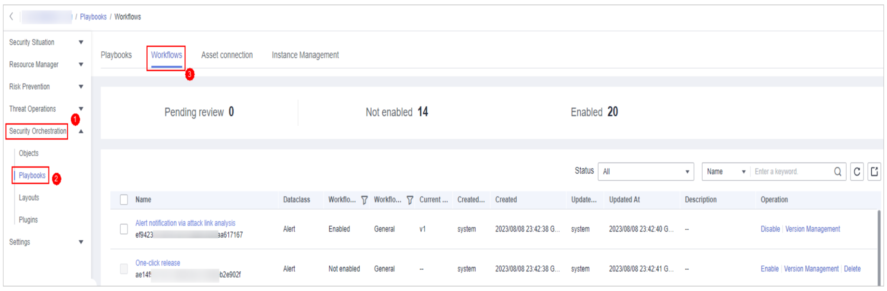
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-2 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

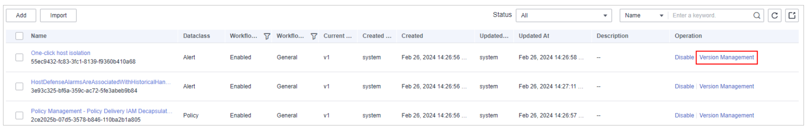
Figure 11-3 Workflows tab page



Copying a workflow version

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-4 Version Management page



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Copy** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.

Editing and submitting a workflow version

Step 8 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Edit** in the **Operation** column.

Step 9 On the workflow drawing page, drag basic, workflow, and plug-in nodes from **Resource Libraries** on the left to the canvas on the right for workflow design.

Table 11-4 Resource Libraries parameters

Parameter			Description
Basic	Basic Node	StartEvent	The start of a workflow. Each workflow can have only one start node. The entire workflow starts from the start node.
		EndEvent	The end of a workflow. Each workflow can have multiple end nodes, but the workflow must end with an end node.
		UserTask	When the workflow execution reaches this node, the workflow is suspended and a to-do task is generated on the **Task Center** page. After you complete the task, the subsequent nodes in the workflow continue to be executed. **Table 11-5** describes the UserTask parameters.
		SubProcess	Another workflow is started to perform cyclic operations. It is equivalent to the loop body in the workflow.
	System Gateway	ExclusiveGateway	During line distribution, one of the multiple lines is selected for execution based on the condition expression. During line aggregation, if one of the multiple lines arrives, the subsequent nodes continue to execute the task.
		ParallelGateway	During line distribution, all lines are executed. During line aggregation, the subsequent nodes are executed only when all the lines arrive. (If one line fails, the entire workflow fails.)
		InclusiveGateway	During line distribution, all expressions that meet the conditions are selected for execution based on the condition expression. During line aggregation, subsequent nodes are executed only when all lines executed during traffic distribution reach the inclusive gateway. (If one line fails, the entire workflow fails.)
Workflows			You can select all released workflows in the current workspace.
Plug-ins			You can select all plug-ins in the current workspace.

Table 11-5 UserTask parameters

Parameter	Description
Primary key ID	The system automatically generates a primary key ID, which can be changed as required.
Workspace Name	Name of the manual review node
Expired	Expiration time of a manual review node
Description	Description of the manual review node
View Parameters	Click . On the **Select Context** page that is displayed, select an existing parameter name. To add a parameter, click **Add Parameter**.
Manual Handling Parameters	Key of the input parameter To add a parameter, click **Add Parameter**.
Processed By	Set the reviewer of the workflow to the IAM user of the current account. If a workflow needs to be approved after the setting, only the owner can handle it on the **Task Center** page. Non-owners can only view the workflow. **NOTE** In first time use, you need to obtain authorization. Detailed operations are as follows: 1. Click **Authorize**. 2. On the **Access Authorization** slide-out panel displayed, select **Agree** and click **OK**.

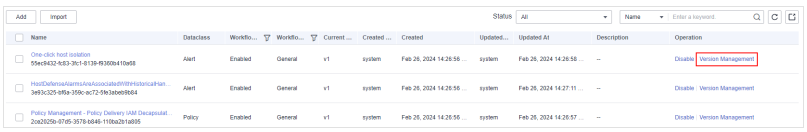
Step 10 After the design is complete, click **Save and Submit** in the upper right corner. In the automatic workflow verification dialog box displayed, click **OK**.

If the workflow verification fails, check the workflow based on the failure message.

Reviewing a workflow version

Step 11 After the workflow version is edited and submitted, the workflow management page is displayed. On the workflow management page, click **Version Management** in the **Operation** column of the target workflow.

Figure 11-5 Version Management page



Step 12 On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target workflow.

Step 13 In the displayed dialog box, set **Comment** to **Passed** and click **OK**.

Activating a workflow version

Step 14 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Activate** in the **Operation** column.

Step 15 In the displayed dialog box, click **OK**.

Enabling a workflow

Step 16 On the **Version Management** slide-out panel, click **Enable** in the **Operation** column of the target workflow.

Step 17 On the slide-out panel displayed, select the workflow version to be enabled and click **OK**.

----End

11.5 (Optional) Configuring and Enabling a Playbook

By default, SecMaster provides playbooks such as **Fetching Indicator from alert**, **Synchronization of HSS alert status**, and **Automatic disabling of repeated alerts**. Most of playbooks are enabled by default. The following playbooks are enabled by default:

HSS alert status synchronization, automatic notification of high-risk vulnerabilities, historical handling information associated with host defense alarms, SecMaster and WAF address group association policy, historical handling information associated with application defense alarms, historical handling information associated with network defense alarms, automatic closure of repeated alarms, and alarm IP metric marking Asset protection status statistics notification, automatic alarm statistics notification, and automatic high-risk alarm notification

If you want to use a playbook that is not enabled, you can enable the initial version of the playbook (V1, activated by default), or modify the playbook and then enable it.

This section describes how to configure and enable a playbook.

- **Enabling a Playbook of the Initial Version**
- **Enabling a Playbook of a Custom Version**

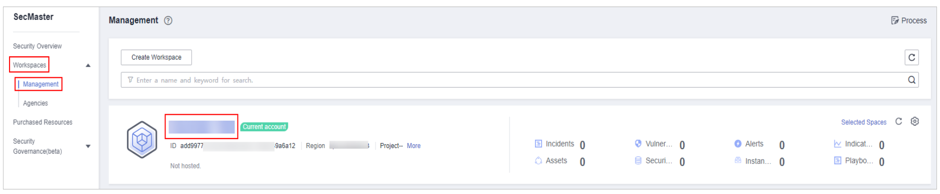
Enabling a Playbook of the Initial Version

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

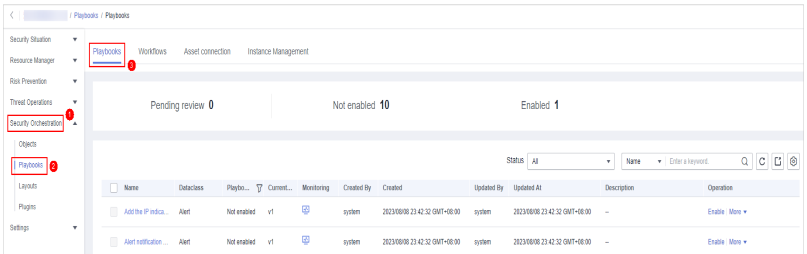
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-6 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-7 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Enable**.

Step 6 Select the playbook version to be enabled and click **OK**.

----End

Enabling a Playbook of a Custom Version

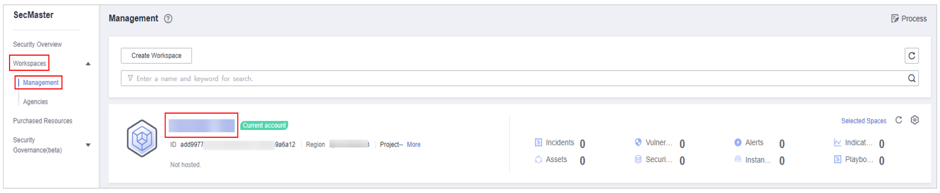
Accessing the Playbook Version Management Page

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

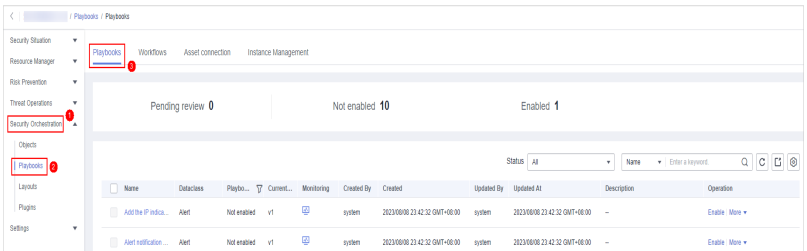
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-8 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

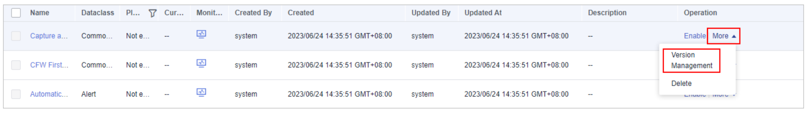
Figure 11-9 Accessing the Playbooks tab



Copying a Playbook Version

Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-10 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, in the **Version Information** area, locate the row containing the desired playbook version, and click **Clone** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.

Editing and Submitting a Playbook Version

Step 8 On the **Version Management** slide-out panel, in the **Version Information** area, locate the row containing the desired playbook version, and click **Edit** in the **Operation** column.

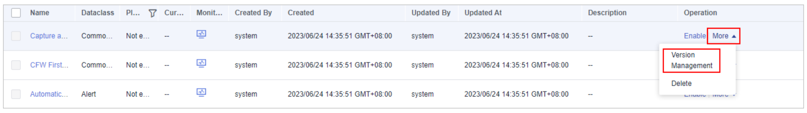
Step 9 On the page for editing a playbook version, edit the version information.

Step 10 Click **OK**.

Reviewing a Playbook Version

Step 11 After the playbook version is edited and submitted, the playbook management page is displayed. On the **Playbooks** page, click **Version Management** in the **Operation** column of the target playbook.

Figure 11-11 Version Management slide-out panel



Step 12 On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target playbook.

Step 13 In the displayed dialog box, set **Comment** to **Passed** and click **OK**.

Enabling a Playbook

Step 14 On the **Version Management** slide-out panel, click **Enable** in the **Operation** column of the target playbook.

Step 15 In the slide-out panel, select the playbook version you want to enable and click **OK**.

----End

11.6 Operation Object Management

11.6.1 Data Class

11.6.1.1 Viewing Data Classes

Scenario

The playbook and workflow running in security orchestration and response need to be bound to a data class. The playbook is triggered by a data object (instance of the data class).

This section describes how to view existing data classes.

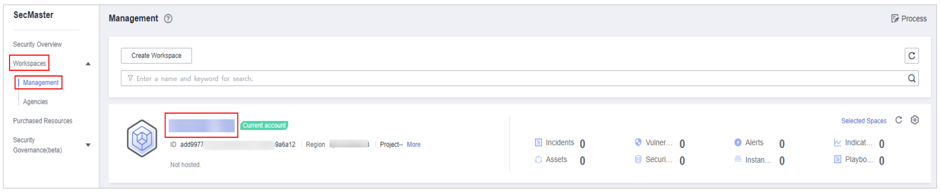
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

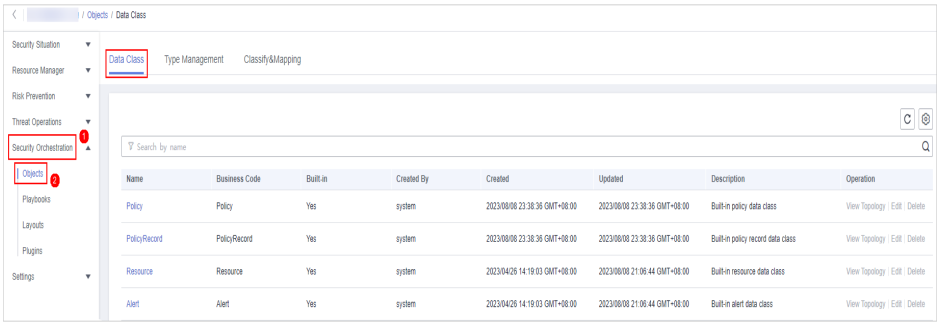
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-12 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. The **Data Class** tab page is displayed by default.

Figure 11-13 Accessing the Data Class tab



Step 5 In the data class list, view the existing data class information.

If there are many data classes, you can use a filter, such as data class name, code, built-in or not, or description, enter a keyword in the search box, and click to quickly search for a specified data class.

Table 11-6 Data Information

Parameter	Description
Name	Name of a data class.
Business Code	Business code of the data type.
Built-in	Indicates whether the data class is a built-in data class.
Created By	Creator information of the data class.
Created	Time when a dataset is created.
Updated	Time when a dataset is updated.
Description	Description of a data class
Operation	You can edit and delete data classes.

Step 6 To view details about a data class, click the name of the target data class. The details page of the target data class is displayed on the right.

----End

11.6.2 Type Management

11.6.2.1 Managing Alert Types

Scenario

This section describes how to manage alert types. The detailed operations are as follows:

- **Viewing Alert Types**: describes how to view existing alert types and their details.
- **Adding an Alert Type**: describes how to create custom alert types.
- **Associating an Alert Type with a Layout**: describes how to associate a custom alert type with an existing layout.
- **Editing an Alert Type**: describes how to edit a custom alert type.
- **Managing an Alert Type**: describes how to enable, disable, and delete a custom alert type.

Limitations and Constraints

- By default, built-in alert types are associated with existing layouts. You **cannot** customize associated layouts.
- Built-in alert types are enabled by default and **cannot** be edited, disabled, or deleted.
- After a customized alert type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

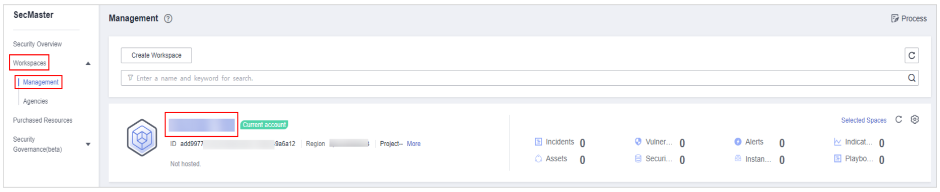
Viewing Alert Types

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

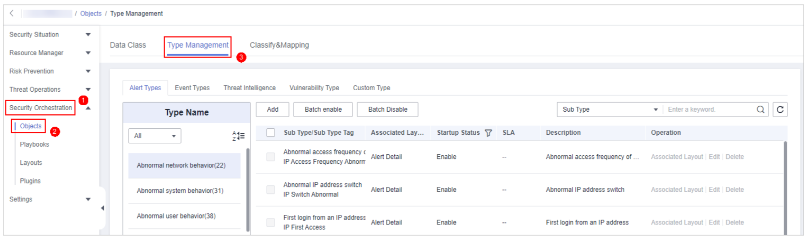
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-14 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-15 Type Management page



Step 5 On the **Type Management** page, click the **Alert Type** tab.

Step 6 On the **Alert Type** tab page, you can view all alert types in the **Type Name** area on the left.

To view details about subtypes of an alert type, click the target type name in **Type Name** on the left. Details about all subtypes are displayed on the right. For details about the parameters, see **Table 11-7**.

If there are many subtypes, you can select the **Sub Type** or **Associated Layout** and enter the corresponding keyword for search.

Table 11-7 Alert type parameters

Parameter	Description
Sub Type/Sub Type Tag	Name and ID of an alert subtype.
Associated Layout	Layout associated with the alert type.
Startup Status	Whether an alert type is enabled ● **Enabled**: The current type has been enabled. ● **Disabled**: The current type has been disabled.

Parameter	Description
SLA	SLA processing time of an alert type.
Description	Description of an alert type
Operation	You can edit and delete alert or incident types.

----End

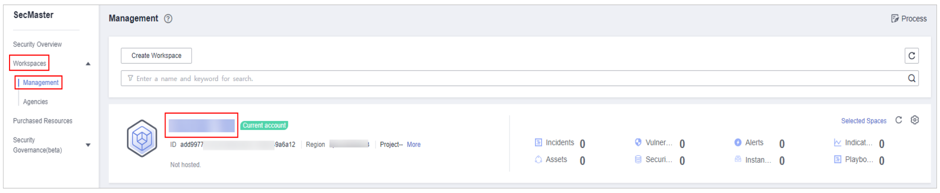
Adding an Alert Type

Step 1 Log in to the management console.

Step 2 Click ≡ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

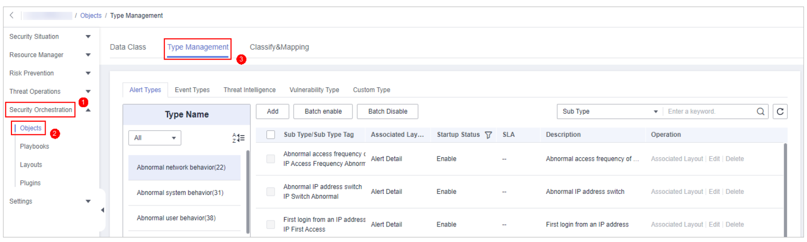
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-16 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-17 Type Management page



Step 5 On the **Type Management** page, click the **Alert Type** tab.

Step 6 On the **Alert Types** tab, click **Add**. On the **Add Alert Type** slide-out panel, set alert type parameters.

Table 11-8 Parameters for adding an alert type

Parameter	Description
Type Name	Customize the name of the new alert type.

Parameter	Description
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. • : indicates that the alert type is enabled. • : indicates that the type is disabled.
SLA	Set the SLA processing time of the alert.
Description	Description of a user-defined alert type

NOTE

After a customized alert type is added, the **Type Name**, **Type Tag**, and **Sub Type Tag** parameters cannot be modified.

Step 7 In the lower right corner of the page, click **OK**.

After the alert type is added, you can view the new alert type in **Type Name** area on the **Alert Types** tab.

----End

Associating an Alert Type with a Layout

NOTE

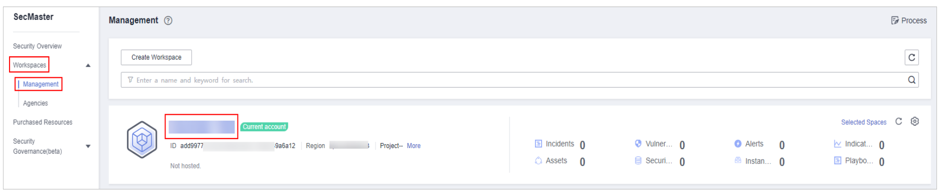
By default, built-in alert types are associated with existing layouts. You cannot customize associated layouts.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

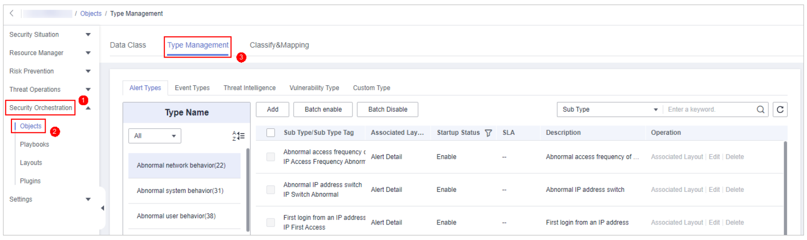
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-18 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-19 Type Management page



Step 5 On the **Type Management** page, click the **Alert Type** tab.

Step 6 On the type management page, select the type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type.

Step 7 In the **Associate Layout** dialog box, select the layout to be associated.

Step 8 Click **OK**.

----End

Editing an Alert Type

NOTE

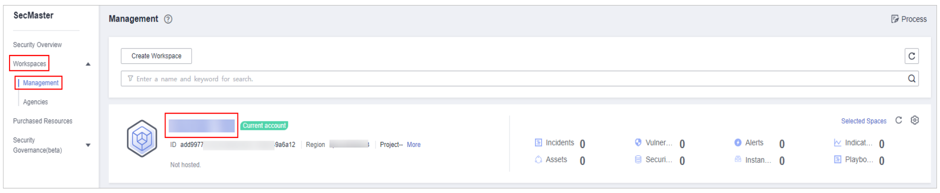
- Currently, the built-in alert type cannot be edited.
- After a customized alert type is added, the **Type Name**, **Type Tag**, and **Sub Type Tag** parameters cannot be modified.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

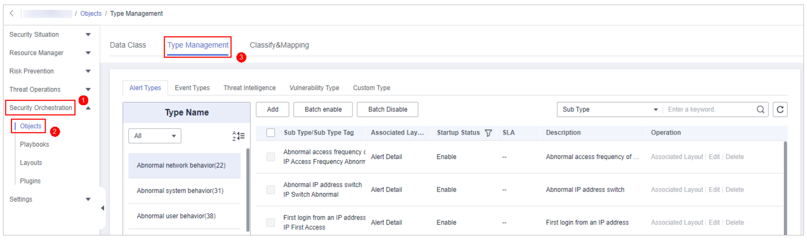
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-20 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-21 Type Management page



Step 5 On the **Type Management** page, click the **Alert Type** tab.

Step 6 In the **Type Name** area on the **Alert Types** tab, click the name of the custom alert type to be edited. Details about the custom alert type are displayed on the right.

Step 7 On the alert list page on the right, locate the row that contains the target type and click **Edit** in the **Operation** column.

Step 8 On the displayed page, modify the parameters of the alert type.

Table 11-9 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. • : indicates that the type is enabled. • : indicates that the type is disabled.
SLA	Set the SLA processing time of the alert.
Description	Description of a custom alert type

Step 9 In the lower right corner of the page, click **OK**.

----End

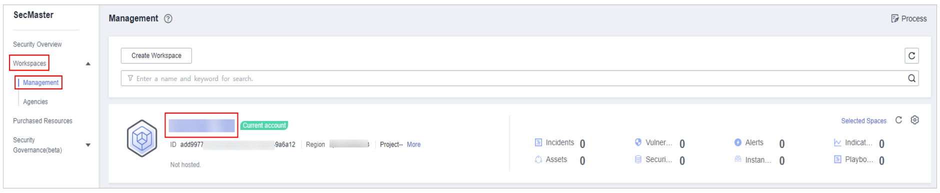
Managing an Alert Type

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

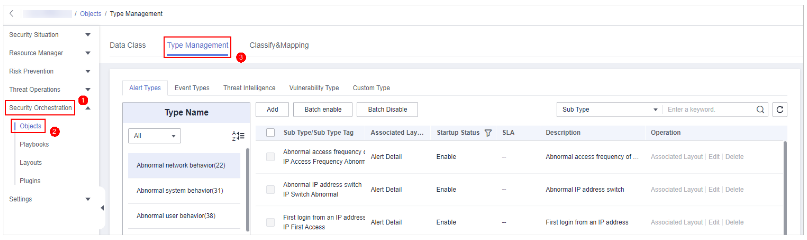
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-22 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-23 Type Management page



Step 5 On the **Type Management** page, click the **Alert Type** tab.

Step 6 On the **Alert Types** tab, manage alert types.

Table 11-10 Managing an alert type

Operation	Description
Enable **NOTE** The built-in alert types are enabled by default. You do not need to manually enable them.	1. On the **Alert Types** tab, select the types you want to enable and click **Batch enable**. Alternatively, locate the row containing the alert type you want to enable, click **Disable** in the **Status** column. 2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the status of the target type changes to **Enable**, the target type is enabled successfully.
Disable **NOTE** Currently, the built-in alert types cannot be disabled.	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.

Operation	Description
Delete **NOTE** Currently, built-in alert types cannot be deleted.	1. On the alert type management page, select the type to be deleted and click **Delete** in the **Operation** column. 2. In the displayed dialog box, click **OK**.

----End

11.6.2.2 Managing Incident Types

Scenario

This section describes how to manage incident types. The detailed operations are as follows:

- **Viewing Incident Types**: describes how to view existing incident types and their details.
- **Adding an Incident Type**: describes how to create custom incident types.
- **Associating an Incident Type with a Layout**: describes how to associate a custom incident type with an existing incident type.
- **Editing an Incident Type**: describes how to edit a custom incident type.
- **Managing Existing Incident Types**: describes how to enable, disable, and delete a custom incident type.

Limitations and Constraints

- By default, built-in incident types are associated with existing layouts. You **cannot** customize associated layouts.
- Built-in incident types are enabled by default and **cannot** be edited, enabled, disabled, or deleted.
- After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

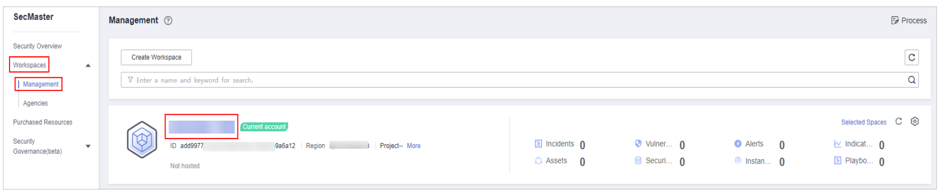
Viewing Incident Types

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

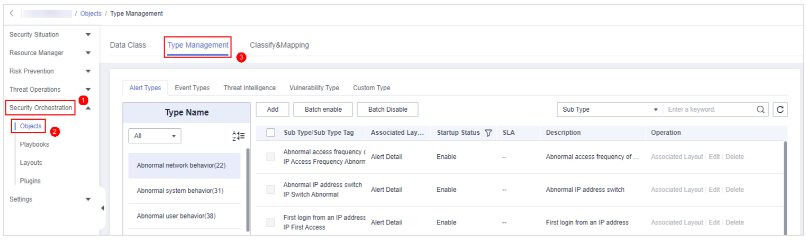
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-24 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-25 Type Management page



Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 On the **Event Types** tab, view the details about existing incident types. For details about the parameters, see **Table 11-11**.

Table 11-11 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

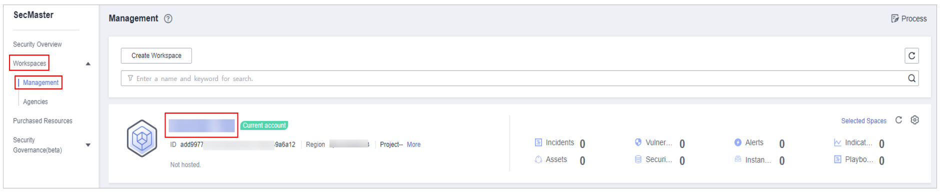
Adding an Incident Type

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

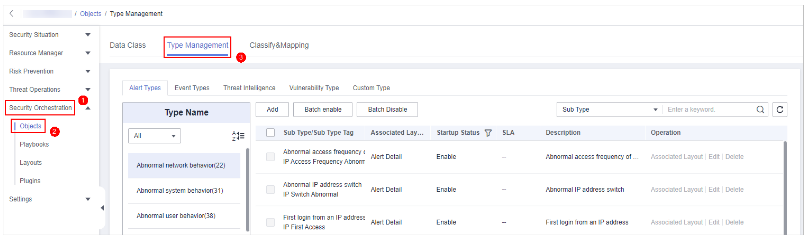
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-26 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-27 Type Management page



Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 On the **Event Types** tab, click **Add**. On the **Add Event Type** slide-out panel, set incident type parameters.

Table 11-12 Incident type parameters

Parameter	Description
Type Name	Customized name of an incident type. The name must comply with the upper camel case naming rules, for example, **TypeName**.
Type Tag	Enter the incident type ID. The keyword must comply with the upper camel case naming rules, for example, **TypeTag**.
Sub Type	Enter the subtype of the incident type. The name must comply with the upper camel case naming rules, for example, **SubType**.
Sub Type Tag	Enter the incident subtype ID. The keyword must comply with the upper camel case naming rules, for example, **SubTypeName**.
Startup Status	Indicates whether an incident type is enabled. • : indicates that the type is enabled. • : indicates that the alert type is disabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

NOTE

After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Step 7 In the lower right corner of the page, click **OK**.

After the incident type is added, you can view the new incident type in **Type Name** on the **Event Type** page.

----End

Associating an Incident Type with a Layout

NOTE

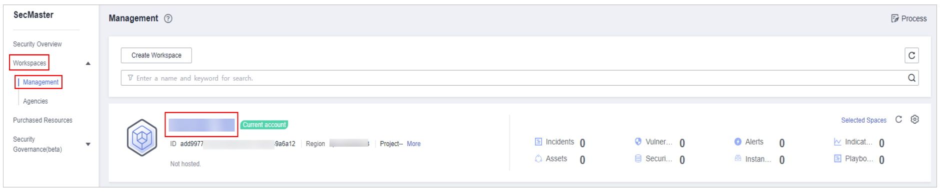
By default, built-in incident types are associated with existing layouts. You cannot customize associated layouts.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

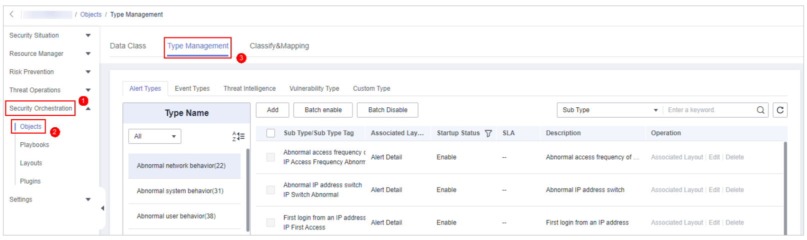
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-28 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-29 Type Management page



Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 On the **Event Type** page, select the incident type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type.

Step 7 In the **Associate Layout** dialog box, select the layout to be associated.

Step 8 Click **OK**.

----End

Editing an Incident Type

NOTE

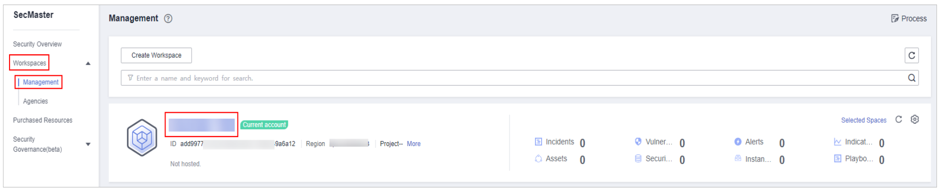
- Currently, the built-in incident type cannot be edited.
- After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

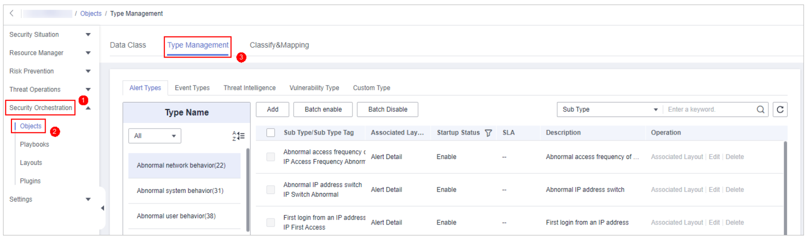
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-30 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-31 Type Management page



Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 In **Type Name** on the **Alarm Types** page, click the name of the customized incident type to be edited. Details about the custom incident type are displayed on the right.

Step 7 On the **Event Type** page, click **Edit** in the **Operation** column of the target type to be edited.

Step 8 In the **Edit Event Type** dialog box, edit parameters.

Table 11-13 Incident type parameters

Parameter	Description
Type Name	Name of an incident type, which **cannot** be modified.
Type Tag	Incident type ID, which **cannot** be modified.

Parameter	Description
Sub Type	Enter the subtype of the incident type.
Sub Type Tag	Incident subtype ID, which **cannot** be modified.
Startup Status	Indicates whether an incident type is enabled. ● : indicates that the type is enabled. ● : indicates that the alert type is disabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

Step 9 In the lower right corner of the page, click **OK**.

----End

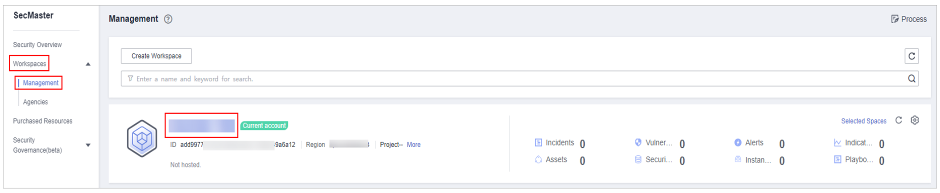
Managing Existing Incident Types

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

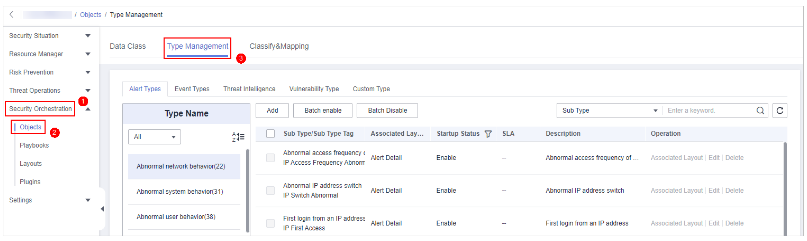
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-32 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-33 Type Management page



Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 On the incident type tab, manage incident types.

Table 11-14 Managing existing incident types

Operation	Description
Enable **NOTE** The built-in incident types are enabled by default. You do not need to manually enable them.	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 **NOTE** Currently, the built-in incident types cannot be disabled.	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 **NOTE** Currently, built-in incident types cannot be deleted.	1. On the incident type management page, select the type to be deleted and click **Delete** in the **Operation** column. 2. In the displayed dialog box, click **OK**.

----End

11.6.2.3 Viewing Threat Intelligence Types

Scenario

This section describes how to view threat intelligence types.

Limitations and Constraints

- By default, built-in intelligence types are associated with existing layouts. You **cannot** customize associated layouts.
- Built-in intelligence types are enabled by default and **cannot** be edited, enabled, disabled, or deleted.

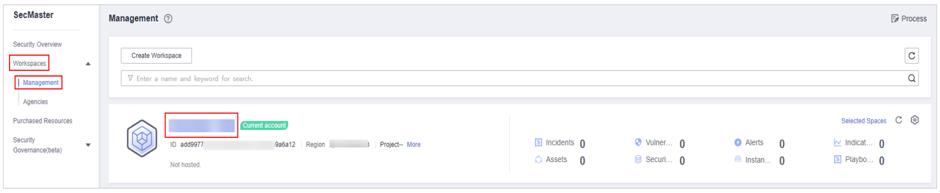
Viewing Threat Intelligence Types

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

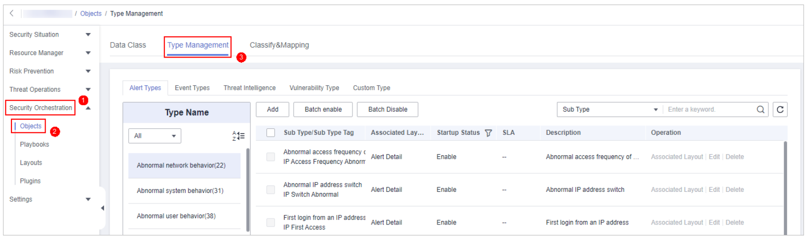
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-34 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-35 Type Management page



Step 5 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 6 On the **Threat Intelligence** page, view details. For details about the parameters, see **Table 11-15**.

Table 11-15 Threat intelligence type parameters

Parameter	Description
Type Name/Type Tag	Name and type tag of threat intelligence
Associated Layout	Layout associated with threat intelligence
Startup Status	Indicates the enabling status of a threat intelligence type: ● **Enabled**: The current type has been enabled. ● **Disabled**: The current type has been disabled.
Expired Time	Expiration time of threat intelligence.
Built-in	Indicates whether the threat intelligence is built in the system.
Description	Description of a threat intelligence
Operation	You can edit and delete the threat intelligence.

----End

11.6.2.4 Managing Vulnerability Types

Scenario

This section describes how to manage vulnerability types. The detailed operations are as follows:

- **Viewing Existing Vulnerability Types**: Describes how to view existing vulnerability types and their details.
- **Adding a Vulnerability Type**: describes how to create custom vulnerability types.
- **Associating a Vulnerability Type with a Layout**: describes how to associate a custom vulnerability type with an existing layout.
- **Editing a Vulnerability Type**: describes how to edit a custom vulnerability type.
- **Managing a Vulnerability Type**: describes how to enable, disable, and delete a custom vulnerability type.

Limitations and Constraints

- Currently, the built-in vulnerability types of the system do not support customized layouts.
- Built-in vulnerability types are enabled by default and **cannot** be edited, enabled, disabled, or deleted.
- After a user-defined vulnerability type is added, the type ID **cannot** be modified.

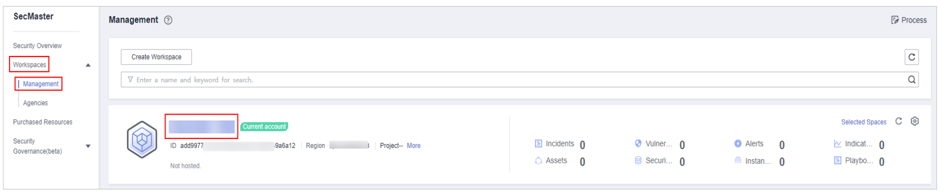
Viewing Existing Vulnerability Types

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

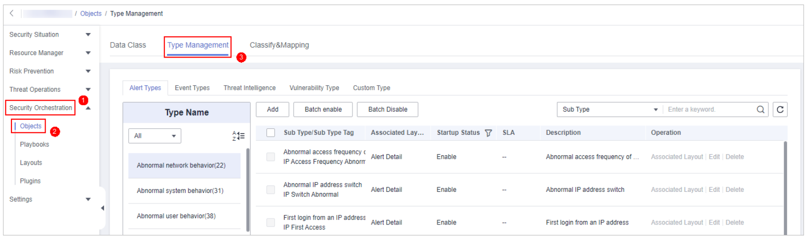
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-36 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-37 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** tab page, view details about existing vulnerability types. For details about the parameters, see **Table 11-16**.

Table 11-16 Vulnerability type parameters

Parameter	Description
Type Name/Type Tag	Name and tag of a vulnerability type
Associated Layout	Layout associated with the vulnerability type.
Startup Status	Indicates the enabling status of a vulnerability type: ● **Enabled**: The current type has been enabled. ● **Disabled**: The current type has been disabled.
Built-in	Indicates whether the vulnerability is a built-in vulnerability type.
Description	Description of a vulnerability type
Operation	You can edit and delete vulnerability types.

----End

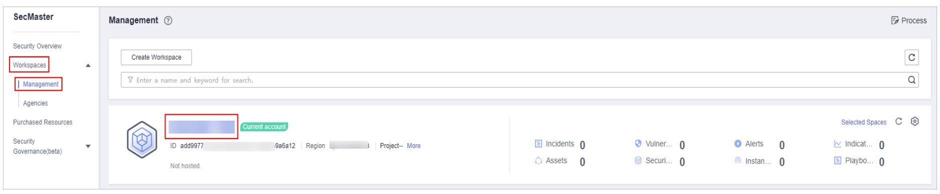
Adding a Vulnerability Type

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

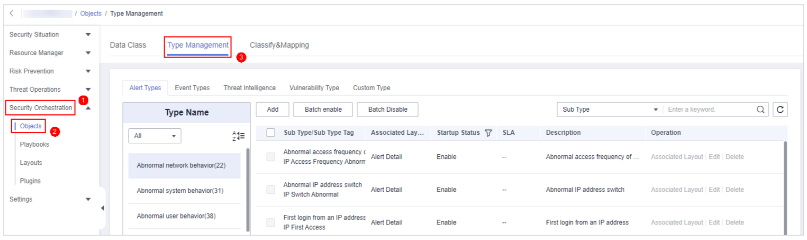
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-38 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-39 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** page, click **Add**. On the **Add Vulnerability Type** slide-out panel, set type parameters.

Table 11-17 Vulnerability type parameters

Parameter	Description
Type Name	Name of the vulnerability type to be added. The name must comply with the upper camel case naming rules, for example, **TypeName**.
Type Tag	Enter the vulnerability type ID. The keyword must comply with the upper camel case naming rules, for example, **TypeTag**.
Startup Status	Indicates the enabling status of the vulnerability type: • : indicates that the type is enabled. • : indicates that the type is disabled.
Description	Description of a user-defined vulnerability

NOTE

After a user-defined vulnerability type is added, the **Type ID** cannot be modified.

Step 7 In the lower right corner of the page, click **Confirm**.

After the threat intelligence type is added, you can view the new type in the table on the **Vulnerability Type** page.

----End

Associating a Vulnerability Type with a Layout

NOTE

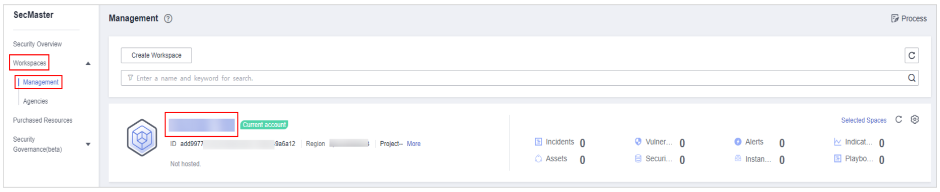
Currently, built-in vulnerability types do not support customized layouts.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

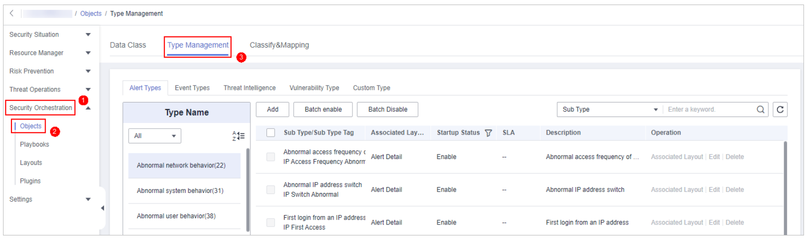
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-40 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-41 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** page, select the vulnerability type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type.

Step 7 In the **Binding/Changing Layouts** box, select the layout to be associated.

Step 8 Click **OK**.

----End

Editing a Vulnerability Type

NOTE

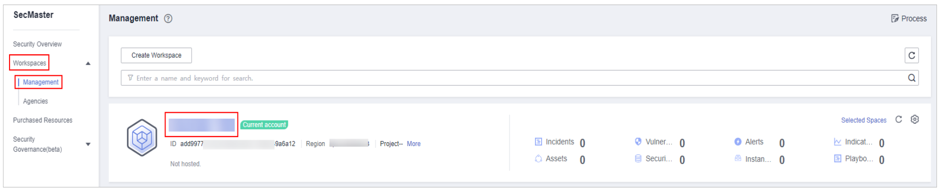
- Currently, the built-in vulnerability types cannot be edited.
- After a user-defined vulnerability type is added, the type ID cannot be modified.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

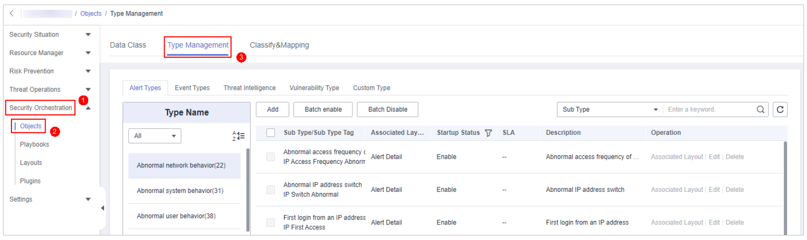
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-42 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-43 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** page, select the type to be edited and click **Edit** in the **Operation** column of the target type.

Step 7 On the displayed page, edit the parameter information of the corresponding type.

Table 11-18 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: • : indicates that the type is enabled. • : indicates that the type is disabled.
Description	Description of a user-defined vulnerability

Step 8 In the lower right corner of the page, click **OK**.

----End

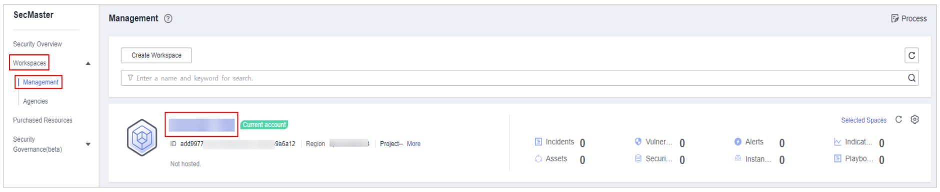
Managing a Vulnerability Type

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

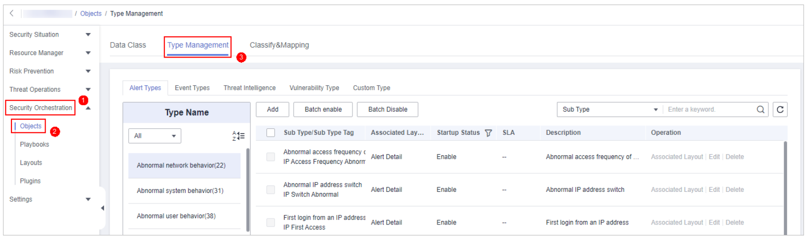
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-44 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-45 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the vulnerability type tab, manage vulnerability types.

Table 11-19 Managing a vulnerability type

Operation	Description
Enable **NOTE** Built-in vulnerability types are enabled by default. You do not need to manually enable them.	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 **NOTE** Currently, the built-in vulnerability types cannot be disabled.	1. On the **Vulnerability Type** page, select the type to be disabled and click **Batch Disable**. Alternatively, locate the row containing the vulnerability type to be disabled, click **Enable** in the **Status** column. 2. In the dialog box displayed, click **OK**. If the system displays a message indicating that the operation is successful and the **Status** of the target type changes to **Disable**, the target type is disabled successfully.

Operation	Description
Delete **NOTE** Currently, the built-in vulnerability types cannot be deleted.	1. On the **Vulnerability Type** tab, select the vulnerability type to be deleted and click **Delete** in the **Operation** column. 2. In the displayed dialog box, click **OK**.

----End

11.6.2.5 Viewing Custom Types

Scenario

This section describes how to view custom threat intelligence types.

Limitations and Constraints

Built-in types and sub-types cannot be associated with layouts, edited, deleted, enabled, or disabled.

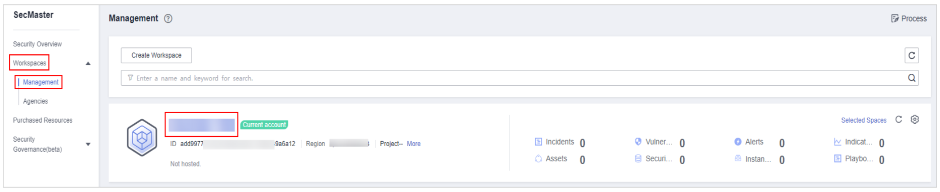
Viewing Custom Types or Subtypes

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

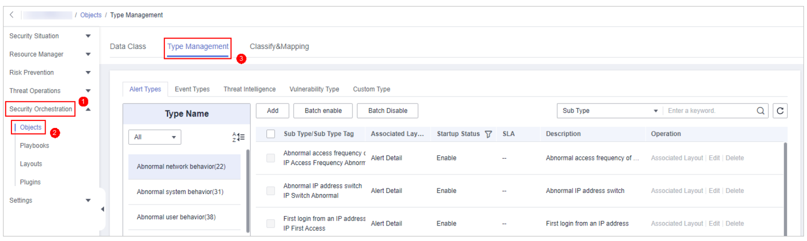
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-46 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-47 Type Management page



Step 5 On the **Type Management** page, click the **Custom Type** tab. On the displayed page, view details about existing custom types or subtypes.

- The type list is displayed on the left, showing the existing types.
- To view details about a type, click the type name in the type list. The type details are displayed on the right. The detailed information is as follows:
  - Basic information about the target type: name, creator, creation time, and associated layout.
  - Subtype list: information about existing subtypes, subtype names, and layouts associated with subtypes.

----End

11.6.3 Classification & Mapping

11.6.3.1 Viewing Categorical Mappings

Scenario

Categorical mappings are used to match alert types and map alert fields for aloud service alerts.

This section describes how to view categorical mappings.

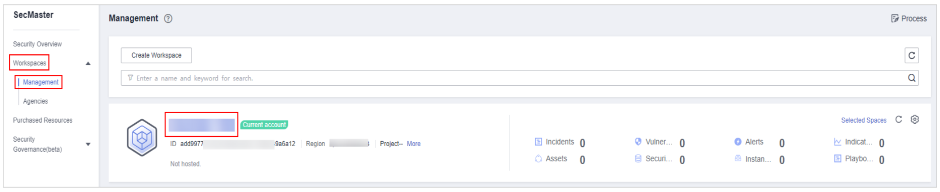
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

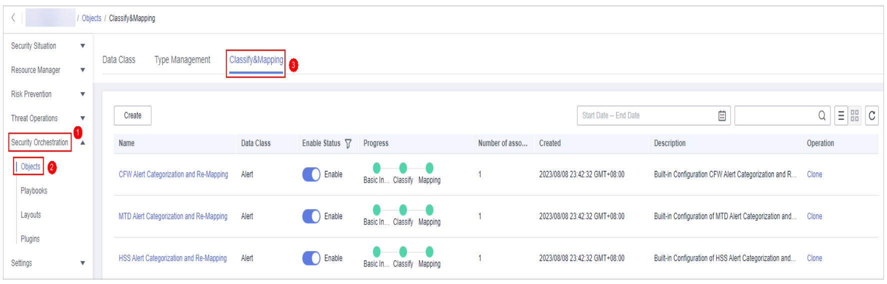
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-48 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-49 Classify&Mapping tab page



Step 5 On the **Classify&Mapping** tab, view details about the created categorical mappings.

Table 11-20 Categorical mappings

Parameter	Description
Name	Name of a categorical mapping.
Data Class	Type of the data class to which the categorical mapping belongs.
Enable Status	Status of a categorical mapping. ● Enable: The current categorical mapping is enabled. ● Disable: The current categorical mapping has been disabled.
Progress	The progress of creating the categorical mapping.
Associated instances	Total number of plug-in instances associated with the categorical mapping.
Created	Time the categorical mapping was created.
Description	Description of the categorical mapping.

Step 6 To view details about a categorical mapping, click the name of the target categorical mapping. The categorical mapping details page is displayed.

----End

11.6.3.2 Creating, Copying, and Editing a Categorical Mapping

Scenario

Classification and mapping are to perform class matching and field mapping for cloud service alerts.

This section walks you through on how to create, edit, and copy a classification and mapping.

Limitations and Constraints

- In a single workspace of a single account, a maximum of 50 classification & mapping templates can be created.
- In a single workspace of a single account, the proportion of a classification to its mappings is 1:100.
- A maximum of 100 classifications and mappings can be added to a workspace of a single account.

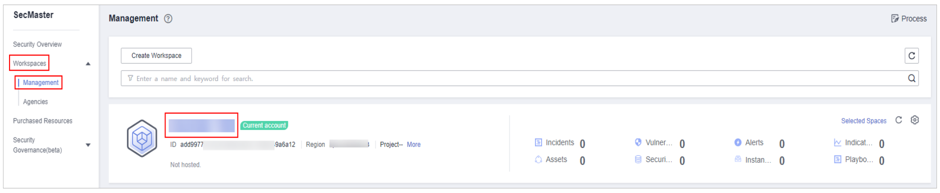
Creating a Categorical Mapping

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

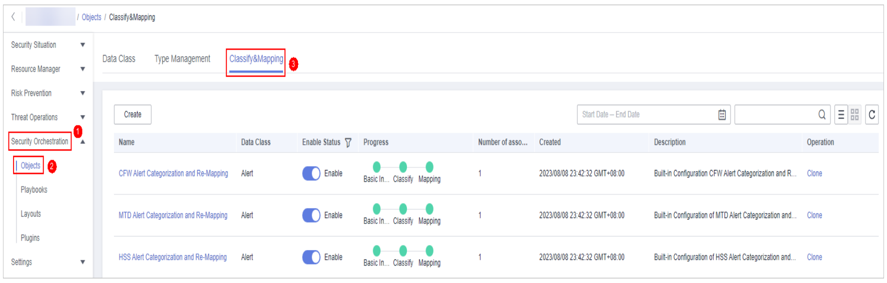
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-50 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

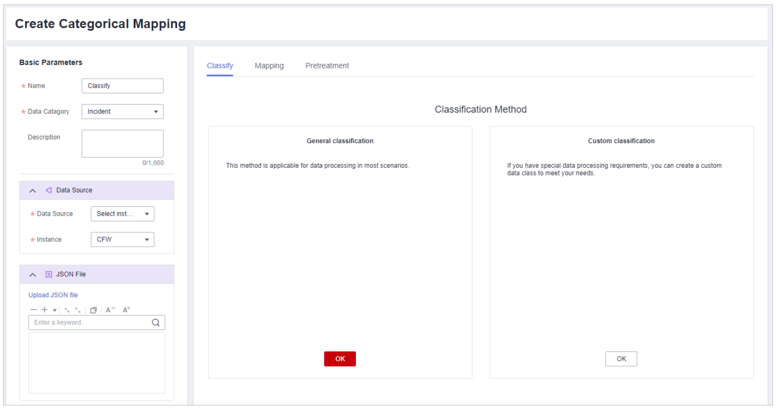
Figure 11-51 Classify&Mapping tab page



Step 5 On the **Classify&Mapping** page, click **Create**.

Step 6 On the **Create Categorical Mapping** page, set categorical mapping parameters.

Figure 11-52 Create Categorical Mapping page



1. In the **Basic Parameters** area on the left, configure basic information about the categorical mapping. For details about the parameters, see **Table 11-21**.

Table 11-21 Configuring basic information

Parameter	Description
Name	Name of a user-defined categorical mapping.
Data Category	Select the corresponding data type.
Description	Description of the custom categorical mapping.

2. In the **Data Source** area on the left, select the data source for categorical mapping.

   When **Data Source** is set to **Upload JSON file**, you need to click **to upload the JSON file** and upload the JSON file.
3. On the **Classify** tab page on the right, select a classification mode and set related parameters.
4. After the classification configuration is complete, click at the upper right corner of the page to save the configuration.
5. On the **Mapping** tab page in the right pane, select a mapping mode and set related parameters.
6. After categorical mapping is complete, click at the upper right corner of the page to save the configuration.
7. On the **Preprocessing** tab page on the right, set preprocessing mapping parameters.
8. Click at the upper right corner of the page to save the configuration.

----End

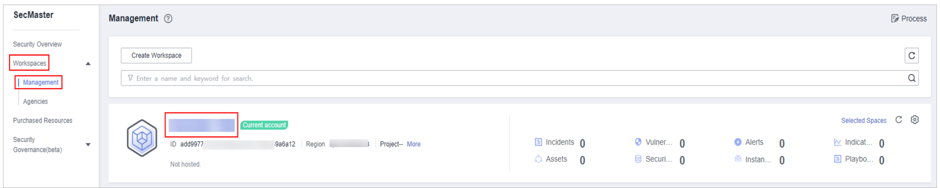
Copying a Categorical Mapping

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

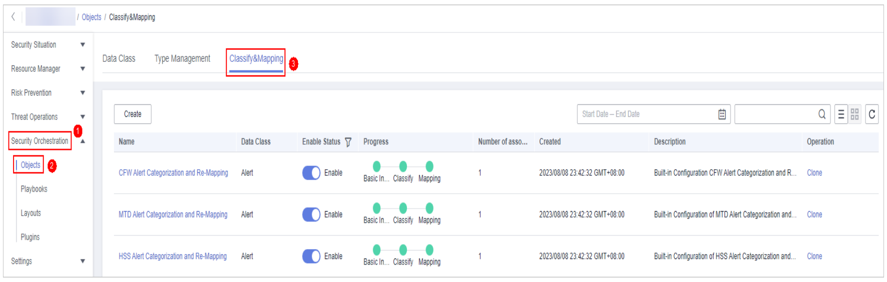
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-53 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-54 Classify&Mapping tab page



Step 5 On the **Classify&Mapping** page, click **Clone** in the **Operation** column of the target categorical mapping.

Step 6 In the displayed dialog box, enter the name for replicated mapping and click **OK**.

----End

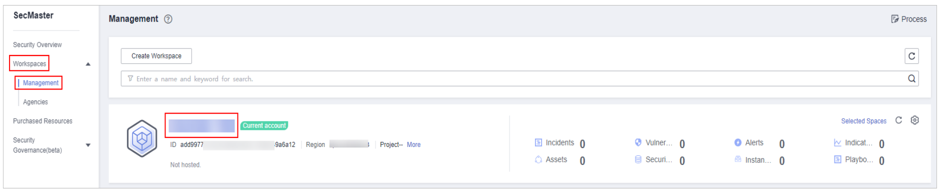
Editing a Categorical Mapping

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

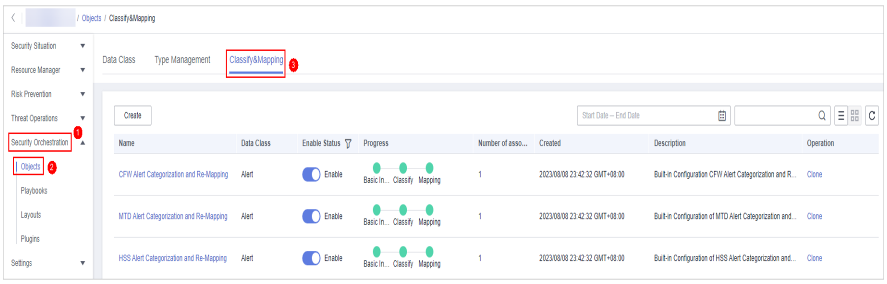
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-55 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-56 Classify&Mapping tab page



Step 5 On the **Classify&Mapping** page, click the target categorical mapping name to go to the edit page.

Step 6 On the **Edit Categorical Mapping** page, set parameters.

1. In the **Basic Parameters** area on the left, configure basic information about the categorical mapping. For details about the parameters, see **Table 11-21**.

Table 11-22 Configuring basic information

Parameter	Description
Name	Name of a user-defined categorical mapping.
Data Category	This field cannot be edited.
Description	Description of the custom categorical mapping.

2. In the **Data Source** area on the left, select the data source for the categorical mapping.

   If **Data Source** is set to **Upload JSON file**, you need to click **Upload JSON file** and upload the JSON file.
3. On the **Classify** tab on the right, select a classification mode and set related parameters.
4. After the classification configuration is complete, click at the upper right corner of the page to save the configuration.
5. On the **Mapping** tab on the right, select a mapping mode and set related parameters.
6. After the categorical mapping is complete, click at the upper right corner of the page to save the configuration.
7. On the **Preprocessing** tab on the right, set preprocessing mapping parameters.
8. Click at the upper right corner of the page to save the configuration.

----End

11.6.3.3 Managing Categorical Mappings

Scenario

This topic describes how to manage categorical mappings, such as enabling, disabling, and deleting a categorical mapping.

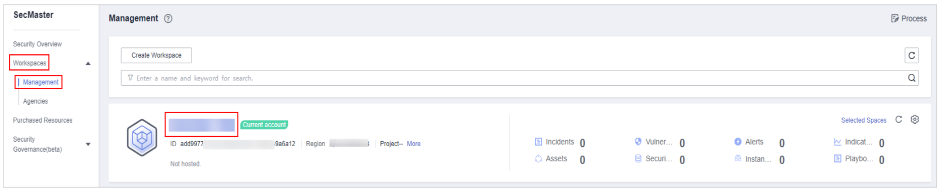
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

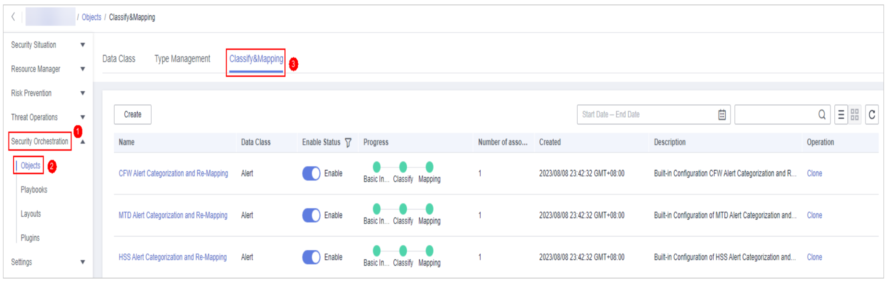
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-57 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-58 Classify&Mapping tab page



Step 5 On the **Classify&Mapping** tab, manage categorical mappings.

Table 11-23 Managing categorical mappings

Operation	Description
Enable **NOTE** Custom categorical mappings cannot be enabled.	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 **NOTE** Custom categorical mappings cannot be disabled.	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 **NOTE** Currently, the built-in categorical mappings cannot be deleted.	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 it will be stopped immediately. – Deleted categorical mappings cannot be restored. Exercise caution when performing this operation.

----End

11.7 Playbook Orchestration Management

11.7.1 Playbooks

11.7.1.1 Submitting a Playbook Version

Scenario

This section describes how to submit a playbook version for review.

Prerequisites

The workflow bound to the playbook has been enabled by referring to **Enabling a Workflow**.

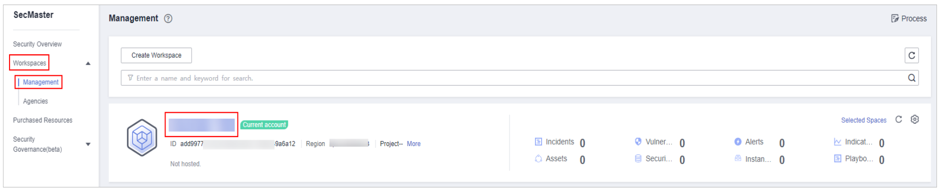
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

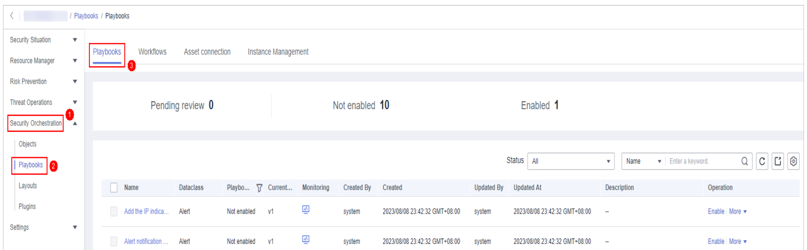
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-59 Workspace management page



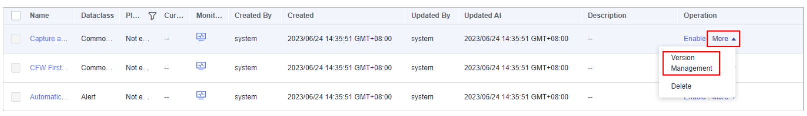
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-60 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-61 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Submit** in the **Operation** column.

Step 7 In the confirmation dialog box, click **OK** to submit the playbook version.

NOTE

- After the playbook version is submitted, **Version Status** changes to **To be reviewed**.
- After a playbook version is submitted, it cannot be edited. If you need to edit it, you can create a version or reject it during review.

----End

Follow-up Operations

A submitted playbook version needs to be reviewed. For details, see **Reviewing a Playbook Version**.

11.7.1.2 Reviewing a Playbook Version

Scenario

This section describes how to review a playbook version.

Prerequisites

The playbook has been submitted by referring to **Submitting a Playbook Version**.

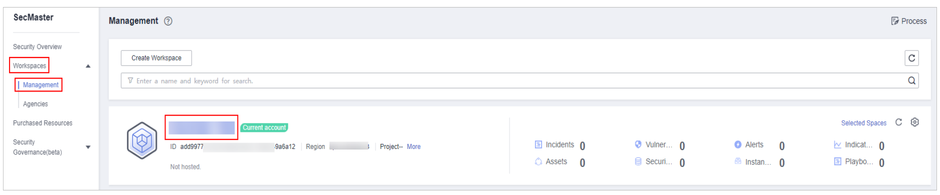
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

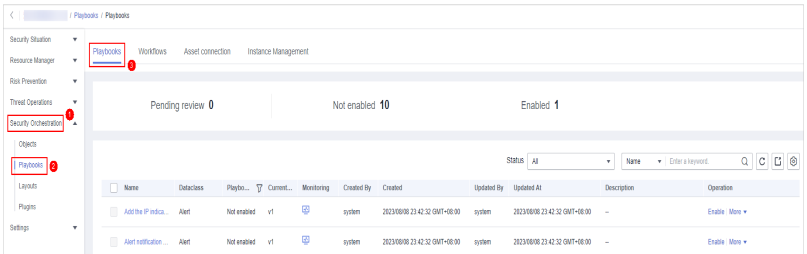
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-62 Workspace management page



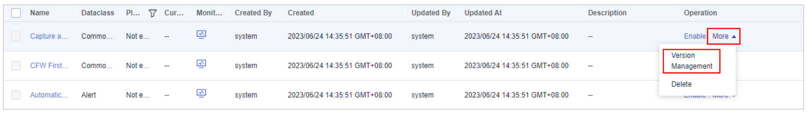
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-63 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-64 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, click **Review**.

Step 7 On the **Review Playbook Version** page, enter the review information. **Table 11-24** describes the parameters for reviewing a playbook version.

Table 11-24 Parameters for reviewing a playbook version

Parameter	Description
Comments	Select the review conclusion. ● If the playbook version is approved, the playbook version status changes to **Activated**. ● Reject. After the playbook version is rejected, the status of the playbook version changes to **Rejected**. You can edit the playbook version and submit it again.
Reason for rejection	This parameter is mandatory when the review comment is Reject. Enter the review comment. This parameter is mandatory when Reject is selected for Review Comment.

NOTE

If the current playbook has only one version, the version is in the activated state by default after being approved.

Step 8 Click **OK** to complete the playbook version review.

----End

Follow-up Operations

An approved playbook version needs to be enabled. For details, see **Enabling a Playbook**.

11.7.1.3 Enabling a Playbook

Scenario

After a playbook version is approved, you can enable the playbook. This section describes how to enable a playbook.

Prerequisites

The playbook version has been activated by referring to **Activating/Deactivating a Playbook Version**.

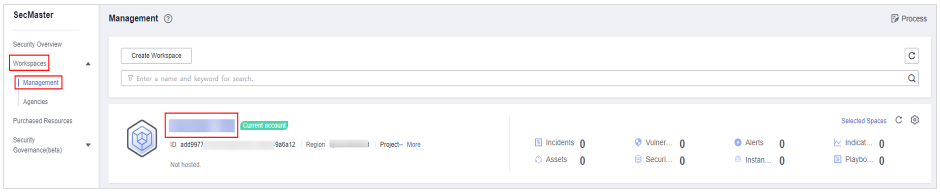
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

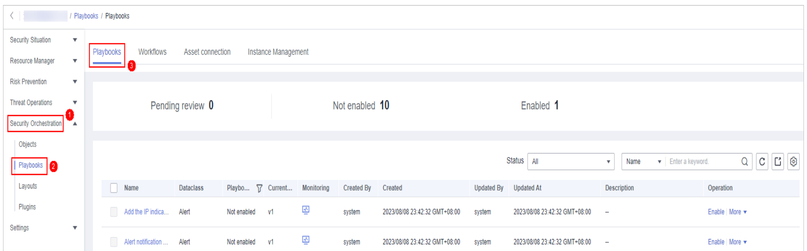
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-65 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-66 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Enable**.

Step 6 After selecting the playbook version to be enabled, click **OK**.

----End

11.7.1.4 Managing Playbooks

Scenario

This section describes how to manage playbooks, including **Viewing Existing Playbooks**, **Exporting Playbooks**, **Disabling a Playbook**, and **Deleting a Playbook**.

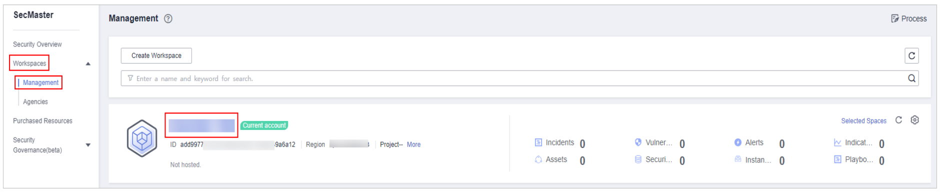
Viewing Existing Playbooks

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

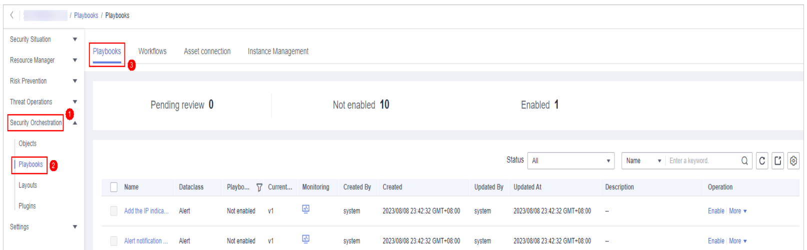
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-67 Workspace management page



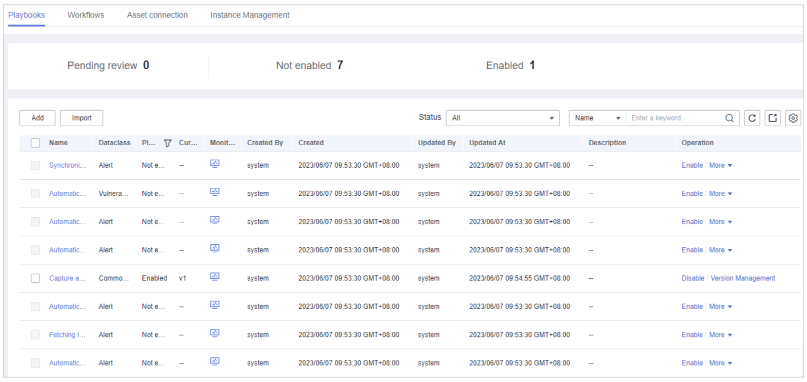
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-68 Accessing the Playbooks tab



Step 5 On the **Playbooks** tab page, view playbook information.

Figure 11-69 Viewing playbook information



- The numbers of **Pending review**, **Not enabled**, and **Enabled** playbooks are displayed above the playbook list.
- View the information about existing playbooks.

  When there are a large number of playbooks, you can use the search function to quickly search for a specified playbook with search filters such as the status, name, description, or data class of the playbook. Enter a keyword in the search box, and click .

Table 11-25 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

Step 6 To view details about a playbook, click the name of the playbook.

----End

Exporting Playbooks

NOTE

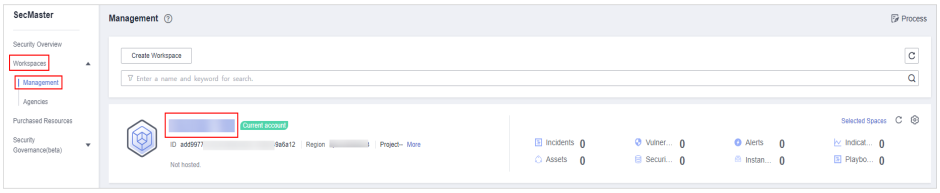
SecMaster supports the export of playbooks whose **Status** is **Enabled**.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

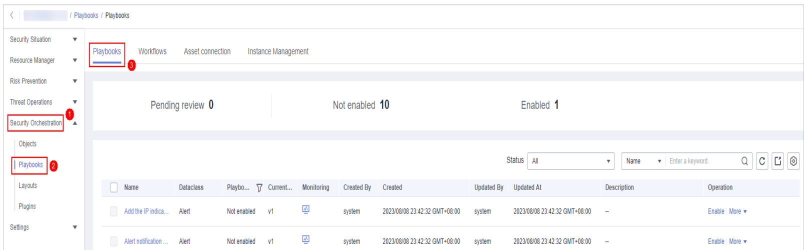
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-70 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-71 Accessing the Playbooks tab



Step 5 Select the playbooks to be exported and click in the upper right corner of the list. The dialog box for confirming the export is displayed.

Step 6 In the dialog box that is displayed, click **OK** to export the playbooks to the local host.

----End

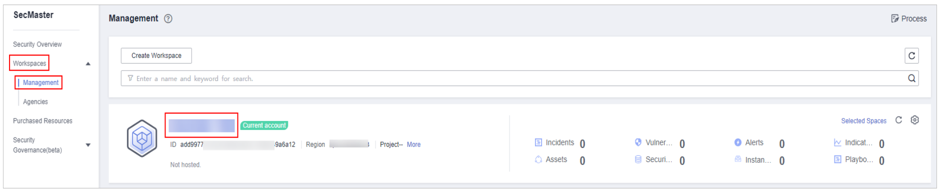
Disabling a Playbook

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

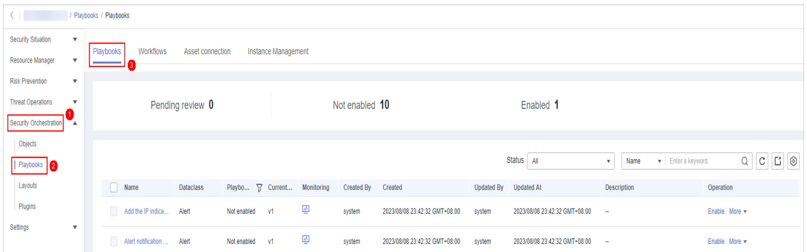
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-72 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-73 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Disable**. A confirmation dialog box is displayed.

Step 6 In the displayed dialog box, click **OK**.

----End

Deleting a Playbook

NOTE

To delete a playbook, the following conditions must be met:

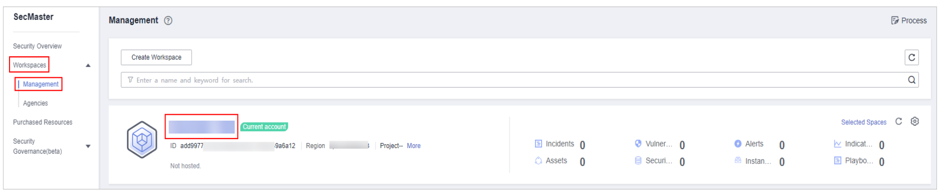
- The playbook is not enabled.
- No activated playbook version exists in the current playbook.
- No running playbook instance exists.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

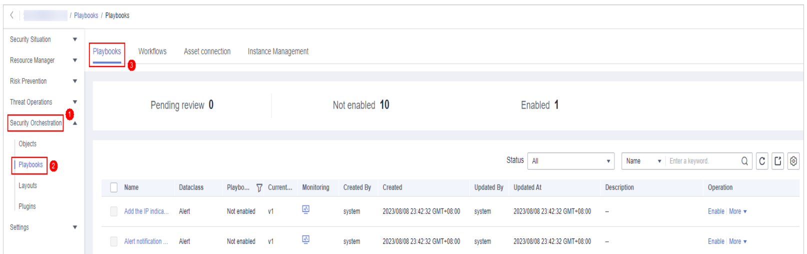
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-74 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-75 Accessing the Playbooks tab



Step 5 In the **Operation** column of the playbook to be deleted, click **Delete**.

Step 6 In the dialog box that is displayed, click **Confirm** to delete the playbook.

NOTE

By default, all playbook versions in the current playbook are deleted. The deletion operation cannot be undone. Exercise caution when performing this operation.

----End

11.7.1.5 Managing Playbook Versions

Scenario

This section describes how to manage playbook versions, including **Previewing Playbook Versions**, **Editing a Playbook Version**, **Activating/Deactivating a Playbook Version**, **Copying a Playbook Version**, and **Deleting a Playbook Version**.

Previewing Playbook Versions

NOTE

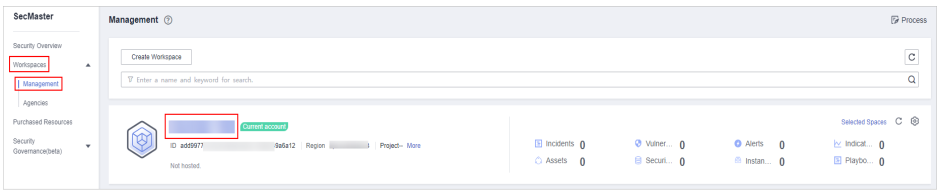
The draft version cannot be previewed.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

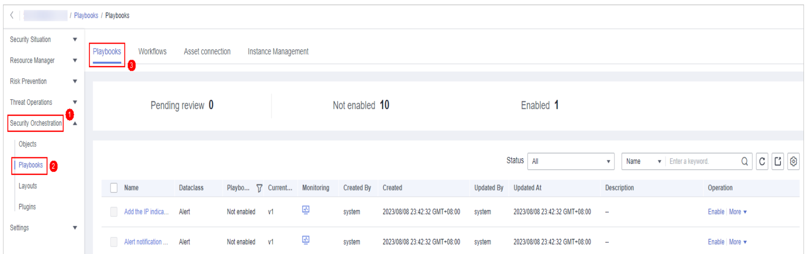
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-76 Workspace management page



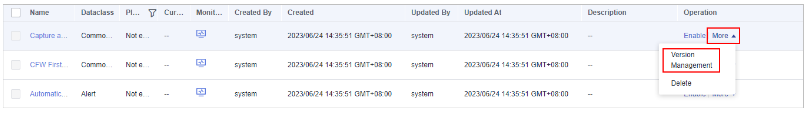
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-77 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-78 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Preview** in the **Operation** column.

Step 7 On the playbook version preview page, you can view the details about the target playbook version, including **Basic Information**, **Version Information**, and **Matching Workflow**.

----End

Editing a Playbook Version

NOTE

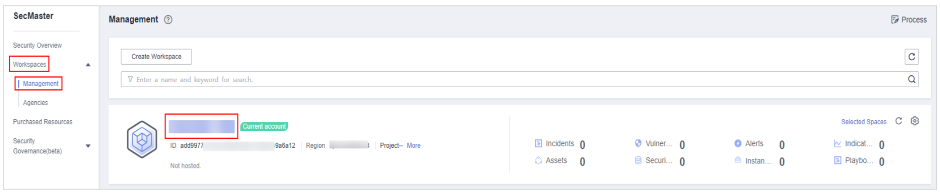
Only playbook versions whose version status is **Unsubmitted** can be edited.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

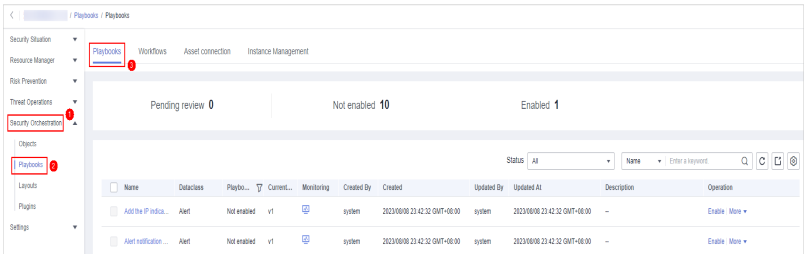
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-79 Workspace management page



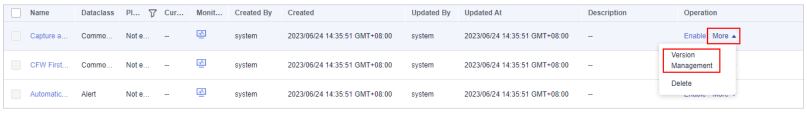
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-80 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-81 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Edit** in the **Operation** column.

Step 7 On the page for editing a playbook version, edit the version information.

Step 8 Click **OK**.

----End

Activating/Deactivating a Playbook Version

NOTE

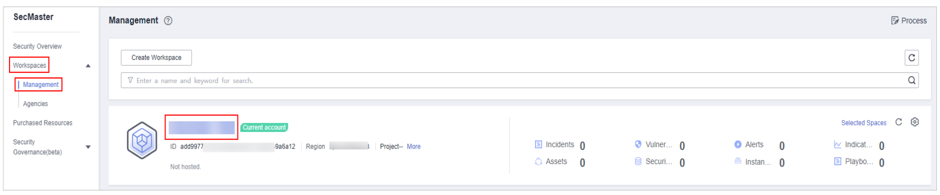
- Only the playbook version that is not activated can be activated.
- Only one activated version is allowed for each playbook.
- After the current version is activated, the previously activated version is deactivated. For example, if the V2 version is activated this time, the V1 version in the activated state is deactivated and changes to the deactivated state.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

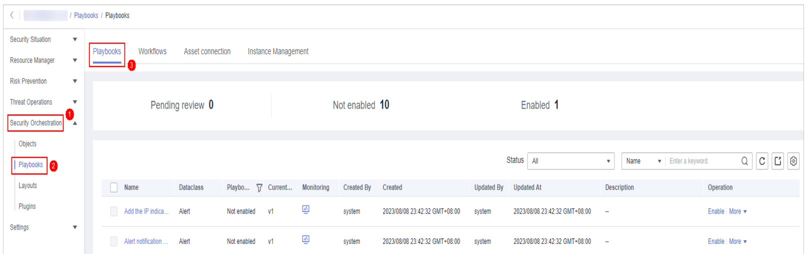
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-82 Workspace management page



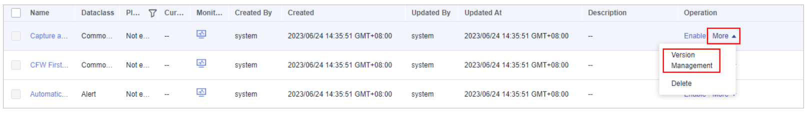
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-83 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-84 Version Management slide-out panel



Step 6 On the **Version Management** page, in the version information area, locate the row containing the desired playbook version, and click **Activate** or **Deactivate** in the **Operation** column.

----End

Copying a Playbook Version

NOTE

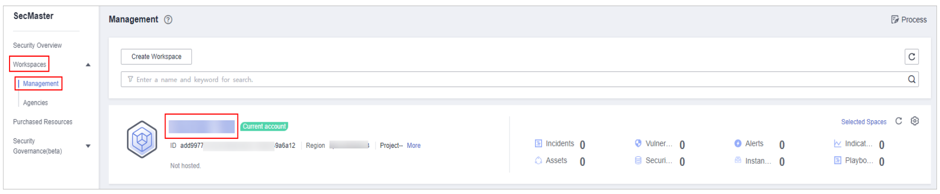
Only playbook versions in the **Activated** or **Inactive** state can be copied.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

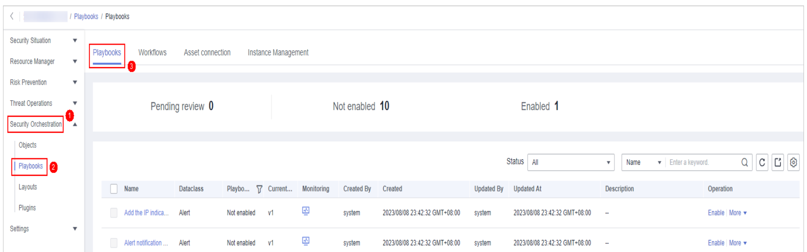
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-85 Workspace management page



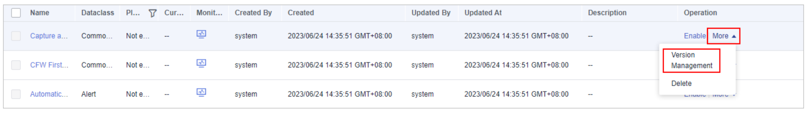
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-86 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-87 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Copy** in the **Operation** column.

Step 7 In the dialog box that is displayed, click **OK**.

----End

Deleting a Playbook Version

NOTE

To delete a playbook version, the following conditions must be met:

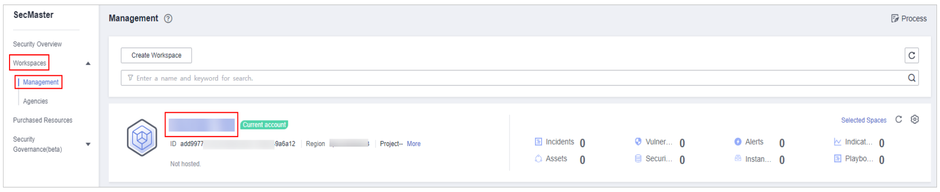
- The playbook version is inactivated.
- No running playbook version instance exists.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

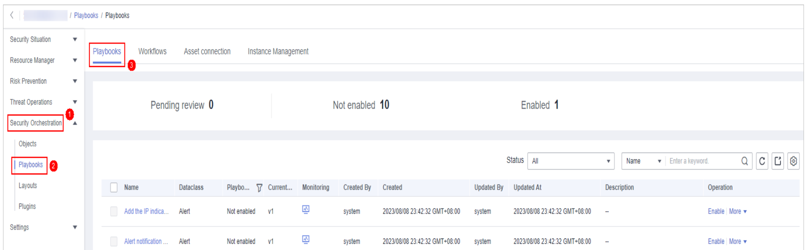
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-88 Workspace management page



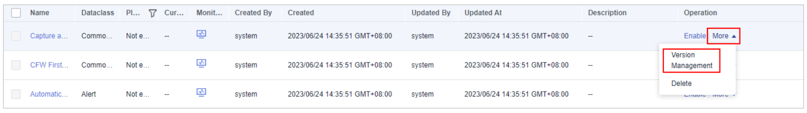
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 11-89 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Figure 11-90 Version Management slide-out panel



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Delete** in the **Operation** column.

NOTE

After a playbook version is deleted, it cannot be retrieved. Exercise caution when performing this operation.

----End

11.7.2 Workflows

11.7.2.1 Reviewing a Workflow Version

Scenario

This topic describes how to review a workflow version.

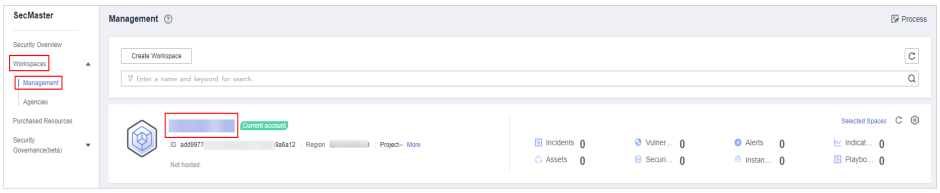
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

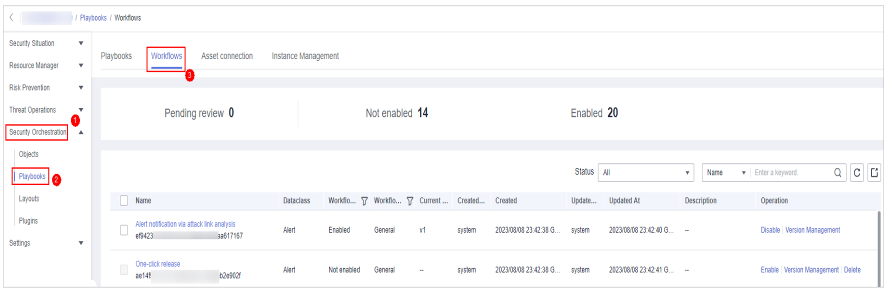
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-91 Workspace management page



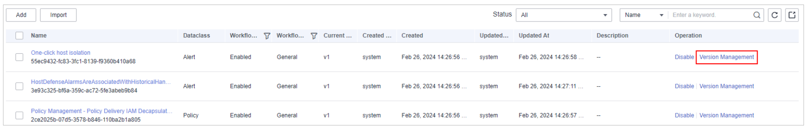
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-92 Workflows tab page



Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-93 Version Management page



Step 6 On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target workflow.

Step 7 Set **Comments**. **Table 11-26** describes the parameters.

Table 11-26 Workflow review parameters

Parameter	Description
Comments	Select the review conclusion. ● If the workflow version is approved, the status of the workflow version changes to **Activated**. ● Reject. After the workflow version is rejected, the status of the workflow version changes to **Rejected**. You can edit the workflow version and submit it again.
Reason for rejection	Enter the review comment. This parameter is mandatory when Reject is selected for Review Comment.

NOTE

- You can edit a rejected workflow version. For details, see **Managing Workflow Versions**.
- Workflow version status change:

  If the current workflow has only one workflow version, the status of the approved workflow **version** is **Activated** by default.

Step 8 Click **OK** to complete the workflow version review.

----End

Follow-up Operations

An approved workflow version needs to be enabled. For details, see **Enabling a Workflow**.

11.7.2.2 Enabling a Workflow

Scenario

This section describes how to enable a workflow.

Prerequisites

A workflow version has been activated by referring to **Managing Workflow Versions**.

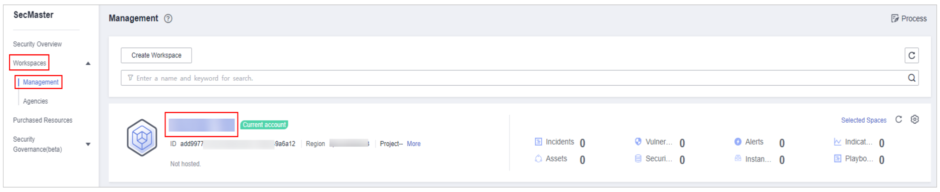
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

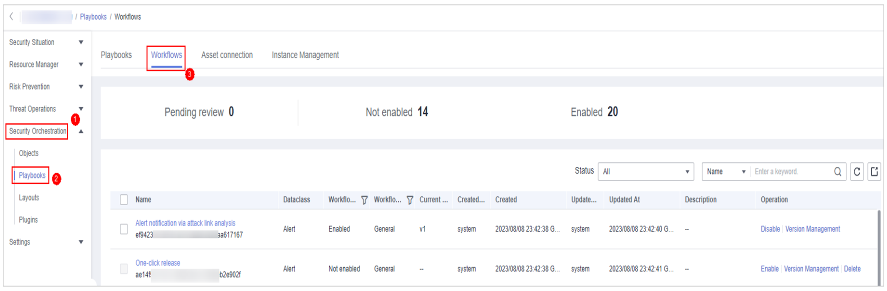
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-94 Workspace management page



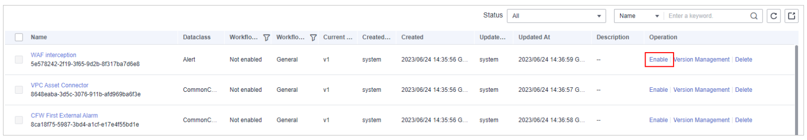
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-95 Workflows tab page



Step 5 In the row containing the target workflow, click **Enable** in the **Operation** column.

Figure 11-96 Enabling a workflow



Step 6 In the slide-out panel that is displayed, select the workflow version to be enabled and click **OK**.

----End

11.7.2.3 Managing Workflows

Scenario

This section describes how to manage workflows, including **Viewing Workflows**, **Exporting Workflows**, **Deleting Workflows**, and **Disabling a Workflow**.

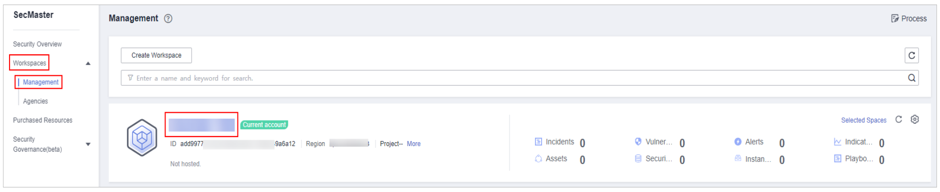
Viewing Workflows

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

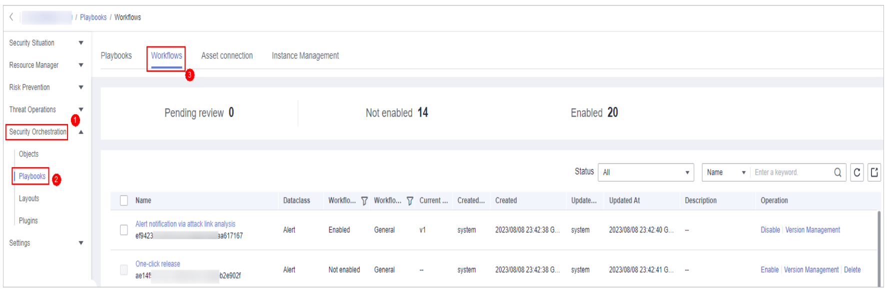
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-97 Workspace management page



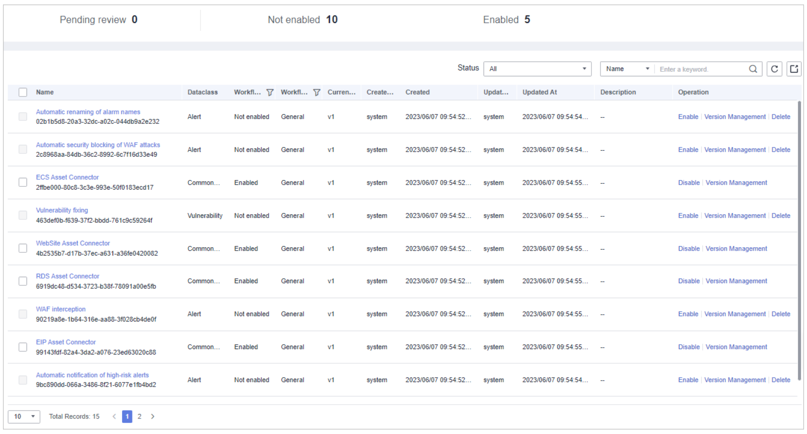
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-98 Workflows tab page



Step 5 On the Workflow Management page, view the information about the created workflow.

Figure 11-99 Viewing workflows



- The numbers of **Pending review**, **Not enabled**, and **Enabled** workflows are displayed above the workflow list.
- View information about existing workflows in the workflow list.

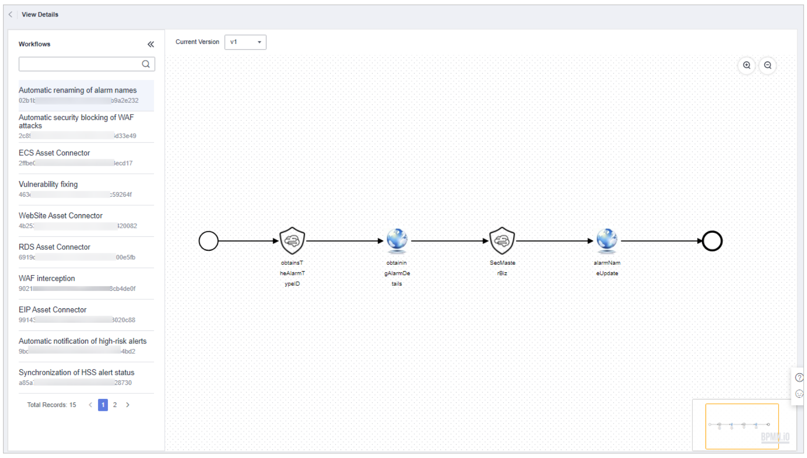
  If there are a large number of workflows, you can select the workflow status, name, description, or data class, enter a keyword in the search box, and click to quickly search for a specified workflow.

Table 11-27 Workflow parameters

Parameter	Description
Name	Workflow name
Dataclass	Data class corresponding to a workflow.
Workflow Status	Current status of a workflow. The status can be **Enabled** or **Disabled**.
Workflow Type	Current type of a workflow.
Current Version	Current version of a workflow.
Created By	User who creates the workflow.
Created	Time when a workflow was created
Updated By	User who modifies the workflow last time.
Updated At	Time when a workflow is last updated.
Description	A description of the workflow.
Operation	You can perform operations such as enabling and managing versions in the **Operation** column.

Step 6 To view details about a workflow, click the name of the workflow to access its details page.

Figure 11-100 Workflow details



----End

Exporting Workflows

NOTE

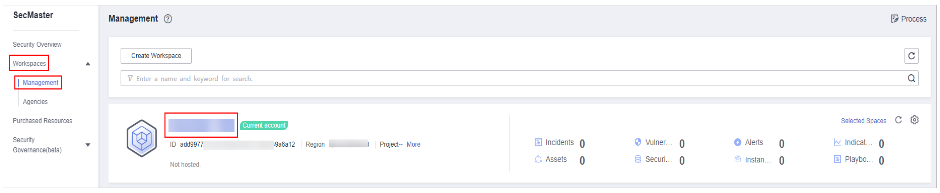
Workflows in the **Enabled** state can be exported.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

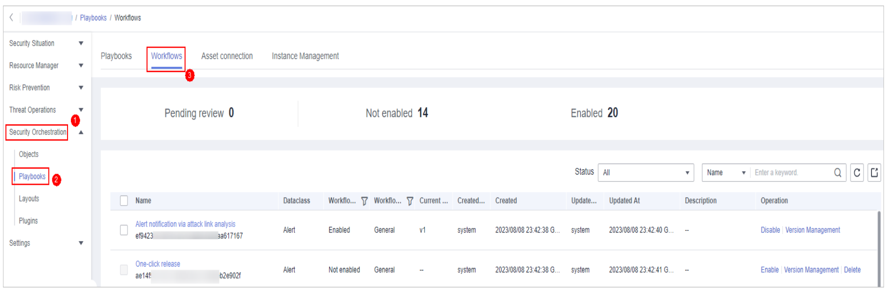
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-101 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-102 Workflows tab page



Step 5 On the **Workflows** tab page, select the workflows to be exported and click in the upper right corner of the list.

Step 6 In the dialog box that is displayed, click **OK**. The system exports the workflows to the local host.

----End

Deleting Workflows

NOTE

All of the following conditions must be met before you can delete a workflow:

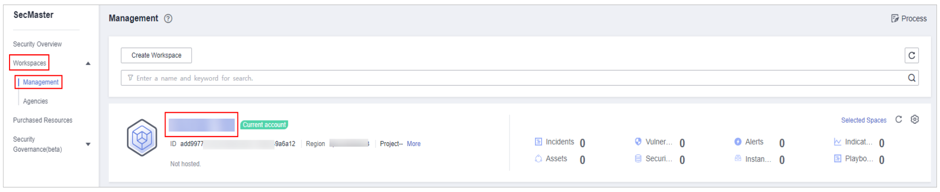
- The workflow is in the **Disabled** state.
- The workflow does not contain an activated workflow version.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

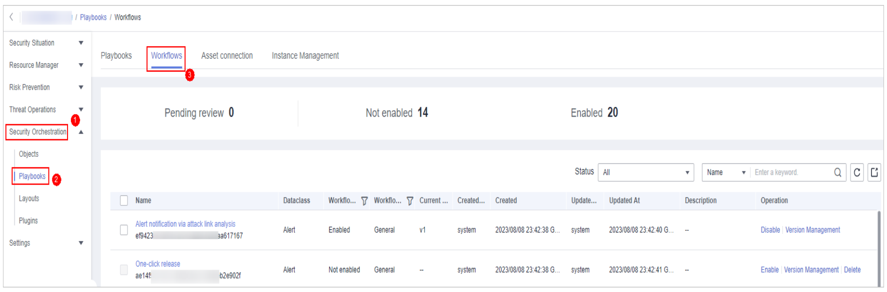
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-103 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-104 Workflows tab page



Step 5 On the **Workflows** tab page, locate the row containing the target workflow and click **Delete** in the **Operation** column.

Step 6 Click **OK** to delete the workflow.

NOTE

During deletion, all historical versions in the current workflow are deleted by default. Deleted versions cannot be restored.

----End

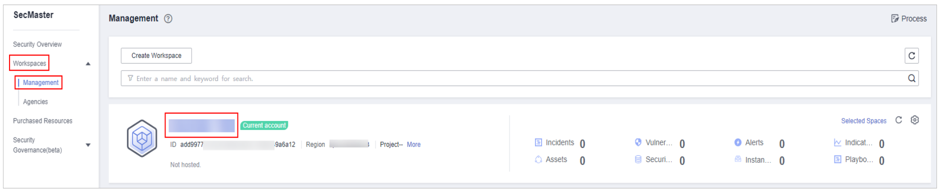
Disabling a Workflow

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

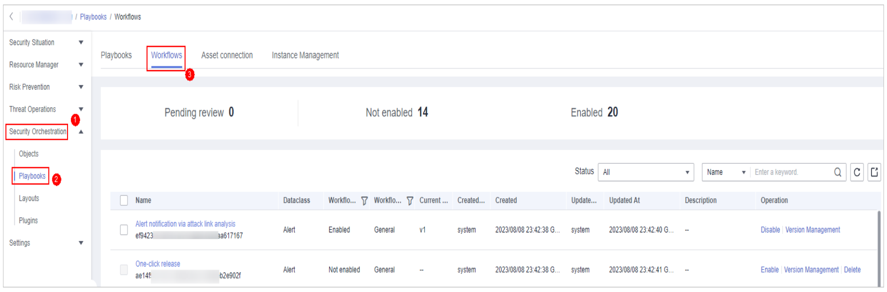
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-105 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-106 Workflows tab page



Step 5 In the row containing the target workflow, click **Disable** in the **Operation** column.

Step 6 In the dialog box that is displayed, click **OK**.

----End

11.7.2.4 Managing Workflow Versions

Scenario

This section describes how to manage workflow versions, including **Copying a Workflow Version**, **Editing a Workflow Version**, **Submitting a Workflow Version**, **Activating/Deactivating a Workflow Version**, and **Deleting a Workflow Version**.

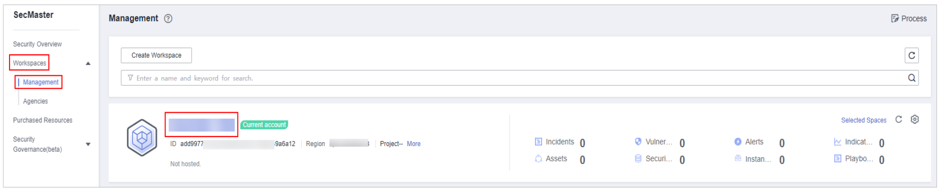
Copying a Workflow Version

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

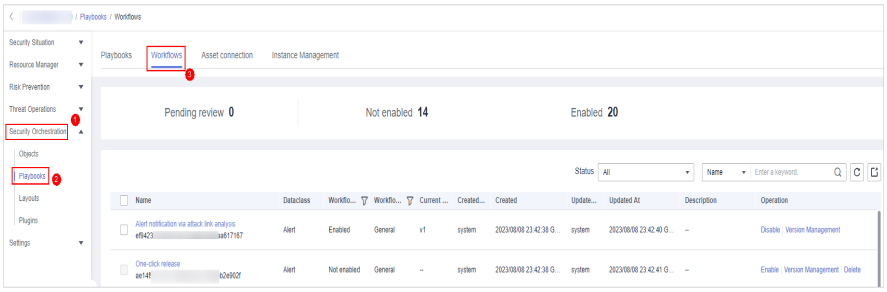
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-107 Workspace management page



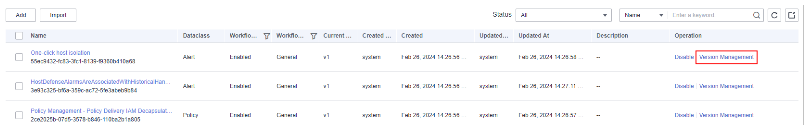
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-108 Workflows tab page



Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-109 Version Management page



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Copy** in the **Operation** column.

Step 7 In the dialog box displayed, click **OK**.

----End

Editing a Workflow Version

NOTE

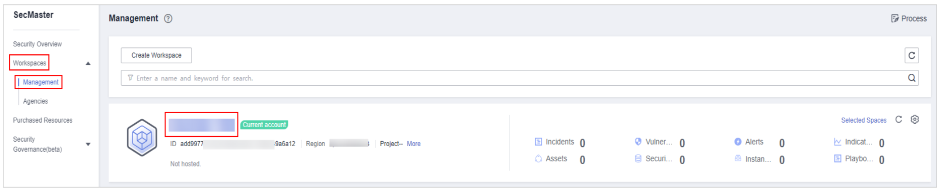
You can only edit a workflow version whose version status is **To be submitted** or **Rejected**.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

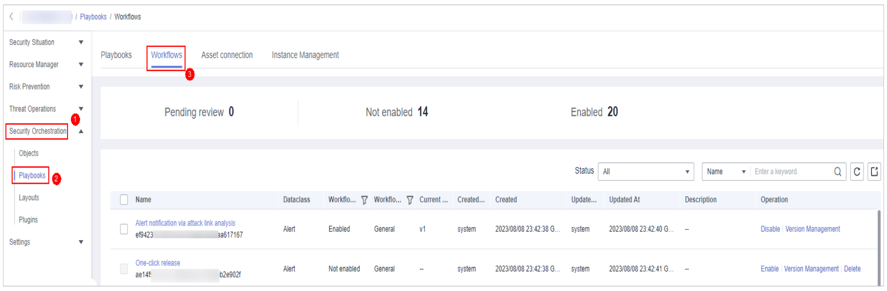
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-110 Workspace management page



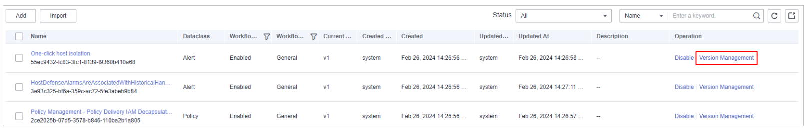
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-111 Workflows tab page



Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-112 Version Management page



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Edit** in the **Operation** column.

Step 7 On the workflow drawing page, drag basic, workflow, and plug-in nodes from **Resource Libraries** on the left to the canvas on the right for workflow design.

Table 11-28 Resource Libraries parameters

Parameter			Description
Basic	Basic Node	StartEvent	The start of a workflow. Each workflow can have only one start node. The entire workflow starts from the start node.

Parameter			Description
		EndEvent	The end of a workflow. Each workflow can have multiple end nodes, but the workflow must end with an end node.
		UserTask	When the workflow execution reaches this node, the workflow is suspended and a to-do task is generated on the **Task Center** page. After you complete the task, the subsequent nodes in the workflow continue to be executed. **Table 11-29** describes the UserTask parameters.
		SubProcess	Another workflow is started to perform cyclic operations. It is equivalent to the loop body in the workflow.
	System Gateway	ExclusiveGateway	During line distribution, one of the multiple lines is selected for execution based on the condition expression. During line aggregation, if one of the multiple lines arrives, the subsequent nodes continue to execute the task.
		ParallelGateway	During line distribution, all lines are executed. During line aggregation, the subsequent nodes are executed only when all the lines arrive. (If one line fails, the entire workflow fails.)
		InclusiveGateway	During line distribution, all expressions that meet the conditions are selected for execution based on the condition expression. During line aggregation, subsequent nodes are executed only when all lines executed during traffic distribution reach the inclusive gateway. (If one line fails, the entire workflow fails.)
Workflows			You can select all released workflows in the current workspace.
Plug-ins			You can select all plug-ins in the current workspace.

Table 11-29 UserTask parameters

Parameter	Description
Primary key ID	The system automatically generates a primary key ID, which can be changed as required.
Workspace Name	Name of the manual review node

Parameter	Description
Expired	Expiration time of a manual review node
Description	Description of the manual review node
View Parameters	Click ». On the **Select Context** page that is displayed, select an existing parameter name. To add a parameter, click **Add Parameter**.
Manual Handling Parameters	Key of the input parameter To add a parameter, click **Add Parameter**.
Processed By	Set the reviewer of the workflow to the IAM user of the current account. If a workflow needs to be approved after the setting, only the owner can handle it on the **Task Center** page. Non-owners can only view the workflow. **NOTE** In first time use, you need to obtain authorization. Detailed operations are as follows: 1. Click **Authorize**. 2. On the **Access Authorization** slide-out panel displayed, select **Agree** and click **OK**.

Step 8 After the design is complete, click **Save and Submit** in the upper right corner. In the automatic workflow verification dialog box displayed, click **OK**.

If the workflow verification fails, check the workflow based on the failure message.

----End

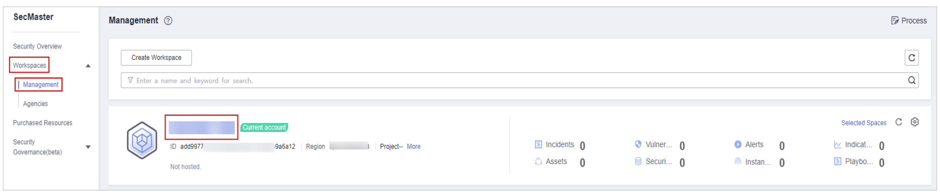
Submitting a Workflow Version

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

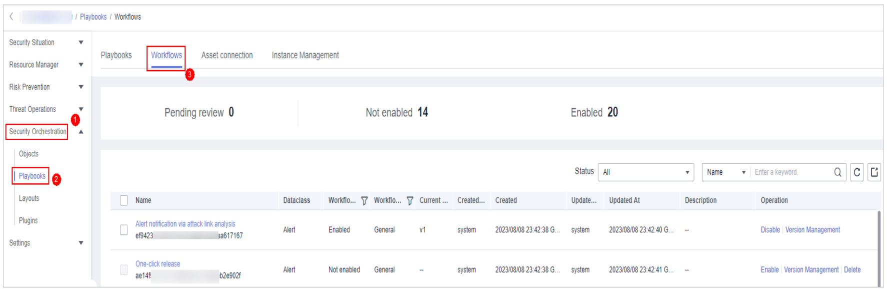
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-113 Workspace management page



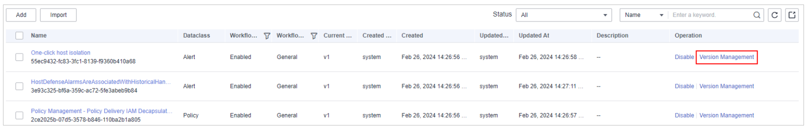
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-114 Workflows tab page



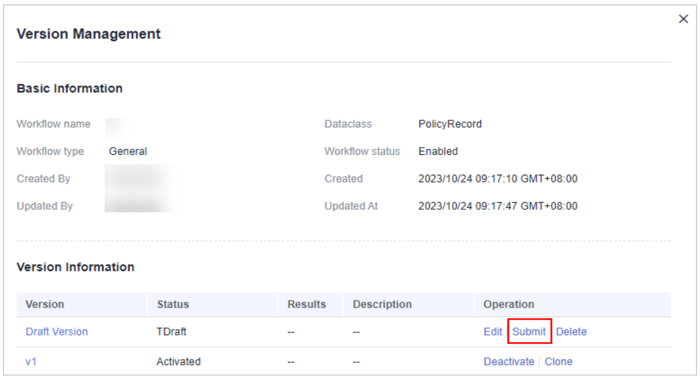
Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-115 Version Management page



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Submit** in the **Operation** column.

Figure 11-116 Submitting a workflow version



Step 7 In the confirmation dialog box, click **OK** to submit the workflow version.

NOTE

- After the workflow version is submitted, the **Version Status** changes to **Pending Review**.
- After a workflow version is submitted, it cannot be edited. If you need to edit it, you can create a version or reject it during review.

----End

Activating/Deactivating a Workflow Version

NOTE

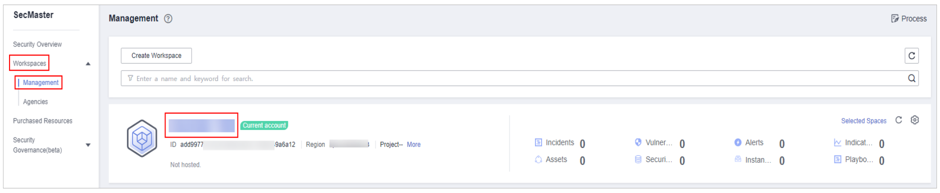
- Only workflow versions in the **Inactive** state can be activated.
- Each workflow can have only one activated version.
- After the current version is activated, the previously activated version is deactivated. For example, if the V2 version is activated this time, the V1 version in the activated state is deactivated and changes to the deactivated state.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

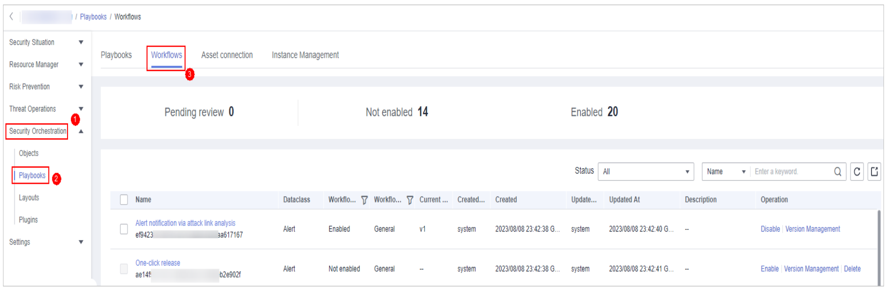
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-117 Workspace management page



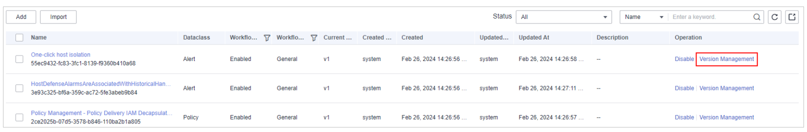
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-118 Workflows tab page



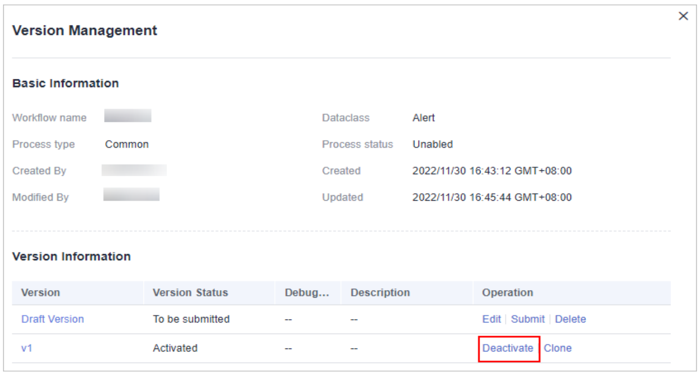
Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-119 Version Management page



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Activate** or **Deactivate** in the **Operation** column.

Figure 11-120 Example deactivating a workflow version



Step 7 In the dialog box that is displayed, click **OK**.

----End

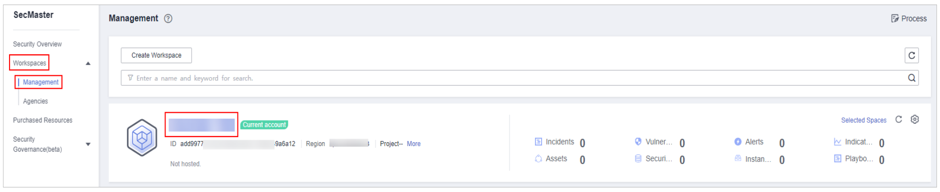
Deleting a Workflow Version

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

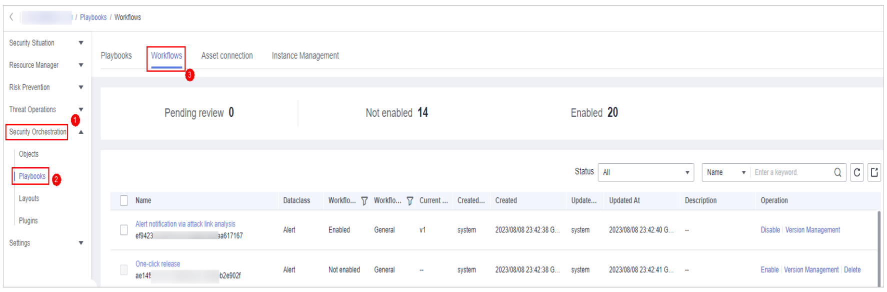
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-121 Workspace management page



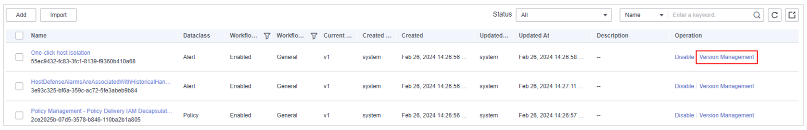
Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

Figure 11-122 Workflows tab page



Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-123 Version Management page



Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Delete** in the **Operation** column. In the dialog box displayed, click **OK**.

NOTE

Deleted workflow versions cannot be retrieved. Exercise caution when performing this operation.

----End

11.7.3 Asset Connections

11.7.3.1 Adding an Asset Connection

Scenario

This topic describes how to create an asset.

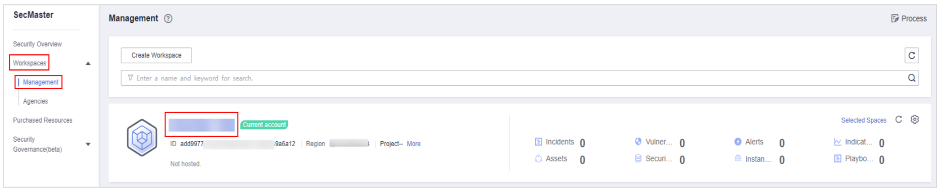
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

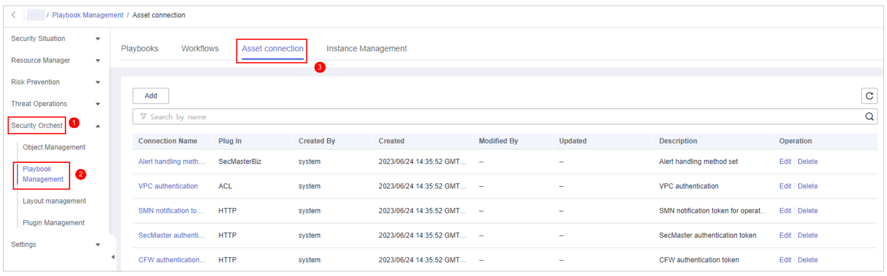
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-124 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-125 Asset connection tab



Step 5 On the **Asset Connection** tab page, click **Add**. The slide-out panel **Add** is displayed on the right.

Step 6 On the panel, set asset connection parameters. For details about the parameters, see **Table 11-30**.

Table 11-30 Asset connection parameters

Parameter	Description
Connection Name	Enter an asset connection name. The naming rules are as follows: ● Only uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and underscores (_) are allowed. ● A maximum of 64 characters are allowed.
Description	(Optional) Enter the asset description. The description can contain a maximum of 64 characters.
Plug In	Select the plug-in required for asset connection. For details about the plug-in, see **Viewing Plug-in Details**.
Connection Type	Select the type of the asset connection.
Credential	Enter the credential information, such as AK and SK, based on the selected connection type.

Step 7 Click **OK**. You can query the created asset connection in the asset connection list.

----End

11.7.3.2 Managing Asset Connections

Scenario

This topic describes **Viewing Asset Connections**, **Editing an Asset Connection**, and **Deleting an Asset Connection**.

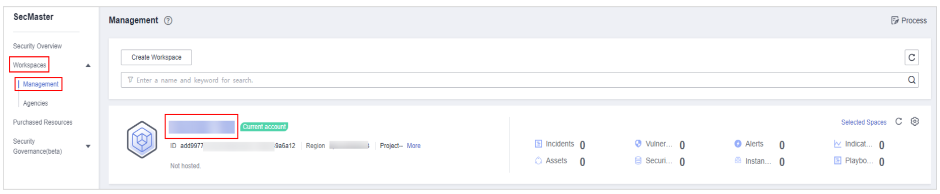
Viewing Asset Connections

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

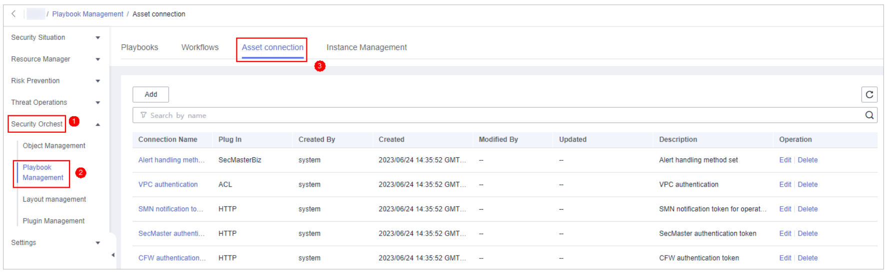
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-126 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-127 Asset connection tab



Step 5 On the **Asset connection** tab page, view information about existing asset connections.

If there are a large number of asset connections, you can use the search function to quickly search for a specified asset connection: Filter asset connections by connection name, plug-in, creator, creation time, person who modified the connection, update time, or description of an asset connection, enter a keyword in the search box, and click .

Figure 11-128 Viewing asset connections

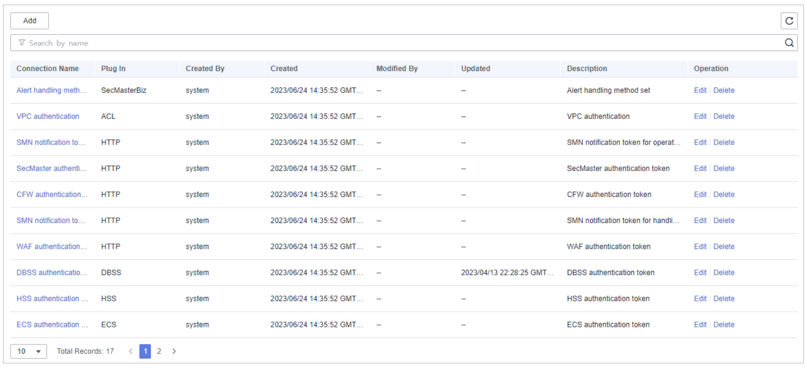


Table 11-31 Asset connection parameters

Parameter	Description
Connection Name	Asset connection name
Plug In	Plug-in corresponding to the asset connection
Created By	User who creates an asset connection
Created	Time when an asset connection is created
User who last updated the information	User who modifies the asset connection last time
Updated	Time when the asset connection was last updated
Description	Description of the asset connection

Parameter	Description
Operation	You can perform operations such as editing and deleting in the **Operation** column.

Step 6 To view details about an asset connection, click the name of the asset connection. The slide-out panel **Detail** is displayed.

----End

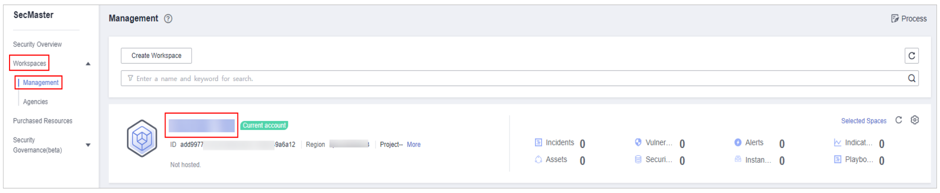
Editing an Asset Connection

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

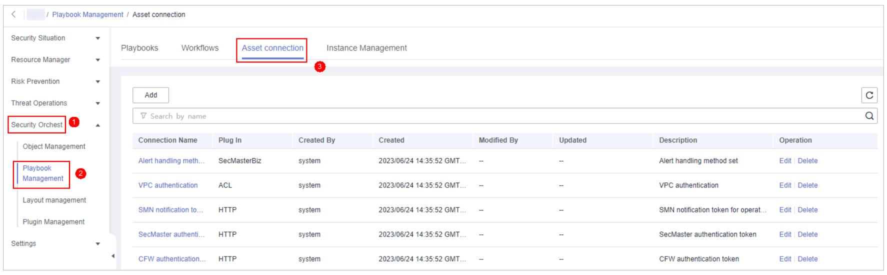
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-129 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-130 Asset connection tab



Step 5 In the row containing a desired asset connection, click **Edit** in the **Operation** column. The slide-out panel **Edit** is displayed.

Step 6 On the **Edit** panel, edit asset connection parameters. For details about the parameters, see **Table 11-32**.

Table 11-32 Asset connection parameters

Parameter	Description
Connection Name	Enter an asset connection name. The naming rules are as follows: ● Only uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and underscores (_) are allowed. ● A maximum of 64 characters are allowed.
Description	(Optional) Enter the asset connection description. The description can contain a maximum of 64 characters.
Plug In	Select the plug-in required for asset connection. For details about the plug-in, see **Viewing Plug-in Details**.
Created By	Creator of the asset connection. This parameter **cannot be modified**.
Created	Time when an asset connection is created. This parameter **cannot be modified**.
Modified By	User who last modifies the asset connection. This parameter **cannot be modified**.
Connection Type	Select the type of the asset connection.
Credential	Enter the credential information, such as AK and SK, based on the selected connection type.

Step 7 Click **OK**.

----End

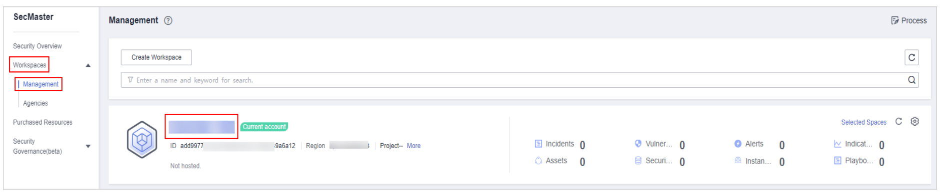
Deleting an Asset Connection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

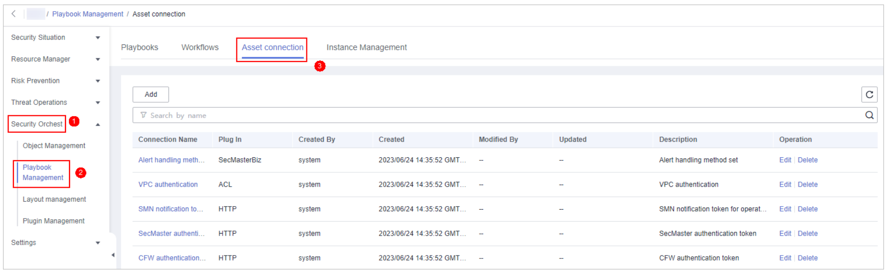
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-131 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-132 Asset connection tab



Step 5 Locate the row that contains a desired asset connection, click **Delete** in the **Operation** column.

Step 6 In the deletion confirmation dialog box that is displayed, click **OK** to confirm the deletion.

NOTE

Deleted assets cannot be restored. Exercise caution when performing this operation.

----End

11.7.4 Instance Management

11.7.4.1 Viewing Monitored Playbook Instances

Scenario

After a playbook is executed, a playbook instance is generated in the playbook instance management list for monitoring. Each record in the instance monitoring list is an instance. You can view the historical instance task list and the statuses of historical instance tasks.

View instance monitoring information.

Limitations and Constraints

The maximum number of retries within a day for a single workspace of a single account is as follows:

- Manual retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
- API retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.

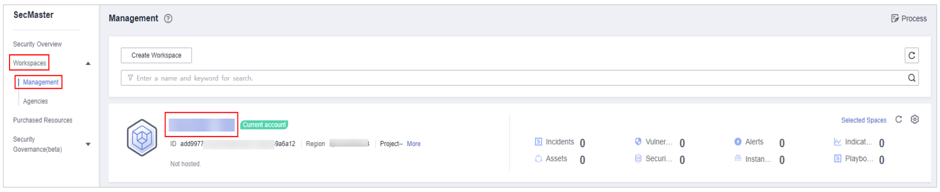
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

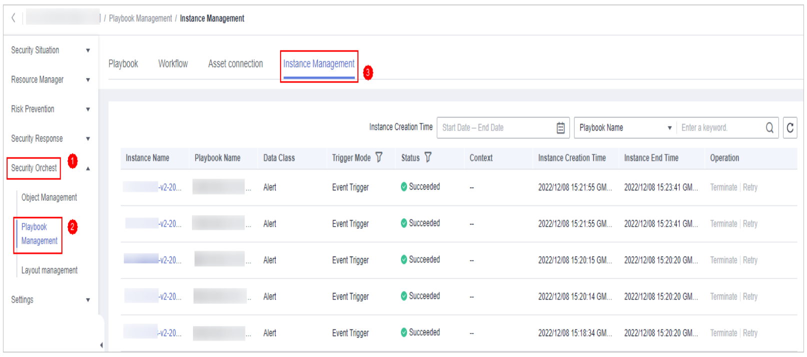
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-133 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Instance Management** tab.

Figure 11-134 Instance Management page



Step 5 In the instance management list, view the instance name, playbook name, and data class. For details about the parameters, see **Table 11-33**.

Figure 11-135 Instances

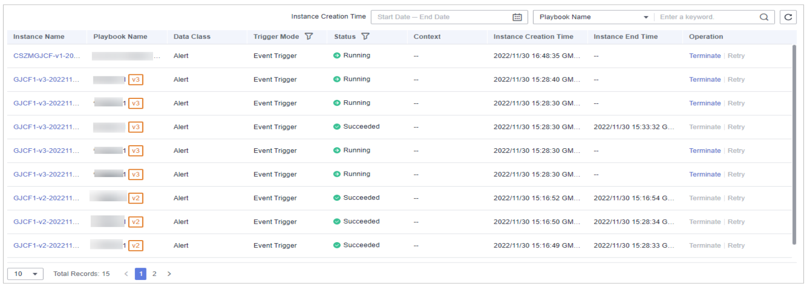


Table 11-33 Parameters in the instance list

Parameter	Description
Instance Name	Name of an instance
Playbook Name	Name of the playbook corresponding to the instance.

Parameter	Description
Data Class	Operation object of a playbook
Trigger Method	Triggering mode of an instance ● **Timer Trigger** ● **Event Trigger**
Status	Status of an instance ● **Succeeded**: The playbook instance is successfully executed. ● **Failed**: The playbook instance fails to be executed. You can click **Retry** in the **Operation** column to execute the playbook again. ● **Running**: The playbook instance is running. You can click **Terminate** in the **Operation** column to terminate the playbook. ● **Retrying**: The playbook instance is being retried. ● **Terminating**: The playbook instance is being terminated. ● **Stopped**: The playbook instance has been terminated.
Context	Context information of an instance
Instance Creation Time	Time when an instance is created.
Instance Ended	Time when an instance ends.
Operation	You can terminate or retry an instance.

Step 6 To view details about an instance, click the instance name. On the displayed page, you can view the instance workflow and workflow node information.

----End

11.8 Layout Management

11.8.1 Viewing an Existing Layout Template

Scenario

The management page and details page templates for alert management, incident management, vulnerability management, analysis report, intelligence management, and large-screen security are available in the layout.

View an existing layout template.

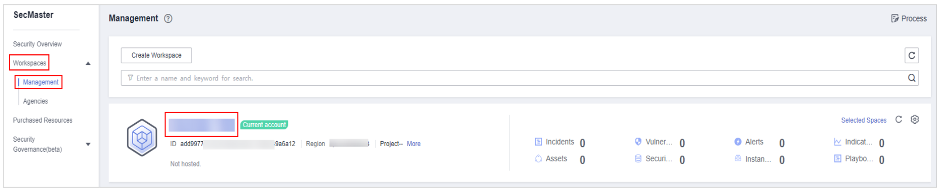
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

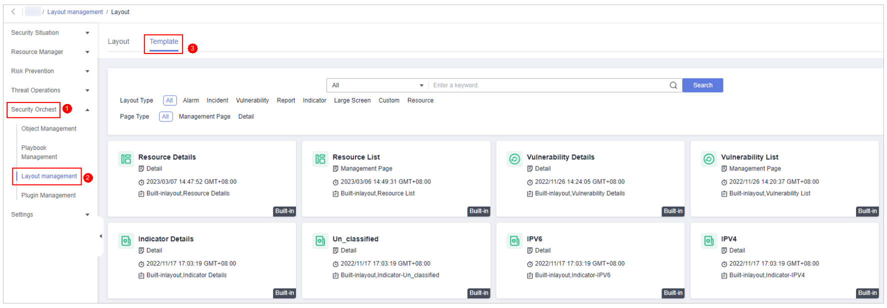
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-136 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Layouts**. On the displayed page, click the **Template** tab.

Figure 11-137 Layout template tab page



Step 5 On the **Template** tab page, view the template information.

You can search for a specified layout template by **Layout Type** or **Page Type**.

- You can view the name, page type, and creation time of an existing template.
- You can edit the name and layout of an existing template.
- You can delete an existing template.

----End

11.8.2 View Existing Layouts

Scenario

This topic describes how to perform the following operation: **Viewing an Existing Layout**.

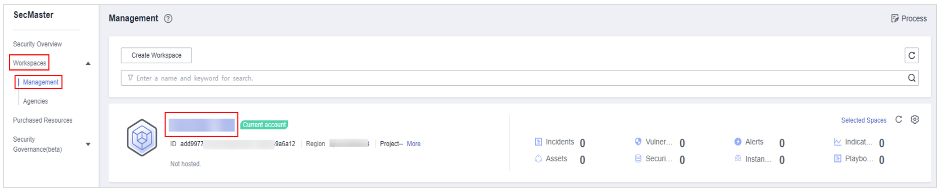
Viewing an Existing Layout

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

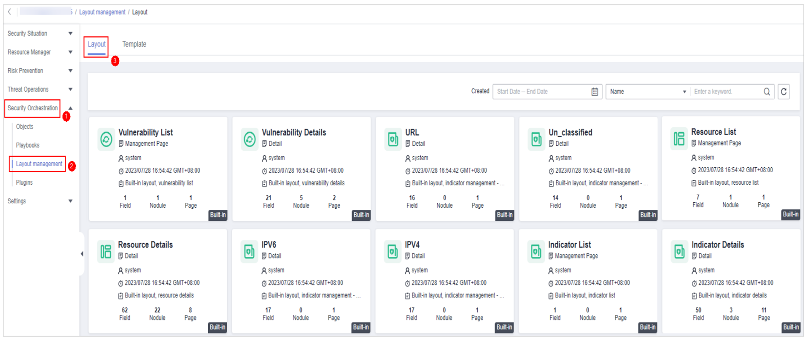
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-138 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Layouts**.

Figure 11-139 Layouts page



Step 5 On the layout management page, view existing layouts.

Hover your cursor over the target layout and click in the upper right corner of the layout. The layout configuration details page is displayed.

----End

11.9 Plug-in Management

11.9.1 Overview

SecMaster supports unified management of plug-ins used in the security orchestration process.

Terms

- **Plug-in**: an aggregation of functions, connectors, and public libraries. There are two types of plug-ins: custom plug-ins and commercial plug-ins. Custom plug-ins can be displayed in marts or used in playbooks.
- **Plug-in set**: a set of plug-ins that have the same service scenario.
- **Function**: an executable function that can be selected in a playbook to perform a specific behavior in the playbook.

- **Connector**: connects to data sources and sends security data such as alerts and incidents to SecMaster. Connectors are classified into incident-triggered connectors and scheduled connectors.
- **Public library**: a public module that contains API calls and public functions that will be used in other components.

11.9.2 Viewing Plug-in Details

Scenario

This section describes how to view SecMaster built-in plug-ins and their details.

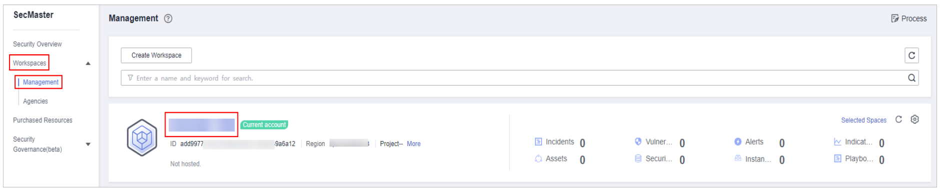
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

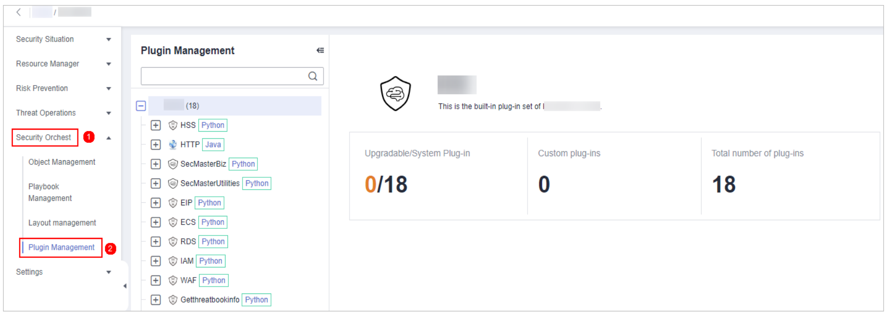
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 11-140 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Plugins**.

Figure 11-141 Plugins page



Step 5 On the **Plugins** page, view plug-in details.

- The navigation pane on the left shows information about all built-in plug-in sets, plug-ins, and functions.
- To view details about a plug-in, click its name. Its details will be displayed in the right pane.

- To view details about a function, expand the plug-in and click the function name. The function details will be displayed in the right pane.

----End

12 Settings

12.1 Data Collection

12.1.1 Data Collection Overview

Data collection refers to the process of using Logstash to collect varied log data in many methods. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Limitations and Constraints

- Currently, the data collection agent can run only on Linux ECSs on x86_64 architecture. ECSs support the following OSs: Huawei Cloud EulerOS 2.5, Huawei Cloud EulerOS 2.9, EulerOS 2.5, EulerOS 2.9, and CentOS 7.9.
- If you want to view information in the console during Agent installation, logging in as an IAM user is mandatory.

Collector Specifications

In collection management, the collector specifications are as follows:

Table 12-1 Collector Specifications

Specifications	Referenced Processing Capability
4U8G50G100G	2000 EPS @ 1KB
8U16G50G100G	5000 EPS @ 1KB
16U32G50G100G	10000 EPS @ 1KB

Log Source Limit

You can add as many as log sources you need to the collectors as long as your cloud resources can accommodate those logs. You can scale cloud resources anytime to meet your needs.

12.1.2 Collecting Data

Scenario

This section describes how to collect data.

Step 1: Buy an ECS

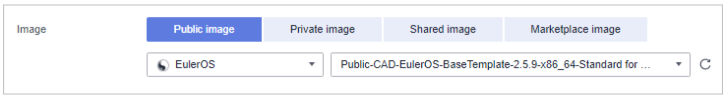
For details, see **Purchasing an ECS**.

CAUTION

- Currently, the data collection agent can run only on Linux ECSs on x86_64 architecture. ECSs support the following OSs: Huawei Cloud EulerOS 2.5, Huawei Cloud EulerOS 2.9, EulerOS 2.5, EulerOS 2.9, and CentOS 7.9.

  Note that you need to select the proper OSs and versions when you buying an ECS.

  Figure 12-1 Selecting an OS version

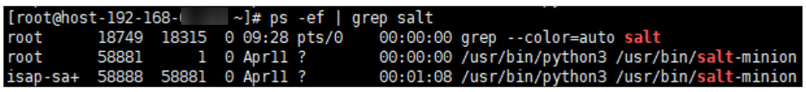
- ECSs are billed. For details about ECS pricing, see **Billing Overview**.

  If you do not need to collect log data later, you need to manually release the ECSs used. For details, see **How Do I Release an ECS or VPC Endpoint?**

Step 2: Install an Agent

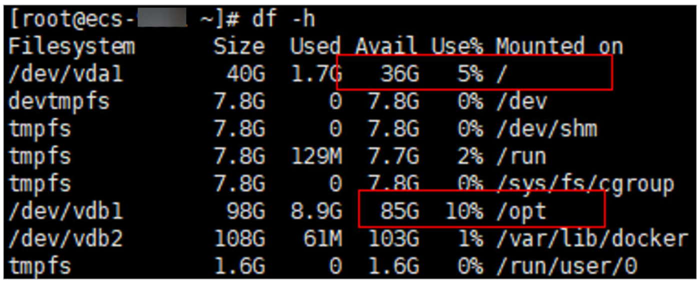
1. Pre-check before installing an agent.
   a. Run the **ps -ef | grep salt** command to check whether the salt-minion process exists on the host.
      - If yes, stop it first.
      - If no, go to **1.b**.

      Figure 12-2 Checking processes

   b. Run the **df -h** command to check whether there are at least 50 GB of disk space reserved for the **root** directory disk or **opt** disk, two CPU cores, and 4 GB of memory.

Figure 12-3 Disks

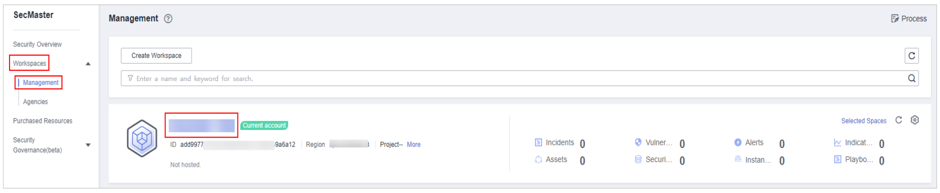


```
[root@ecs-[redacted] ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        40G  1.7G   36G   5% /
devtmpfs        7.8G     0  7.8G   0% /dev
tmpfs           7.8G     0  7.8G   0% /dev/shm
tmpfs           7.8G  129M  7.7G   2% /run
tmpfs           7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/vdb1        98G  8.9G   85G  10% /opt
/dev/vdb2       108G   61M  103G   1% /var/lib/docker
tmpfs           1.6G     0  1.6G   0% /run/user/0
```

If the memory is insufficient, stop some applications with high memory usage or expand the memory capacity before the installation. For details about capacity expansion, see **Modifying ECS Specifications**.

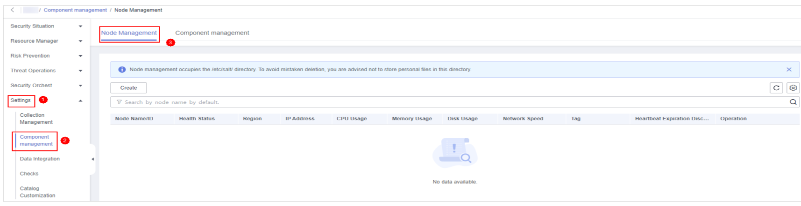
2. Log in to the management console.
3. Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.
4. In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-4 Workspace management page



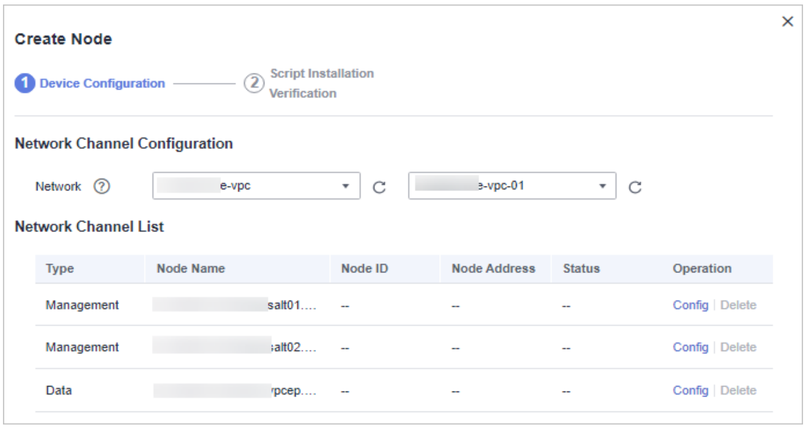
5. In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-5 Accessing the node management page



6. On the **Node Management** tab page, click **Create**.
7. On the **Create Node** page, set parameters.

Figure 12-6 Create Node



a. In the **Network Channel Configuration** area, select the VPC and subnet the network channel belongs to.

b. In the network channel list, locate the row that contains the target channel and click **Config** in the **Operation** column. In the displayed confirmation dialog box, click **OK**.

NOTE

VPC endpoints you use for log collection are billed. For details about pricing, see **Billing Overview**.

If you do not need to collect log data later, you need to manually release the VPC endpoints used. For details, see **How Do I Release an ECS or VPC Endpoint?**

8. Click **Next** in the lower right corner of the page. On the page for verifying the script installation, click to copy the command for installing the Agent.
9. Remotely log in to the ECS where you want to install the agent.
   - **Huawei Cloud servers**
     - Log in to the ECS console, locate the target server, and click **Remote Login** in the **Operation** column to log in to the server. For details, see **Login Using VNC**.
     - If your server has an EIP bound, you can also use a remote management tool, such as PuTTY or Xshell, to log in to the server and install the agent on the server as user **root**.
   - **Non-Huawei Cloud servers**

     Use a remote management tool (such as PuTTY or Xshell) to connect to the EIP of your server and remotely log in to your server.
10. Run the **cd /opt/cloud** command to go to the installation directory.

CAUTION

The recommended installation path is **/opt/cloud**. This section also uses this path as an example. If you want to install the Agent in another path, change the path based on site requirements.

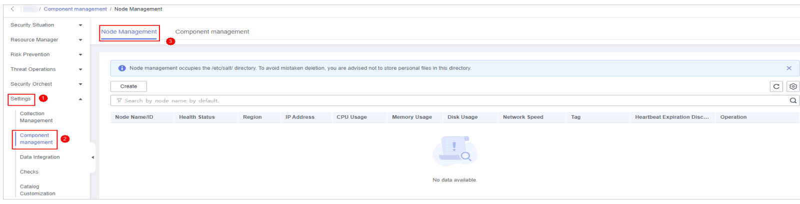
11. Run the command copied in 8 as user **root** to install the Agent on the ECS.
12. Enter the IAM username and password for logging in to the console when prompted.
13. If information similar to the following is displayed, the agent is successfully installed:

```
install isap-agent successfully
```

Step 3: Create a Node

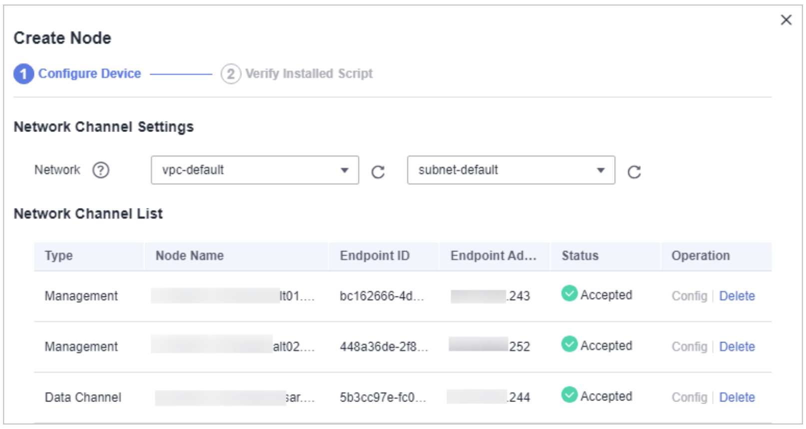
1. In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-7 Accessing the node management page



2. On the **Node Management** tab page, click **Create**.
3. On the **Create Node** page, set parameters.

Figure 12-8 Create Node



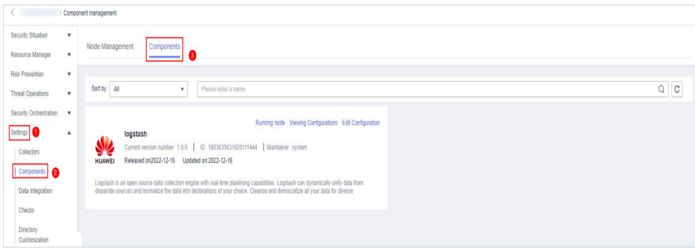
   a. In the **Network Channel Configuration** area, select the VPC and subnet the network channel belongs to.
   b. In the network channel list, locate the row that contains the target channel and click **Config** in the **Operation** column. In the displayed confirmation dialog box, click **OK**.

4. Click **Next** in the lower right corner of the page to go to the **Script Installation Verification** page.
5. After confirming that the installation is complete, click **Confirm** in the lower right corner of the page.

Step 4: Configure Components

1. In the navigation pane on the left, choose **Settings** > **Components** and click the **Components** tab.

Figure 12-9 Accessing the Components tab page

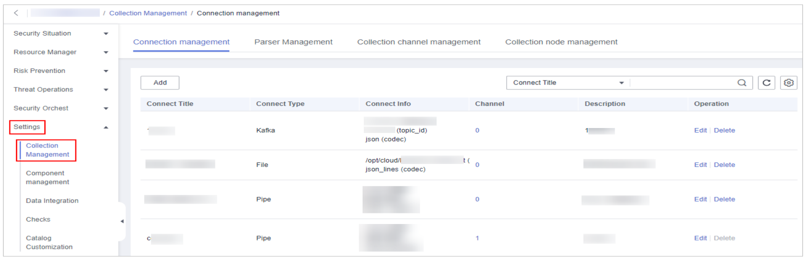


2. On the **Components** tab page, click **Edit Configuration** in the upper right corner of the component to be viewed. The configuration management page of the component is displayed on the right.
3. In the **Node Configuration** area, click **Add** in the upper left corner of the node list. In the **Add Node** dialog box displayed, select a node and click **OK**.
4. Click **Save and Apply** in the lower right corner of the page.

Step 5: Add a Data Connection

1. In the navigation pane on the left, choose **Settings** > **Collection Management**.

Figure 12-10 Accessing the collections page



2. On the **Connection Management** tab page, click **Add**.
3. Add a data connection source.

   In the **Source** column, select the source of the data source type and set parameters based on the selected type.

   The following data source types are supported: **Transmission Control Protocol (TCP)**, **File**, **User Data Protocol (UDP)**, **Object Storage Service (OBS)**, **Message Queue (Kafka)**, and **SecMaster Pipeline**.
4. Add a data source connection destination.

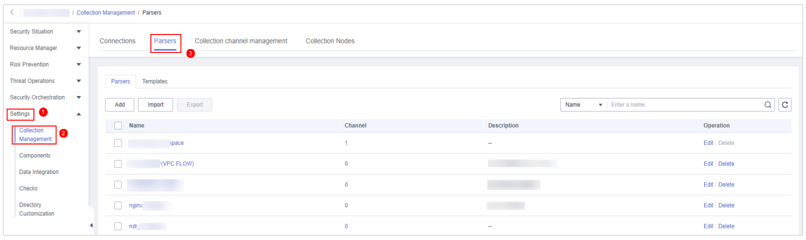
   Click the **Target** tab, select the destination of the data source type, and then set the parameters according to the selected type.

   The following data source types are supported: **File**, **Transmission Control Protocol (TCP)**, **User Data Protocol (UDP)**, **Message Queue (Kafka)**, **Object Storage Service (OBS)**, and **SecMaster Pipeline**.
5. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

(Optional) Step 6: Configure the Parser

1. In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-11 Accessing the Parsers tab page



2. Customize a parser or create a parser from a template.
   - **Customizing a parser**
     i. On the **Parsers** tab page, click **Add**.
     ii. On the **Parsers** tab page, set parameters.

Table 12-2 Parameters for adding a parser

Parameter		Description
Basic Information	Parser Name	Set a parser name.
	Description	Enter the parser description.
Rule list		Set the parsing rule of the parser. Perform the following steps: 1. Click **Add** and select a rule type. ● **Parsing rules**: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules. ● **Conditional control**: Select the conditions for the parser. You can select **If**, **Else**, or **Else if**. 2. Set parameters based on the selected rule.

     iii. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.
   - **Creating a parser from a template**
     i. On the **Parsers** tab page, click the **Templates** tab.
     ii. On the displayed page, locate the row that contains the target template, click **Created by Template** in the **Operation** column.
     iii. On the **Parsers** tab page, set parameters.

Table 12-3 Parameters for adding a parser

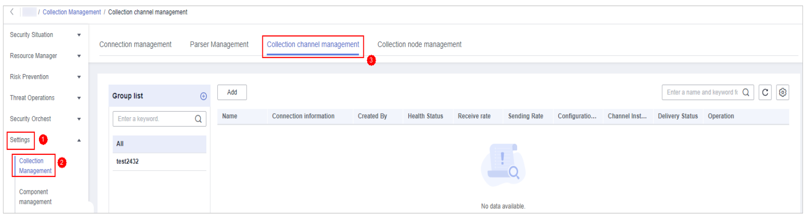
<table>
<tr><th colspan="2">Parameter</th><th>Description</th></tr>
<tr><td rowspan="2">Basic Information</td><td>Parser Name</td><td>Parser name, which is automatically generated by the system based on the template and can be changed.</td></tr>
<tr><td>Description</td><td>Parser description, which is automatically generated by the system based on the template and can be modified.</td></tr>
<tr><td colspan="2">Rule list</td><td>Parsing rule, which is automatically generated by the system based on the template and can be modified.
To add a rule, click Add, select a rule type, and set parameters based on the selected rule.
● Parsing rules: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules.
● Conditional control: Select the conditions for the parser. You can select If, Else, or Else if.</td></tr>
</table>

iv. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

Step 7: Add a Collection Channel

1. In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-12 Collection channel management tab page



2. Add a channel group.

   a. On the collection channel management page, click next to **Group list**.

   b. 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.

3. On the right of the group list, click **Add**.

4. On the displayed page, in the **Basic Configuration** phase, configure basic information.

Table 12-4 Basic configuration parameters

Parameter		Description
Basic Information	Name	User-defined collection channel name.
	Channel grouping	Select the group the collection channel belongs to.
	(Optional) Description	(Optional) Enter the description of the collection channel.
Source Configuration	Source Name	Select the source name of the collection channel. After you select a source, the system automatically generates the information about the selected source.
Destination	Destination Name	Select the destination name of the collection channel. After you select a source, the system automatically generates the information about the selected source.

5. After the basic configuration is complete, click **Next** in the lower right corner of the page.
6. On the parser configuration page, select a parser to view its details.

   If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see **Managing Parsers**.
7. After the parser is configured, click **Next** in the lower right corner of the page.
8. On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node and click **OK**.
   - Running parameters: After a node is added, if you want to configure parameters for the added node, perform the following steps:
     i. In the node list, locate the row that contains the target node, and click **Running Parameters** in the **Operation** column.
     ii. Click **Add Configuration** and set **Key** and **Value**.
   - Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.
9. After the running node is selected, click **Next** in the lower right corner of the page.
10. On the **Channel Details Preview** page, confirm the configuration and click **OK**.

Related Operations

Troubleshooting the Agent Installation Failure

12.1.3 Collection Management

12.1.3.1 Managing Connections

Scenario

This topic describes how to perform the following operations: **Adding a Connection**, **Viewing Connections**, **Editing a Data Connection**, and **Deleting a Data Connection**.

Limitations and Constraints

- After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed.

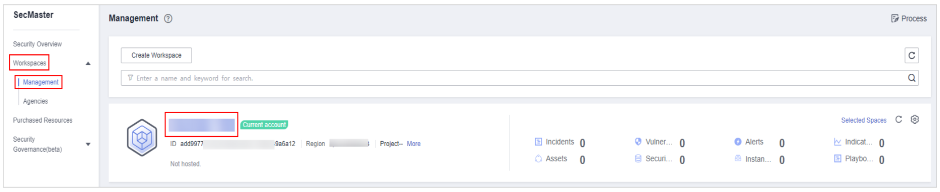
Adding a Connection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

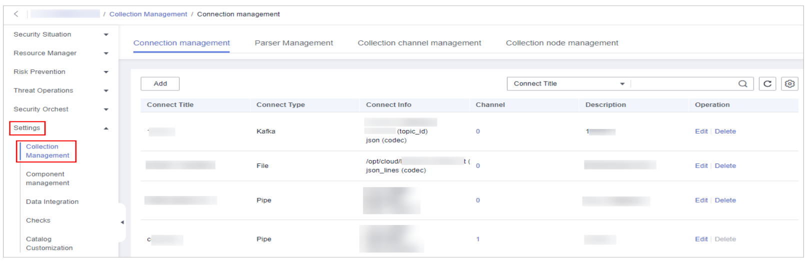
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-13 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**.

Figure 12-14 Accessing the collections page



Step 5 On the **Connections** tab, click **Add**.

Step 6 Add a data connection source.

In the **Source** column, select the source of the data source type and set parameters based on the selected type.

The following data source types are supported: **Transmission Control Protocol (TCP)**, **File**, **User Data Protocol (UDP)**, **Object Storage Service (OBS)**, **Message Queue (Kafka)**, and **SecMaster Pipeline**.

Step 7 Add a data source connection destination.

Click the **Target** tab, select the destination of the data source type, and then set the parameters according to the selected type.

The following data source types are supported: **File**, **Transmission Control Protocol (TCP)**, **User Data Protocol (UDP)**, **Message Queue (Kafka)**, **Object Storage Service (OBS)**, and **SecMaster Pipeline**.

Step 8 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

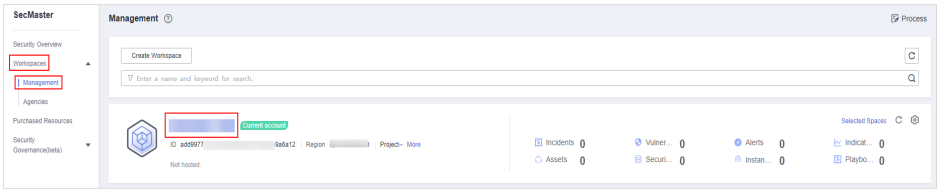
Viewing Connections

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

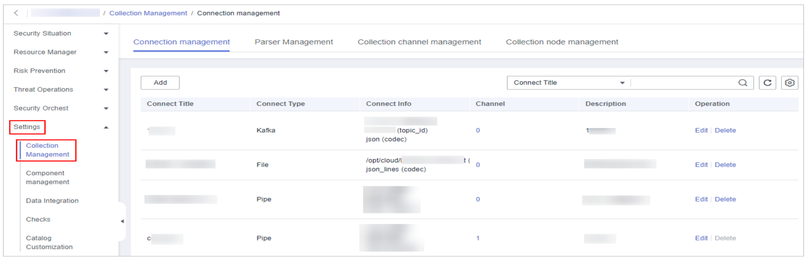
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-15 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**.

Figure 12-16 Accessing the collections page



Step 5 On the **Connections** tab, view connection details.

Table 12-5 Connection parameters

Parameter	Description
Connection Name	Connection name
Connection Type	Connection type
Connection Info	Information about a connection

Parameter	Description
Reference Channels	Number of channels that are referenced by the connection
Description	Description of the connection
Operation	Operations such as editing or deleting connections

----End

Editing a Data Connection

NOTE

After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed.

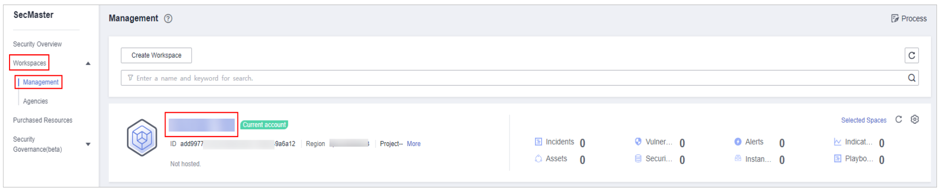
For example, if you select **File** as the data source type when adding a data connection, you can modify only the parameters in the file type but cannot change the **File** type.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

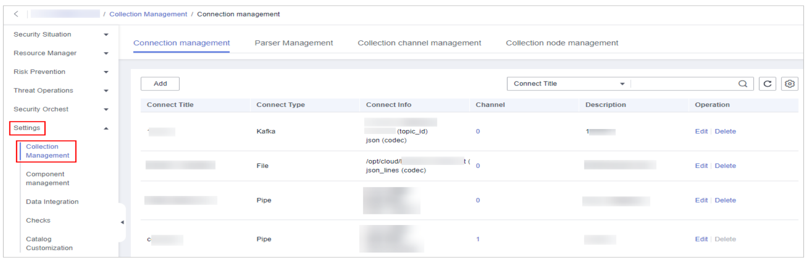
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-17 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**.

Figure 12-18 Accessing the collections page



Step 5 On the Connections page, locate the row that contains the target connection and click **Edit** in the **Operation** column.

Step 6 On the **Select Data Source Type** page, edit the parameters of the data source type.

Step 7 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

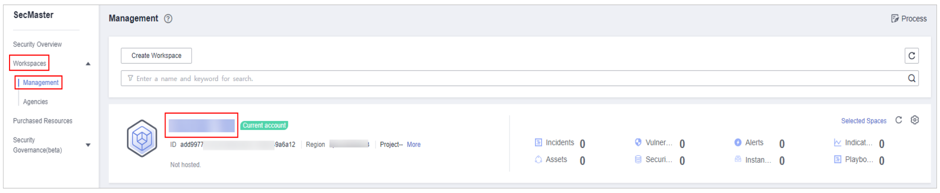
Deleting a Data Connection

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

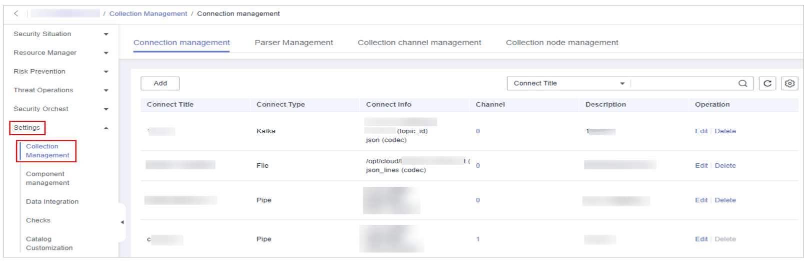
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-19 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**.

Figure 12-20 Accessing the collections page



Step 5 On the Connections page, locate the row that contains the target connection and click **Delete** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.

----End

12.1.3.2 Managing Parsers

Scenario

This topic describes how to perform the following operations: **Creating a Parser**, **Viewing Parsers**, **Importing a Parser**, **Editing a Parser**, **Exporting a Parser**, and **Deleting a Parser**.

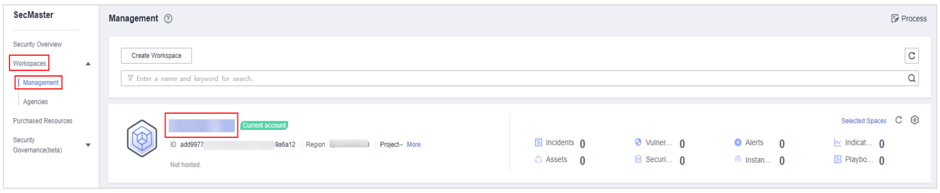
Creating a Parser

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

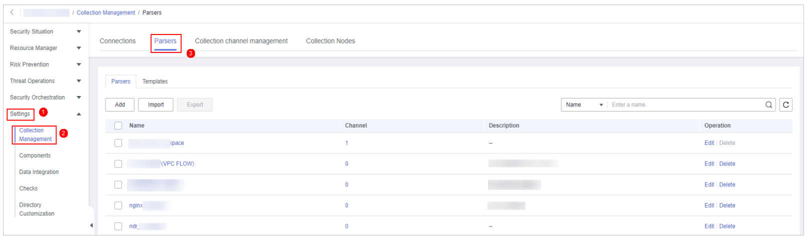
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-21 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-22 Accessing the Parsers tab page



Step 5 Customize a parser or create a parser from a template.

- **Customizing a parser**
  a. On the **Parsers** tab page, click **Add**.
  b. On the **Parsers** tab page, set parameters.

Table 12-6 Parameters for adding a parser

Parameter		Description
Basic Information	Parser Name	Set the parser name.
	Description	Enter the parser description.

Parameter	Description
Rule list	Set the parsing rule of the parser. Perform the following steps: 1. Click **Add** and select a rule type. ○ **Parsing rules**: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules. ○ **Conditional control**: Select the conditions for the parser. You can select **If**, **Else**, or **Else if**. 2. Set parameters based on the selected rule.

c. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

- **Creating a parser from a template**

a. On the **Parsers** tab page, click the **Templates** tab.

b. On the displayed page, locate the row that contains the target template, click **Created by Template** in the **Operation** column.

c. On the **Parsers** tab page, set parameters.

Table 12-7 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 rules**: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules. ▪ **Conditional control**: Select the conditions for the parser. You can select **If**, **Else**, or **Else if**.

d. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

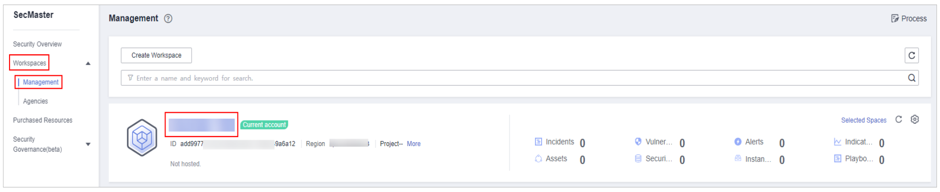
Viewing Parsers

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

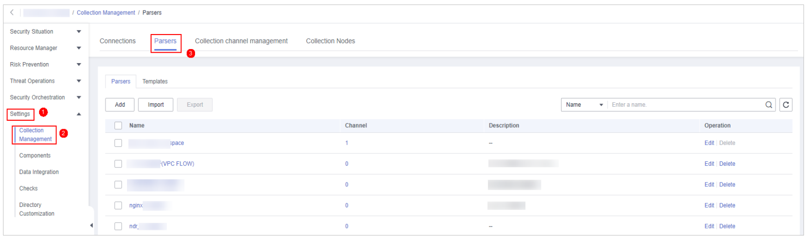
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-23 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-24 Accessing the Parsers tab page



Step 5 On the **Parsers** page, view the detailed information about parsers.

Table 12-8 Parsers parameters

Parameter	Description
Parser Name	Name of the parser.
Reference Channels	Number of channels referenced by the parser.
Description	Description of the parser.
Operation	You can edit and delete parsers.

Step 6 On the **Parsers** page, click the **Templates** tab.

Step 7 On the **Templates** tab displayed, view the parser template information.

Table 12-9 Parser template parameters

Parameter	Description
Template Name	Name of a parser template
Description	Description of the parser template
Operation	You can create a parser template.

----End

Importing a Parser

NOTE

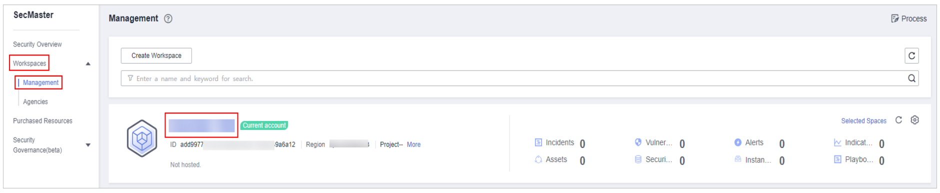
- Only .json files no larger than 1 MB can be imported.
- A maximum of five parser files can be imported at a time, and each parser file can contain a maximum of 100 parsers.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

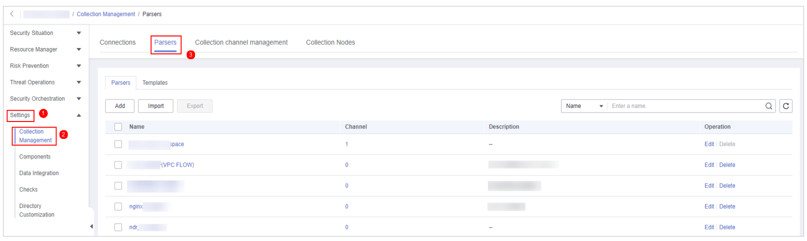
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-25 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-26 Accessing the Parsers tab page



Step 5 On the **Parsers** tab, click **Import** in the upper left corner of the parser list.

Step 6 In the displayed **Import** dialog box, click **Select File** and select the JSON file you want to import.

CAUTION

- Only .json files no larger than 1 MB can be imported.
- A maximum of five parser files can be imported at a time, and each parser file can contain a maximum of 100 parsers.

Step 7 Click **OK**.

After the parsers are imported, you can view the imported parser information in the parser list.

----End

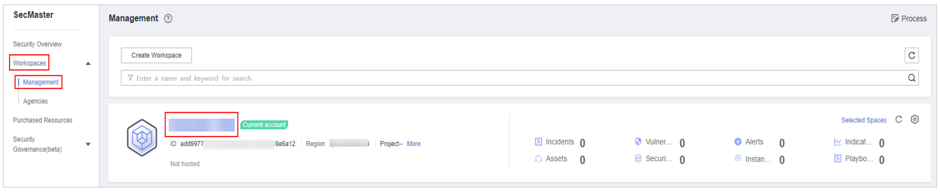
Editing a Parser

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

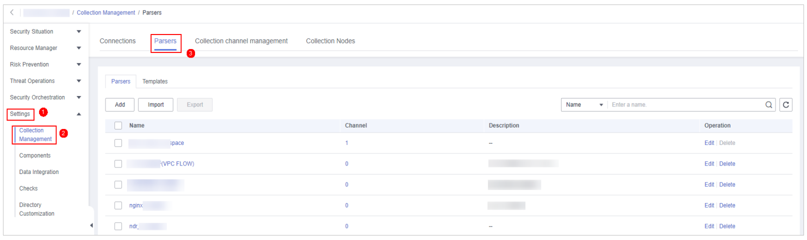
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-27 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-28 Accessing the Parsers tab page



Step 5 On the **Parsers** tab, locate the row containing your desired parser and click **Edit** in the **Operation** column.

Step 6 In the **Edit Parser** dialog box, edit the parser information.

Table 12-10 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 rules**: Select the parsing rule of the parser. ● **Conditional control**: Select the conditional control principle of the parser.

Step 7 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

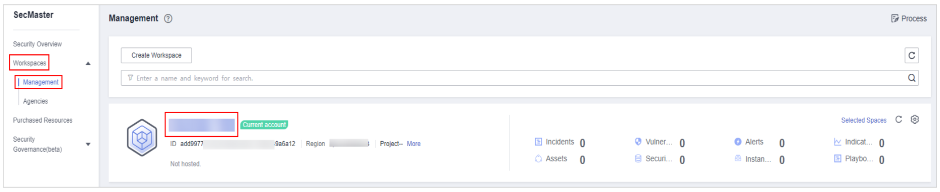
Exporting a Parser

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

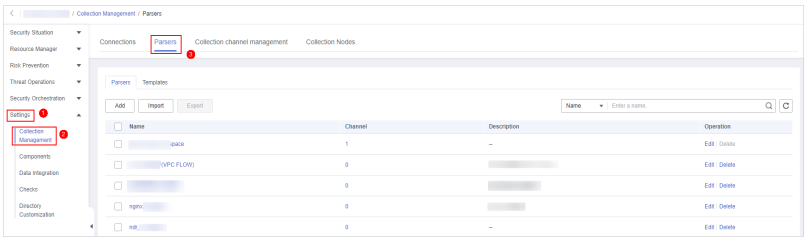
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-29 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-30 Accessing the Parsers tab page



Step 5 On the **Parsers** page, select the parsers you want to export and click **Export** above the list.

The system automatically downloads the parser file in .json format to the local PC.

----End

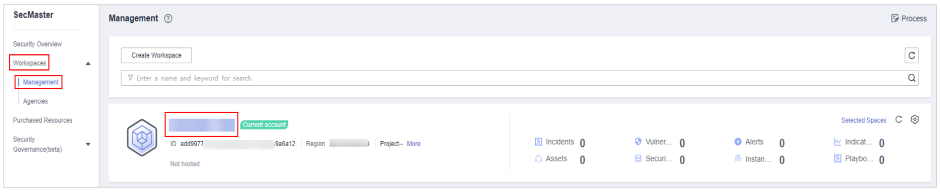
Deleting a Parser

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

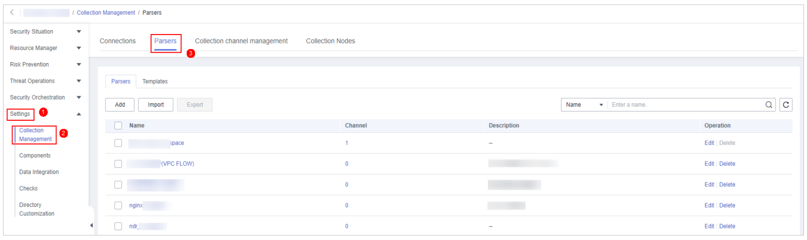
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-31 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the displayed page, click the **Parsers** tab.

Figure 12-32 Accessing the Parsers tab page



Step 5 On the **Parsers** tab, locate the row that contains the target parser and click **Delete** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.

----End

12.1.3.3 Managing Collection Channels

Scenario

This topic describes how to perform the following operations: **Adding a Collection Channel**, **Viewing Collection Channels**, **Editing a collection channel**, **Deleting a collection channel**, and **Enabling/Disabling/Restarting a Collection Channel**.

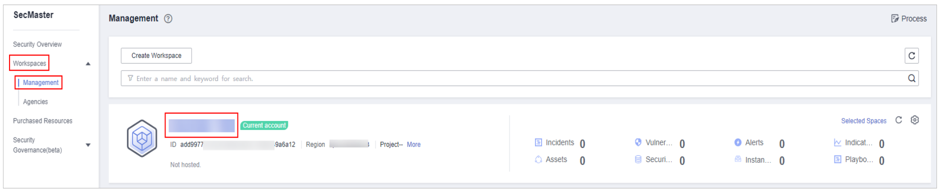
Adding a Collection Channel

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

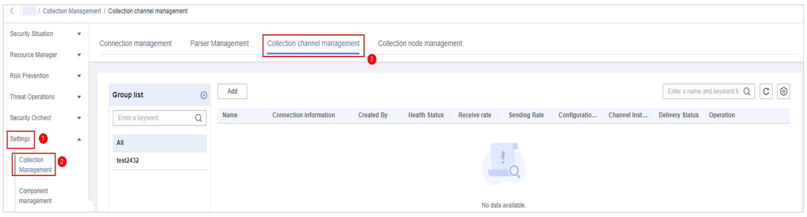
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-33 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-34 Collection channel management tab page



Step 5 Add a channel group.

1. On the collection channel management page, click next to **Group list**.
2. Enter a group name and click .

To edit or delete a group, hover the cursor over the group name and click the edit or deletion icon.

Step 6 On the right of the group list, click **Add**.

Step 7 On the displayed page, in the **Basic Configuration** phase, configure basic information.

Table 12-11 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.

Parameter		Description
Source Configuration	Source Name	Select the source name of the collection channel. After you select a source, the system automatically generates the information about the selected source.
Destination	Destination Name	Select the destination name of the collection channel. After you select a source, the system automatically generates the information about the selected source.

Step 8 After the basic configuration is complete, click **Next** in the lower right corner of the page.

Step 9 On the parser configuration page, select a parser to view its details.

If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see **Managing Parsers**.

Step 10 After the parser is configured, click **Next** in the lower right corner of the page.

Step 11 On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node and click **OK**.

- Running parameters: After a node is added, if you want to configure parameters for the added node, perform the following steps:
  a. In the node list, locate the row that contains the target node, and click **Running Parameters** in the **Operation** column.
  b. Click **Add Configuration** and set **Key** and **Value**.
- Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.

Step 12 After the running node is selected, click **Next** in the lower right corner of the page.

Step 13 On the **Channel Details Preview** page, confirm the configuration and click **OK**.

----End

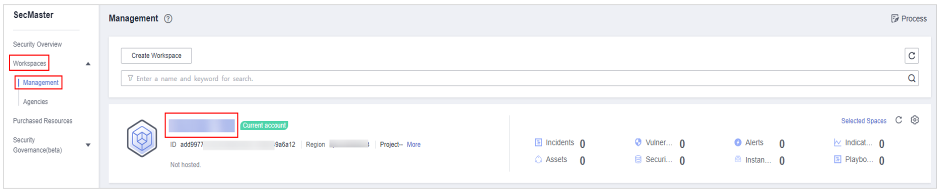
Viewing Collection Channels

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

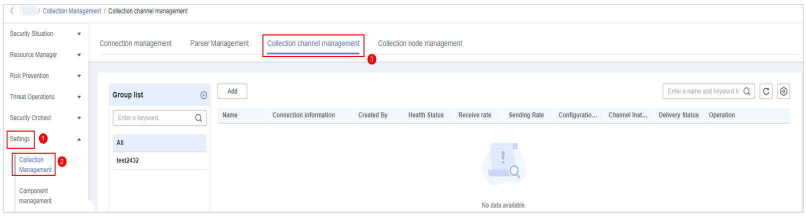
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-35 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-36 Collection channel management tab page



Step 5 On the **Collection Channels** page, view the detailed information about collection channels.

Table 12-12 Collection channel parameters

Parameter	Description
Channel Groups	List of collection channel groups and group names.
Channel Name	Name of the collection channel.
Connection Information	Collect channel connection information
Created By	Creator of the collection channel
Health Status	Health status of the collection channel
Receive Rate	Receive rate of the collection channel
Transmit Rate	Transmit rate of the collection channel
Configuration Status	Configuration status of the collection channel
Channel Instances	Number of collection channels
Running Status	Running status of a collection channel
Operation	You can edit and stop collection channels.

----End

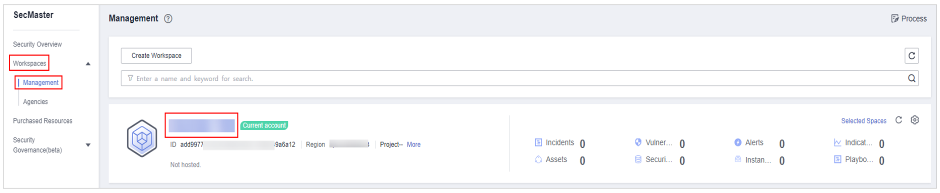
Editing a collection channel

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

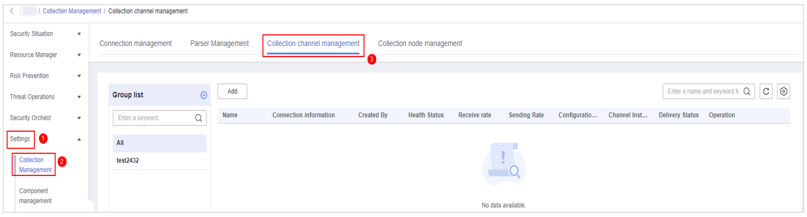
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-37 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-38 Collection channel management tab page



Step 5 In the collection channel list, locate the row that contains the target channel, click **More** > **Edit** in the **Operation** column. The **Edit Collection Channel** page is displayed.

Step 6 On the displayed page, in the **Basic Configuration** phase, configure basic information.

Table 12-13 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.

Parameter		Description
	Destination Name	Select the destination name of the collection channel. After you select a destination, the system automatically generates the information about the selected destination.

Step 7 After the basic configuration is complete, click **Next** in the lower right corner of the page.

Step 8 On the parser configuration page, select a parser to view its details.

If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see **Managing Parsers**.

Step 9 After the parser is configured, click **Next** in the lower right corner of the page.

Step 10 On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node and click **OK**.

- Running parameters: After a node is added, if you want to configure parameters for the added node, perform the following steps:
  a. In the node list, locate the row that contains the target node, and click **Running Parameters** in the **Operation** column.
  b. Click **Add Configuration** and set **Key** and **Value**.
- Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.

Step 11 After the running node is selected, click **Next** in the lower right corner of the page.

Step 12 On the **Channel Details Preview** page, confirm the configuration and click **OK**.

----End

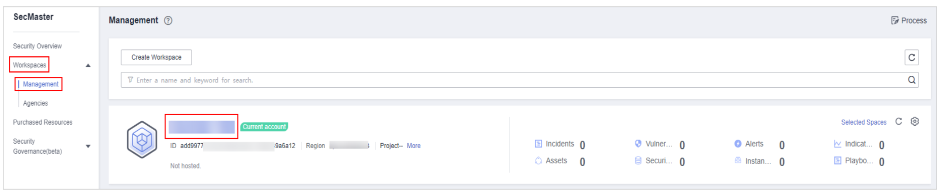
Deleting a collection channel

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

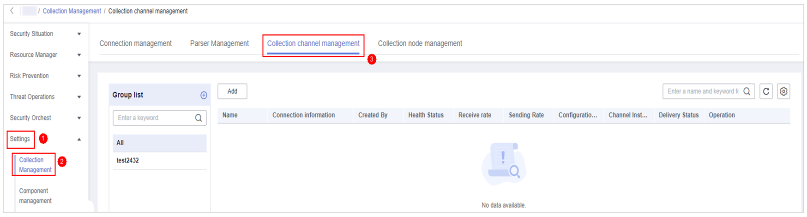
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-39 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-40 Collection channel management tab page



Step 5 In the collection channel list, locate the row that contains the target channel, click **More** > **Delete** in the **Operation** column.

NOTE

You can delete a collection channel only when it is stopped.

Step 6 In the displayed dialog box, click **OK**.

----End

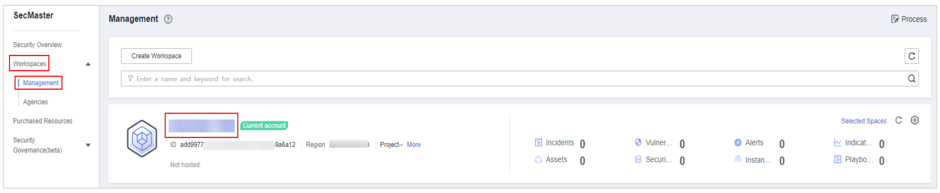
Enabling/Disabling/Restarting a Collection Channel

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

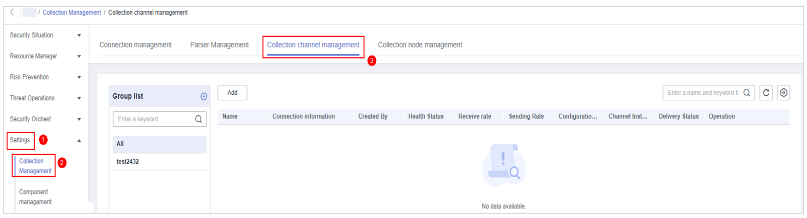
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-41 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-42 Collection channel management tab page



Step 5 In the collection stream management list, locate the row that contains the target stream and click **Enable**, **Stop**, or **Restart** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.

----End

12.1.3.4 Managing Collection Nodes

Scenario

This topic describes how to perform the **Viewing Collection Nodes** operation.

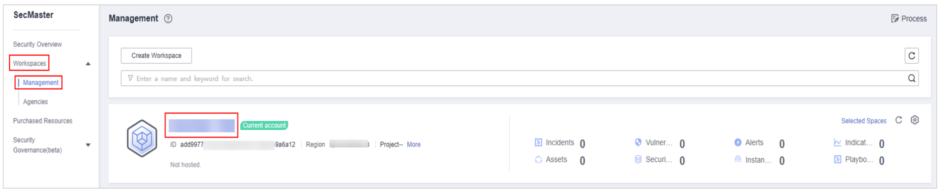
Viewing Collection Nodes

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

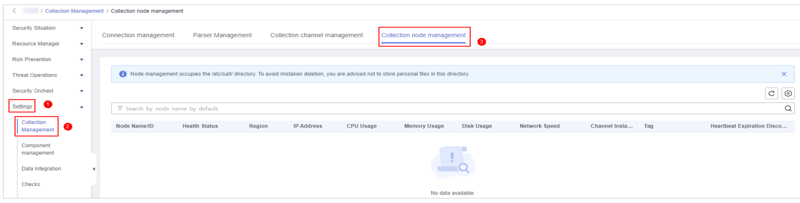
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-43 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Collection Management**. On the Collection Management page, click the **Collection Nodes** tab.

Figure 12-44 Accessing the collection nodes page



Step 5 On the **Collection Nodes** page, view the detailed information about collection nodes.

If there are a large number of nodes, you can select **Node Name** or **Node ID**, enter a keyword in the search box, and click to quickly search for a specified node.

Table 12-14 Collection node parameters

Parameter	Description
Node Name/ID	Name or ID of a node
Health Status	Node health status

Parameter	Description
Region	Region where the node is located
IP Address	Node IP address
CPU Usage	CPU usage of the node
Memory Usage	Memory usage of the node
Disk Usage	Node disk usage
Network Speed	Network rate of a node
Label	Label information of a node
Heartbeat Expiration Mark	Indicates whether the node is disconnected due to heartbeat expiration.

Step 6 To view details about a node, click the node name.

----End

12.1.4 Component Management

12.1.4.1 Managing Collection Nodes

Scenario

This topic describes how to perform operations such as **Creating a Node**, **Viewing Nodes**, **Editing a Node**, and **Deregistering a Node**.

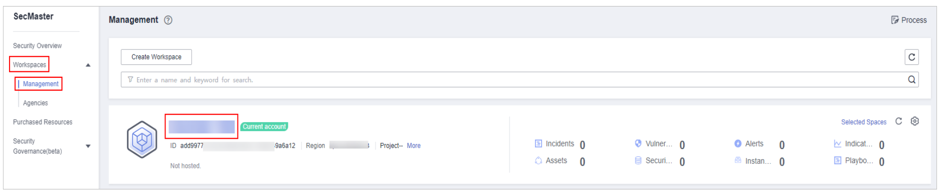
Creating a Node

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

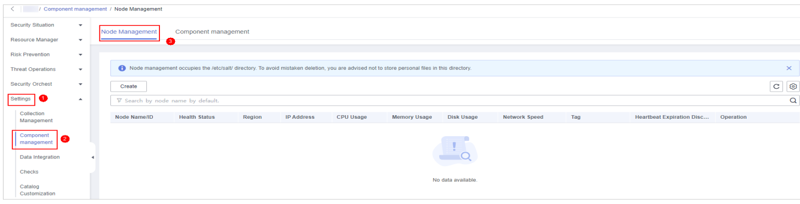
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-45 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-46 Accessing the node management page



Step 5 On the **Nodes** tab, click **Create**. The **Create Node** page is displayed on the right.

Step 6 Click **Next** in the lower right corner of the page to go to the **Script Installation Verification** page.

Step 7 After confirming that the installation is complete, click **Confirm** in the lower right corner of the page.

If it is not installed, rectify the fault by referring to **Step 2: Install an Agent**.

----End

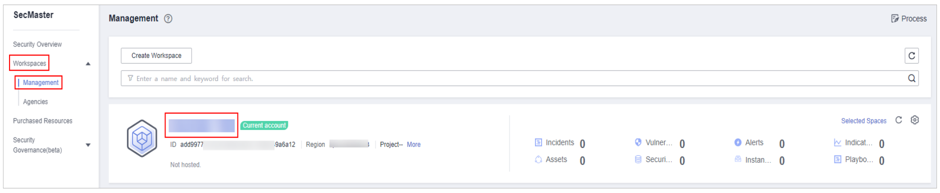
Viewing Nodes

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

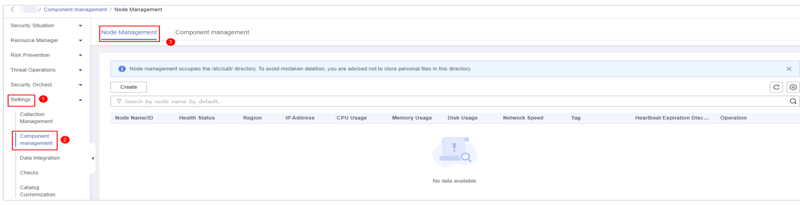
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-47 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-48 Accessing the node management page



Step 5 On the **Nodes** tab, view the details about nodes.

If there are a large number of nodes, you can select **Node Name** or **Node ID**, enter a keyword in the search box, and click to quickly search for a specified node.

Table 12-15 Collection node parameters

Parameter	Description
Node Name/ID	Name or ID of a node
Health Status	Node health status
Region	Region where the node is located
IP Address	Node IP address
CPU Usage	CPU usage of the node
Memory Usage	Memory usage of the node
Disk Usage	Node disk usage
Network Speed	Network rate of a node
Label	Label information of a node
Heartbeat Expiration Mark	Indicates whether the node is disconnected due to heartbeat expiration.

Step 6 To view details about a node, click the node name.

----End

Editing a Node

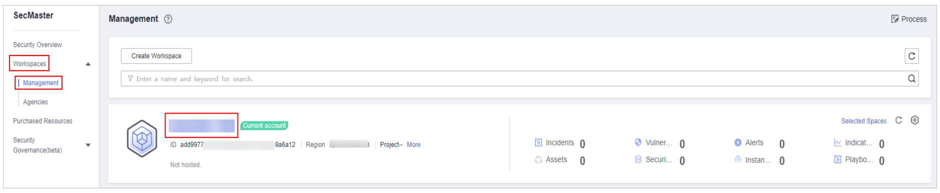
After a node is added, you can only modify the supplementary information about the node.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

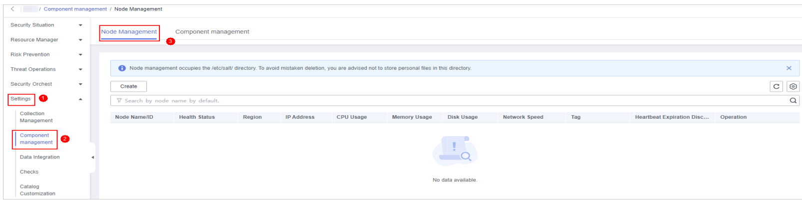
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-49 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-50 Accessing the node management page



Step 5 On the **Nodes** tab, locate the row that contains the target node and click **Edit** in the **Operation** column.

Step 6 On the **Edit Node** panel, edit the node information.

Table 12-16 Parameters of node information

Parameter	Description
Data Center	User-defined data center name
Network Plane	Select the network plane of the node.
Tag	Set the tag for the node.
Description	Description of a user-defined node.
Maintained By	Select a node owner.

Step 7 Click **Confirm**.

----End

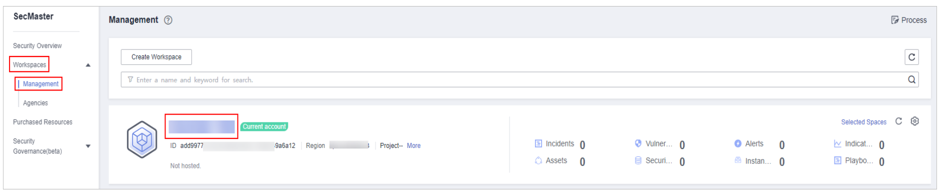
Deregistering a Node

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

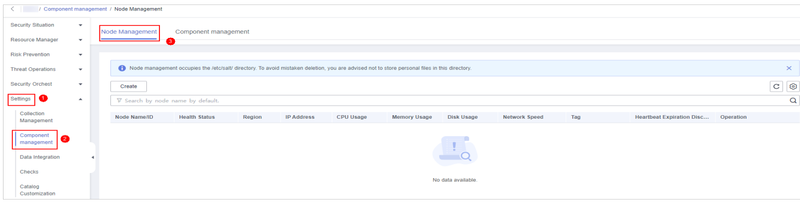
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-51 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Components**.

Figure 12-52 Accessing the node management page



Step 5 On the **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.

NOTE

Only the node is deregistered. The ECS and endpoint interface resources are not deleted.

----End

12.1.4.2 Managing Components

Scenario

This topic describes how to configure and view a component.

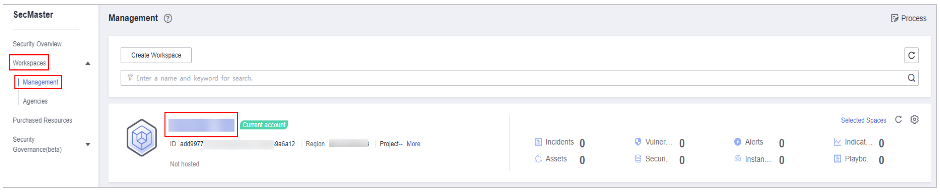
Configuring a Component

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

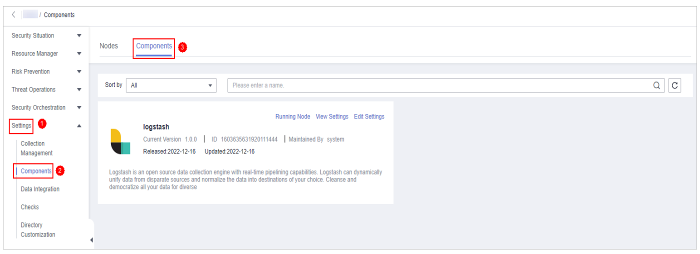
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-53 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Components** and click the **Components** tab.

Figure 12-54 Accessing the Components tab



Step 5 On the **Components** tab page, click **Edit Settings** in the upper right corner of the component to be viewed. The configuration management page of the component is displayed on the right.

Step 6 In the **Node Configuration** area, click **Add** in the upper left corner of the node list. In the **Add Node** dialog box displayed, select a node and click **OK**.

Step 7 Click **Save and Apply** in the lower right corner of the page.

----End

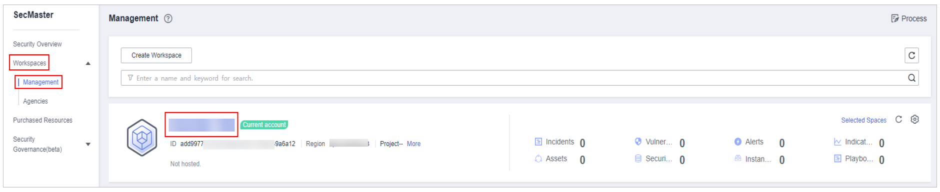
Viewing Component Details

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

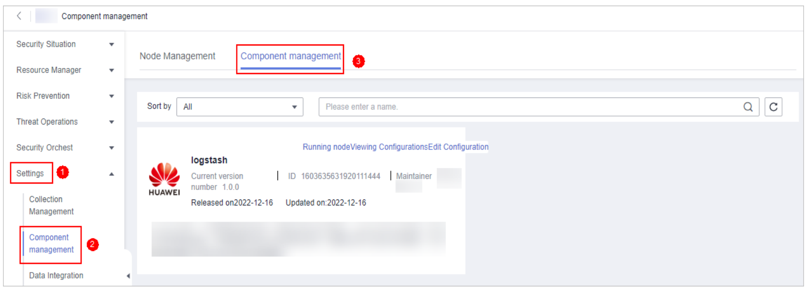
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-55 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Components** > **Components**.

Figure 12-56 Accessing the components page



Step 5 On the **Components** page, view the component details.

- **Running node:**

  Click the **Running Node** in the upper right corner of a component. The running node information of the component is displayed on the right.

- **View Settings**

  Click **View Settings** in the upper right corner of the component to be viewed. The configuration details about the component are displayed on the right.

- **Edit Settings**

a. Click **Edit Settings** in the upper right corner of the component to be viewed. The **Configuration Management** panel of the component is displayed on the right.

b. In the **Node Configuration** area, edit the node configuration information.

- Adding a node: Click **Add** in the upper left corner of the node list. In the **Add Node** dialog box that is displayed, select a node and click **OK**.
- Editing node parameters: Click next to the node name to expand the node configuration information and edit the node parameters.
- Running Parameter: Locate the row that contains the target node, click **Run Parameter** in the **Operation** column.
- Removing a node: Locate the row that contains the target node and click **Removed** in the **Operation** column.
- Batch deletion: Select the nodes to be removed and click **Batch Remove** in the upper left corner of the list.
- To view historical versions, click **Historical Version** at the lower right corner of the panel.

c. Click the **Apply** at the lower right corner of the page.

----End

12.2 Data Integration

12.2.1 Log Access Supported by SecMaster

SecMaster can integrate logs of multiple Huawei Cloud services, such as Web Application Firewall (WAF), Host Security Server (HSS), and Object Storage Service (OBS). You can search for and analyze all collected logs in SecMaster. By default, the logs are stored for 7 days.

Table 12-17 Log Access Supported by SecMaster

Cloud Service	Log Description	Log	Log Lifecycle
Web Application Firewall (WAF)	Attack logs	waf-attack	7 to 30 days
	Access logs	waf-access	
SecMaster	Compliance baseline log	secmaster-baseline	7 to 10 days
Intrusion Prevention System (IPS)	Attack logs	nip-attack	7 to 30 days
Managed Threat Detection (MTD)	Alarm logs	mtd-alarm	7 to 30 days

Cloud Service	Log Description	Log	Log Lifecycle
Host Security Service (HSS)	HSS alarms	hss-alarm	7 to 30 days
	HSS vulnerability scan results	hss-vul	7 days
	HSS security logs	hss-log	7 to 15 days
Cloud Trace Service (CTS)	CTS logs	cts-audit	7 to 30 days
Cloud Firewall (CFW)	Access control logs	cfw-block	7 to 30 days
	Traffic logs	cfw-flow	7 to 15 days
	Attack event logs	cfw-risk	7 to 30 days

12.2.2 Access Data

Scenario

SecMaster can access logs of Huawei Cloud services with your authorization, services such as Web Application Firewall (WAF), Host Security Server (HSS), and Object Storage Service (OBS). After you authorize the access, you can manage logs centrally and search and analyze all collected logs.

For details, see **Log Access Supported by SecMaster**.

This topic describes how to access logs and view where logs are stored.

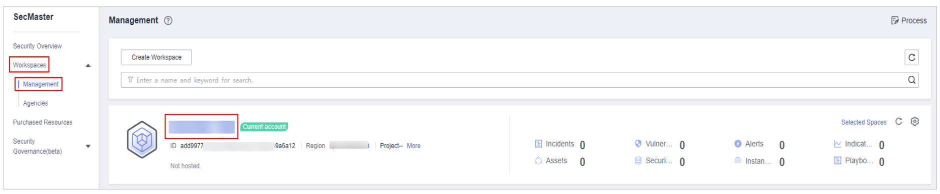
Allowing SecMaster to Access Service Logs

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

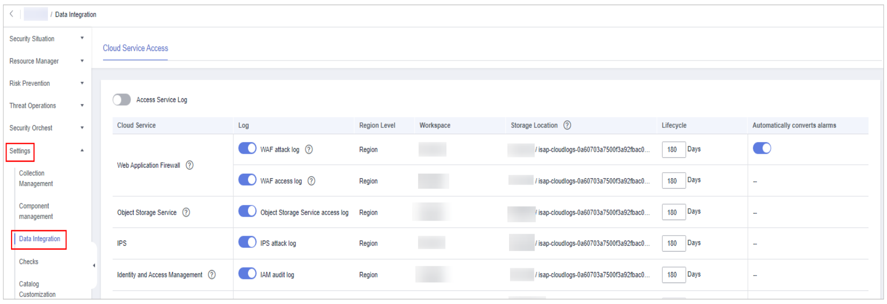
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-57 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Data Integration**.

Figure 12-58 Data Integration page



Step 5 Locate the cloud service from which you want to collect logs, click in the **Logs** column to enable log access.

To access logs of all cloud services in the current region, click on the left of **Access Service Logs**.

Step 6 Set the lifecycle.

By default, data is stored for 7 days. You can set the storage period as required.

Step 7 Set **Automatically converts alarms**.

In the **Automatically converts alarms** column of your desired cloud products, click to enable the function of automatically converting cloud service logs to alerts when the logs meet certain alert rules and displaying the alerts on the **Alerts** page.

NOTE

- If this function is disabled, logs that meet certain alert rules will not be converted to alerts or displayed on the **Alerts** page.
- You can access host vulnerability scan results on the **Vulnerabilities** page of SecMaster. If such results have been accessed during data integration but this conversion function is disabled, the results will not be displayed on the **Vulnerabilities** page.

Step 8 Click **Save**. In the displayed dialog box, click **OK**.

After the access completes, a default data space and pipeline are created.

----End

Viewing the Log Storage Location

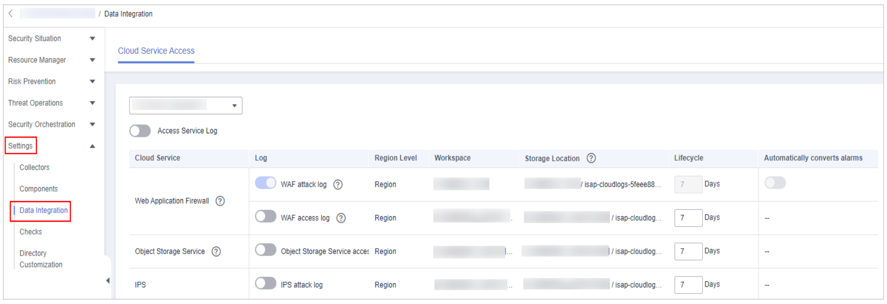
Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

Step 3 In the navigation pane on the left, choose **Settings** > **Data Integration**. On the displayed **Cloud Service Access** tab, view the log data storage location in the **Storage Location** column.

You can go to the corresponding pipeline in the target workspace to view the accessed logs.

Figure 12-59 Viewing the log storage location



----End

Related Operations

- Canceling Data Access
  a. In the **Log** column of the target cloud services, click to disable the access to cloud service logs.
  b. Click **Save**.
- Editing the Data Access Lifecycle
  a. In the **Lifecycle** column of the target cloud services, enter the data storage period.
  b. Click **Save**.
- Canceling Automatic Converting Logs to Alarms
  a. In the **Automatically converts alarms** column of the target cloud products, click to disable the alarms.
  b. Click **Save**.

12.3 Checks

Scenario

This topic describes how to create baseline check plans. To use cloud service baseline inspection, you need to create check plans first.

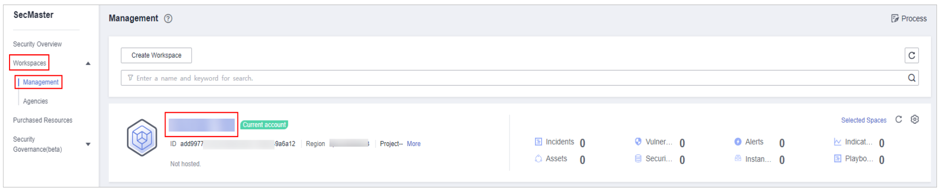
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

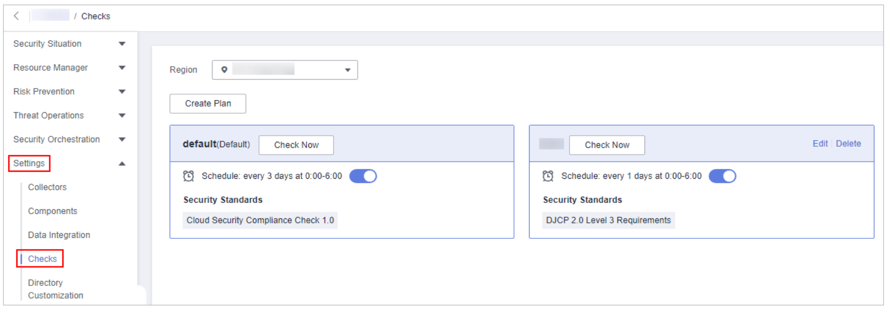
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-60 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Checks**.

Figure 12-61 Checks page



Step 5 On the **Checks** page, click **Create Plan**. The pane for creating a check plan is displayed on the right.

Step 6 Configure the check plan.

1. Enter the basic information by referring to **Table 12-18**.

Table 12-18 Basic information about a check plan

Parameter	Description
Name	Plan name
Schedule	Select how often and when the check plan is executed. – Schedule: every day, every 3 days, every 7 days, every 15 days, or every 30 days – Check start time: 00:00-06:00, 06:00-12:00, 12:00-18:00, or 18:00-24:00

2. Select a security standard for the plan.

   Select the baseline check items to be checked.

Step 7 Click **OK**.

After the check plan is created, SecMaster performs cloud service baseline scanning at the specified time. You can choose **Risk Prevention** > **Baseline Check** to view the scanning result.

----End

12.4 Customizing Directories

Scenario

You can customize directories on SecMaster. This section includes the following content:

- Viewing Existing Directories
- Changing Layout

Limitations and Constraints

- Built-in directories **cannot** be edited or deleted.

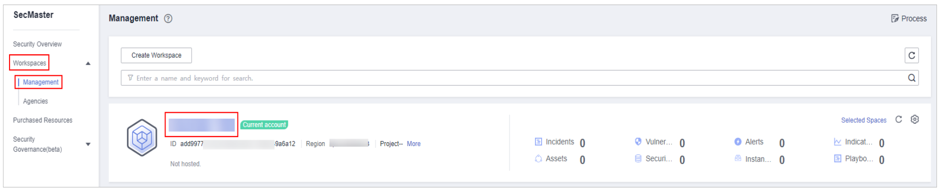
Viewing Existing Directories

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

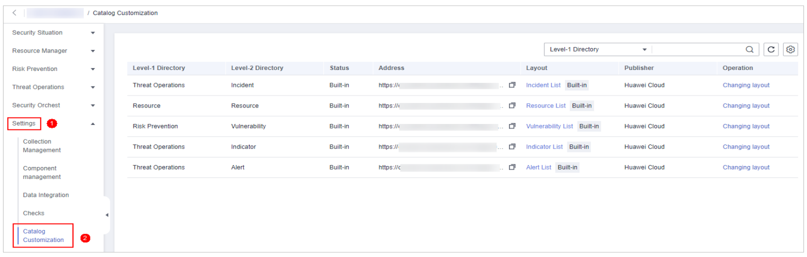
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-62 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Directory Customization**.

Figure 12-63 Directory Customization page



Step 5 In the directory list, view the directory details.

Table 12-19 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

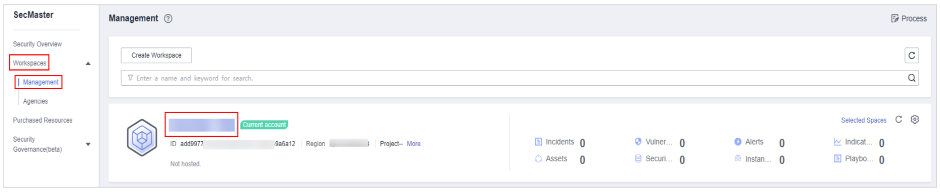
Changing Layout

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

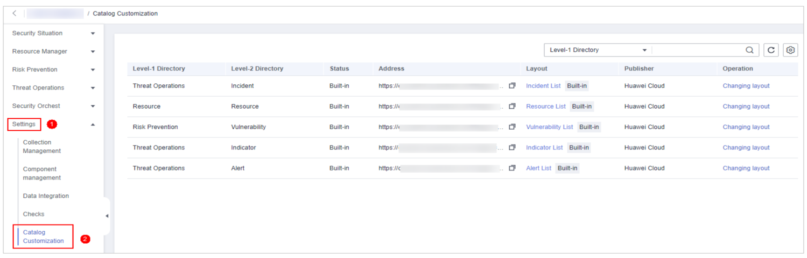
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 12-64 Workspace management page



Step 4 In the navigation pane on the left, choose **Settings** > **Directory Customization**.

Figure 12-65 Directory Customization page



Step 5 Click **Changing layout** in the **Operation** column of the target directory.

Step 6 On the **Changing layout** page, select the layout to be changed.

Step 7 Click **OK**.

----End

13 How to Use Playbooks

13.1 Overview

SecMaster automatically executes code written in playbooks to enable automatic response to alerts and incidents. While some playbooks still need some custom settings for custom data processing. Those playbooks include the ones for automatically updating alert names, reporting high-risk vulnerabilities, and reporting high-risk alerts.

This document describes how to customize settings and enable playbooks that require custom data processing.

Playbooks, Workflows, and Plug-ins

The relationships between playbooks, workflows, and plug-ins are as follows:

- A playbook is a combination of workflows. Playbooks are used for complex data processing in many ways.
- A workflow is composed of a combination of a series of plug-in nodes for complex data processing.
- A plug-in is the encapsulation of function code. It is the minimum unit of a playbook and implements specific functions.

13.2 Automatic Renaming of Alert Names

13.2.1 Overview

Scenario

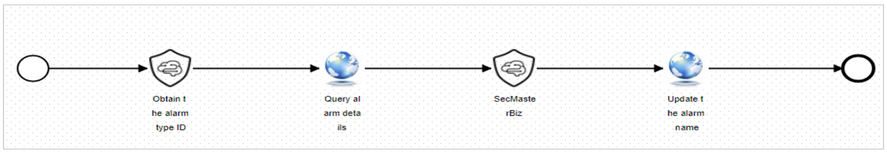
SecMaster provides a built-in playbook that can automatically rename alert names. You can customize alert names with this playbook to meet your needs.

How the Playbook Works

The **Automatic renaming of alarm names** playbook has matched the **Automatic renaming of alarm names** workflow. To configure this playbook, you need to configure the matched workflow and plug-ins the workflow uses.

The **Automatic renaming of alarm names** workflow has four plug-in nodes, one for obtaining alert type IDs, one for obtaining alert details, the SecMasterBiz node, and one for updating alert names. In this workflow, you only need to configure the SecMasterBiz node. This node is used to customize alert names.

Figure 13-1 Automatic renaming of alarm names workflow



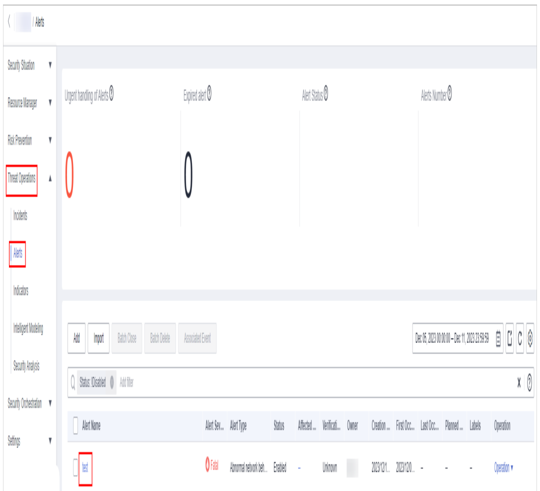
Limitations and Constraints

Currently, only names for web shell attack alerts can be modified.

Verification

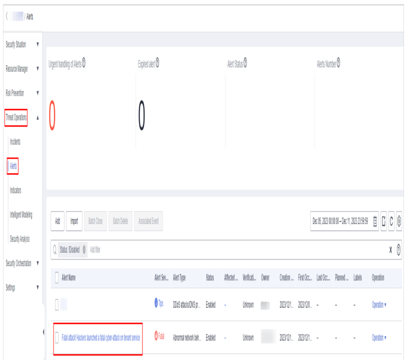
The following figure shows default alert names.

Figure 13-2 Before processing



The following figure shows customized alert names.

Figure 13-3 After processing



13.2.2 Configuring and Enabling the Playbook

Scenario

This topic walks you through on how to configure the SecMasterBiz node, enable the automatic renaming of alert name workflow, and enable the automatic renaming of alert name playbook.

Step 1: Configure and Enable the Workflow

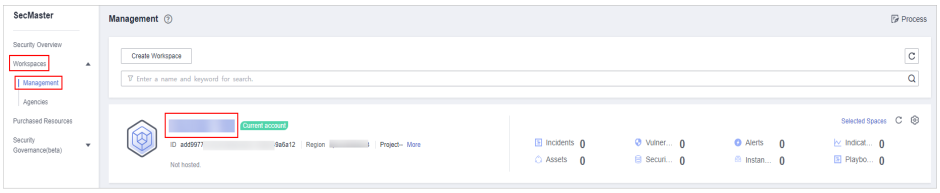
Accessing the workflow management page

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

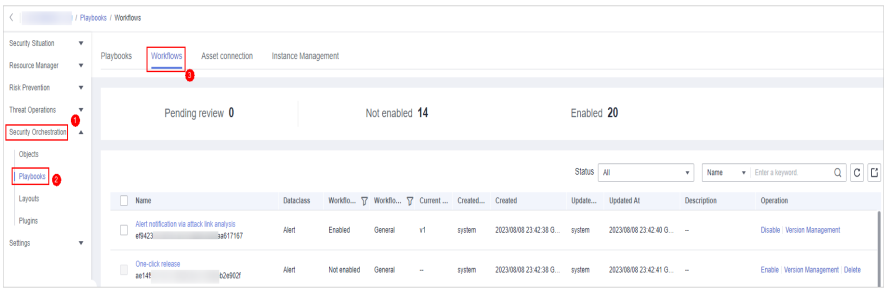
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-4 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**. Click **Workflows**.

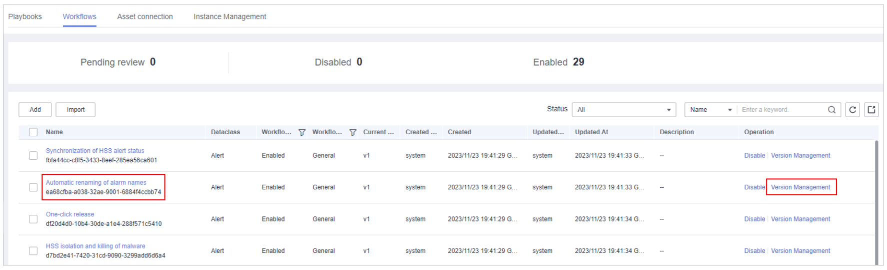
Figure 13-5 Workflows tab page



Copying a workflow version

Step 5 Locate the row containing the **Automatic renaming of alarm names** workflow. In the **Operation** column, click **Version Management**.

Figure 13-6 Version Management page



Step 6 On the **Version Management** page displayed, go to the **Version Information** area, locate the row where the initial version (v1) is listed, and click **Clone** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.

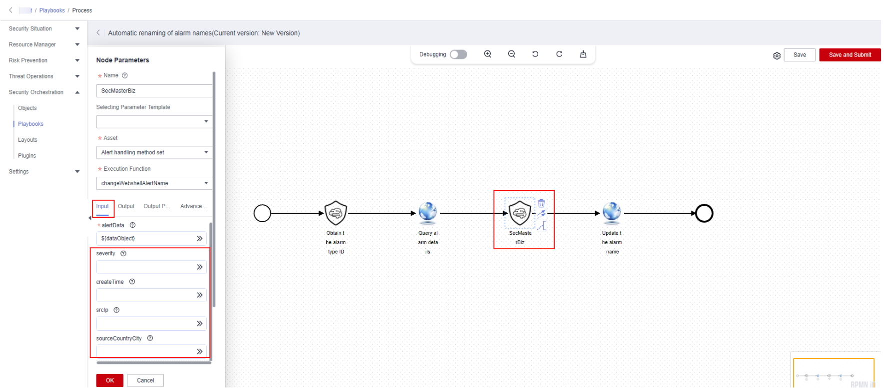
Editing and submitting a workflow version

Step 8 On the **Version Management** slide-out panel for the **Automatic renaming of alarm names** workflow, go to the **Version Information** area, locate the row containing the copied workflow version, and click **Edit** in the **Operation** column.

Step 9 On the drawing page, click the **SecMasterBiz** plug-in and configure it in the **Node Parameters** pane displayed from the right.

For details about SecMasterBiz plug-in parameters, see **What Is SecMasterBiz**.

Figure 13-7 SecMasterBiz plug-in



Step 10 After the configuration is complete, click **Save and Submit** in the upper right corner. In the dialog box displayed, click **OK**.

Reviewing a workflow version

Step 11 On the **Workflows** page, locate the **Automatic renaming of alarm names** workflow and click **Version Management** in the **Operation** column.

Step 12 On the displayed **Version Management** page, locate the row that contains the edited workflow version, and click **Review** in the **Operation** column.

Step 13 In the displayed dialog box, set **Comment** to **Passed** and click **OK**.

Activating a workflow version

Step 14 On the **Version Management** page, locate the row that contains the reviewed workflow version and click **Activate** in the **Operation** column.

Step 15 In the displayed dialog box, click **OK**.

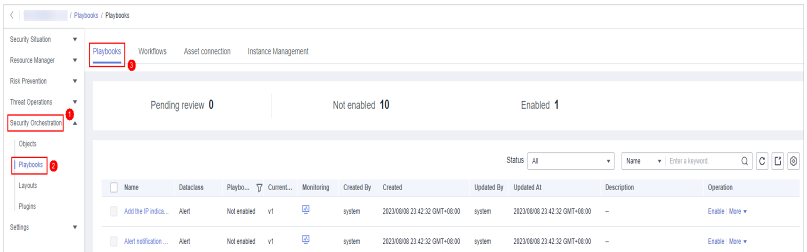
After a workflow version is activated, the workflow is enabled by default.

----End

Step 2: Configure and Enable the Playbook

Step 1 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-8 Accessing the Playbooks tab



Step 2 On the **Playbooks**, locate the row that contains the playbook for automatically renaming alert names, and click **Enable** in the **Operation** column.

Step 3 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

What Is SecMasterBiz

SecMasterBiz is a plug-in used in the workflow for automatically renaming alert names. It analyzes and processes web shell alert names. You can combine alert names in the way you want and let the system return the alert names as you configured.

The SecMasterBiz plug-in contains multiple actions. The **changeWebshellAlertName** action provides several input parameters for you to customize. Each input parameter indicates an analysis dimension.

You can select different dimension parameters as required to combine alert names. If a parameter is not selected, then it will not be returned in alert names by default. If you enter **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 13-1 Parameter configuration

Parameter	Description	Value Range
severity	Indicates the alert severity.	y/n

Parameter	Description	Value Range
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

13.2.3 Verifying the Playbook

Scenario

If the playbook for **Automatic renaming of alarm names** is enabled, you can verify the playbook status.

This topic describes how to verify a playbook.

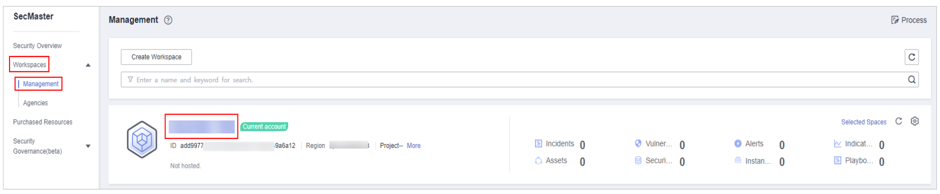
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

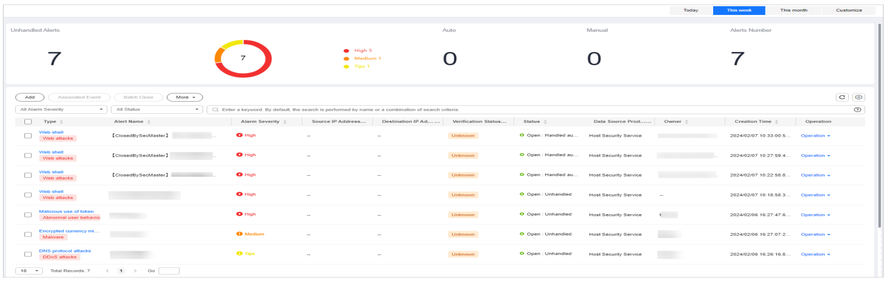
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-9 Workspace management page



Step 4 In the navigation pane on the left, choose **Threat Operations** > **Alerts**.

Figure 13-10 Alerts



Step 5 Click **Add**. Configure parameters in the **Add** slide-out panel.

- **Alert Name**: Enter a name for the alert.
- **Alert Type**: Select **Web attacks** and then **Web shell**.
- **Debugging data**: Select **Yes**.
- **Description**: Description of the custom alert.
- Retain the default values for other parameters.

Step 6 Click **OK**.

Step 7 Refresh the page and check whether alert names have been updated.

If the playbook is enabled, the playbook automatically processes new alerts and displays new alert names.

Figure 13-11 Output when no parameters are selected (default)

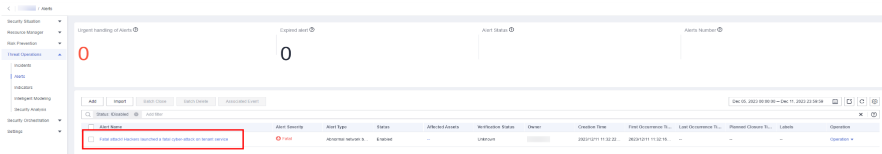
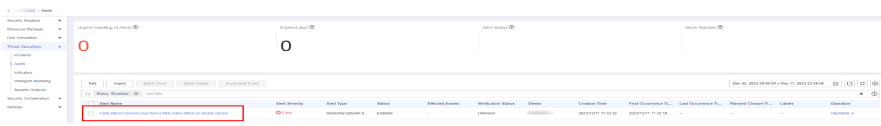


Figure 13-12 Output when only severity is selected



----End

13.3 Attack Link Analysis Alert Notification

13.3.1 Overview

Scenario

After a domain name was attacked, the attacker typically further attacked the backend servers. SecMaster provides an attack link analysis playbook that will automatically send alert notifications to specified operations personnel once it detects server attacks.

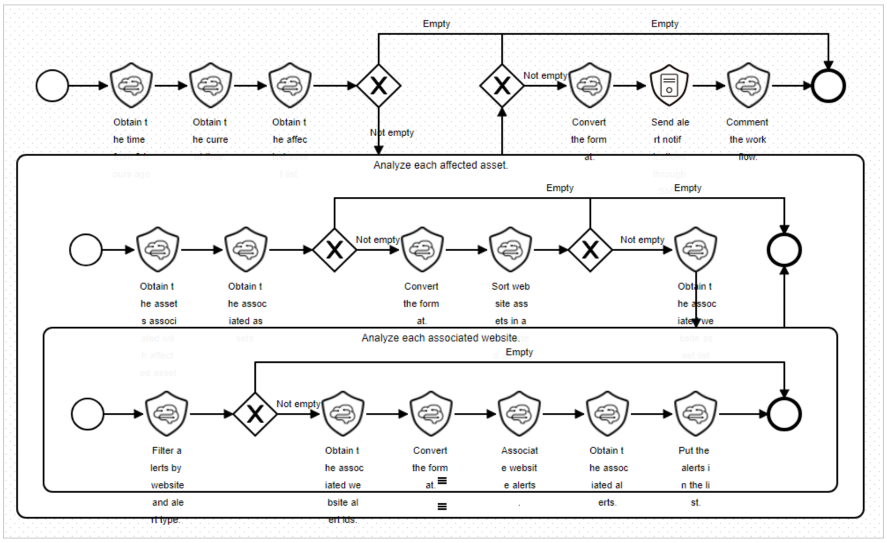
How the Playbook Works

The **Attack link analysis alert notification** playbook has been matched the **Attack link analysis alert notification** workflow. This workflow needs to use Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.

The **Attack link analysis alert notification** workflow queries the list of website assets associated with the assets affected by HSS alerts through asset associations. By default, a maximum of 3 website assets can be queried.

- If there are associated website assets, the workflow queries WAF alerts generated for each website asset from 3 hours ago to the current time. A maximum of 3 alerts can be queried. The alert types include XSS, SQL injection, command injection, local file inclusion, remote file inclusion, web shell, and vulnerability exploits.
- If there is an alert generated in WAF, the workflow associates the WAF alert with the corresponding HSS alert and sends a notification the email box you specified through SMN.

Figure 13-13 Attack link analysis alert notification

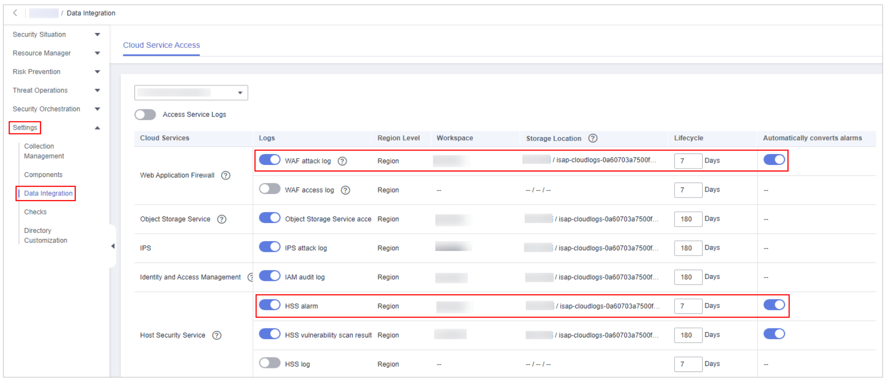


Prerequisites

- You have enabled HSS and WAF alert access in SecMaster on the **Data Integration** page under the **Settings** pane in the current workspace.

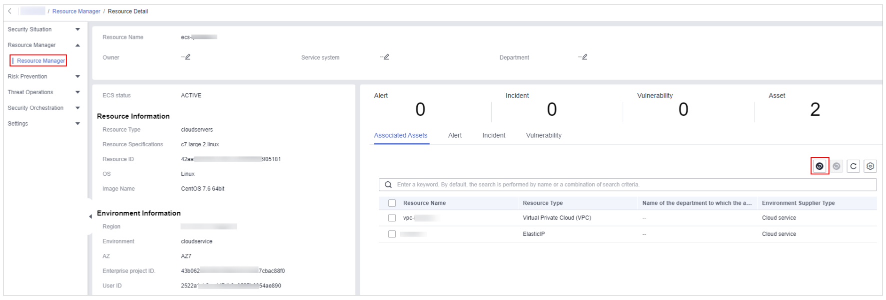
  For details about how to enable HSS and WAF alert access in SecMaster, see **Data Integration**.

Figure 13-14 Alert access



- On the **Resource Manager** page in the current SecMaster workspace, click an asset name. On the asset details page displayed, associate the website asset with the server asset.

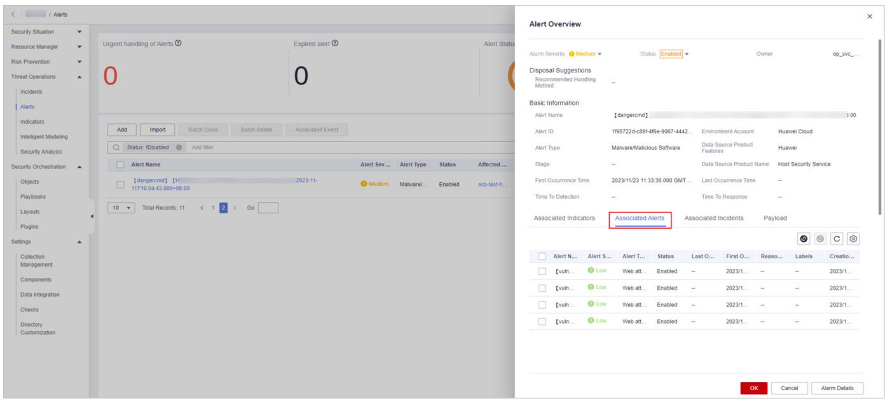
Figure 13-15 Associated Assets



Verification

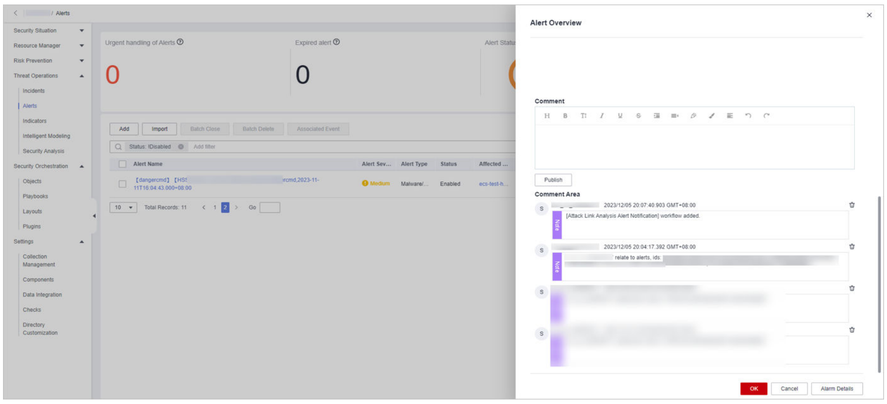
After the attack link analysis notification playbook is executed, server assets and the website assets will be associated based on corresponding HSS and WAF alerts.

Figure 13-16 Associated alerts



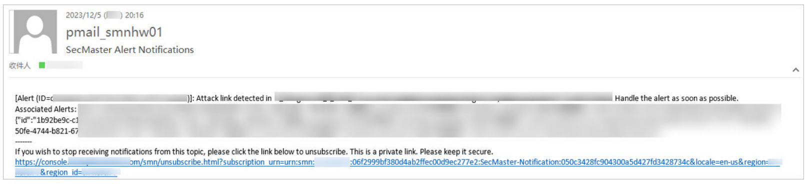
Comments on the corresponding alert added to the playbook

Figure 13-17 Comment



Alert notification email sent to specified personnel

Figure 13-18 Email notifications



13.3.2 Creating and Subscribing to a Topic

Scenario

The **Attack link analysis alert notification** workflow needs to use Simple Message Notification (SMN) to create and subscribe to a notification topic.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

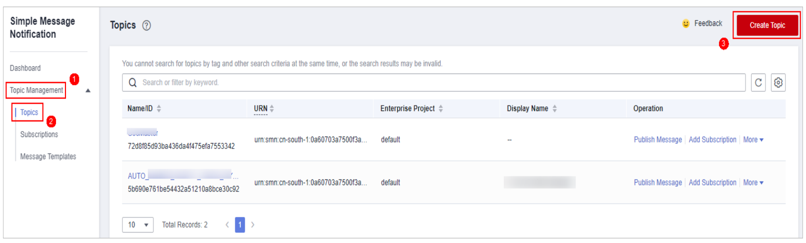
Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, click and choose **Management and Governance** > **Simple Message Notification**.

Step 3 Create a topic.

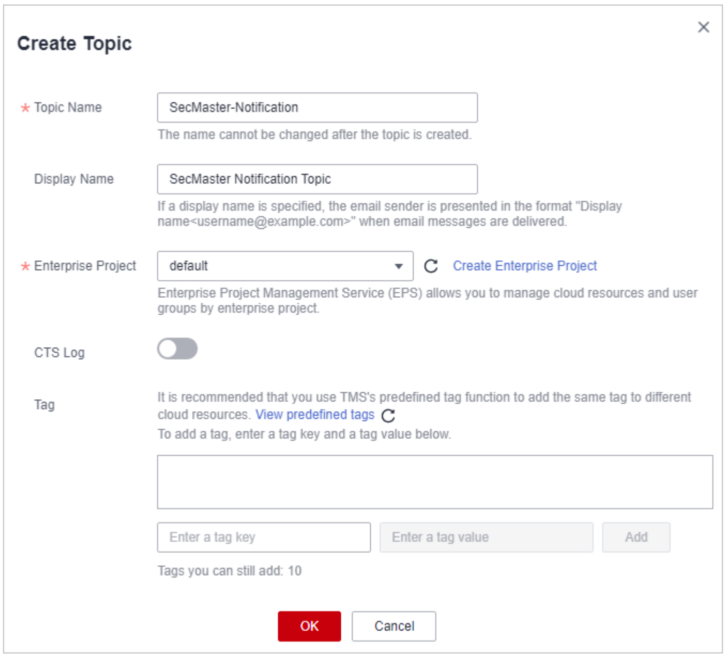
1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

Figure 13-19 Create Topic



2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.
   - **Topic Name**: **SecMaster-Notification** is recommended.
   - **Display Name**: **SecMaster notification topic** is recommended.
   - Retain the default values for other parameters.

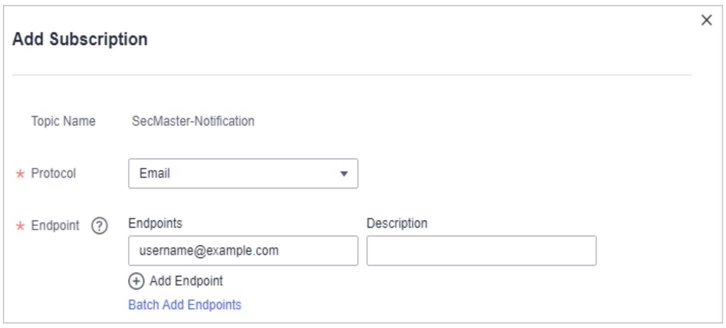
Figure 13-20 Configuring a topic



Step 4 Add a subscription.

1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
   - **Protocol**: Select **Email**.
   - **Endpoint**: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-21 Add Subscription



----End

13.3.3 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Attack link analysis alert notification** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **attack link analysis alarm notification** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Attack link analysis alert notification** playbook.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

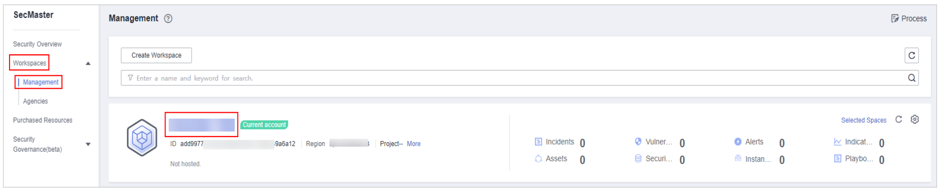
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

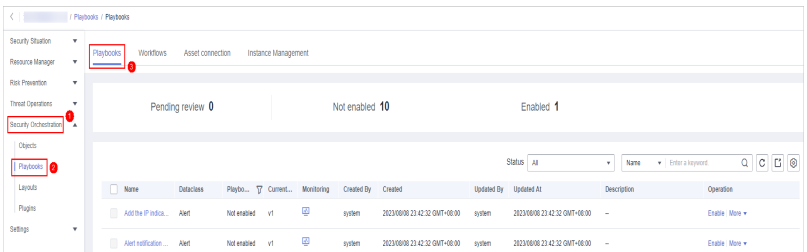
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-22 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-23 Accessing the Playbooks tab



Step 5 On the **Playbooks** page, locate the row that contains the **Attack link analysis alert notification** playbook and click **Enable** in the **Operation** column.

Step 6 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.4 Automatic Notification of High-Risk Vulnerabilities

13.4.1 Overview

Scenario

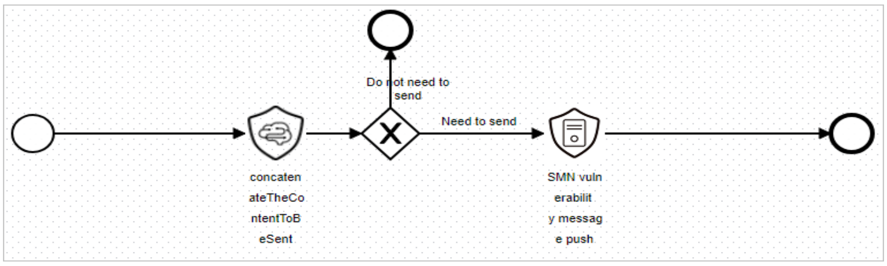
SecMaster provides a playbook that can automatically notify of high-risk server vulnerabilities to operations personnel.

How the Playbook Works

The **Automatic notification of high-risk vulnerabilities** playbook has been matched the **Automatic notification of high-risk vulnerabilities** workflow. This workflow needs to use Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.

If a high-risk vulnerability was reported by HSS, SMN sends a notification to operations personnel.

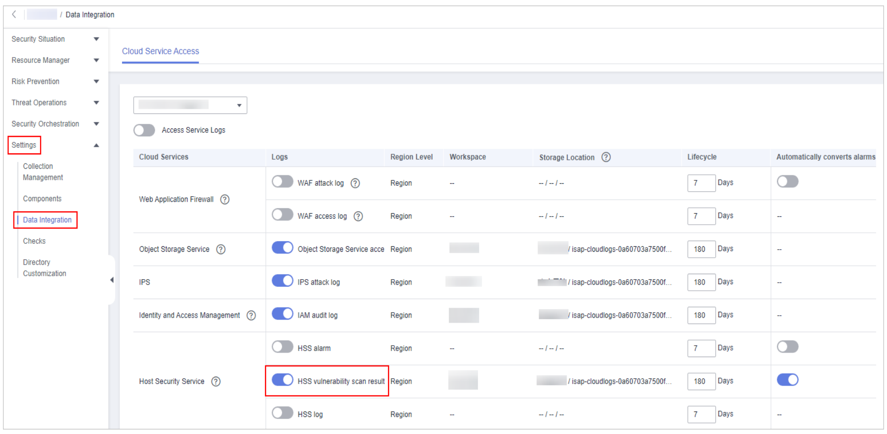
Figure 13-24 Automatic notification of high-risk vulnerabilities workflow



Prerequisites

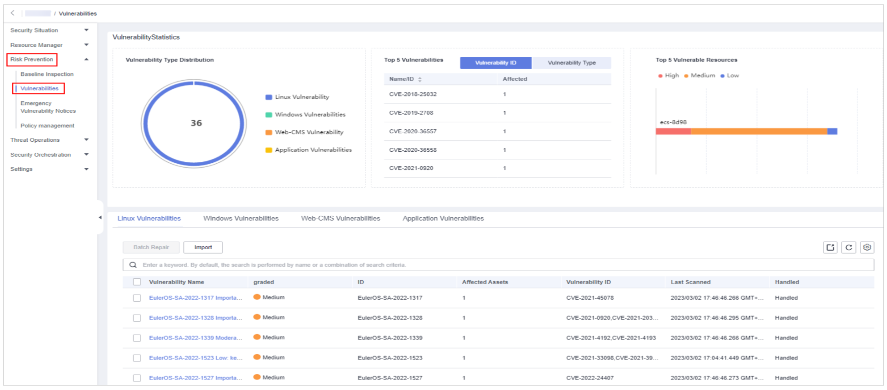
You have enabled Host Security Service (HSS) alarm access on the **Data Integration** page under the **Settings** pane. For details, see **Data Integration**.

Figure 13-25 Accessing HSS alerts



To view accessed data, choose **Risk Prevention** > **Vulnerabilities**.

Figure 13-26 Viewing alerts



13.4.2 Creating and Subscribing to a Topic

Scenario

The **Automatic notification of high-risk vulnerabilities** workflow uses Simple Message Notification (SMN) to send notifications. You need to create and subscribe to a topic for receiving notifications.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

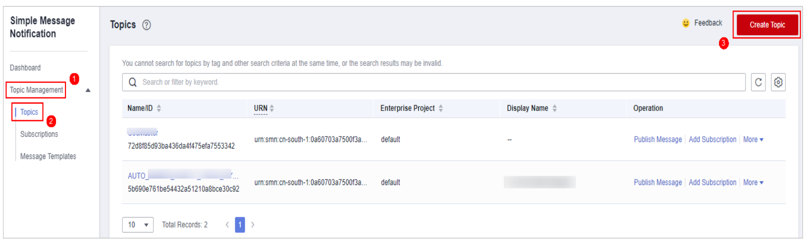
Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, click and choose **Management and Governance** > **Simple Message Notification**.

Step 3 Create a topic.

1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

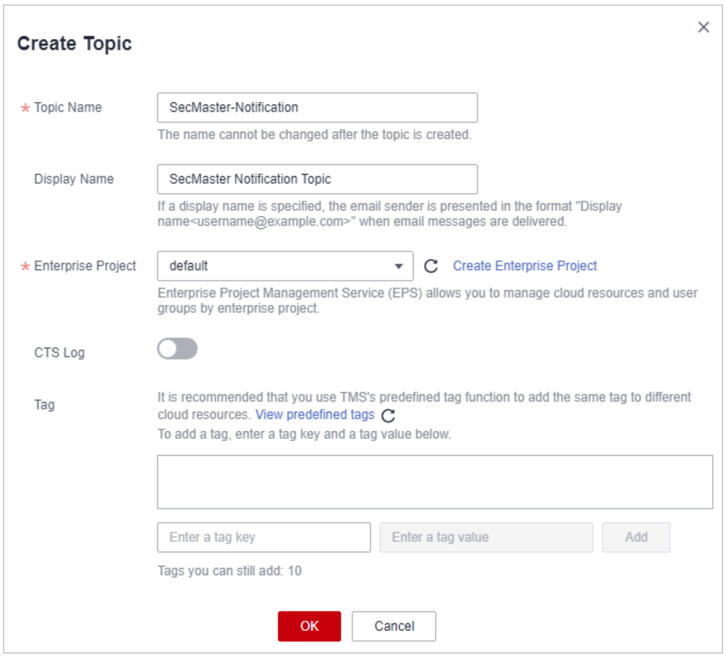
Figure 13-27 Create Topic



2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.
   – **Topic Name**: **SecMaster-Notification** is recommended.
   – **Display Name**: **SecMaster notification topic** is recommended.

– Retain the default values for other parameters.

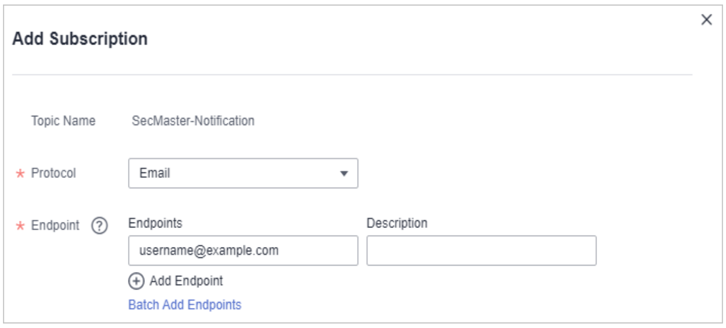
Figure 13-28 Configuring a topic



Step 4 Add a subscription.

1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
   – **Protocol**: Select **Email**.
   – **Endpoint**: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-29 Add Subscription



----End

13.4.3 Configuring an Asset Connection

Scenario

Before using the **Automatic notification of high-risk vulnerabilities** workflow, you need to configure the **SMN notification token for operational personnel** asset connection first.

This topic describes how to configure an asset connection.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

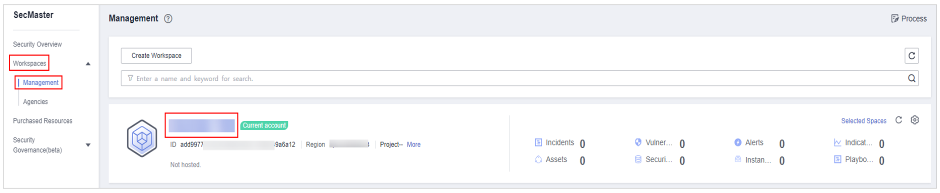
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

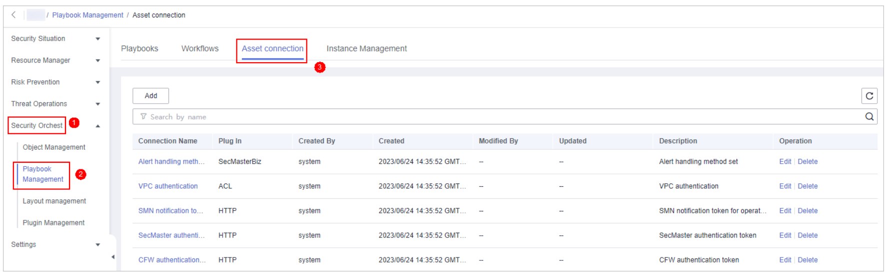
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-30 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

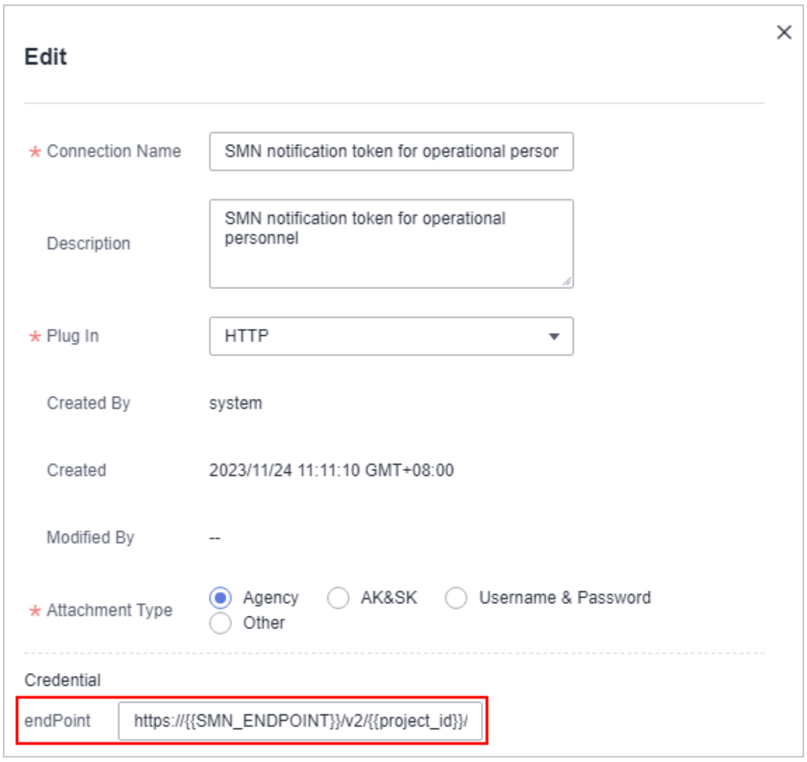
Figure 13-31 Asset connection tab



Step 5 On the **Asset connection** page, locate the row that contains the **SMN notification token for operational personnel** connection and click **Edit** in the **Operation** column.

Step 6 On the **Edit** pane sliding out from the right, configure endpoint information.

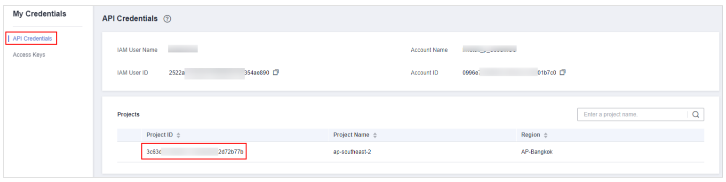
Figure 13-32 Editing an asset connection



endPoint: Set this field to **https://***{{SMN_ENDPOINT}}***/ v2 /***{{project_id}}***/ notifications/topics/***urn:smn:{{region_id}}:{{project_id}}:SecMaster-Notification*.

- *SMN_ENDPOINT*: Enter the domain name for invoking the SMN service. The value is in the format of **endpoint:443**. Obtain the endpoint information from the **Regions and Endpoints**. For example, if you choose **CN North-Beijing4**, enter "smn.cn-north-4.myhuaweicloud.com:443" in this field.
- *project_id*: Enter the ID of the project that the current workspace belongs to. To view the project ID, take the following steps:
  a. Log in to the management console, hover the mouse over the username in the upper right corner, and select **My Credentials** from the drop-down list. The **API Credentials** page is displayed by default.
  b. On the **API Credentials** page, view the project ID in the project list.

  Figure 13-33 Project ID

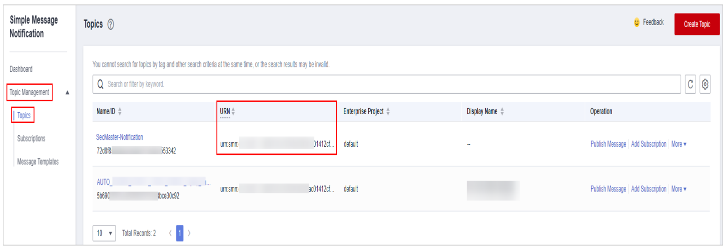
  

- *urn:smn:{{region_id}}:{{project_id}}:SecMaster-Notification*: Enter the URN of the SMN topic for sending email notifications. To view the URN, take the following steps:
  a. In the upper left corner of the page, click ☰ and choose **Management and Governance** > **Simple Message Notification**.

b. In the navigation pane on the left, choose **Topic Management** > **Topics**.

c. In the topic list, view the topic URN of the topic created in **Creating and Subscribing to a Topic**.

Figure 13-34 Topic URN



Step 7 After the configuration, click **OK**.

----End

13.4.4 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Automatic notification of high-risk vulnerabilities** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Automatic notification of high-risk vulnerabilities** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Automatic notification of high-risk vulnerabilities** playbook.

Prerequisites

- You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.
- Asset connections have been configured. For details, see **Configuring an Asset Connection**.

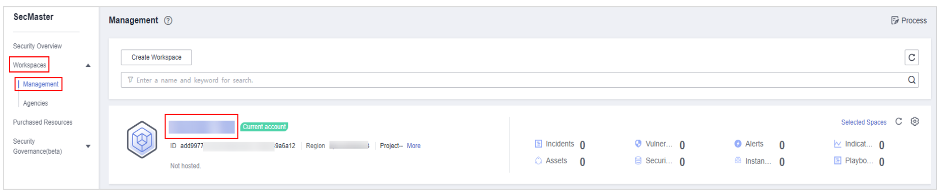
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

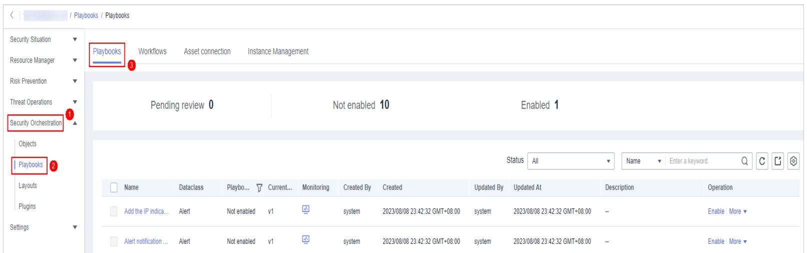
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-35 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-36 Accessing the Playbooks tab



Step 5 On the **Playbooks** page, locate the row that contains the **Automatic notification of high-risk vulnerabilities** playbook and click **Enable** in the **Operation** column.

Step 6 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.5 Automatic Notification of High-Risk Alerts

13.5.1 Overview

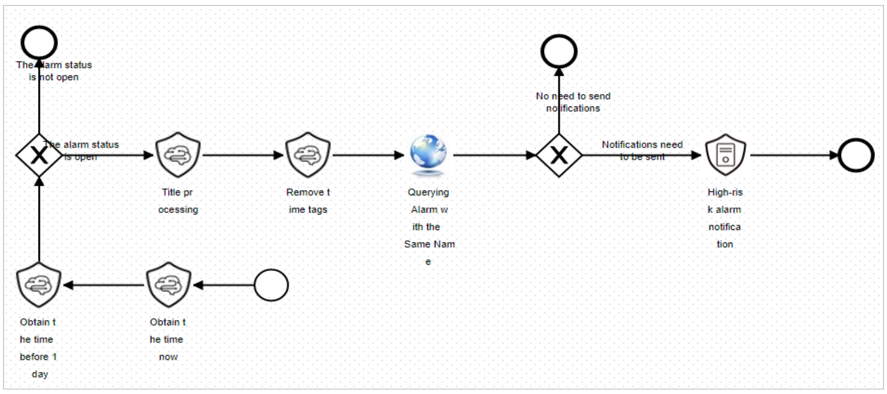
Scenario

SecMaster provides this playbook for automatically notifying you of new high-risk alerts after removing repeated ones.

How the Playbook Works

The **Automatic notification of high-risk alerts** playbook has been matched the **Automatic notification of high-risk alerts** workflow. This workflow uses Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.

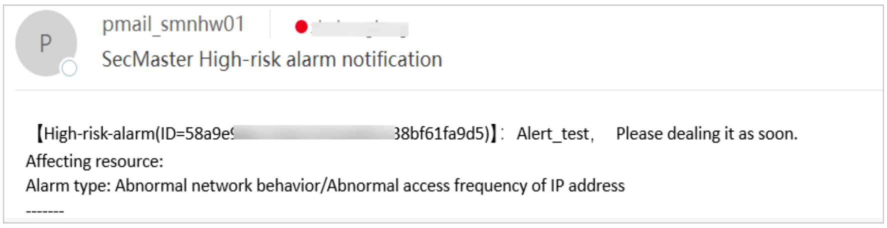
Figure 13-37 Automatic notification of high-risk alerts workflow



Verification

Email sent when the playbook was triggered by high-risk alerts

Figure 13-38 Alert notification email



13.5.2 Creating and Subscribing to a Topic

Scenario

The **Automatic notification of high-risk alerts** workflow uses Simple Message Notification (SMN) to send notifications. You need to create and subscribe to a topic for receiving notifications.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

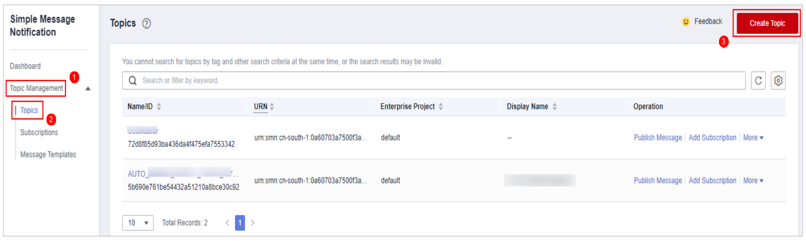
Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, click ☰ and choose **Management and Governance** > **Simple Message Notification**.

Step 3 Create a topic.

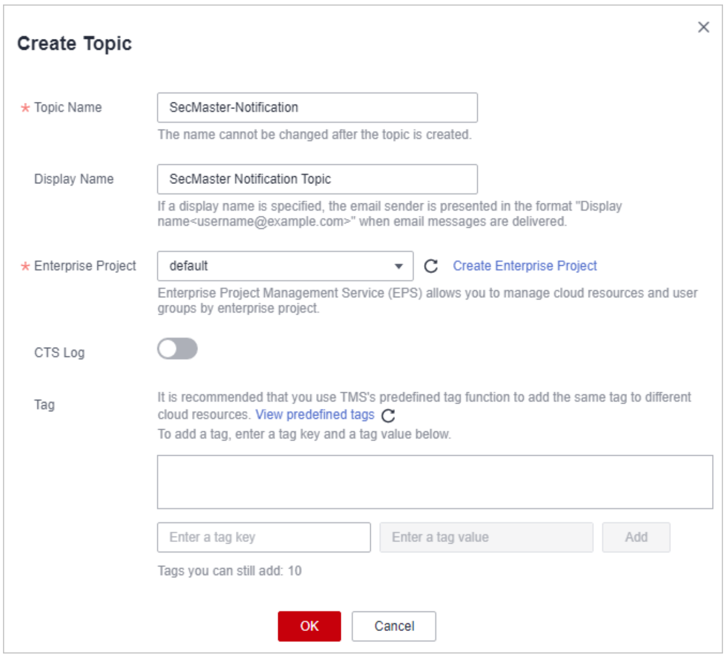
1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

   Figure 13-39 Create Topic

2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.
   - **Topic Name**: **SecMaster-Notification** is recommended.
   - **Display Name**: **SecMaster notification topic** is recommended.
   - Retain the default values for other parameters.

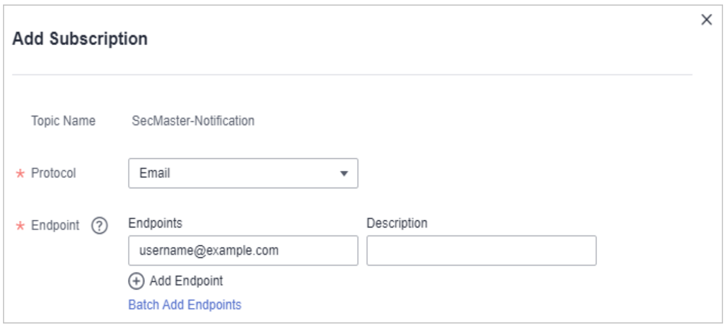
Figure 13-40 Configuring a topic



Step 4 Add a subscription.

1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
   – **Protocol**: Select **Email**.
   – **Endpoint**: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-41 Add Subscription



----End

13.5.3 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Automatic notification of high-risk alerts** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Automatic notification of high-risk alerts** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Automatic notification of high-risk alerts** playbook.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

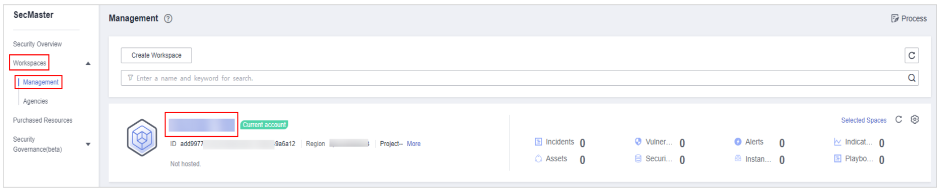
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

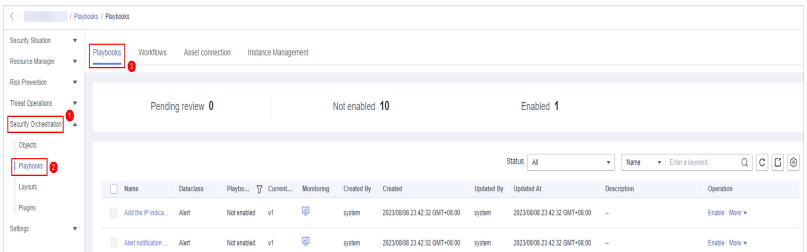
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-42 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-43 Accessing the Playbooks tab



Step 5 On the **Playbooks** page, locate the row that contains the **Automatic notification of high-risk alerts** playbook and click **Enable** in the **Operation** column.

Step 6 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.6 Automatic Security Blocking of WAF Attacks

13.6.1 Overview

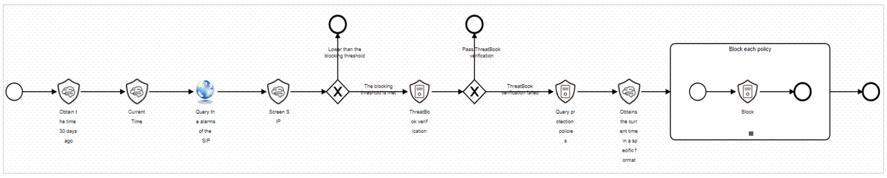
Scenario

SecMaster provides this built-in playbook to automatically blacklist source IP addresses reported in high-risk alerts in WAF.

How the Playbook Works

The **Automatic security blocking of WAF attacks** playbook has matched the **Automatic security blocking of WAF attacks** workflow.

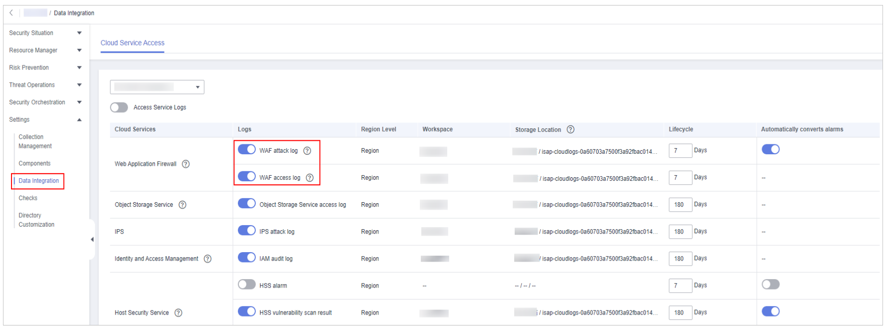
Figure 13-44 Automatic security blocking of WAF attacks



Prerequisites

- You have enabled WAF access logs or WAF attack logs on the **Data Integration** page under **Settings** in the current workspace. For details, see **Data Integration**.

  Figure 13-45 Enabling Access to WAF logs

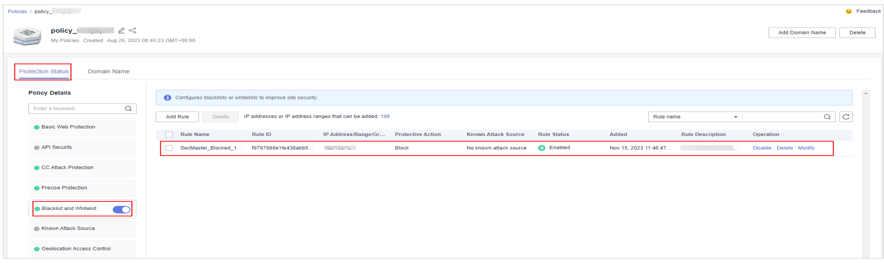
- The ThreatBook quota is sufficient.

Verification

If the IP address is blocked, the IP address should be included in the WAF blacklist. The procedure is as follows:

1. Log in to the WAF console, go to the **Policies** page, and click the name of the target protection policy.
2. On the protection policy details page, click **Blacklist and Whitelist** in the **Protection Details** area. You can see that the IP address is listed in the WAF blacklist.

Figure 13-46 Blacklist and Whitelist



13.6.2 Configuring an Asset Connection

Scenario

Before using **Automatic security blocking of WAF attacks** workflow, you need to configure the API key of the ThreatBook plug-in used for the workflow. You can obtain it in the **threatbook authentication token** asset connection.

This topic describes how to configure an asset connection.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

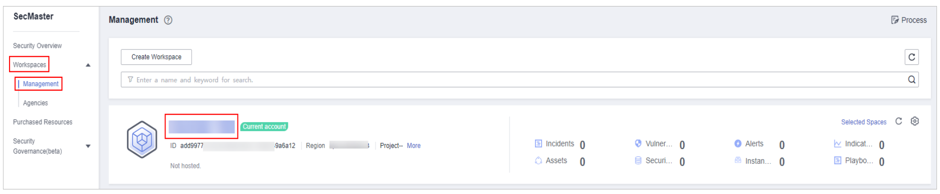
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

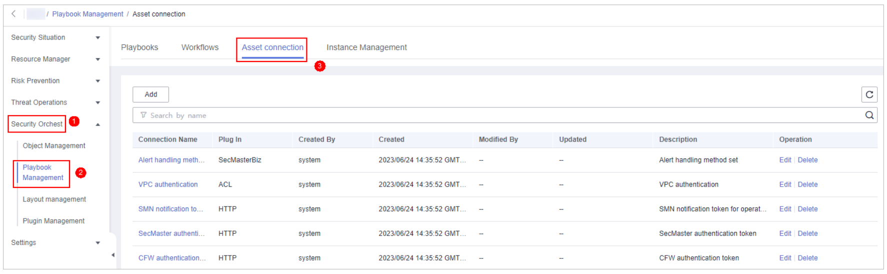
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-47 Workspace management page



Step 4 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 13-48 Asset connection tab

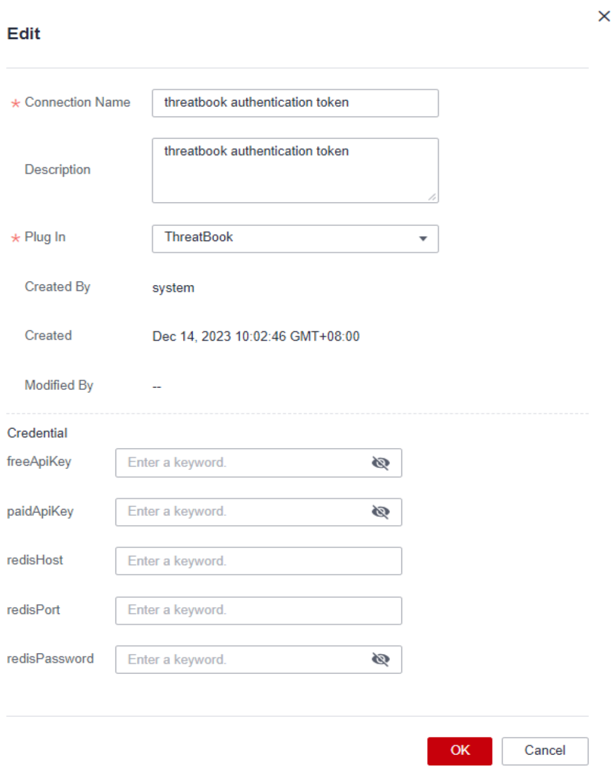


Step 5 On the **Asset connection** page, locate the row that contains the **threatbook authentication token** asset connection and click **Edit** in the **Operation** column.

Step 6 On the **Edit** pane sliding out from the right, configure the token.

- **freeApiKey** or **payApiKey**: Set either of them. The value can be obtained after you buy ThreatBook quota.
- **redisHost**: IP address of your Redis resources. If there are no IP addresses, leave this parameter blank.
- **redisPort**: Port of your Redis resources. If there are no such ports, leave this parameter blank.
- **redisPassword**: Passwords of your Redis resources. If there are no such passwords, leave this parameter blank.

Figure 13-49 Edit credential information



Step 7 After the configuration, click **OK**.

----End

13.6.3 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Automatic security blocking of WAF attacks** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Automatic security blocking of WAF attacks** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Automatic security blocking of WAF attacks** playbook.

Prerequisites

Asset connections have been configured. For details, see **Configuring an Asset Connection**.

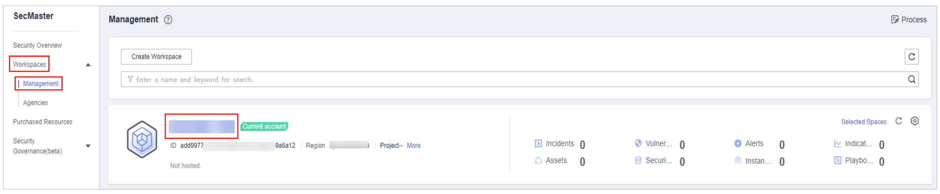
Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

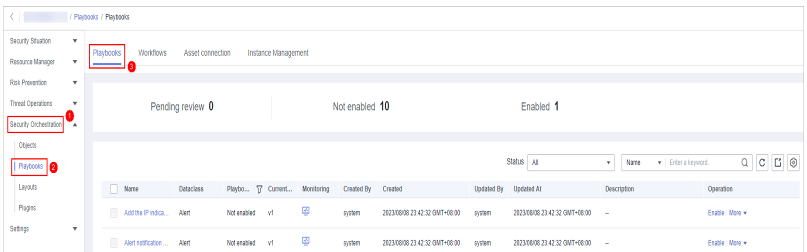
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-50 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-51 Accessing the Playbooks tab



Step 5 On the **Playbooks** page, locate the row that contains the **Automatic security blocking of WAF attacks** playbook and click **Enable** in the **Operation** column.

Step 6 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

13.7 HSS Isolation and Killing of Malware

13.7.1 Overview

Scenario

SecMaster provides this built-in playbook based on HSS to isolate and kill malware automatically.

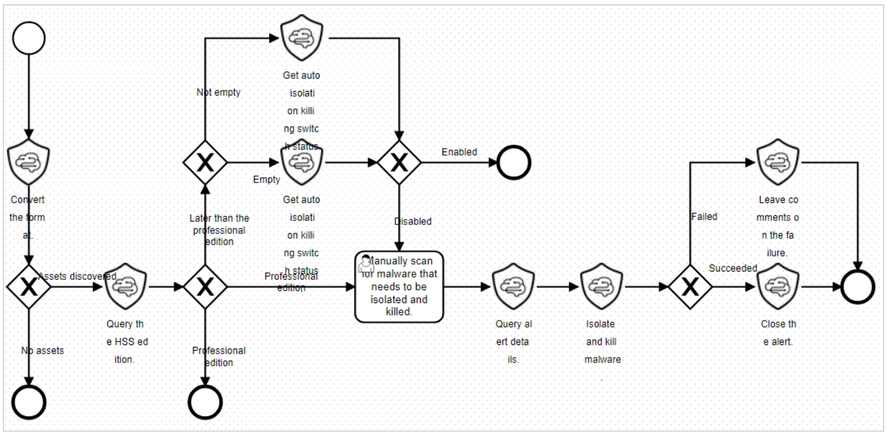
How the Playbook Works

The **HSS isolation and killing of malware** playbook has matched the **HSS isolation and killing of malware** workflow.

The **HSS isolation and killing of malware** workflow uses HSS to isolate and kill malware ransomware alerts.

If you are using the HSS professional edition or above to protect assets but have not enabled automatic isolation and killing of malware, manually review is required. If you agree to isolate or kill the infected file, HSS alerts will be generated. The alert is cleared when the malware has been isolated and killed. If the malware is not isolated, a comment on manual handling details will be left.

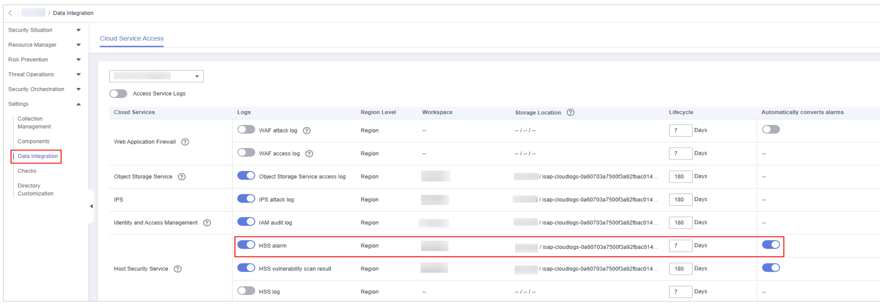
Figure 13-52 HSS isolation and killing of malware workflow



Prerequisites

You have enabled HSS access logs on **Data Integration** page under **Settings** in the current workspace. For details, see **Data Integration**.

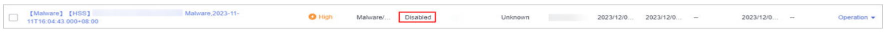
Figure 13-53 Accessing HSS alerts



Verification

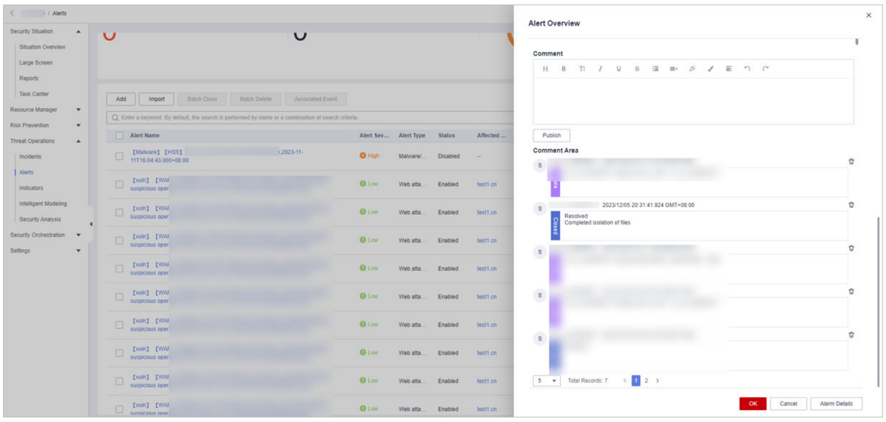
- The malware has been killed and the alert is closed automatically.

  Figure 13-54 Alerts automatically cleared

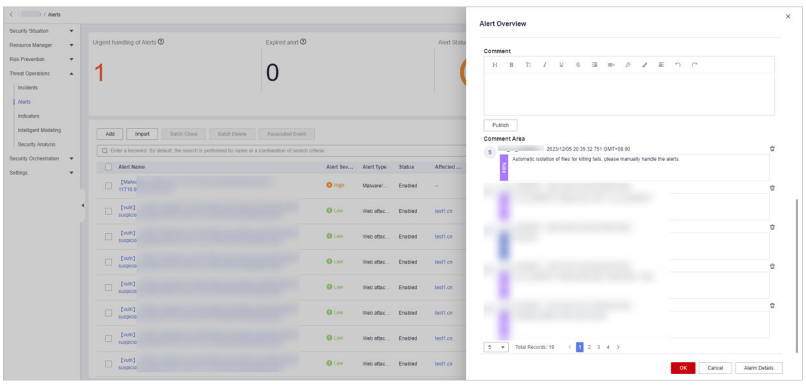
- If the malware is isolated and killed, a comment will be left indicating that the alert has been cleared.

  Figure 13-55 Comment on succeeded isolation and killing of malware

- If the malware fails to be isolated or killed, a comment will be left indicating that manual handling is required.

  Figure 13-56 Comment on failed isolation and killing of malware

13.7.2 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **HSS isolation and killing of malware** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **HSS isolation and killing of malware** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **HSS isolation and killing of malware** playbook.

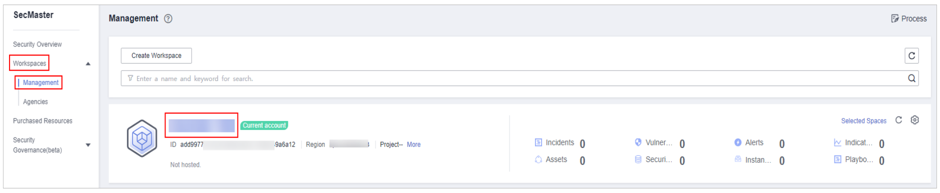
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

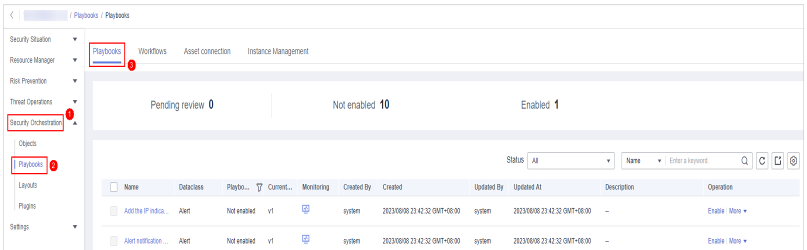
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-57 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-58 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

13.8 Real-time Notification of Critical Organization and Management Operations

13.8.1 Overview

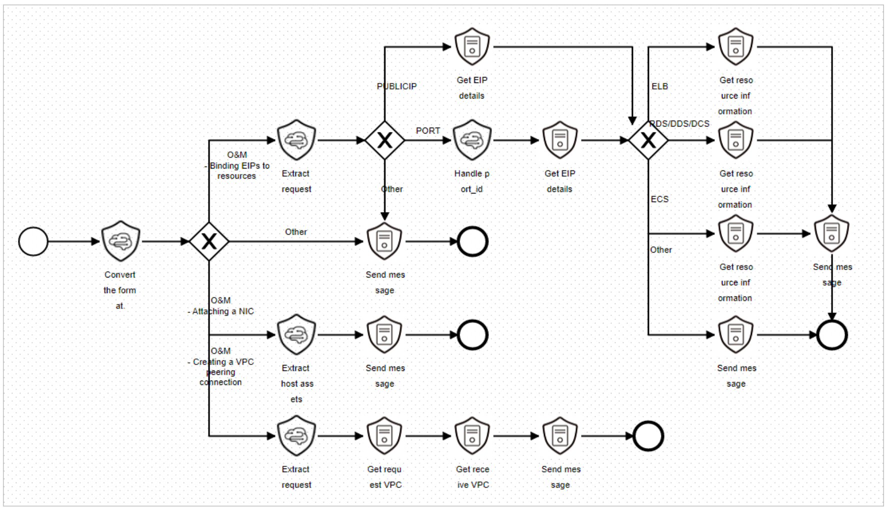
Scenario

SecMaster provides this playbook for real-time notification of key O&M operations. Based on O&M operations, SecMaster notifies you of key O&M operations by email in real time.

How the Playbook Works

The **Real-time notification of critical Organization and Management operations** playbook has matched the **Real-time notification of critical Organization and Management operations** workflow. This workflow uses Simple Message Notification (SMN) to send notifications. So you need to create and subscribe to a notification topic in SMN.

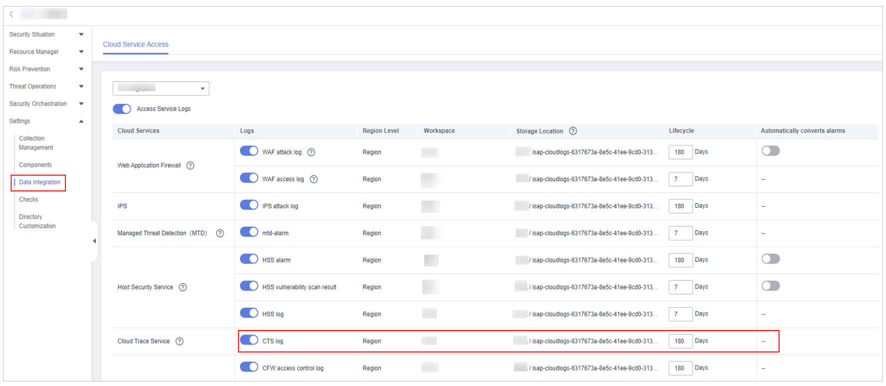
Figure 13-59 Real-time notification of critical Organization and Management operations workflow



Prerequisites

- You have enabled CTS logs on the **Data Integration** page under **Settings** in the current workspace. For details, see **Data Integration**.

Figure 13-60 Access to CTS logs

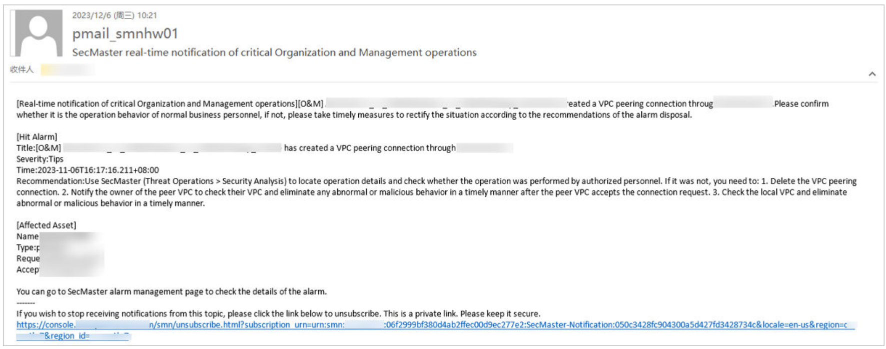


- The corresponding O&M defense model has been enabled. For details, see **Enabling an Alert Model**.

Verification

When a key O&M operation is performed, this playbook is triggered. The playbook will send an email notification as configured. The following is an example.

Figure 13-61 Operation notifications



13.8.2 Enabling an Alert Model

Scenario

Before using **Real-time notification of critical Organization and Management operations** playbook, you need to enable some alert models, including the ones for O&M - Attaching NICs, O&M - Creating VPC peering connections, and O&M-Binding EIPs to resources.

This topic describes how to enable an alert model.

Procedure

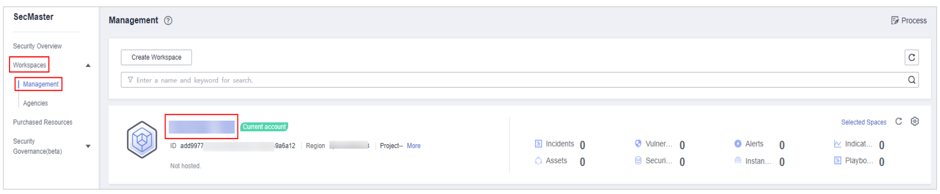
Creating an alert model

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

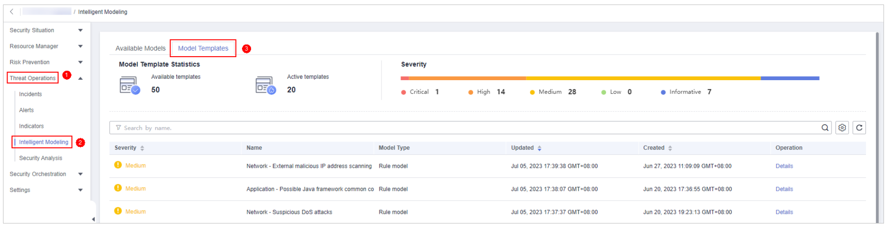
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-62 Workspace management page



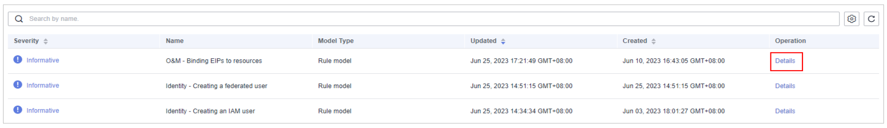
Step 4 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**. On the displayed page, click the **Model Templates** tab.

Figure 13-63 Model Templates tab



Step 5 In the model template list, click **Details** in the **Operation** column of the target model template. The template details page is displayed on the right.

Figure 13-64 Template details



Step 6 On the details page, click **Create Model** in the lower right corner. The page for creating an alert model is displayed.

Step 7 On the **Create Alert Model** page, configure basic information.

- **Pipeline Name**: Select an execution pipeline for the alert model.

Table 13-2 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 of other parameters.

Step 8 After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

Step 9 Set the model logic. You are advised to retain the default value.

Step 10 After completing the basic settings, click **Next** in the lower right corner of the page.

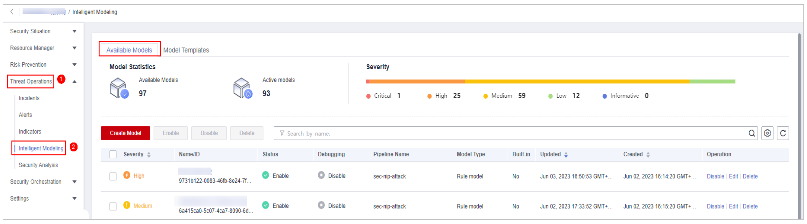
Step 11 After confirming that the model is correct, click **OK** in the lower right corner of the page.

Step 12 Repeat **Step 5** to **Step 11** to create alert models with other templates.

Enabling an alert model

Step 13 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**.

Figure 13-65 Available Models



Step 14 To enable models in batches, select all models you want to enable and click **Enable** in the upper left corner of the list.

Step 15 If the model status changes to **Enable**, the model is successfully enabled.

----End

13.8.3 Creating and Subscribing to a Topic

Scenario

The **Real-time notification of critical Organization and Management operations** workflow uses Simple Message Notification (SMN) to send notifications. You need to create and subscribe to a topic for receiving notifications.

This topic describes how to create a topic and subscribe to it in SMN.

Procedure

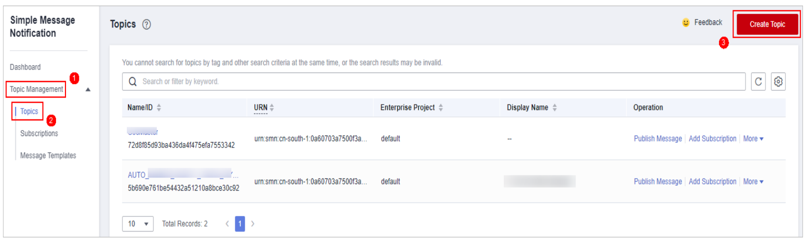
Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, click and choose **Management and Governance** > **Simple Message Notification**.

Step 3 Create a topic.

1. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the upper right corner of the displayed page, click **Create Topic**.

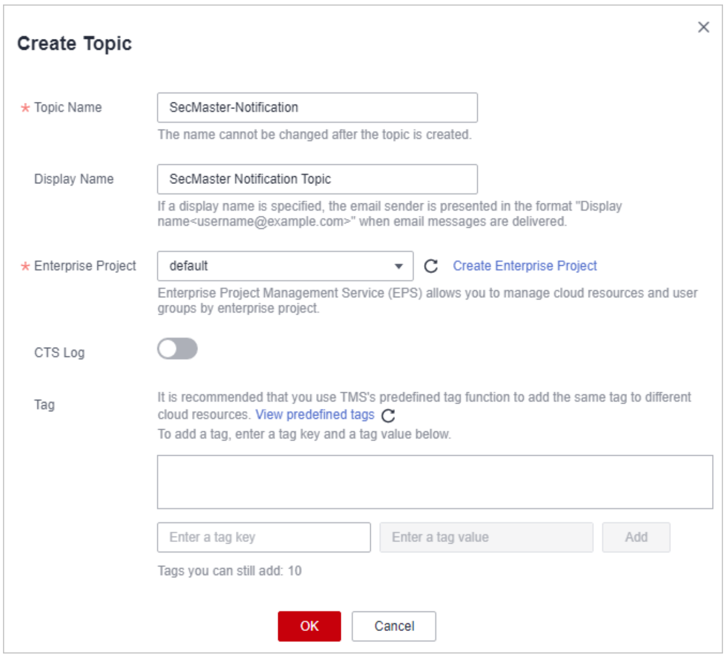
Figure 13-66 Create Topic



2. In the **Create Topic** dialog box displayed, configure topic information and click **OK**.

– **Topic Name**: **SecMaster-Notification** is recommended.
– **Display Name**: **SecMaster notification topic** is recommended.
– Retain the default values for other parameters.

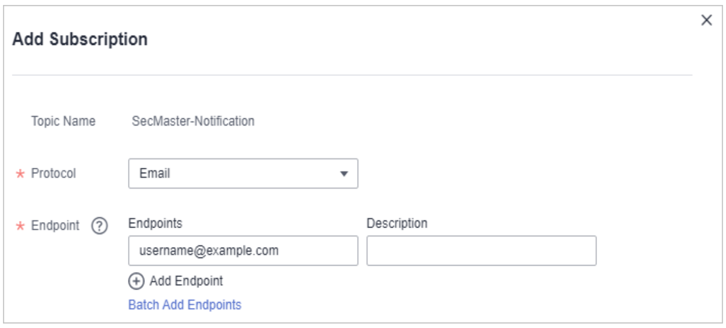
Figure 13-67 Configuring a topic



Step 4 Add a subscription.

1. On the **Topics** page, locate the row that contains the **SecMaster-Notification** topic and click **Add Subscription** in the **Operation** column.
2. On the displayed **Add Subscription** slide-out panel, configure subscription information and click **OK**.
   – **Protocol**: Select **Email**.
   – **Endpoint**: Enter the email address of the subscription endpoint, for example, username@example.com.

Figure 13-68 Add Subscription



----End

13.8.4 Configuring and Enabling the Playbook

Scenario

In SecMaster, the initial version (V1) of the **Real-time notification of critical Organization and Management operations** workflow is enabled by default. You do not need to manually enable it. The initial version (V1) of the **Real-time notification of critical Organization and Management operations** playbook is also activated by default. To use it, you only need to enable it.

This topic describes how to enable the **Real-time notification of critical Organization and Management operations** playbook.

Prerequisites

You have subscribed to an SMN topic. For details, see **Creating and Subscribing to a Topic**.

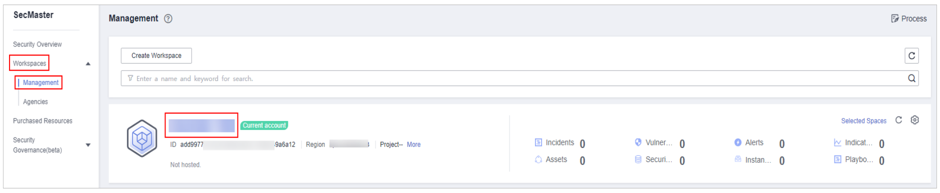
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**.

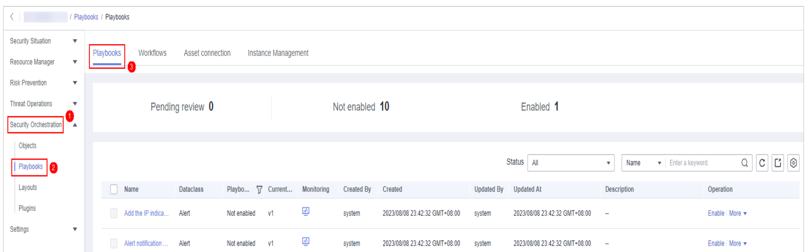
Step 3 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 13-69 Workspace management page



Step 4 In the left navigation pane, choose **Security Orchestration** > **Playbooks**.

Figure 13-70 Accessing the Playbooks tab



Step 5 On the **Playbooks** page, locate the row that contains the **Real-time notification of critical Organization and Management operations** playbook and click **Enable** in the **Operation** column.

Step 6 In the dialog box displayed, select the initial playbook version v1 and click **OK**.

----End

14 Permissions Management

14.1 Creating a User and Granting Permissions

This topic describes how to use **IAM** to implement fine-grained permissions control for your SecMaster. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing SecMaster resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your SecMaster resources.

If your account does not require individual IAM users, skip over this section.

The following walks you through how to grant permissions. **Figure 14-1** shows the process.

Prerequisites

Learn about the permissions supported by SecMaster and choose policies or roles based on your requirements. For details, see **SecMaster Permissions**.

Table 14-1 lists all the system-defined roles and policies supported by SecMaster.

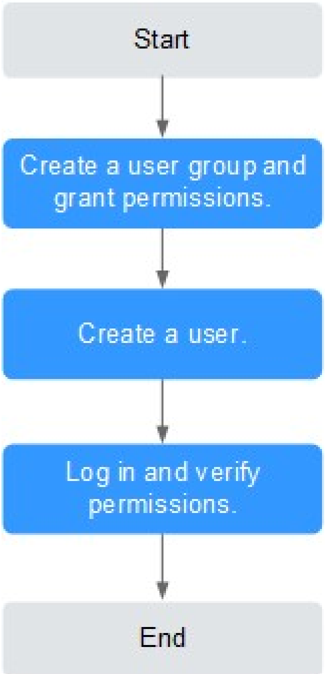
Table 14-1 System-defined permissions supported by SecMaster

Policy Name	Description	Type	Dependency
SecMaster FullAccess	All permissions of SecMaster.	System-defined policy	None

Policy Name	Description	Type	Dependency
SecMaster ReadOnlyAccess	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	System-defined policy	None

Permission Granting Process

Figure 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	uploadAttachement
Creating a Plug-in Template	component	createComponentTem-plate

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 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

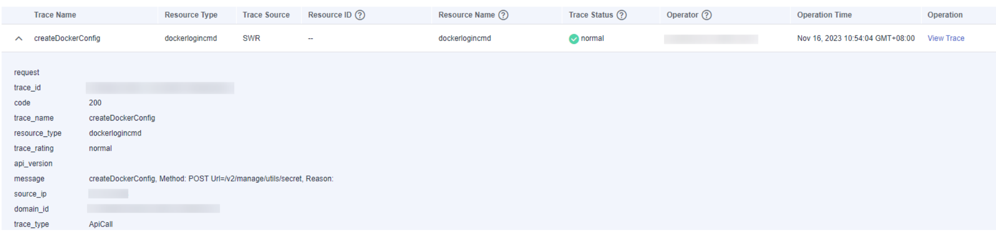
- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

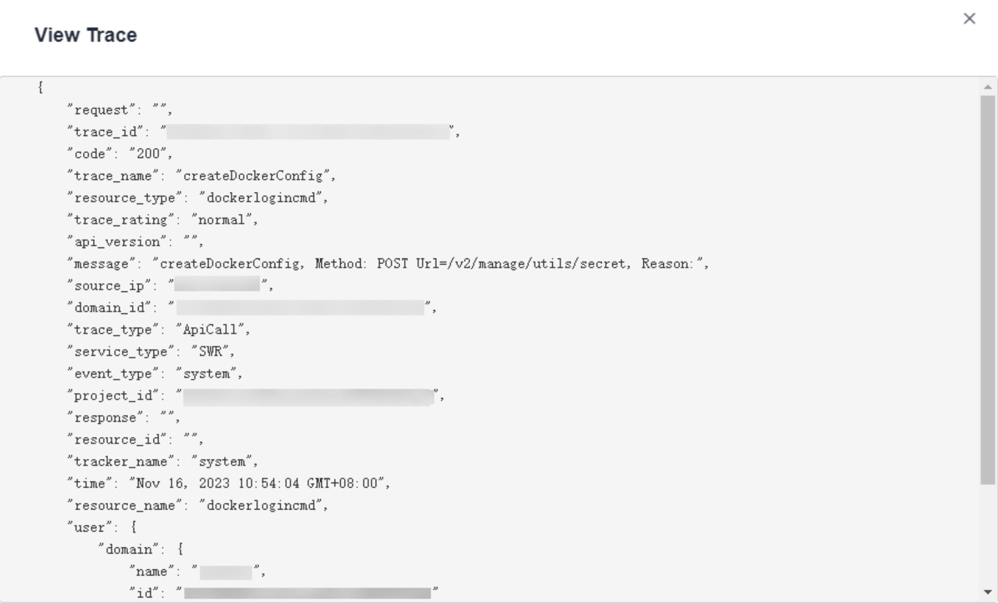
1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
   - Enter any keyword in the search box and click 🔍 to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
   - Click ↻ to view the latest information about traces.
   - Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: You can query traces generated during any time range in the last seven days.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click ⟳ 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.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

A Change History

Released On	Description
2024-03-28	This issue is the tenth official release. ● Updated **Overview** and **Adding or Editing an Emergency Policy**: Updated restrictions, and added the description of recommended emergency policy configurations. ● Updated **Collecting Data**: Added descriptions about ECS sand VPC endpoints. ● Updated **Security Orchestration Overview** and **Viewing Monitored Playbook Instances**: Updated the restrictions on playbooks and workflow instances. ● Updated **Viewing Baseline Inspection Results**: Added the procedure for viewing the check result. ● Updated the description of viewing data in **Viewing Resource Information**, **Viewing Vulnerability Details**, **Viewing Incidents**, **Viewing Alerts**, and **Viewing Indicators**. ● Added **One-click Blocking or Unblocking**.

Released On	Description
2024-02-29	This issue is the ninth official release. • Updated **Editing a Workspace**. Added content about interconnecting SecMaster with Tag Management Service (TMS). • Updated **Creating an Agency**. Added content about interconnecting SecMaster with Organizations. • Updated **Viewing Alerts**. Updated some descriptions as the alert details page on the console was optimized. • Updated **Viewing Baseline Inspection Results**. Added the description of the check result page. • Updated **Handling Baseline Inspection Results**. Added the operation guide for importing and exporting check results. • Updated **Log Access Supported by SecMaster**: Added description of accessing SecMaster baseline check results to the security analysis pipelines. • Updated **Workspace Overview** and **Security Analysis Overview**: Added restrictions on workspaces and security analysis. • Updated **Built-in Playbooks and Workflows**. Details about built-in playbooks, workflows, and asset connections were added.

Released On	Description
2023-12-11	This issue is the eighth official release. • Updated **Buying SecMaster**. Added descriptions of interconnection between SecMaster and TMS. • Updated **Creating and Copying a Security Report** and **Viewing a Security Report**. The description of the weekly reports were added. • Updated **Overview**, **Situation Overview**, **Overall Situation Screen**, **Monitoring Statistics Screen**, **Asset Security Screen**, **Threat Situation Screen**, and **Vulnerable Assets Screen** and added the statistical periods of metrics. • Updated contents in **Viewing Completed Tasks**. • Added the description of SecMaster agency permissions in section **Authorizing SecMaster**. • Added **Collecting Data**. • Updated **Built-in Playbooks and Workflows**. Details about built-in playbooks, workflows, and asset connections were added. • Deleted sections "Purchasing an ECS", "Installing an Agent", "Adding a Node", "Configuring Components", "Adding Connections", "Configuring Parsers", and "Adding Collection Channels". • Moved content in formerly "Unblocking IP Address in Batches" to section **Blocking or Canceling Blocking of an IP Address or IP Address Range**. • Optimized some descriptions.
2023-10-30	This issue is the seventh official release. • Updated **Creating and Copying a Security Report**. Description of configuration of sending report information were added. • Updated **Viewing a Security Report**. The description of the monthly report were added. • Added **Built-in Playbooks and Workflows**. Details about built-in playbooks, workflows, and asset connections were added. • Added **Log Access Supported by SecMaster**. Details about cloud service log access were added. • Added **Configuring Defense Policies**. • Moved content in "Submitting a Workflow Version" to **Managing Workflow Versions**. • Updated the description in **Buying the Standard Edition** and **Buying the Professional Edition**. • Adjusted the document structure and optimized some descriptions.

Released On	Description
2023-09-25	This issue is the sixth official release. • Added **Overview**. Descriptions of asset sources and corresponding security services were provided. • Updated **Log Fields**. The description of WAF attack log fields were updated. • Updated **Workspace Overview**. Restrictions on workspaces were updated. • Added **Delivering Logs to LTS**. • Optimized some descriptions.

Released On	Description
2023-08-10	This issue is the fifth official release. • Updated **Downloading a Security Report**. Reports in multiple formats can be downloaded. • Added remarks in **Viewing To-Do Tasks**. • Added **Viewing Completed Tasks**. Handled tasks can be viewed. • Added **Configuring Resource Subscription**. SecMaster supports subscriptions to information about other regions. • Added **Policy Management**. SecMaster supports centralized management of defense and emergency policies. • Updated **Viewing Incidents**. Users can view the affected consultation information. • Updated **Closing or Deleting Incidents**. Incidents can be closed and deleted in batches. • Updated **Viewing Alerts**. Users can view the affected consultation information. • Added operations for associating alerts with incidents in **Converting an Alert to an Incident or Associating an Alert with an Incident**. • Updated **Closing or Deleting an Alert**. Alerts can be closed and deleted in batches. • Added **Handling Alerts based on Suggestions**. Handling suggestions are provided for top alerts. • Added the description of MTD alarm fields in **Log Fields**. • Updated the content in **Security Orchestration Process**. The built-in playbook is activated by default. No manual operation is required. • Added **Viewing Custom Types**. Types can be customized. • Updated the description in **Adding an Asset Connection** and **Managing Asset Connections**. • Added the supported installation systems in **Data Collection Overview**. • Added the supported installation systems in **Buy an ECS**. • Updated **Managing Parsers**. Parsers can be imported and exported. • Deleted "Modifying the Asset Information Synchronization Policy." The system automatically synchronizes asset information without using playbooks.

Released On	Description
2023-06-30	This issue is the fourth official release. ● Added **(Optional) Configuring and Enabling a Workflow** and **(Optional) Configuring and Enabling a Playbook**. ● Optimized descriptions in **Security Orchestration Overview** and **Security Orchestration Process**. ● Deleted sections "Adding a Playbook", "Adding a Workflow", "Adding a Layout", "Adding a Data Class", and "Adding a Data Field."
2023-05-25	This issue is the third official release. ● Added **Data Delivery** and **Authorizing SecMaster**. ● Deleted sections "Asset Access Authorization" and "Baseline Inspection Access Authorization" as authorization is assigned in a centralized manner. ● Updated the detailed data description in **Overall Situation Screen**, **Monitoring Statistics Screen**, **Asset Security Screen**, **Threat Situation Screen**, and **Vulnerable Assets Screen**. ● Optimized some descriptions.

Released On	Description
2023-04-25	This issue is the second official release. • Added **Workspace Agencies**. • Added **Viewing Purchased Resources** to support unified management of purchased resources. • Added **Vulnerable Assets Screen**, **Asset Security Screen**, and **Threat Situation Screen**. • Added **Downloading a Security Report**. • Added **Importing and Exporting Assets** and **Configuring Asset Management Policies** to support asset import and asset synchronization policy management. • Added **Fixing Vulnerabilities**, **Importing and Exporting Vulnerabilities**, and **Ignoring and Unignoring a Vulnerability**. • Added **Plug-in Management**. • Added **Data Collection** to support unified management of collected data on SecMaster. • Added **Importing and Exporting Incidents**, **Importing and Exporting Alerts**, and **Importing and Exporting Intelligence Indicators**. • Updated **Buying SecMaster** and added the intelligent analysis value-added package and version upgrade content. • Updated the parameter description in **Creating a Workspace**. • Updated **Creating and Copying a Security Report**: added the description that weekly and monthly reports can be created. • Updated **Viewing a Security Report** and added the description of security report templates. • Updated the description of asset category display in section **Viewing Resource Information**. • Updated **Data Integration** and added the description of newly accessed data sources.
2023-02-28	This issue is the first official release.