SecMaster

Getting Started

Issue	05
Date	2024-09-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Contents

1 Before You Start

SecMaster (SecMaster) is a next-generation cloud native security operations center Huawei Cloud provides for you. With SecMaster, you can enjoy one-stop cloud security management. You can centrally manage cloud assets, security posture, security information, and incidents, improving security operations efficiency and responding to threats faster.

This topic describes how to quickly use SecMaster for security operations.

Figure 1-1 Process of using SecMaster

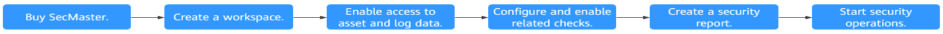

Buy SecMaster.
Create a workspace.
Enable access to asset and log data.
Configure and enable related checks.
Create a security report.
Start security operations.

Table 1-1 Process description

Step	Description
Step 1: Buy SecMaster	Buy the SecMaster edition, quota, and value-added package based on your service needs.
Step 2: Create a Workspace	You can create different workspaces to group resources by scenarios. This will makes you easier to manage security when you have a large number of resources.
Step 3: Enable Access to Asset and Log Data	You can enable security data access to SecMaster and manage all security data in SecMaster. ● **Subscribe to asset data**: Subscribe to all asset data in the current region under the current account for centralized asset management. ● **Enable log access**: Logs of other services are aggregated into SecMaster for centralized management and analysis. – Aggregation of logs from Huawei Cloud services – (Optional) Aggregation of logs from non-Huawei Cloud services

Step	Description
Step 4: Configure and Enable Related Checks	You can enable alert models, activate playbooks, start baseline inspections, and configure security policies. SecMaster will help check all your resources comprehensively. - **Enable preconfigured models**: You can use models to monitor logs. If any content that meets the trigger condition is detected, an alert is generated. - **Enable playbooks**: You can use playbooks to enable automated security incident responses. - **Perform a baseline check**: You can learn the latest baseline configuration status and risky settings. - **(Optional) Configure defense policies and emergency policies**: You can configure defense policies to implement full-process protection and configure emergency policies to control risks.
Step 5: Create a Security Report	You can specify how you would like SecMaster to automatically send security operations reports.
Step 6: Start Security Operations	You can start security operations, such as asset management, threat detection, and alert investigation, based on the integrated data.

2 Step 1: Buy SecMaster

SecMaster provides **basic**, **standard**, and **professional** editions. Each edition has situation awareness, baseline inspection, query and analysis, and security orchestration functions.

This topic walks you through how to buy the professional edition SecMaster and value-added package billed yearly/monthly. For more details, see **Buy SecMaster**.

Procedure

Step 1 Log in to the management console.

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

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

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

Step 5 (Optional) Obtain purchase authorization.

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

Step 6 On the purchase page, configure required parameters.

Table 2-1 Parameters for purchasing the professional edition in yearly/monthly mode

Parameter	Example Value	Description
Billing Mode	**Yearly/ Monthly**	Billing mode of your SecMaster. ● Yearly/Monthly billing is a prepaid mode in which you pay for the service before using it. Your bill is settled based on the required period. The longer you use the service, the more discounts you got. ● Pay-per-use billing is a postpaid mode in which you pay for what you use. You are billed by second based on the actual usage. Your bill is settled by the hour. With the pay-per-use billing mode, you can easily adapt to resource requirement changes, reducing the risk of over-provisioning of resources or lacking capacity. In this mode, there are no upfront commitments required.
Region	**AP-Bangkok**	Select the region where your cloud resources are located.
Edition	**Professional**	SecMaster provides basic, standard, and professional editions for your choice. For details about their differences, see **Edition Differences**.
ECS Quota	--	The maximum number of ECSs you want to protect. The quota cannot less than the total number of ECSs you have in the current account. This value cannot be changed to a smaller one after your purchase completes. ● The maximum quota is 10,000. ● If some of your ECSs are not protected by SecMaster, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. To prevent this, increase the quota upon an increase of your host quantity.
Large Screen	**Enabled**	**Large Screen**, **Log Audit**, **Security Analysis**, and **Security Orchestration** are optional functions. To buy them, set the purchase quantity as required. For details about the value-added package and recommended configurations, see **Value-Added Package Description**.
Log Audit	**Buy now** and set the specifications based on the number of logs generated each day.	

Parameter	Example Value	Description
Security Analysis	**Buy now** and set the daily quota for each server as needed.	
Security Orchestration	**Buy now** and set the data collection and retention quotas.	
Tag	--	Tags attached to SecMaster to identify resources. For details about tags, see **Tag Management Service**.
Required Duration	--	Select the required duration as required. You do not need to configure this parameter in **pay-per-use** mode. The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

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

Step 8 After confirming that the order details are correct, read the *SecMaster Disclaimer* and select "I have read and agree to the SecMaster Disclaimer", and click **Pay Now**.

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

----End

3 Step 2: Create a Workspace

Workspace is a top-level workbench of SecMaster. Before using SecMaster, you need to create workspaces to group resources based on work scenarios. This will enable faster resource search and security operations.

This topic 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

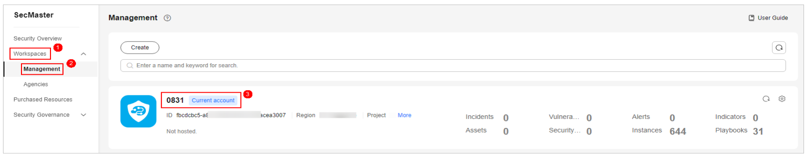
Step 1 Log in to the management console.

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

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

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

Figure 3-1 Workspace management page



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

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

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

Step 6 On the workspace management page, click **Create**. On the **Create Workspace** panel displayed, configure parameters.

Table 3-1 Parameters for creating a workspace

Parameter	Example Value	Description
Region	**AP-Bangkok**	Select the region based on where your cloud resources are deployed.
Project Type	**default**	Project that the workspace belongs to
Workspace Name	**SecMaster**	Name of the security operations workspace, which cannot be modified once the workspace is created.
Tag	--	Tag attached to the workspace. The tag can be edited.
Description	--	Description of the workspace.

Step 7 Click **OK**.

----End

4 Step 3: Access Security Data

4.1 Enabling Asset Subscription

SecMaster can synchronize asset information only in the workspace where asset subscription is enabled. If you enable asset subscription, SecMaster updates asset information within one minute.

The first workspace in each region automatically loads all assets in the corresponding region. The non-first workspaces do not load assets automatically. You need to manually configure asset subscriptions based on your security operations needs.

This topic describes how to manually access asset data.

NOTE

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

Procedure

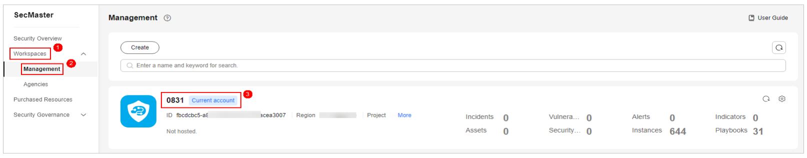
Step 1 Log in to the management console.

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

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

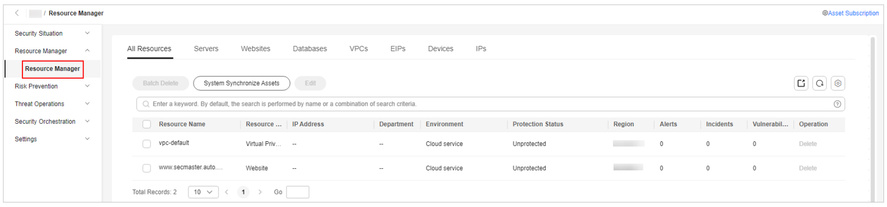
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 4-1 Workspace management page



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

Figure 4-2 Resource Manager



Resource Name	Resource ...	IP Address	Department	Environment	Protection Status	Region	Alerts	Incidents	Vulnerabil...	Operation
vpc-default	Virtual Priv...	--	--	Cloud service	Unprotected	[redacted]	0	0	0	Delete
www.secmaster.auto....	Website	--	--	Cloud service	Unprotected	[redacted]	0	0	0	Delete

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

Step 7 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 8 Click **OK**.

If you enable asset subscription, SecMaster updates asset information within one minute. Then, asset information will be automatically synchronized every night.

----End

4.2 Enabling Log Access

SecMaster can integrate log data of multiple Huawei Cloud services, such as Web Application Firewall (WAF), Host Security Server (HSS), and Object Storage Service (OBS). After the integration, you can search for and analyze all collected logs.

For the first workspace in each region, SecMaster automatically enables access to logs of most cloud services. No manual actions are required. For non-first workspaces, you need to manually configure log data access based on your security operations needs.

This topic describes how to manually enable access to cloud service logs you may need.

Enabling Access to Huawei Cloud Service Logs

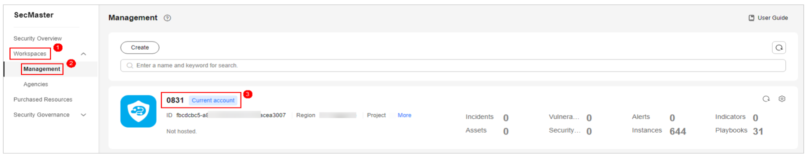
Step 1 Log in to the management console.

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

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

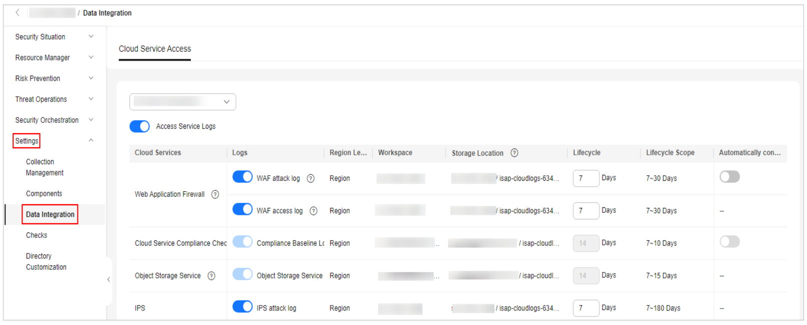
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 4-3 Workspace management page



Step 5 In the navigation pane on the left, choose **Settings** > **Data Integration**.

Figure 4-4 Data Integration page



Cloud Services	Logs	Region Le...	Workspace	Storage Location	Lifecycle	Lifecycle Scope	Automatically con...
Web Application Firewall	WAF attack log	Region	[redacted]	[redacted] / isap-cloudlogs-634...	7 Days	7~30 Days	
	WAF access log	Region	[redacted]	[redacted] / isap-cloudlogs-634...	7 Days	7~30 Days	--
Cloud Service Compliance Chec	Compliance Baseline Lc	Region	[redacted] ...	[redacted] / isap-cloudl...	14 Days	7~10 Days	
Object Storage Service	Object Storage Service	Region	[redacted] ...	[redacted] / isap-cloudl...	14 Days	7~15 Days	--
IPS	IPS attack log	Region	[redacted]	[redacted] / isap-cloudlogs-634...	7 Days	7~180 Days	--

Step 6 Locate the cloud service for which you want to collect logs, click ○ in the **Log** column to enable the log function.

You are advised to click ○ on the left of **Access Service Log** to access all cloud service logs in the current region.

Step 7 Set the lifecycle. You are advised to retain the default value.

Step 8 (Optional) Set **Automatically converts alarms**.

Locate the target cloud service, click ○ in the **Automatically converts alarms** column to enable the function. Then, if a cloud service log meets certain alarm rules, the log is converted into an alert.

Step 9 Click **Save**.

After the access completes, a default data space and pipeline are created.

----End

(Optional) Enabling Access to Logs from non-Huawei Cloud Services

You can aggregate security logs from third-party (non-Huawei Cloud) services to SecMaster. For details, see Data Collection.

5 Step 4: Configure and Enable Related Checks

5.1 Enabling an Alert Model

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

For the first workspace in each region, SecMaster automatically enables some preconfigured models. For non-first workspaces in each region, you need to enable preconfigured models manually and create custom alert models to meet your operation needs.

If you want to use a model that is not enabled by default or enable a model in a new workspace, perform the following procedure.

The following part describes how to create and enable a model.

Procedure

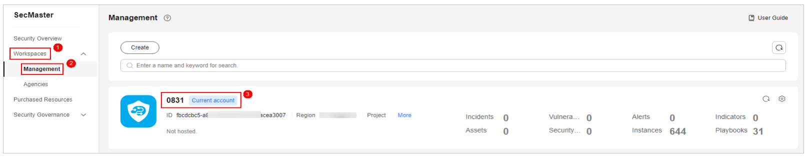
Step 1 Log in to the management console.

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

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

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

Figure 5-1 Workspace management page



0831

ID fbcdcbc5-a[redacted]acea3007 Region [redacted] Project

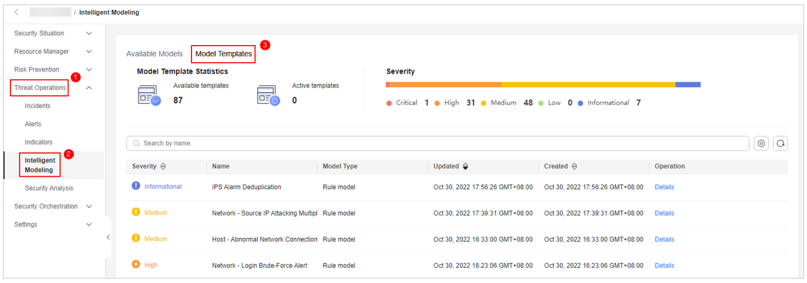
Not hosted.

Incidents 0 Vulnera... 0 Alerts 0 Indicators 0

Assets 0 Security... 0 Instances 644 Playbooks 31

Step 5 In the navigation pane on the left, choose **Threat Operations** > **Intelligent Modeling**, and select the **Model Templates** tab.

Figure 5-2 Model Templates tab



Model Template Statistics

Available templates 87

Active templates 0

Severity

● Critical 1 ● High 31 ● Medium 48 ● Low 0 ● Informational 7

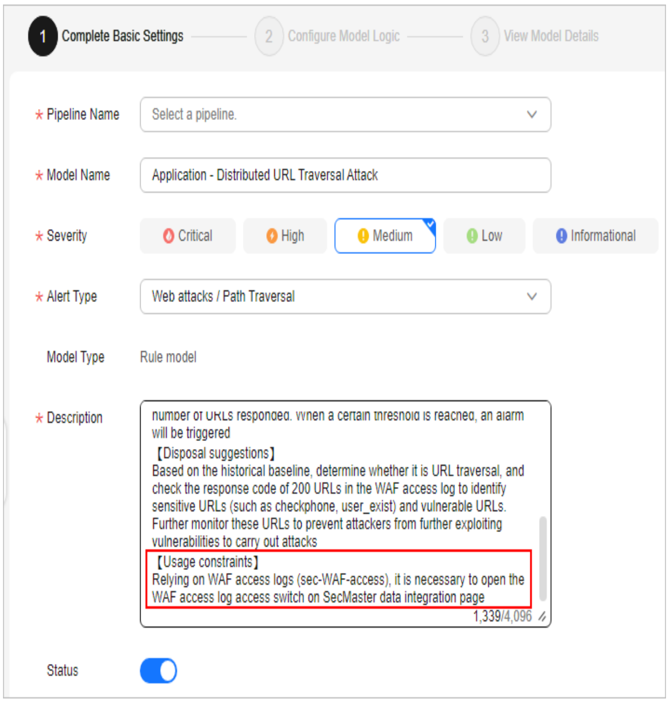
Severity	Name	Model Type	Updated	Created	Operation
Informational	IPS Alarm Deduplication	Rule model	Oct 30, 2022 17:56:26 GMT+08:00	Oct 30, 2022 17:56:26 GMT+08:00	Details
Medium	Network - Source IP Attacking Multipl	Rule model	Oct 30, 2022 17:39:31 GMT+08:00	Oct 30, 2022 17:39:31 GMT+08:00	Details
Medium	Host - Abnormal Network Connection	Rule model	Oct 30, 2022 16:33:00 GMT+08:00	Oct 30, 2022 16:33:00 GMT+08:00	Details
High	Network - Login Brute-Force Alert	Rule model	Oct 30, 2022 16:23:06 GMT+08:00	Oct 30, 2022 16:23:06 GMT+08:00	Details

Step 6 In the model template list, locate the target model template and click **Details** in the **Operation** column. On the template details panel displayed on the right, click **Create Model** in the lower right corner.

Step 7 On the **Create Alert Model** page, configure basic information.

- **Pipeline Name**: Select a pipeline for the alert model. You can select a pipeline based on the **Usage constraints** in the description.

Figure 5-3 Obtaining a pipeline name



* Pipeline Name: Select a pipeline.

* Model Name: Application - Distributed URL Traversal Attack

* Severity: Critical | High | [✓ Medium] | Low | Informational

* Alert Type: Web attacks / Path Traversal

Model Type: Rule model

* Description:

number of URLs responded. When a certain threshold is reached, an alarm will be triggered
【Disposal suggestions】
Based on the historical baseline, determine whether it is URL traversal, and check the response code of 200 URLs in the WAF access log to identify sensitive URLs (such as checkphone, user_exist) and vulnerable URLs. Further monitor these URLs to prevent attackers from further exploiting vulnerabilities to carry out attacks
【Usage constraints】
Relying on WAF access logs (sec-WAF-access), it is necessary to open the WAF access log access switch on SecMaster data integration page
1,339/4,096

Status: ●

- Retain default values of other parameters.

Step 8 Complete all settings and 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 Complete all settings and click **Next** in the lower right corner of the page.

Step 11 Review all settings and click **OK** in the lower right corner of the page.

Step 12 Repeat **Step 6** to **Step 11** to create alert models with other templates.

----End

5.2 Enabling a Playbook

After you enable log access, SecMaster provides some security orchestration playbooks to help with automated cloud security incident response, reduce the average response time (MTTR), and improve the overall security protection capability.

For the first workspace in each region, preconfigured playbooks that are most-frequently-used are enabled by SecMaster automatically. For non-first workspaces in each region, you need to enable them manually to meet your operation needs.

You can follow the following procedure to enable other playbooks.

Procedure

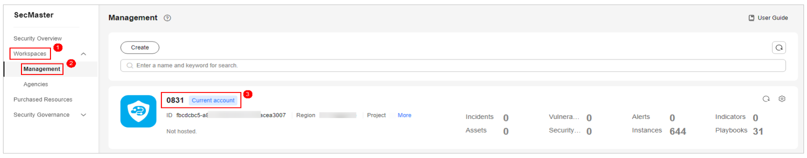
Step 1 Log in to the management console.

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

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

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

Figure 5-4 Workspace management page



0831 Current account

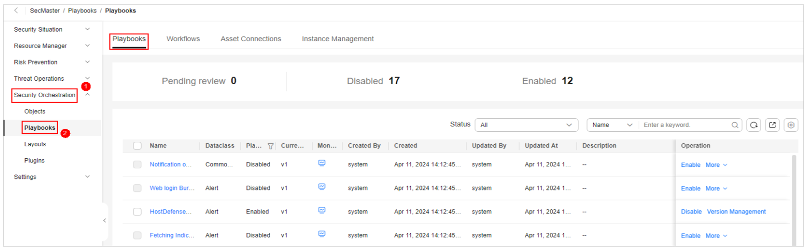
ID fbcdcbc5-a[redacted]cea3007 | Region [redacted] | Project More

Not hosted.

Incidents 0 Assets 0 Vulnera... 0 Security... 0 Alerts 0 Instances 644 Indicators 0 Playbooks 31

Step 5 In the navigation pane on the left, choose **Security Orchestration** > **Playbooks**.

Figure 5-5 Accessing the Playbooks tab



Pending review 0 Disabled 17 Enabled 12

□	Name	Dataclass	Pla...	Curre...	Mon...	Created By	Created	Updated By	Updated At	Description	Operation
□	Notification o...	Commo...	Disabled	v1	🖵	system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Enable More
□	Web login Bur...	Alert	Disabled	v1	🖵	system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Enable More
□	HostDefense...	Alert	Enabled	v1	🖵	system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Disable Version Management
□	Fetching Indic...	Alert	Disabled	v1	🖵	system	Apr 11, 2024 14:12:45...	system	Apr 11, 2024 1...	--	Enable More

Step 6 On the **Playbooks** page, locate the row that contains the target playbook and click **Enable** in the **Operation** column.

Step 7 In the displayed dialog box, select the version v1 you want to enable and click **OK**.

----End

5.3 Conducting a Baseline Inspection

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

The following describes how to start an immediate check for check items in a compliance pack.

Procedure

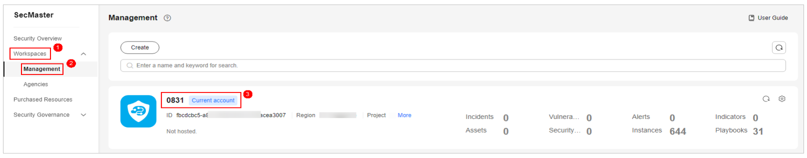
Step 1 Log in to the management console.

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

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

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

Figure 5-6 Workspace management page



Step 5 In the navigation pane on the left, choose **Risk Prevention** > **Baseline Inspection**. In the upper right corner of the page, click **Check Now** to execute the task immediately.

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

5.4 (Optional) Configuring a Security Policy

You can enable, configure, and apply protection policies for seven layers of defense and enjoy comprehensive protection. This topic walks you how to configure a protection policy in WAF in the application defense layer.

Procedure

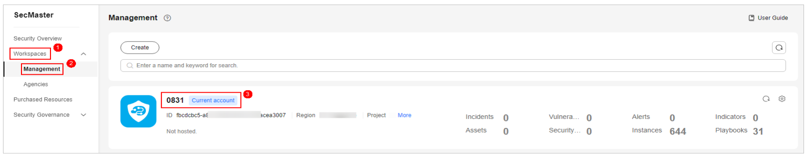
Step 1 Log in to the management console.

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

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

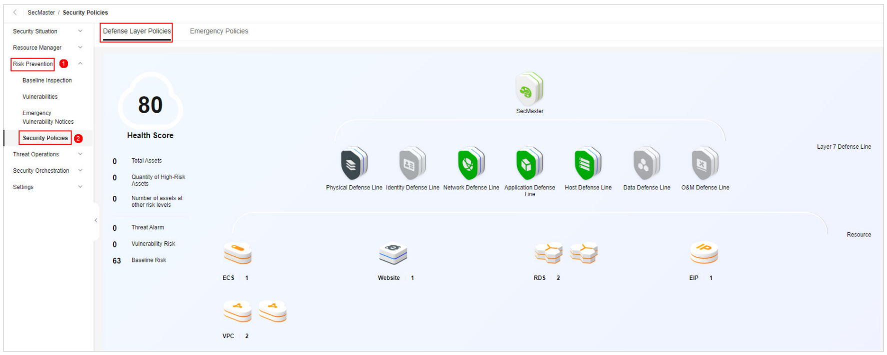
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 5-7 Workspace management page



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

Figure 5-8 Defense Layer Policies



Step 6 Click the name of the application defense line. The cloud product information corresponding to the application defense line is displayed on the right.

Step 7 On the WAF tab, click **Protection Policy**. The WAF protection policy configuration page is displayed.

If you have not purchased WAF, click **WAF**. On the WAF console page displayed, click **Buy WAF**. On the purchase page, enable WAF by referring to **Buying WAF**.

Step 8 On the WAF protection policy configuration page, click the **Policy Management** tab. On the displayed page, click **Add Policy** in the upper left corner of the list.

Step 9 In the displayed dialog box, enter the policy name and click **Confirm**. The added policy will be displayed in the policy list.

Step 10 In the row containing the target policy, click the policy name. On the displayed page, add rules to the policy by referring to **Configuring Protection Rules**.

----End

6 Step 5: Create a Security Report

Security reports can be sent by SecMaster automatically. You will see security scores, baseline check results, security vulnerabilities, and policy coverage in a security report. This helps you learn about asset security status in a timely manner.

This topic describes how to create a daily security operations report.

Procedure

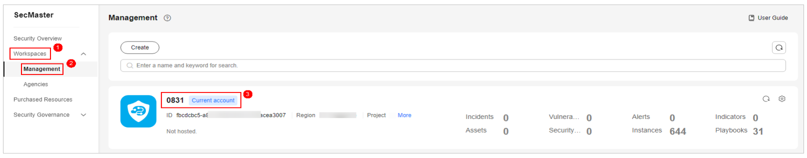
Step 1 Log in to the management console.

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

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

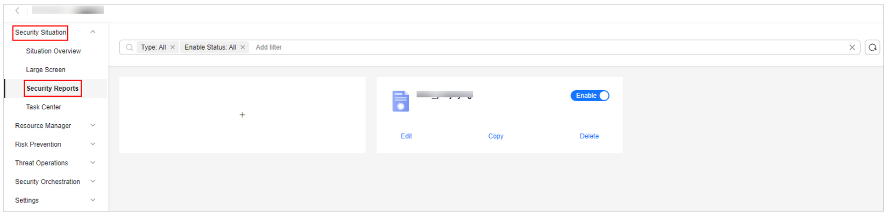
Step 4 In the navigation pane on the left, choose **Workspaces** > **Management**. In the workspace list, click the name of the target workspace.

Figure 6-1 Workspace management page



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

Figure 6-2 Security Reports



Step 6 On the security report page, click +. On the displayed page, configure basic report information.

Table 6-1 Report parameters

Parameter	Example Value	Description
Report Name	**Security situation report - Daily report**	Name of the report you want to create.
Schedule	**Daily**	Select the type of the security situation report.
Data Scope	--	This field displays the data scope based on **Schedule** you specified. No manual actions are required.
Report Schedule	--	Set the time when you want SecMaster to send the security report. For daily reports, the security data from 00:00:00 to 23:59:59 on the previous day will be sent by default.
Email Subject	**SecMaster Security Situation Daily Report**	Set the subject of the email for sending the report.
Recipient Email	**test01@example.com**	Add the email address of each recipient. ● You can add up to 100 email addresses. ● Separate multiple email addresses with semicolons (;). Example: test01@example.com;test02@example.com
(Optional) Copy To	**test03@example.com**	Add the email address of each recipient you want to copy the report to. ● You can add up to 100 email addresses. ● Separate multiple email addresses with semicolons (;). Example: test03@example.com;test04@example.com
(Optional) Remarks	--	Remarks for the security report.

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

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

In this example, a **Daily** report is selected.

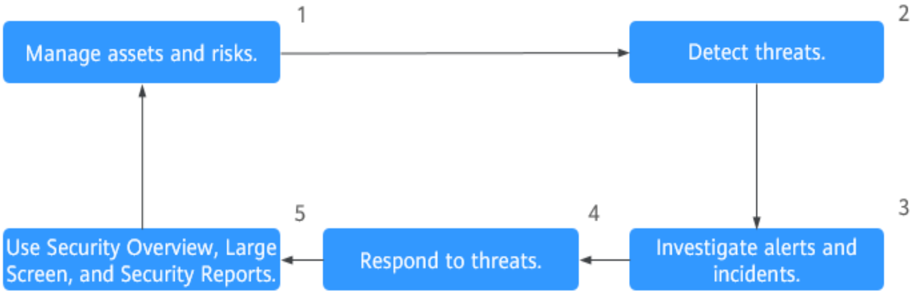
Step 9 Click **Complete** in the lower right corner. Go back to the **Security Reports** page, view the created security report.

----End

7 Step 6: Start Security Operations

You can now start security operations, such as asset management, threat detection, and alert investigation, based on the integrated data.

Figure 7-1 Secure operations


1
Manage assets and risks.
2
Detect threats.
3
Investigate alerts and incidents.
4
Respond to threats.
5
Use Security Overview, Large Screen, and Security Reports.

1. **Manage assets and risks.**

   The essence of security operations is security risk management. According to the definition of ISO, there are three elements, assets, vulnerabilities, and threats involved in security operations. Sorting the assets you want to protect is the starting point of the security operations service flow.

Table 7-1 Managing assets and risks

Operation	Description
Sorting out and managing assets	SecMaster helps you: ● Aggregate cloud assets from different accounts and regions into one place. ● Import off-cloud assets to SecMaster and mark the environment assets belong to. ● SecMaster marks asset security status to show whether there are unsafe settings, OS or application vulnerabilities, suspicious intrusions, or unprotected cloud services. For example, all ECSs must be protected with HSS, and all domain names must be protected with WAF. For details, see **Managing Assets**.
Checking and clearing unsafe settings	During security operations, the most common vulnerabilities are unsafe settings. Based on security compliance experience, SecMaster forms a baseline for automatic checks and provides baseline check packages based on common specifications and standards in the industry. ● SecMaster can automatically check cloud service settings. For example, SecMaster can check whether permissions are assigned by role in IAM, whether security groups allow all inbound access in VPC, and whether WAF protection policies are enabled. You can harden the configuration based on the recommended methods. For details, see **Baseline Inspection**.
Discovering and fixing vulnerabilities	SecMaster can also help you detect and fix security vulnerabilities. You can manage Linux, Windows, Web-CMS, and application vulnerabilities in SecMaster. You will have an overview of vulnerabilities in real time, including vulnerability scan details, vulnerability statistics, vulnerability types and distribution, top 5 vulnerabilities, and top 5 risky servers. For details, see **Vulnerability Management**.

2. **Detect threats.**

   As we have sorted out assets we need to protect and fixed unsafe settings and vulnerabilities, after data sources are connected to SecMaster, the next move is to identify suspicious activities and threats.

   SecMaster provides multiple preconfigured models to detect threats. These models were designed by security experts and analysis teams based on known threats, common attack media, and suspicious activities. You will receive notifications once suspicious activities trigger those models. These models automatically search the entire environment for suspicious activities. You can also create custom threat detection models to meet your needs.

SecMaster also provides the log data query function to help you discover threats.

For details, see **Creating a Model** and **Security Analysis**.

3. **Investigate alerts and incidents.**

Table 7-2 Investigating alerts and incidents

Operation	Description
Investigating alerts	Threat detection models analyze security cloud service logs to find suspected intrusion behaviors and generate alerts. An alert in SecMaster contains the following fields: name, severity, asset/threat that initiates suspicious activities, and compromised assets. Security operations personnel need to analyze and investigate alerts to find out real threats. If the risk is low, they will disable the alert (such as repeated alerts and O&M operations). If the risk is high, they will convert the alert to an incident. For more details, see **Viewing Alerts** and **Converting an Alert to an Incident**.
Investigating incidents	After an alert is converted to an incident, you can view incident in the incident management module. You can investigate and analyze the incident and initiate emergency response to it. You can associate an incident with entities related to suspicious activities. The entities include assets (such as VMs), indicators (such as attack source IP addresses), accounts (such as leaked accounts), and processes (such as Trojans). You can also associate an incident with similar historical alerts or incidents. For details, see **Viewing an Incident** and **Editing an Incident**.

4. **Respond to threats.**

   You can use playbooks to enable automated alert and incident responses.

   For details, see **Security Orchestration**.

5. Use **Security Overview**, **Large Screen**, and **Security Reports**.

Table 7-3 Security Overview, Large Screen, and Security Reports

Function	Description
Security Overview	This page displays the security scores of resources in the current workspace, so you can quickly learn about the security status. For details, see **Situation Overview**.
Large Screen	You can view the real-time situation of resources and handle attack incidents. This function helps security operations teams monitor and analyze security threats and incidents in real time and quickly respond to them. For details, see **Large Screen**.
Security Reports	Security reports are sent by SecMaster automatically. You will see security scores, baseline check results, security vulnerabilities, and policy coverage in a security report. This helps you learn about asset security status in a timely manner. For details, see **Security Reports**.

8 Getting Started Through Common Practices

After creating a workspace, collecting data, and enabling some checks in SecMaster, you can refer to practices provided in this topic to meet your service requirements.

Table 8-1 Common practices

Practice	Description
Security Panels	SecMaster can work with other security services and display overall cloud asset security posture in real time on SecMaster security panels.
Resource Manager	SecMaster automatically discovers and manages all assets on and off the cloud and displays the real-time security status of your assets.
Security Analysis	This topic describes how to use SecMaster to manage, aggregate, and analyze security alarms and logs of other cloud products concurrently so that you can obtain attack information and proactively discover threats.
Automatic Response Playbooks	This topic introduces security orchestration in SecMaster, which can help automatically respond to and handle security incidents in time.
Aggregating Log Data from a Non-Huawei Cloud System or Product to SecMaster or Transferring Security Logs from SecMaster to a Third-Party System or Product	This topic describes log collection methods, how to parse, transfer, query the collected log data in a visualized manner, as well as how to create threat models.