Introduction

About Nova Command

Focusing on visualized security and coordinated defense, Nova Command is designed to provide an intelligent, precise big data security analysis platform and unified security operations center that support joint defense and emergency response by dedicated experts. It detects threats, issues warnings, and makes responses in real time to help you perceive and manage security threats easily in this increasingly complex nova security environment.

Based on complete traffic analysis, Nova Command collects key data across the whole network through security components such as Nova Sensor, Sangfor devices, and third-party security devices, uses technologies such as threat intelligence, behavior analysis, user and entity behavior analytics (UEBA), machine learning, big data association analysis, and visualization, to implement visualized security and detection of all threats across the network. At the same time, Nova Command provides an easy-to-operate support system for security service experts or relevant O&M systems to make interventions and emergency responses so that they can respond to security events more quickly and detect advanced threats more easily.

Key Features

Nova Command is a big data security analysis product for general industries. It is positioned as a local security brain that integrates detection, visualization, and response capabilities for enterprises and organizations. Its key features are as follows:

1. Holistic visualized security

Nova command has various capabilities, such as complete traffic analysis, effective multidimensional data collection, and intelligent analysis. It monitors the overall security threats, lateral threats, outbound threats on business systems, and server vulnerabilities in real time to help you confirm whether the whole network is secure, which part of the network is not secure, where the vulnerability is, and where the attack entry point is. Centering around the attack chain, Nova Command also offers a set of security capabilities based on "check before an incident, analysis during an incident, and detection after an incident" to help you detect threats over the network and make correct decisions.

2. Big data analysis and search capabilities

Nova Command is designed within a big data framework and by referring to the Elasticsearch engine, thus supporting storage of and association analysis on terabytes of data by default and can be scaled out through clustering. At the same time, our data analysis team has been engaged in the research and development of big data performance optimization for years to enable Nova Command to manage terabytes of data and query data in seconds.

3. Intelligent analysis capability to respond to unknown threats

As hackers develop their technologies and variant viruses and escape technologies continue to evolve, traditional security devices are far from enough to meet user needs by just relying on their static rules to detect threats. This is because these rules can detect only a small part of known threats but can do nothing to help detect the latest attacks and unknown threats. Nova Command uses various technologies, such as machine learning, association analysis, and UEBA, to detect advanced threats like advanced persistent threats (APT) and insider lateral movement on the network. In one word, Nova Command is able to detect the latest threats without updating detection rules.

4. Real-time monitoring and precise warning

Nova Command collects and analyzes the complete traffic, endpoint logs, and third-party logs to monitor known threats (such as zombies, Trojans, worms, viruses, abnormal traffic, and business vulnerabilities) and unknown threats (such as cyber zombies, APTs, and 0-day vulnerabilities) in real time the whole day. It also combines intelligent analysis and convenient human intervention-based operations support to issue precise warnings of the detected threats, thus simplifying the O&M process and effectively reporting the threats to affected parties.

5. Effective coordinated response to prevent risk spread and help fix security issues

Nova Command collaborates with security devices of Sangfor to serve as basic components, which not only collect security data but also intercept and control any major security incidents or risks that are spreading internally. The collaboration involves network interdiction, Internet access management, and virus scan on hosts, which effectively help you fix security issues.

6. Threat forensics and impact evaluation

Conventional security analysis focuses on logs and takes IP addresses as the source of analysis, thus making it hard to display the evidence of an incident in detail or fully understand the damage.

On the contrary, Nova Command can automatically classify IP addresses by asset type and display the damage to different types of assets in terms of business security and host security so that O&M staff can focus on business assets. Meanwhile, in combination with detailed attack forensics, multidimensional latent threats, and traffic-based GoldenEye Traceback, Nova Command can see the impact of threats clearly and intuitively and evaluate the damage.

7. Traceability support

The key to realizing traceability is to effectively extract data. Relying on the effective data extraction capability of complete traffic and third-party logs (such as logs of middleware, OS, and security devices), Nova Command extracts key metadata in real time for threat analysis and security issue tracing. It also can save metadata for at least one year by using storage with terabytes of space and the cluster deployment capability. At the same time, using visualization technology, Nova Command implements a traceability support system based on various technologies, such as traffic visualization, GoldenEye Traceback, visual stages of an attack, centralized search, and big data capability, to provide strong support for security experts in traceability analysis.

Home

Home consists of three modules: Overview, Monitor, and Data Center. It provides all-around and visualized security monitoring services.

Overview

The Overview module mainly contains two parts: Overview and ATT&CK Capabilities.

Overview

This part mainly contains Overall Security, Server Security, Host Security, and Assets.

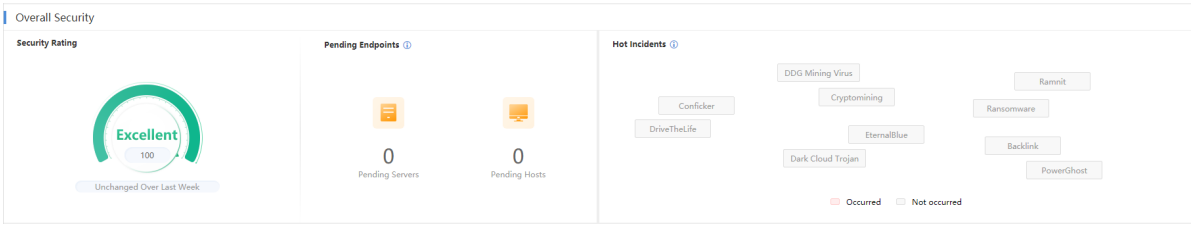
Display options

You can specify the modules to display on the homepage. The following modules are available:

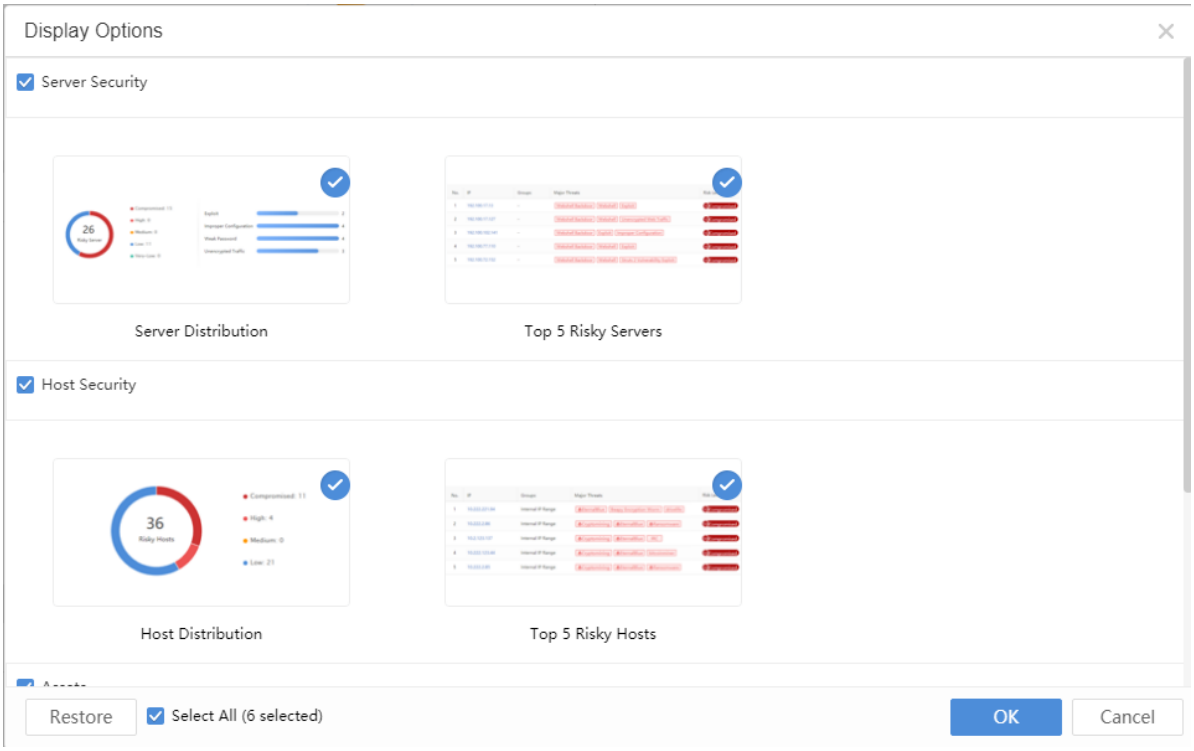
Server Security (Server Distribution, Top 5 Risky Servers)

Host Security (Host Distribution, Top 5 Risky Hosts)

Assets (Assets, UEBA)

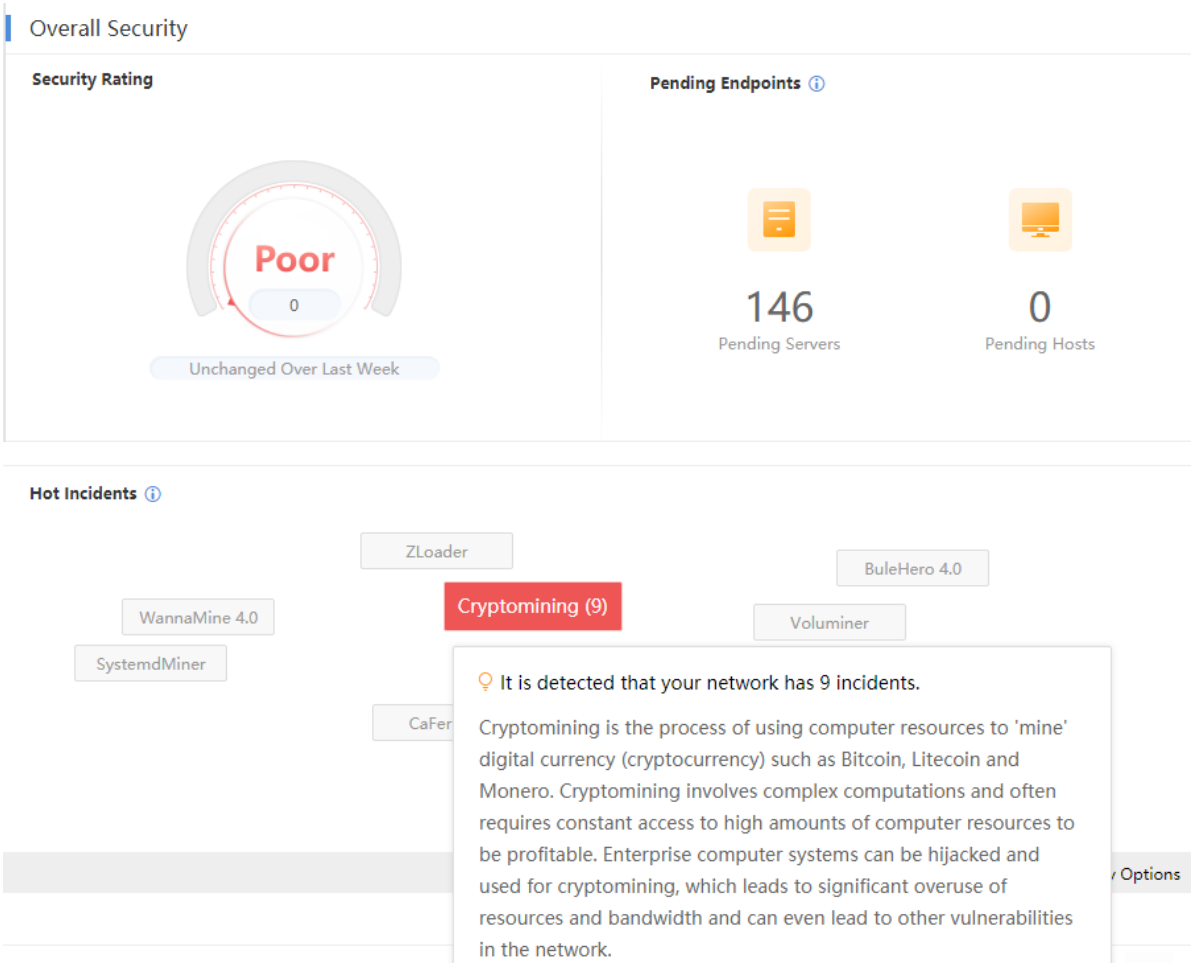


You can click <Display Options> and select the modules that you want to display on the homepage, as shown in the figure below.



Overall Security

Overall Security displays the overall security, security rating, pending endpoints, GoldenEye Traceback, and hot incidents, as shown in the figure below.



Description of the content displayed:

<Security Rating: >This area displays the security of the current network by a score and rating. The total score is 100 points, and the ratings are Excellent (91–100 points), Good (81–90 points), Fair (61–80 points), and Poor (60 points or less). The default rating standards are shown in the following table.

Table 1 Default rating standards

	Points to Deduct	Deduction Upper Limit
Compromised Endpoint	10	100
High Risk Endpoint	3	39
Medium Risk Endpoint	2	19
Low Risk Endpoint	1	9
Very-Low Risk Endpoint	0.1	2

Note:

You can customize the rating standards. First, hover the mouse over the rating. Then, perform the following steps:

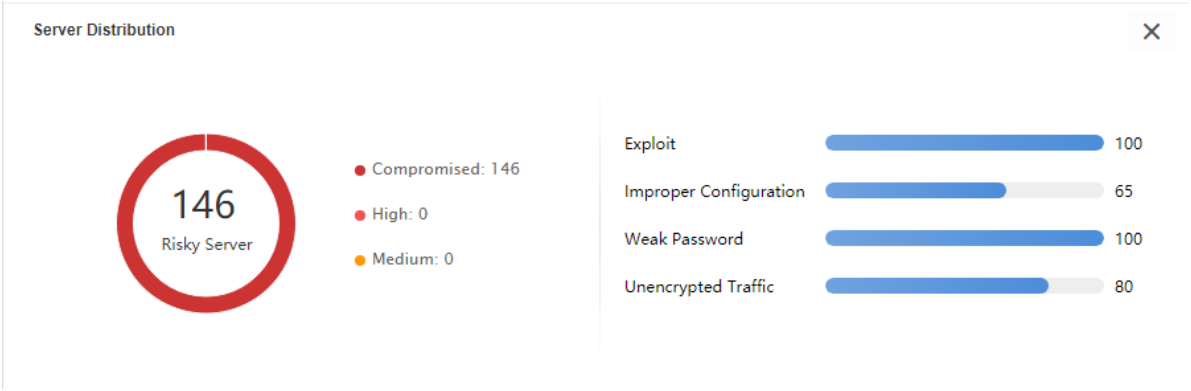
1. Click the edit button on the right of [Rating Description] and select [Auto-scored] or [Specified]. If you select the latter, you can directly modify the score.
2. Click the edit button on the right of [Standards] to modify the rating standards for auto system scoring.

<Pending Endpoints: >This area displays the number of servers and hosts whose risks are to be fixed.

<Hot Incidents: >This area displays hot network security incidents in recent times and highlights those affecting the customer network. Incidents that have occurred in the customer environment are highlighted in red and should be prioritized. Meanwhile, you can hover the mouse over the incident tag to view the details.

Server security

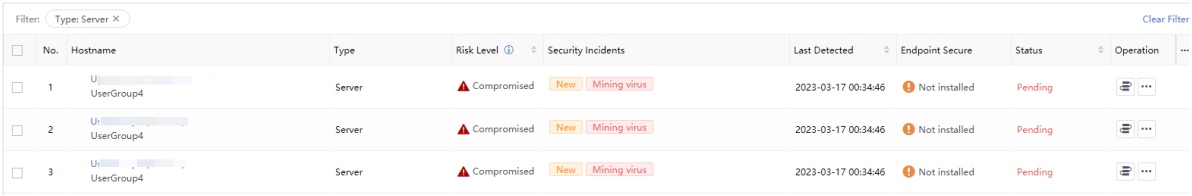
This part displays the distribution of servers in different security states, including compromised, high risk, and medium risk servers and top 5 risky servers, as shown in the figure below.



Description of the content displayed:

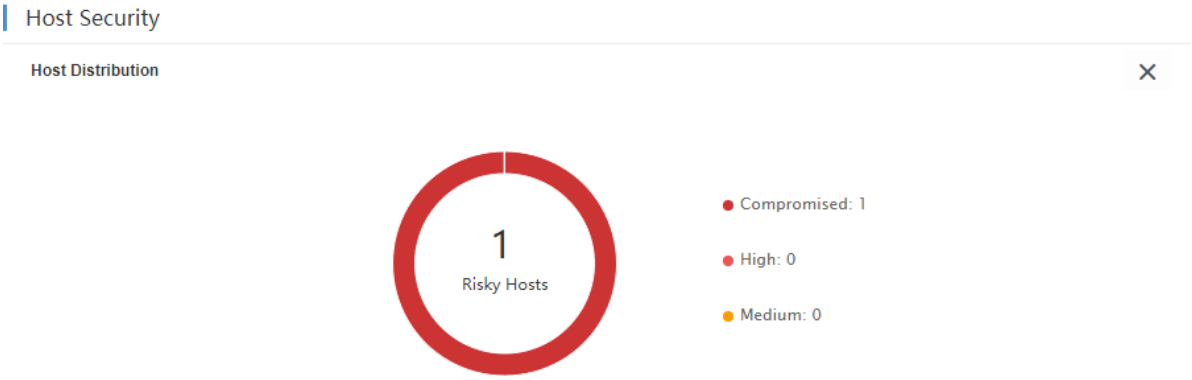
<Server Distribution: >This area displays the number of compromised, high risk, medium risk, low risk, and very-low risk endpoints in the current network as well as weaknesses, including exploits, improper configurations, weak passwords, and unencrypted traffic.

<Top 5 Risky Servers: >This area displays the top 5 risky servers. You can click <View More> to go to [Response/Risky Assets] to view the details.



Host security

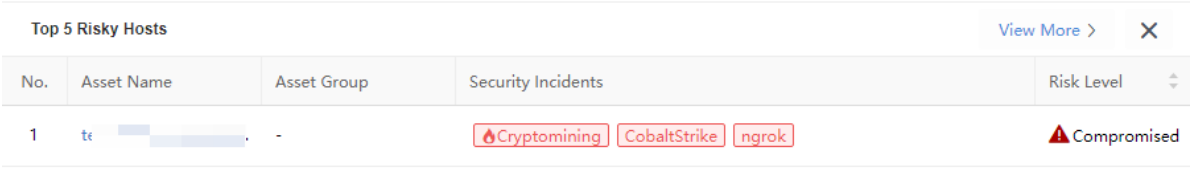
This part displays the distribution of hosts in different security states, including the number of compromised, high risk, and medium risk hosts and top 5 risky hosts, as shown in the figure below.



Description of the content displayed:

<Host Distribution: >This area displays the number of compromised, high risk, medium risk, low risk, and very-low risk hosts in the current network.

<Top 5 Risky Hosts:> This area displays the top 5 risky hosts. You can click <View More> to go to [Response/Risky Assets] to view details.



Threats

This part displays the threat distribution and the statistics of security incidents in the network from the perspective of security incidents, as shown in the figure below.



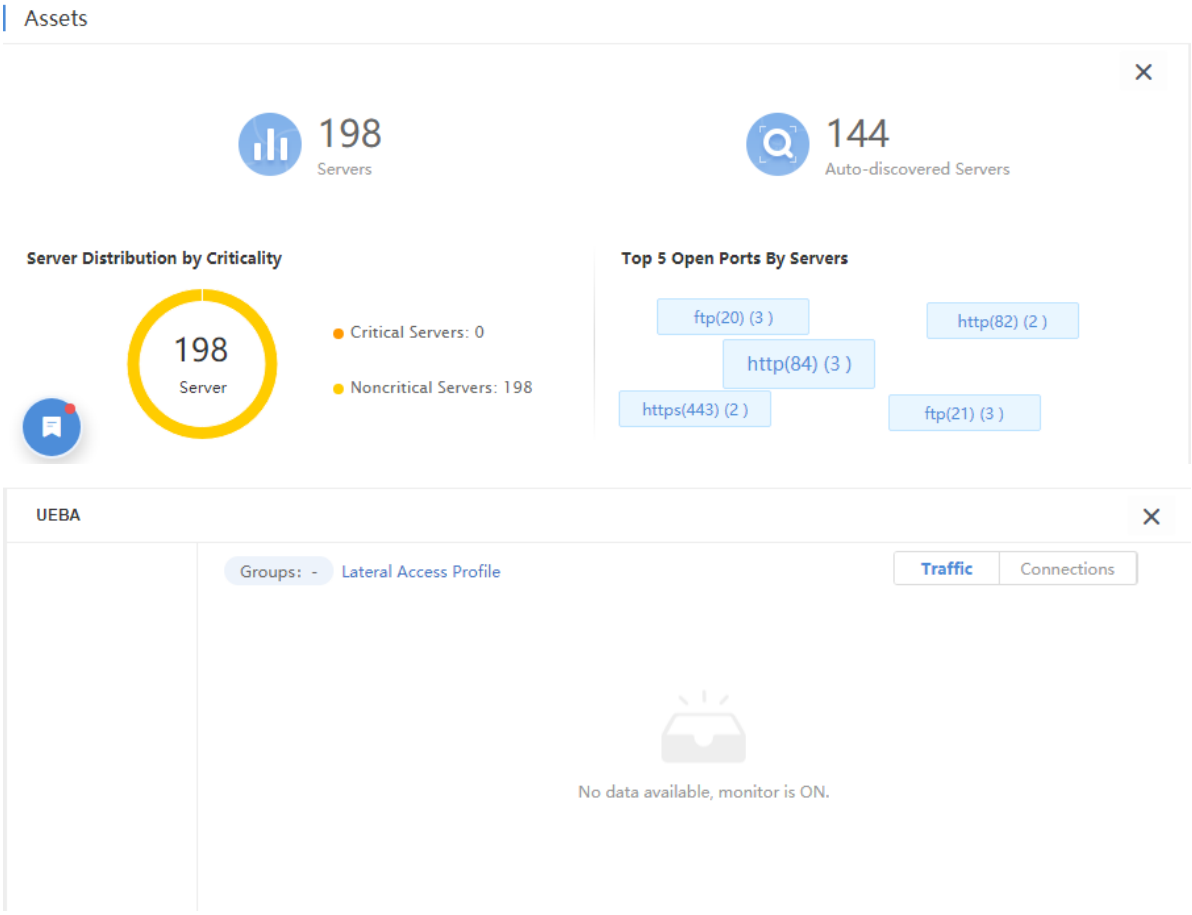
Description of the content displayed:

<Threat Distribution: >This area displays the number of threats every day, including inbound threats, lateral threats, and outbound threats. You can select the statistical period in the top right corner, such as the last 7 or 30 days. You can see the statistics on a threat by hovering the mouse over the part of the threat on the corresponding rectangular bar.

<Security Incidents: >This area displays the top 5 attacks. You can select the statistical period in the top right corner, such as the last 7 or 30 days. You can see the statistics on a security incident by hovering the mouse over the rectangular bar corresponding to the security incident. You can click <View More> to go to [Response/Threats] to view the risk details.

Assets

This part displays the information about server assets identified in the network. It also lists the UEBA of the top 5 servers with the most network traffic according to the rule that a server with more network traffic is displayed with higher priority, as shown in the figure below.



Description of the content displayed:

<Assets: >You can view the number of servers added compared with the same period of last week. You can click tags such as <Servers> and <Critical Servers> to go to the [Assets] page to view the details.

<Sever Distribution by Criticality: >This area can be displayed only when the criticality of server assets is specified.

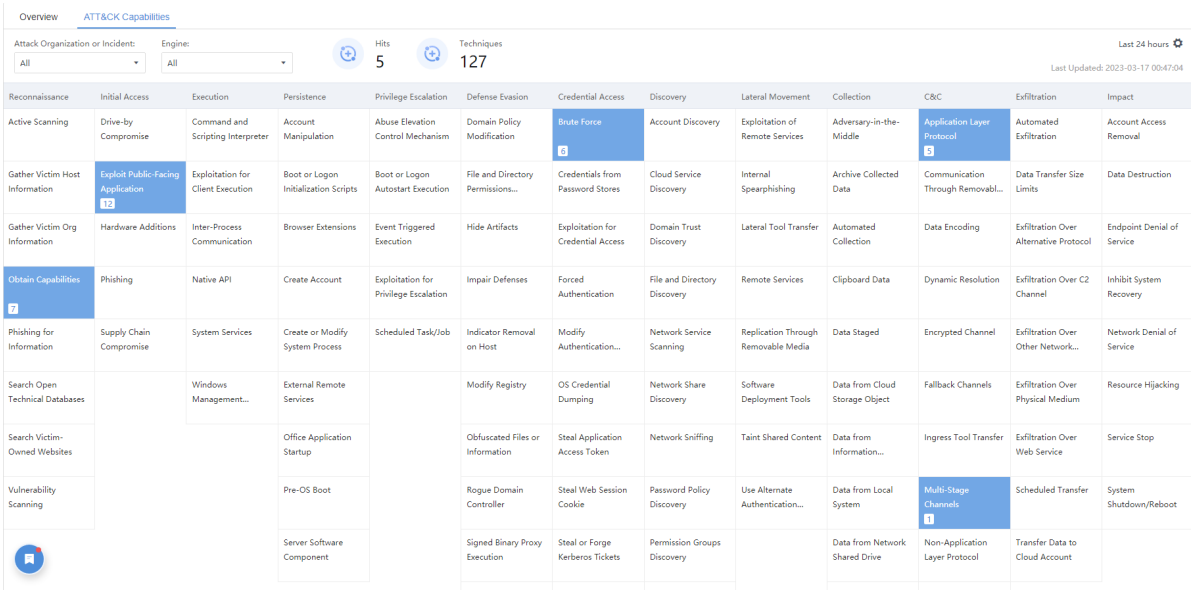
<UEBA: >This area displays abnormal servers first, followed by the UEBA of top 5 servers with the most traffic. You can click the bar tag of the abnormal server to go to [Detection/Anomalies/UEBA] to view details.

Note:

The baseline for anomalies is obtained after three weeks of endpoint behavior learning. (You can go to [Detection/UEBA] to view details.) The baseline is generated based on actual values three weeks ago, rather than average values in the last three weeks. \
In the figure above, the red dotted-line represents the baseline, and each bar represents the actual value of a day. When an actual value exceeds the baseline, a baseline anomaly occurs, and the corresponding bar will turn red.

ATT&CK Capabilities

The ATT&CK model consolidates past attacker organizations and attacks and links different attack policies to corresponding techniques and software based on attack policies. It provides an executable and moderately abstract model for information security practitioners. The ATT&CK Capabilities module maps the LAN security situation to different stages of the model, as shown in the figure below.



Description of the content displayed:

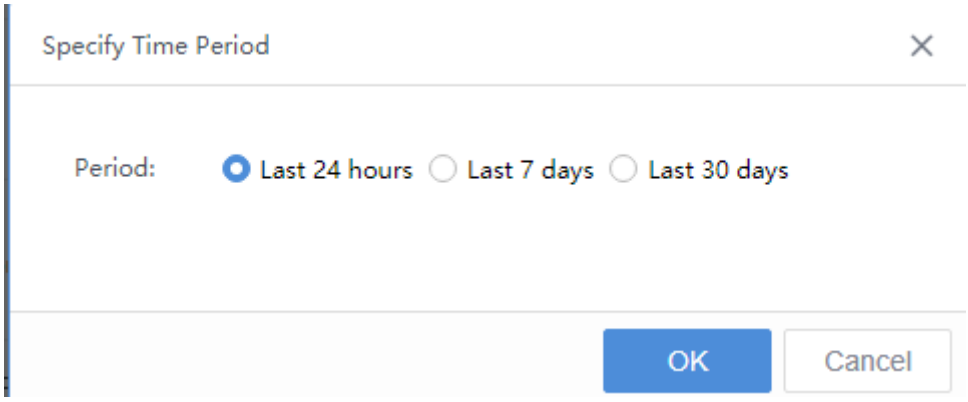
Attacker Organization or Incident: former famous attacker organizations or attacks, such as APT32, APT28, DarkVishnya, and Kinsing.

<Engine: >five engines of Nova Command, namely File Analytics Engine, Rule Engine, Attack Analytics Engine, Threat Intelligence Engine, and Abnormal Behavior Analytics Engine.

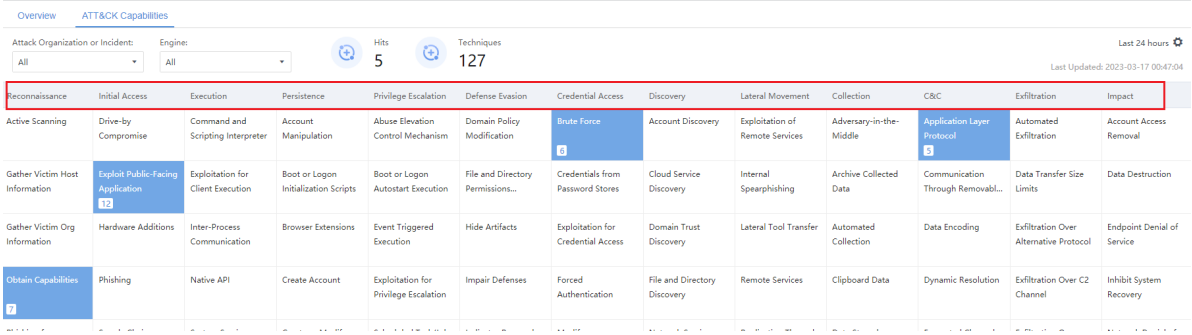
Hits: The cells in blue indicate hit techniques.

Techniques: Techniques supported by CC are all displayed on this page.

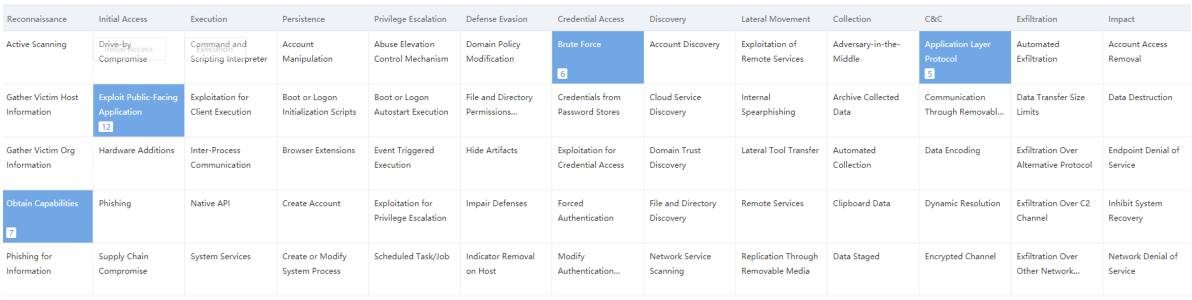
Specify Time Period: Data of the last 24 hours is displayed by default. You can also choose to display data of the last 7 or 30 days by clicking < ⚙ > and then specifying the time period, as shown in the figure below.



ATT&CK model stages: Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, C&C, Exfiltration, and Impact, as shown in the figure below.



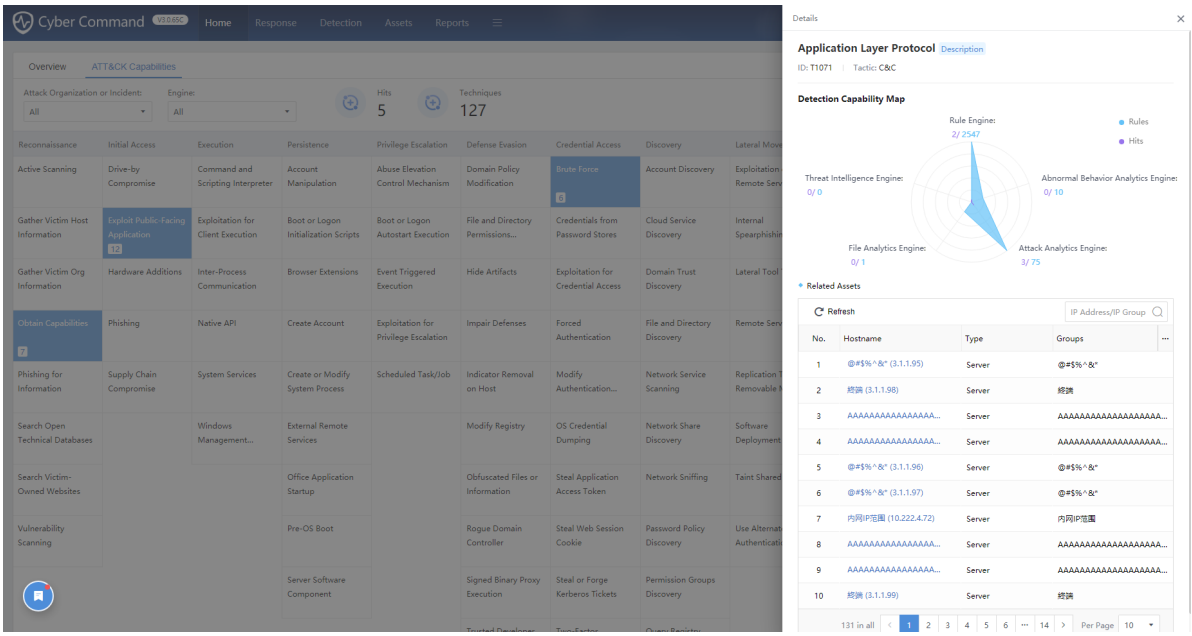
Technique cells: When a technique cell under a stage of ATT&CK Capabilities is shaded in a dark color, it means that the technique is a hit; when it is shaded in white with a technique name displayed, it means that the technique is available in Nova Command, but it is not a hit, as shown in the figure below.



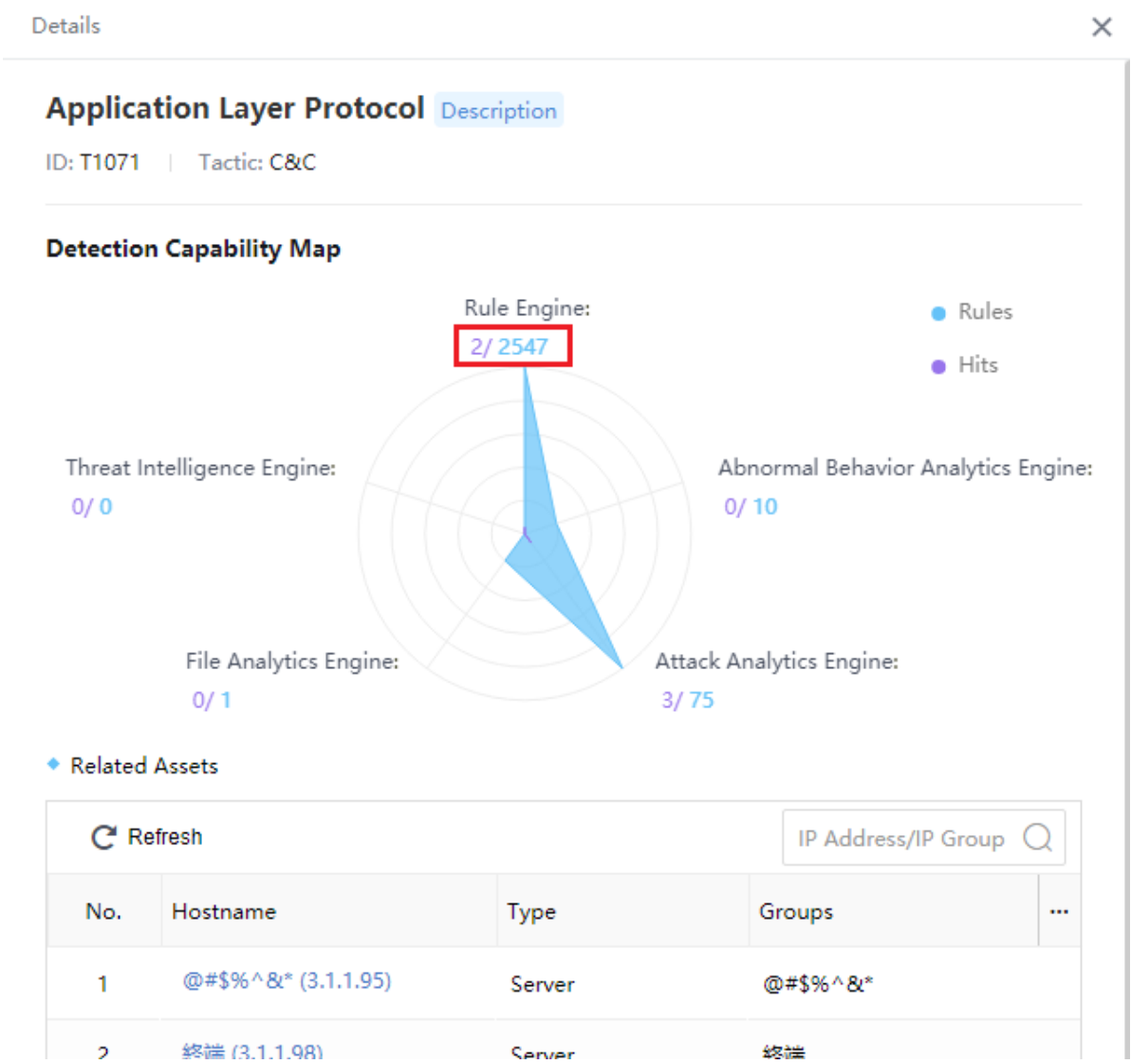
Note:

The distribution of colors and techniques in the ATT&CK Capabilities module changes with the version of Nova Command, the time when Nova Command is implemented in LAN environments, and the changes in abnormal traffic such as attacks.

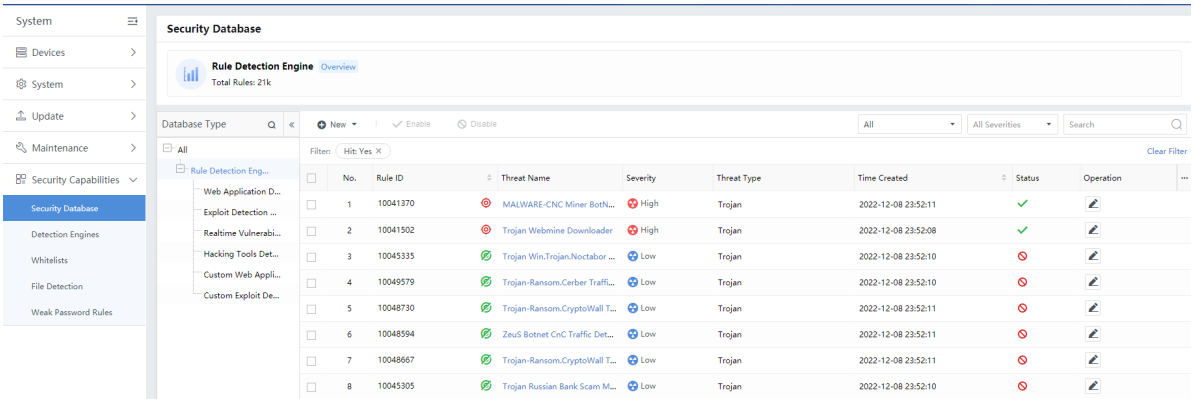
Several techniques will be mapped to each stage of ATT&CK Capabilities. You can click a technique to show the <Details> page on the right side, as shown in the figure below.



The <Details> page mainly displays the detection capability map and a description of the attack that corresponds to the technique. Supported engines include File Analytics Engine, Rule Engine, Attack Analytics Engine, Threat Intelligence Engine, and Abnormal Behavior Analytics Engine. The number in blue represents the rules covered by the engine and that in purple represents the rules hit in the current time period, as shown in the figure below.



You can click the number to go to the [System/Security Capabilities/Detection Engines] page, as shown in the figure below.

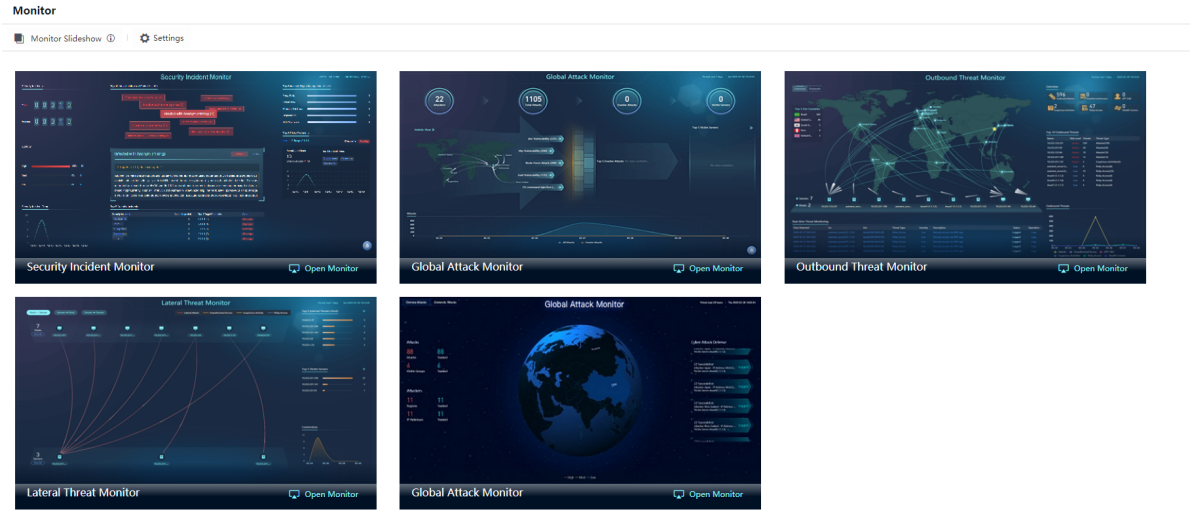


Note:

ATT&CK and Security Alerts are two independent modules that have no logical dependencies on each other. The attributes of a rule include columns of both ATT&CK and Detection Engines.

Monitor

The Monitor module provides five monitors for displaying data on a large screen or in the form of a slideshow, including Security Incident Monitor, Global Attack Monitor, Outbound Threat Monitor, Lateral Threat Monitor, and Global Attack Monitor, to display the security status of the whole network visually, as shown in the figure below.



Note:

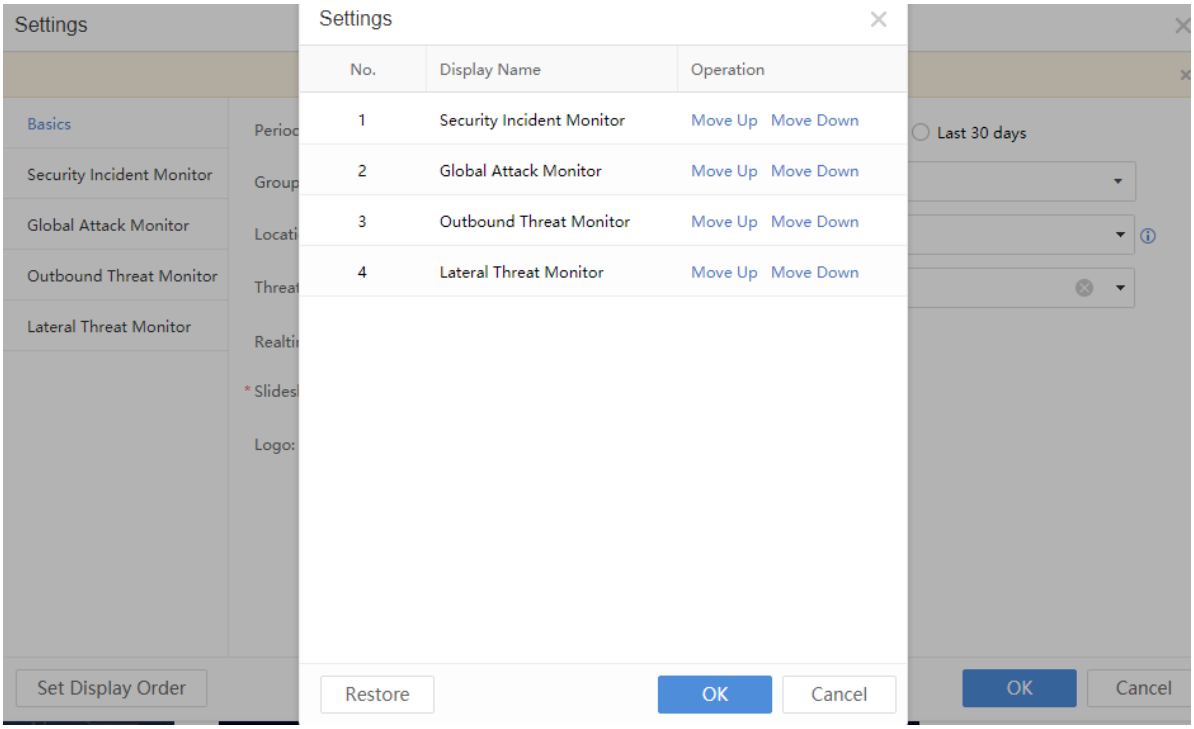
Monitor Slideshow is applicable to single screen display and can display all monitors in the form of a slideshow. You can go to the [Monitor/Settings] page to specify the slideshow interval.

Monitor Settings

This page allows you to set the display order, global parameters, and exclusive parameters for each monitor.

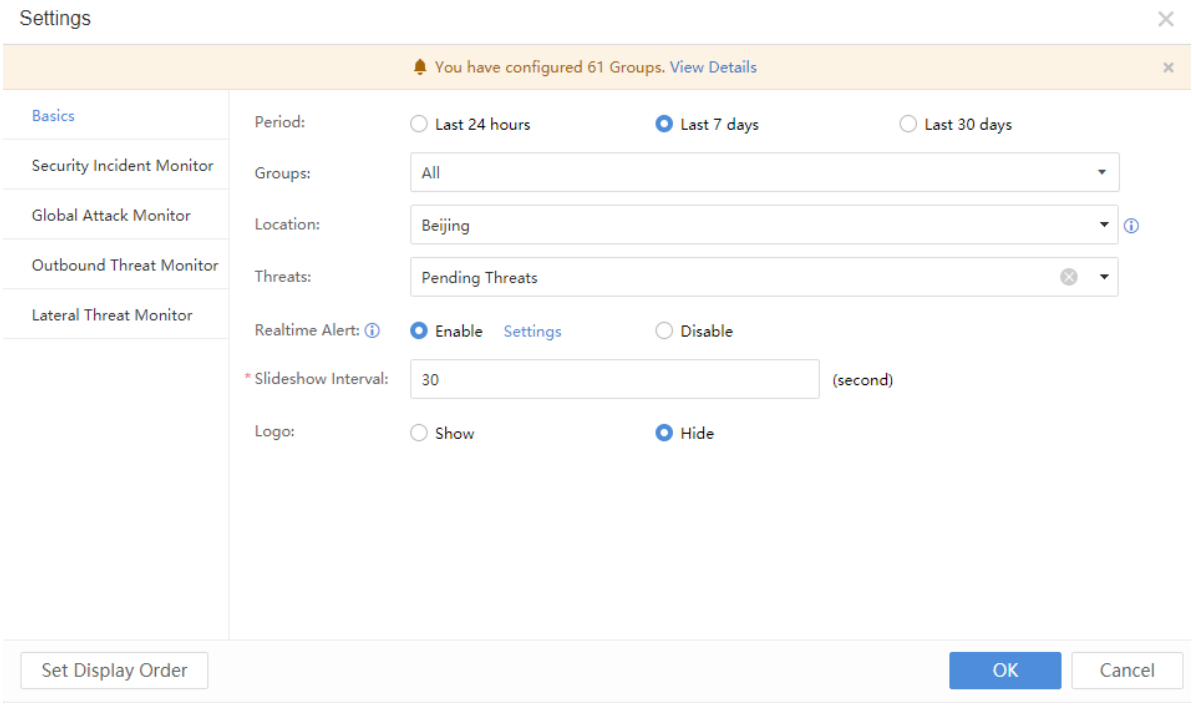
Monitor display order settings

You can go to [Home/Monitor/Settings], click Set Display Order on the page that appears, and then click Move Up or Move Down to adjust the display order of each monitor, as shown in the figure below.



Global settings

You can click Basics to set global parameters, as shown in the figure below.



Description of the content displayed:

<Period: >This is the statistical period of all monitors. You can select "Last 24 hours". "Last 7 days", and "Last 30 days".

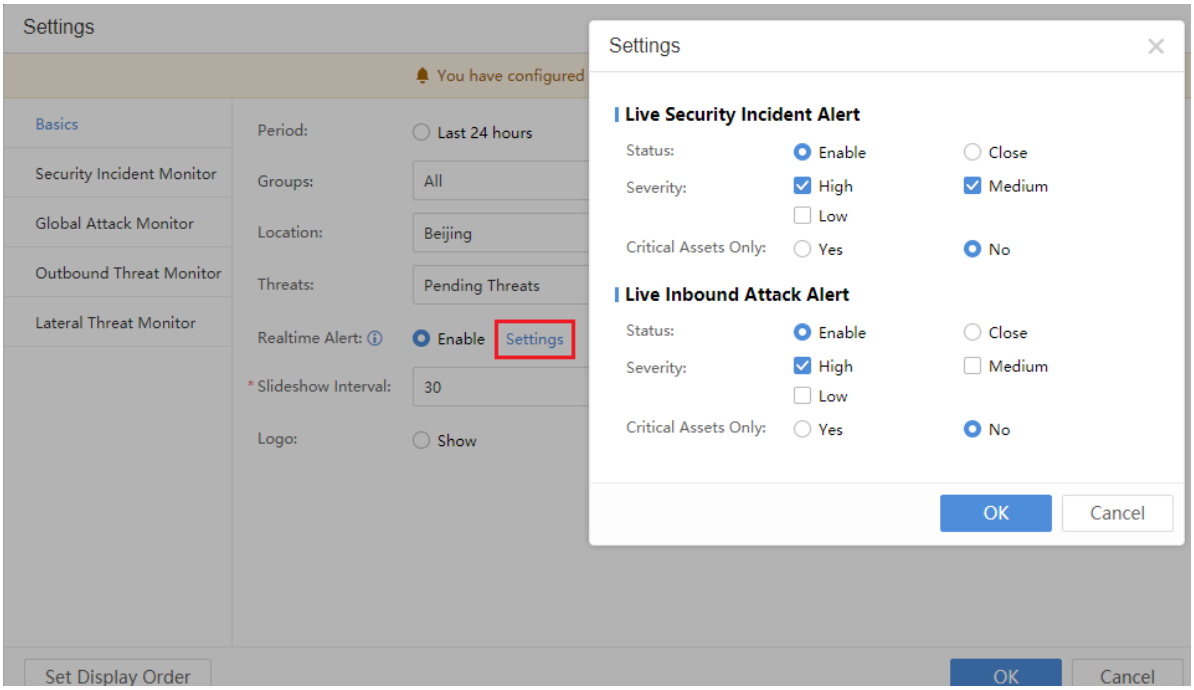
<Groups: >The asset group name displayed here is configured under [Assets/Assets/Assets]. When it is configured, only data of the corresponding group will be displayed on all monitors.

Note:

You can view the current asset group name and modify it by setting the "Panel Name" parameter in the [Other] section under [Assets/Assets/Settings].

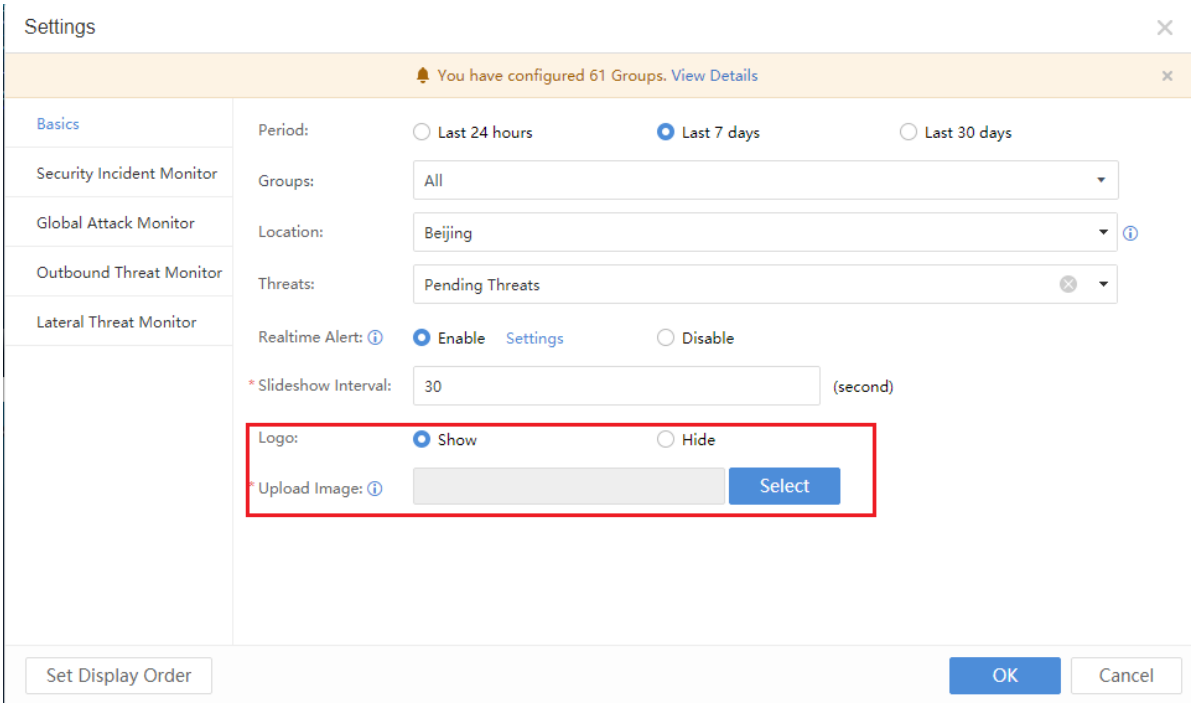
<Threats: >You can select "Fixed Threats", "Pending Threats", or "All".

<Realtime Alert: >When enabled, a new threat will be popped up on the large screen in real time. You can click <Settings> to complete the settings for Live Security Incident Alert and Live Inbound Attack Alert, as shown in the figure below.



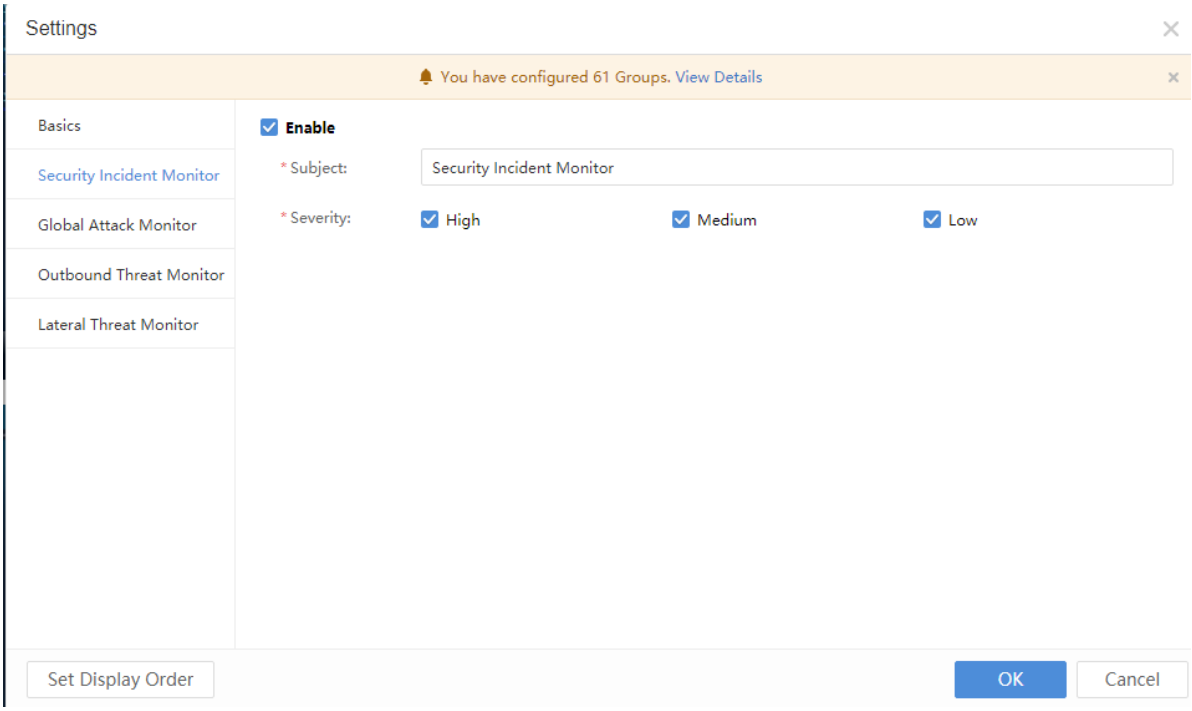
<Slideshow Interval: >You can specify the interval for displaying two monitors.

<Logo: >An exclusive logo can be displayed on the large screen. The logo file must be in PNG format and cannot exceed 1 MB.



Settings for each monitor

On the [Monitor/Settings] page, you can modify the configurations of each monitor based on their features. For example, you can modify the subject, display mode, and display items to meet your requirements in different scenarios.



Monitors

Monitors that are provided include Security Incident Monitor, Global Attack Monitor (2D), Outbound Threat Monitor, Lateral Threat Monitor, and Global Attack Monitor (3D).

Note:

The monitor names above were those displayed in the environment that we referred to when we wrote this manual. You can change the names after communicating with the customer.

Security Incident Monitor

It monitors the security incidents in the LAN and the latest hot incidents in the cybersecurity industry in real time to provide you with a quick look at the security situation of the LAN. The figure below shows the monitor page.



Global Attack Monitor (2D & 3D)

With this monitor, you can monitor inbound attacks from around the world, and view real-time information about attackers, targets, and attack techniques.

The figure below shows the monitor page.

2D monitor page



3D monitor page



Note:

For a 3D monitor, the display PC must be equipped with a discrete graphics card to avoid lagging and stuttering problems.

Outbound Threat Monitor

It monitors secure outbound access and shows which areas of the external network are accessed and which servers and hosts launch the most outbound access.

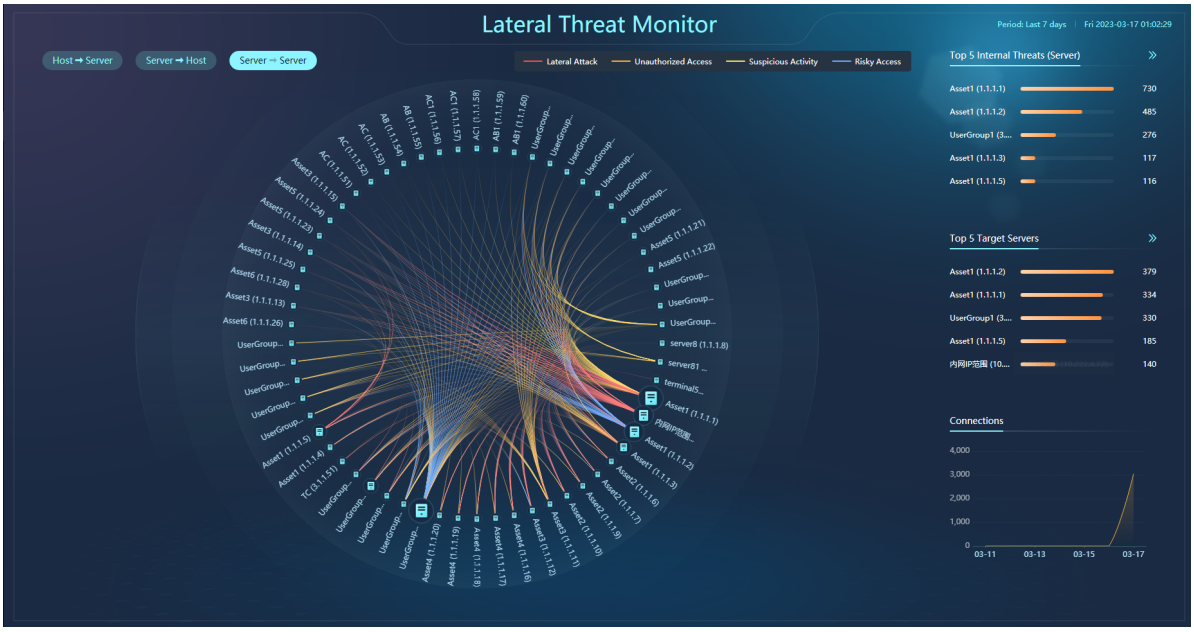
The figure below shows the monitor page.



Lateral Threat Monitor

It monitors lateral threat movement in the LAN and shows risks such as lateral attacks, unauthorized access, suspicious activities, and risky access.

The figure below shows the monitor page.

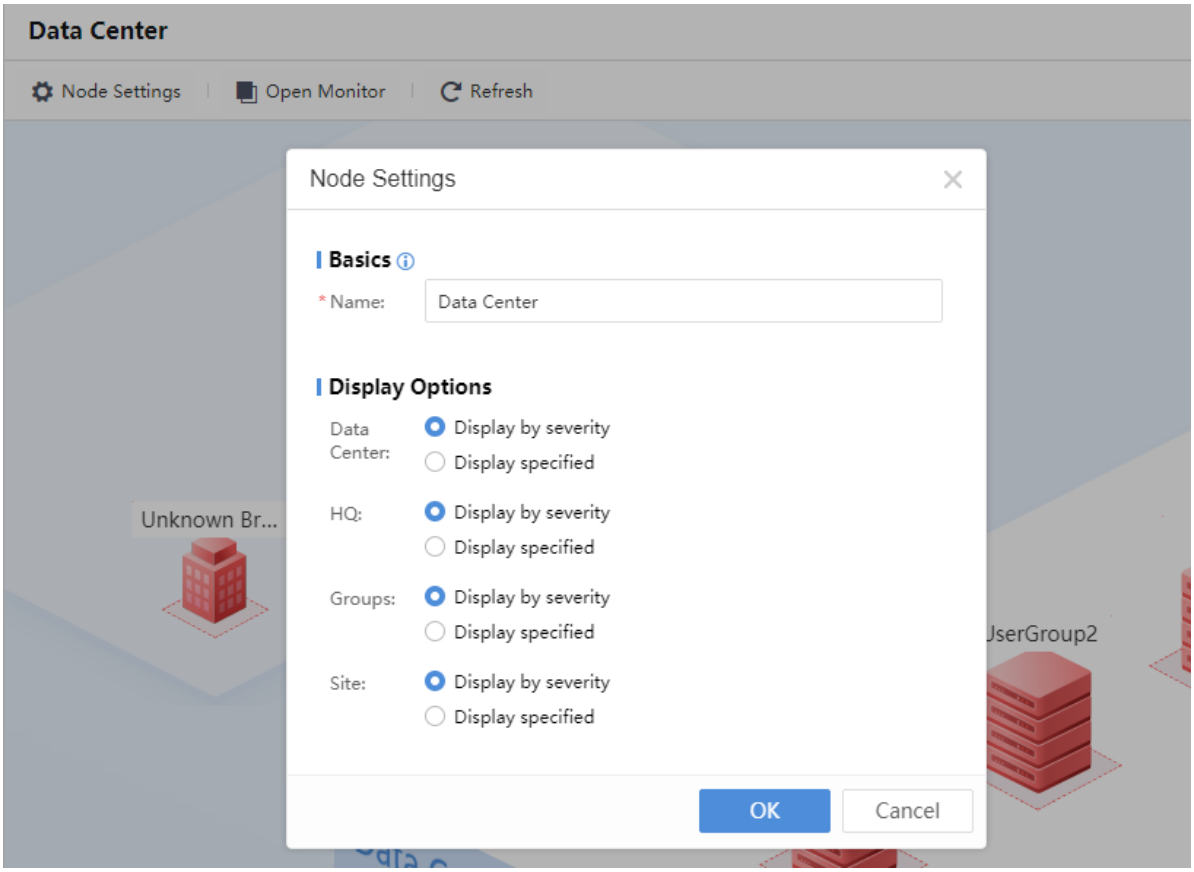


Data Center

On the [Home/Data Center] page, you can view the access between servers and their inbound and lateral attacks and filter the data to display by time period.

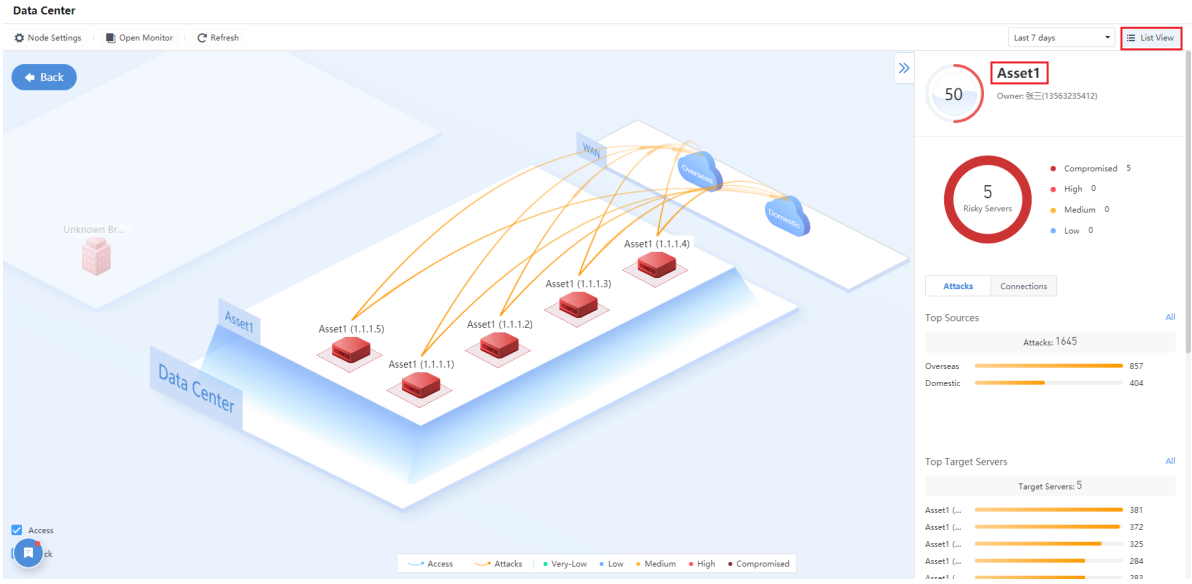
Node settings

On the [Data Center] page, you can click [Node Settings] to customize the name of the server zone and the visualization zone display, as shown in the figure below.

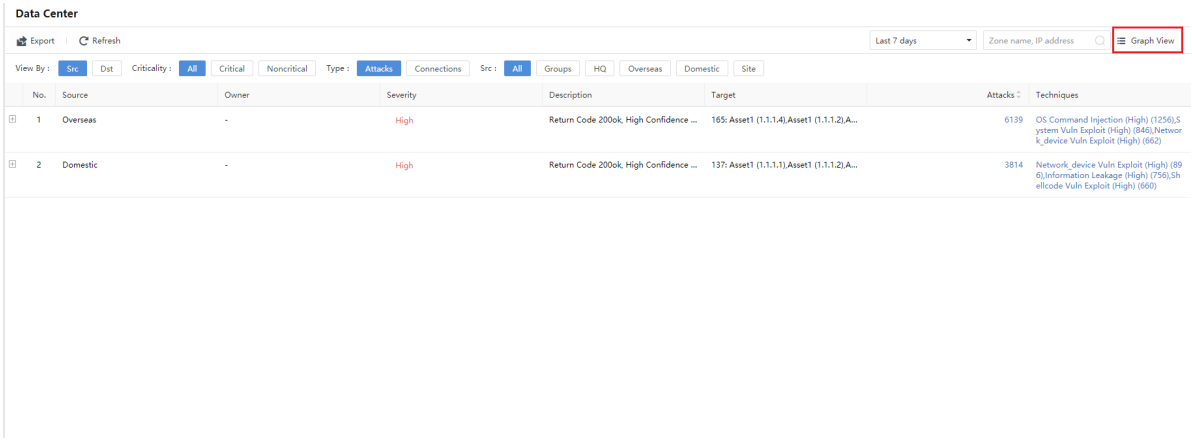


Display mode

The display mode for [Data Center] can be set to the list or graphics (default) mode. You can click the switch icon in the top right corner to switch between display modes. The data center displayed in graphics mode is shown below. When you click a specific asset group, the corresponding threats will be displayed on the right, as shown in the figure below.

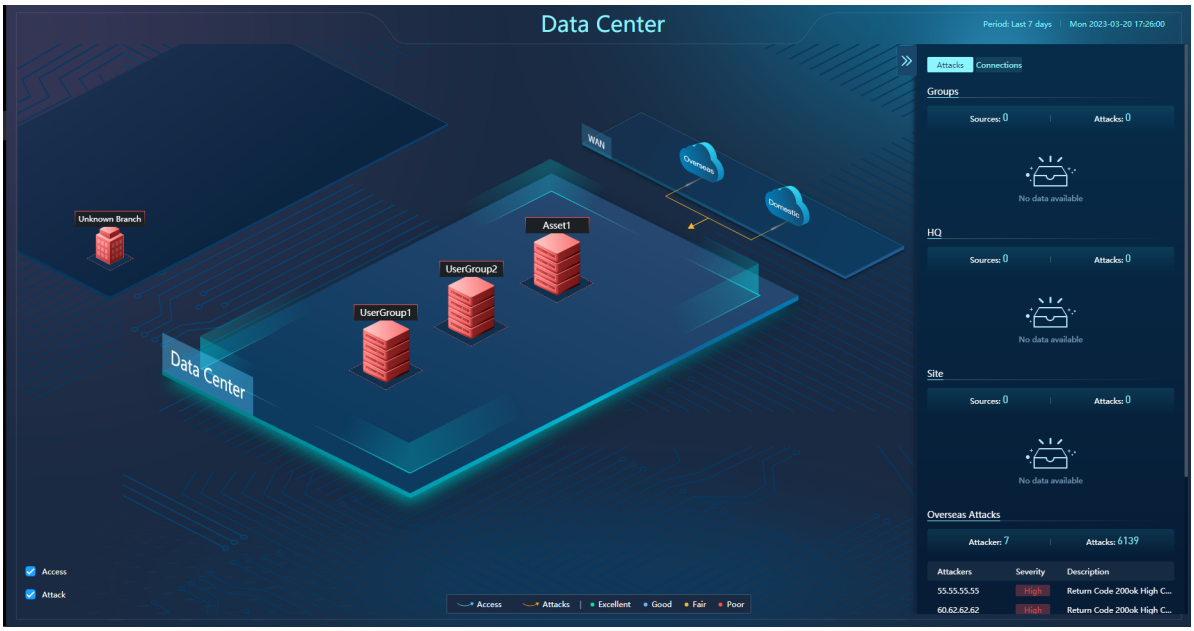


The data center in list mode is shown below. In this mode, you can filter attacks in different dimensions such as the period, view, and server level, and can export current status by clicking the <Export> button.



Display on a large screen

In graphics mode, you can click <Cast Screen> to display the data on a large screen, as shown in the figure below.

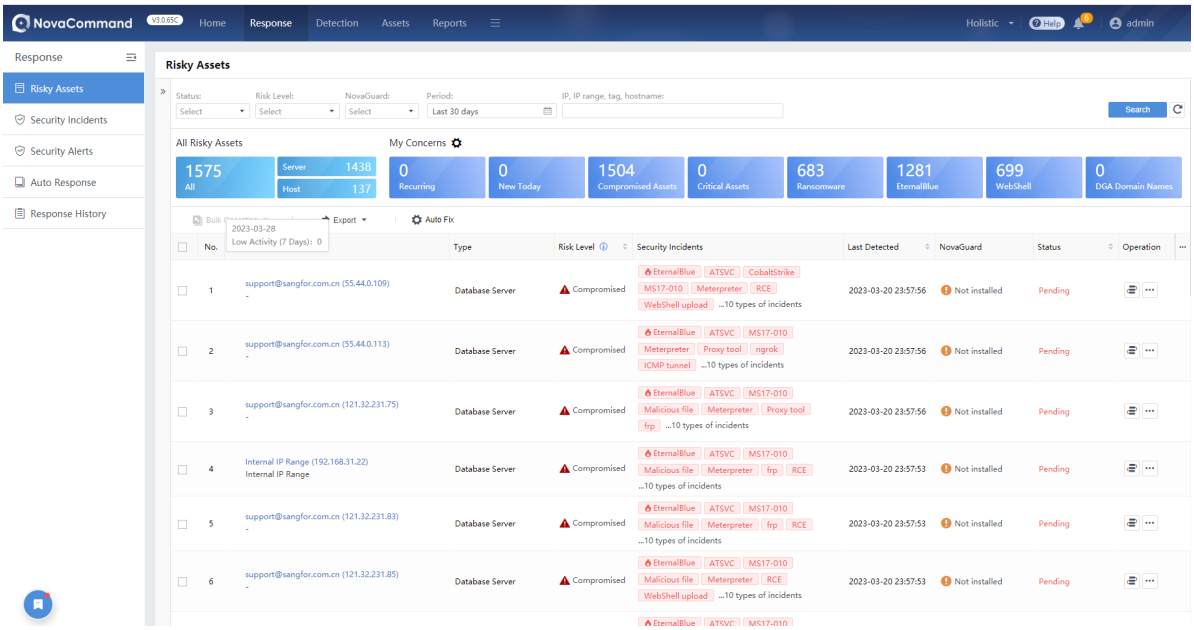


Response

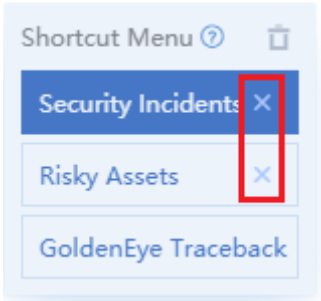
Nova Command collects logs through Stealth Threat Analysis (Nova Sensor), Next Generation Application Firewall (NGAF), and other connected devices and uses big data analytics to derive security alerts and security incidents for assets. The Response module can identify risky assets involved in these security incidents and analyze and respond to these incidents properly.

Shortcut Menu

On the [Response] page, when you move the mouse to the [Response] menu, the Open in New Page sign **(⊕)** appears. By clicking the sign, you can see [Risky Assets] in the shortcut menu that appears in the bottom left corner of the page after you click "", as shown in the figure below.



You can open a new page in the browser by clicking the corresponding option in the shortcut menu. The data displayed on each page does not change during page switching to facilitate operations. You can click the "×" sign next to each option to close the corresponding page, as shown in the figure below.



Click the Clear sign " " at the top right to delete all options from the shortcut menu and restore the default settings.

Risky Assets

Nova Command allows you to filter risky assets by Risk Level, Status, NovaGuard, and other supported criteria, which makes the response efficiently.

Risky asset filtration

Log into Nova Command as an administrator and filter risky assets on the [Response/Risky Assets] page in the following ways:

1. Filter risky assets by **Groups** on the left sidebar.
2. Filter risky assets by **Status** for bulk operation purposes. The states are "All", "Pending", "Suspended", "Fixing", and "Fixed".
3. Filter risky assets by **Risk Level**. The risk levels are "All", "Compromised", "High Risk", and "Medium Risk". You need to make timely responses to compromised, high risk, and medium risk assets to avoid business interruption caused by risk spread.
4. Filter risky assets by NovaGuard. The NovaGuard options are "Offline", "Online", "Disable", "Uninstall", "Unauthorized", and "Not installed". This search condition is displayed only when NovaGuard is connected to Nova Command.

Note:

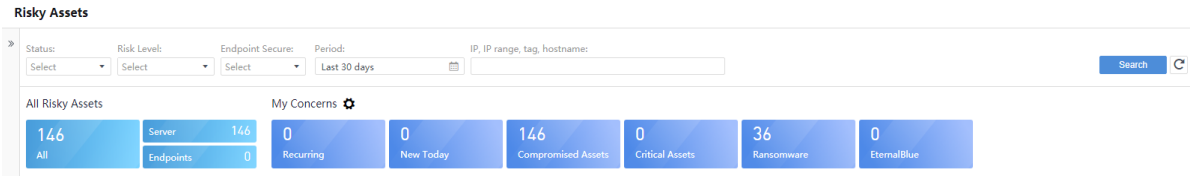
[Compromised]: Security-compromising incidents such as C&C, lateral movement, and attack success occurred on the endpoint. The endpoint has been or is about to be controlled. Please make a response as soon as possible.

[High Risk] The endpoint is found with weaknesses or is under reconnaissance or intrusion. In this case, the endpoint might be exploited. Please make a response soon as possible.

[Medium Risk] The endpoint has been affected by medium risk viruses and might be exploited. Please check and make a response.

---

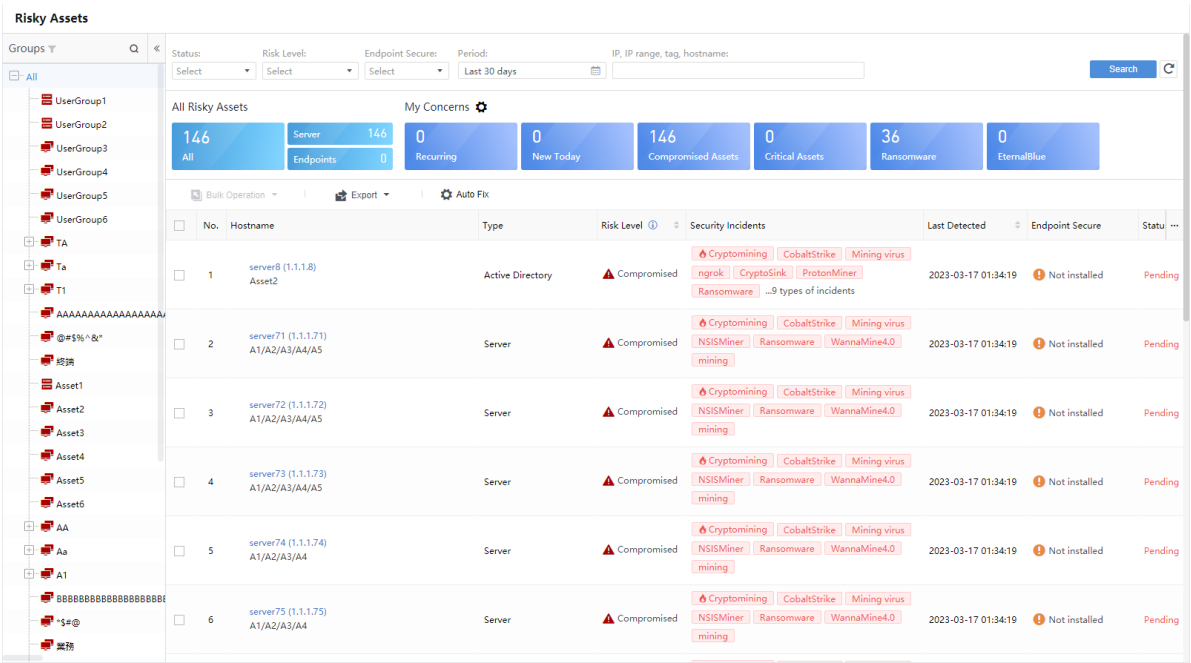
5. Filter risky assets by **Period** to view and fix risks that occurred within the specified period. The periods are "Last 30 days", "Last 7 days", "Last 24 hours", and "Custom".
6. Filter risky assets by IP address, IP range, asset group, or hostname.
7. Filter risky assets in the My Concerns module. For example, you can click <Server> to display only risky assets of the server type in the list.



By filtering risky assets in one or multiple ways, you can accurately locate risky assets, analyze them from different dimensions, and make a response. You can filter data in All Risky Assets, My Concerns, and the asset list. The search boxes can remember your selection last time, so you do not need to select them again next time.

Risky Asset Viewing

You can view the asset group structure of the current platform, statistics on all risky assets, risky assets that you are concerned about, and the risky assets list, as shown in the figure below.



All risky assets

Risky assets of the last one month are displayed by default, and are classified into risky hosts and servers by the platform. You can filter them as needed. The filtering takes effect at the same time on data displayed in the Groups and My Concerns modules as well as on data in the asset list. By clicking Server or Endpoints, you can view the details of risky server assets or endpoint assets in the asset list.

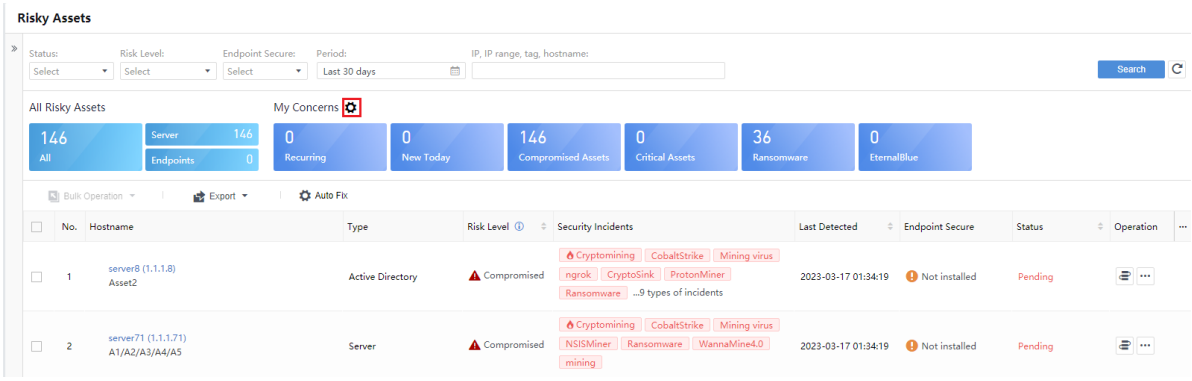
Assets to concern about

You can specify the assets to concern about in the <My Concerns> module. You can click a card in this module to filter assets to display and click the card again to cancel the filtering.

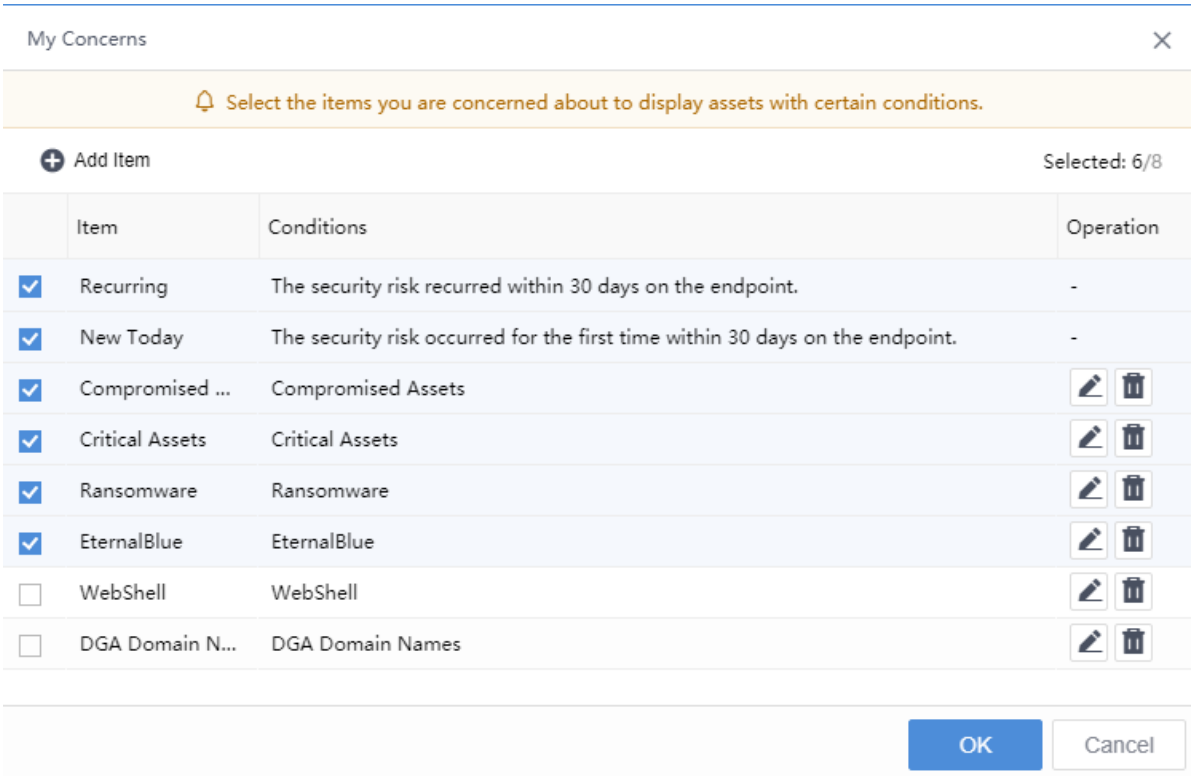
Setting of assets to concern about

You can click the settings button <

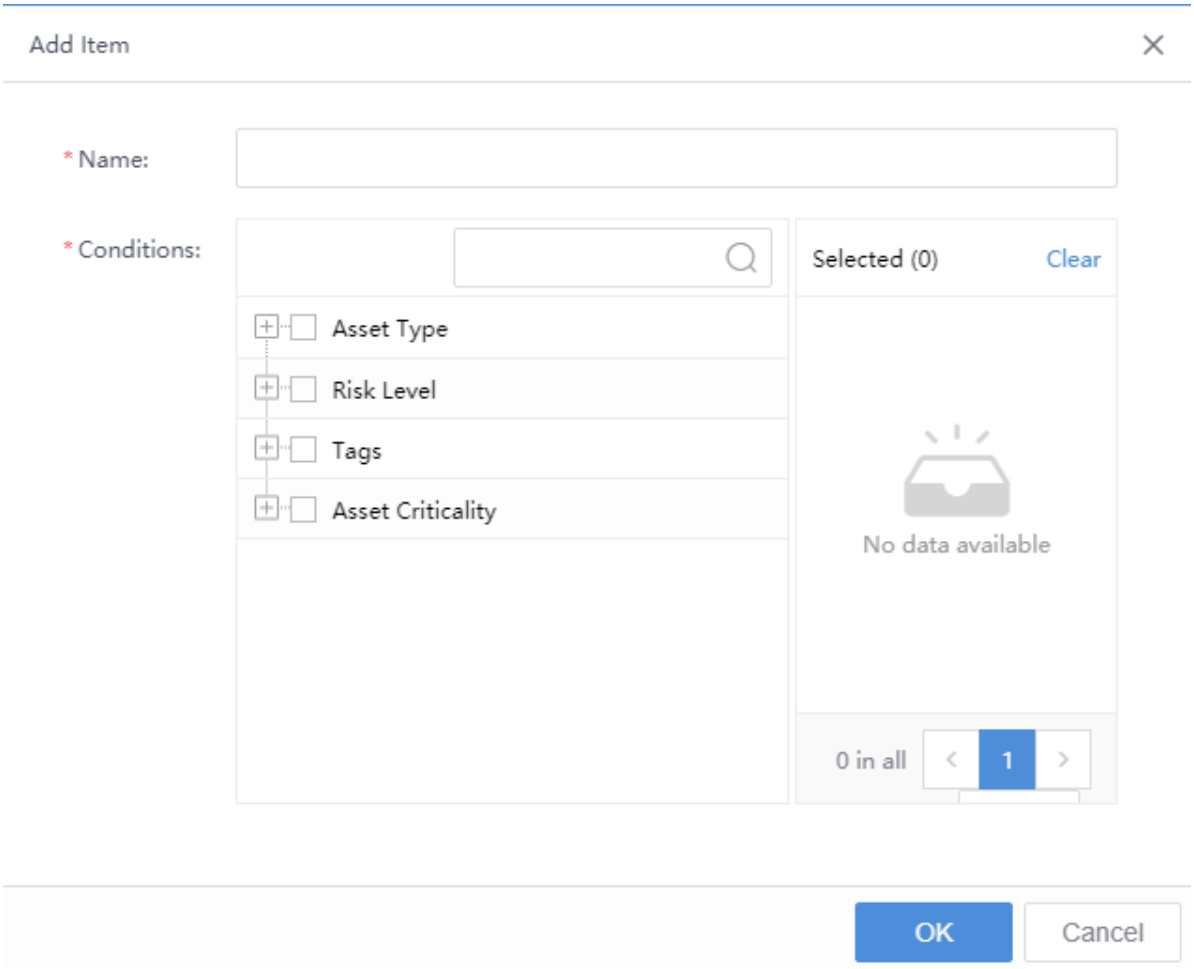
> next to My Concerns to set assets to concern about, as shown in the figure below.



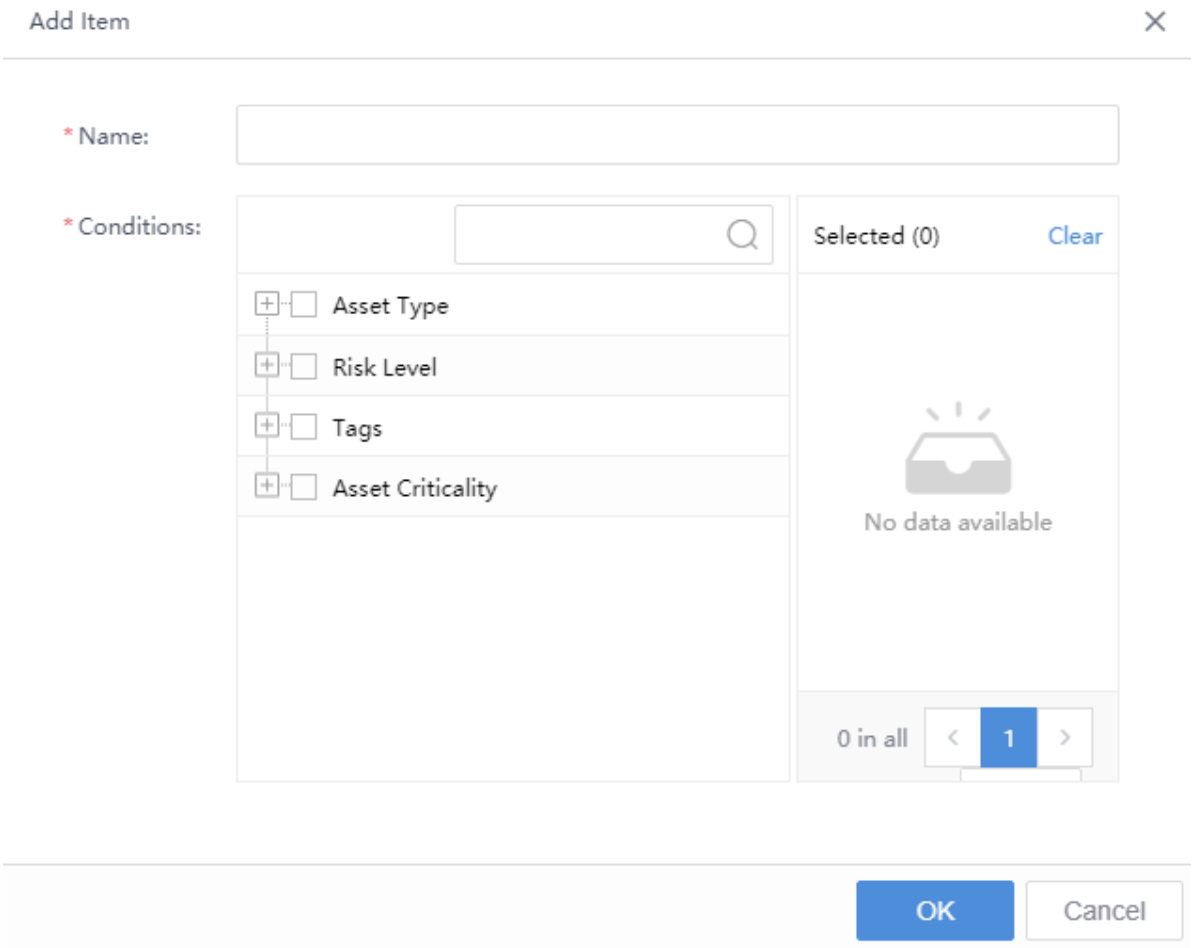
The default asset groups are "Recurring", "New Today", "Compromised Assets", and "Critical Assets". If you do not want to display assets in any of these groups, you can deselect their checkboxes.



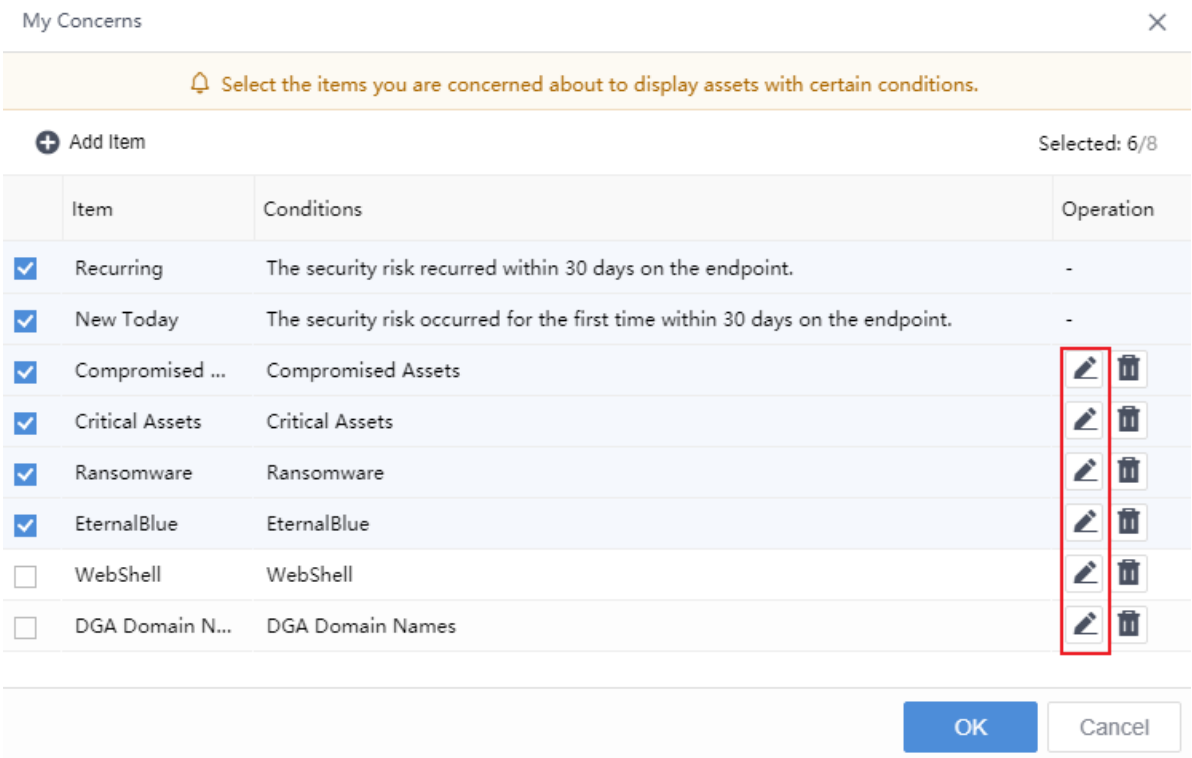
You can also add groups by clicking <Add Item>.



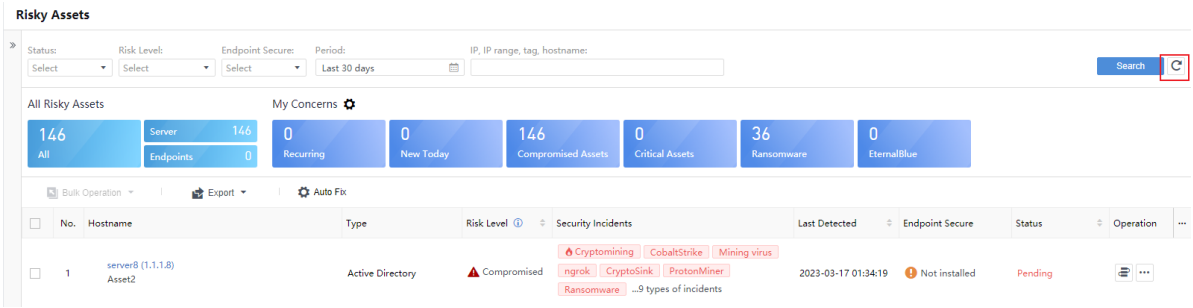
Specify the name and then select [Asset Type], [Risk Level], and [Asset Criticality] to specify conditions, as shown in the figure below.



You can edit the groups you are concerned about by clicking the < > button.

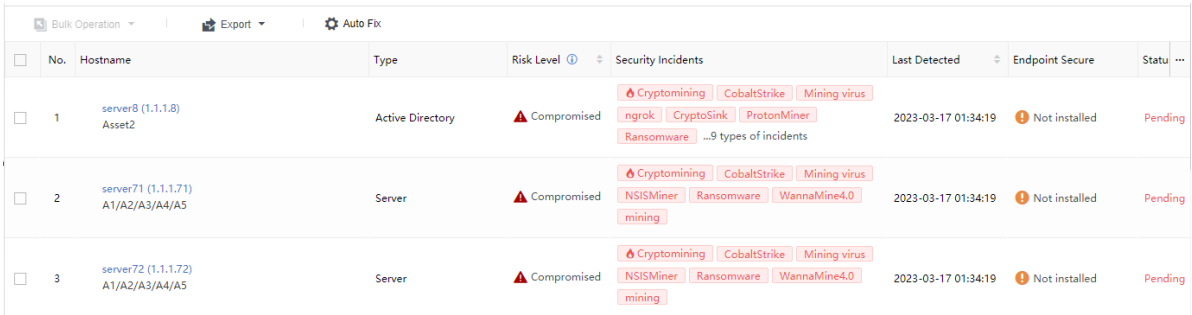


You can click <Refresh> to view new groups added to My Concerns, as shown in the figure below.



Risky assets list

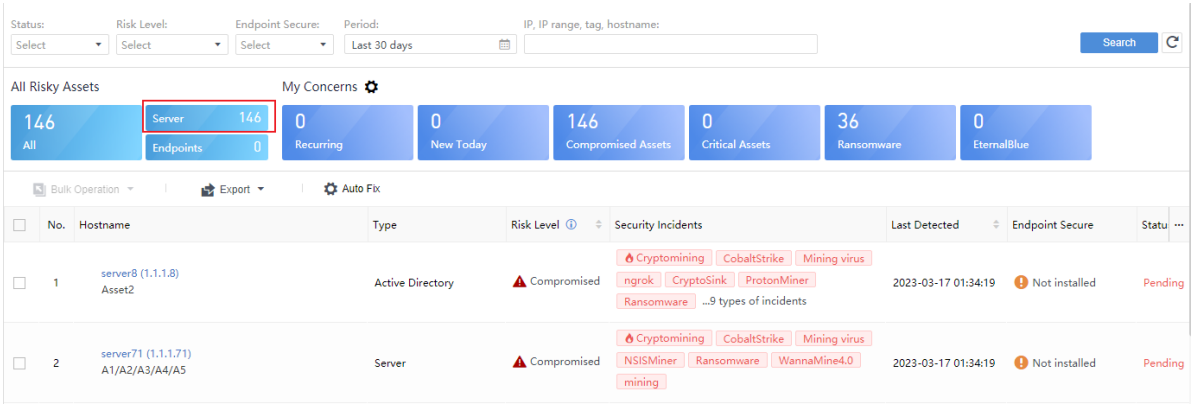
You can view the asset name, risk level, security incident, the last detection time, status, and NovaGuard in the list.



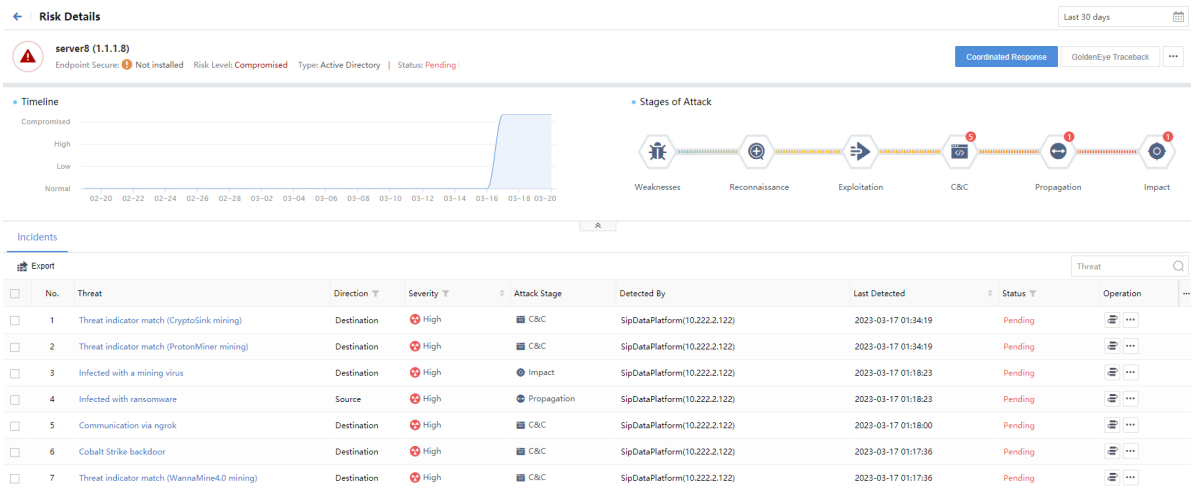
You can click <...> to select a response operation to perform on the incident.

Risky servers

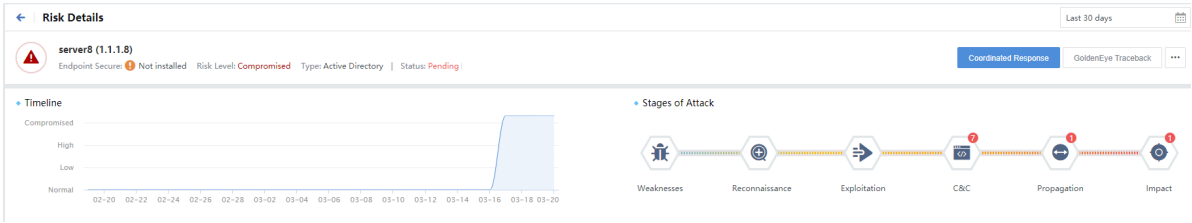
Under All Risky Assets, you can click <**Server**> to display only the risky assets of the server type in the risky assets list.



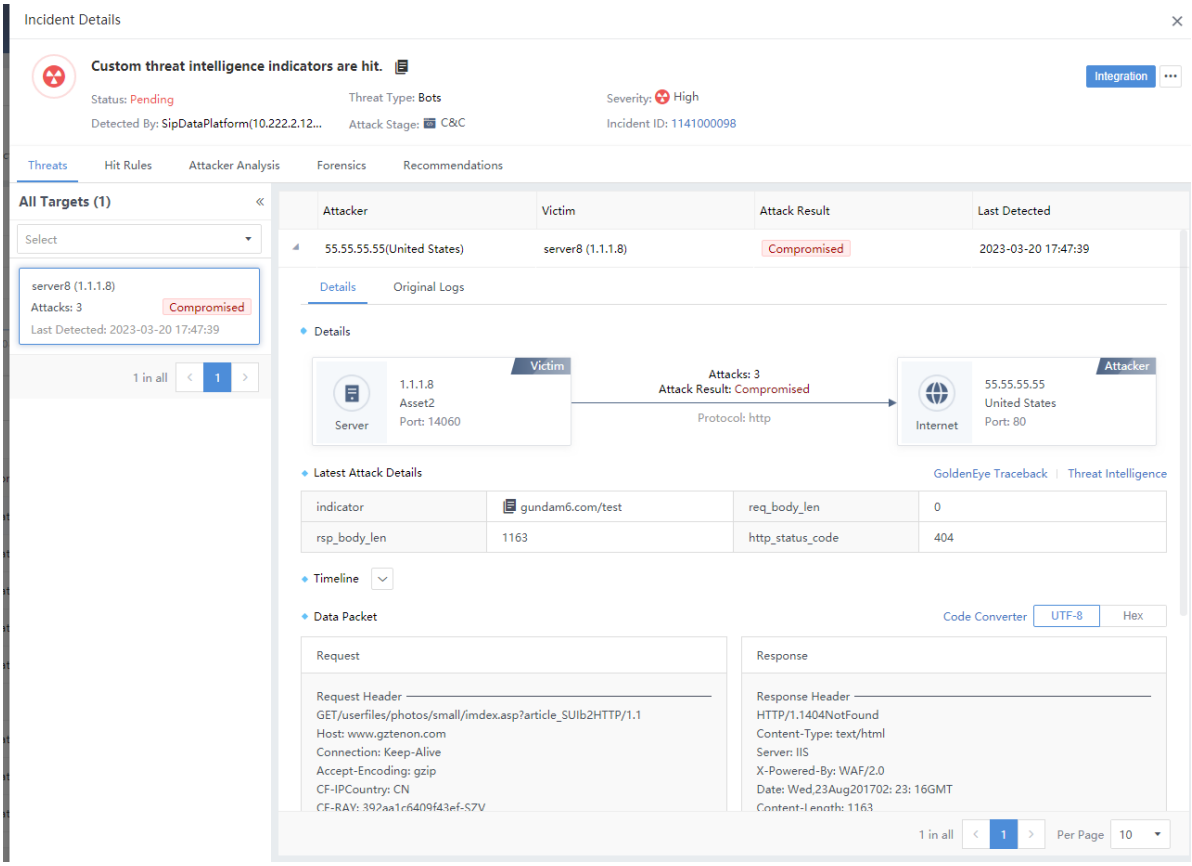
You can click an asset name to view the risk details of a risky server, including statistics, security incidents, incident view, and threats, as shown in the figure below.

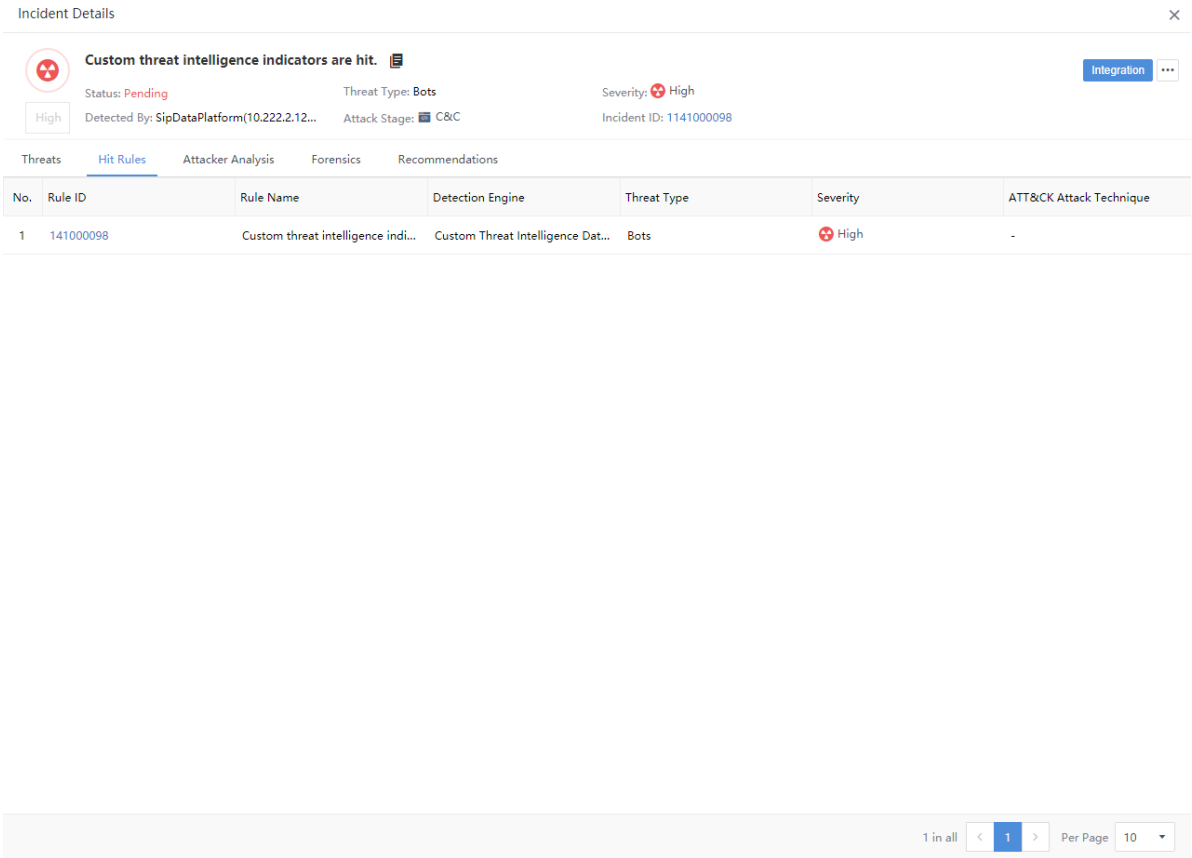


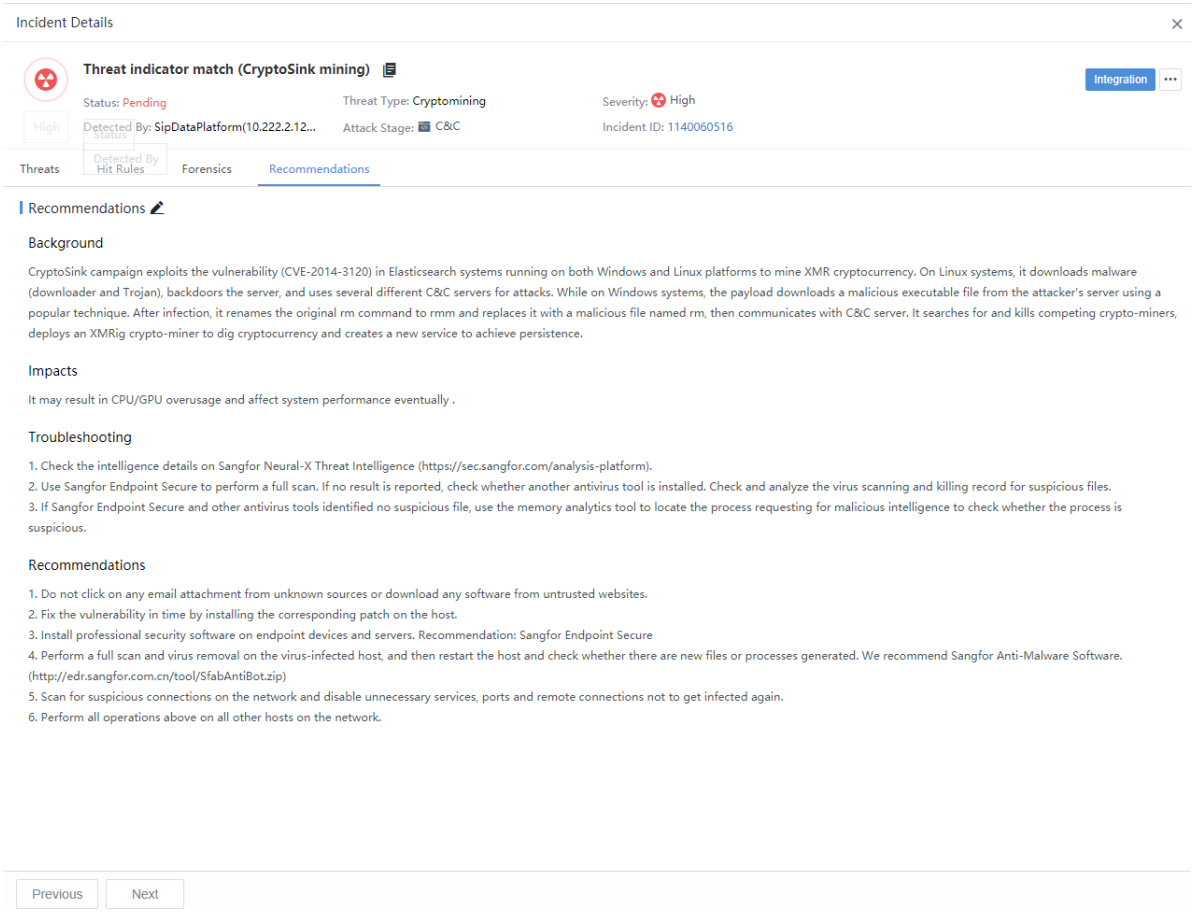
In the statistics zone, risk level trend and stages of attack are displayed by default, as shown in the figure below.



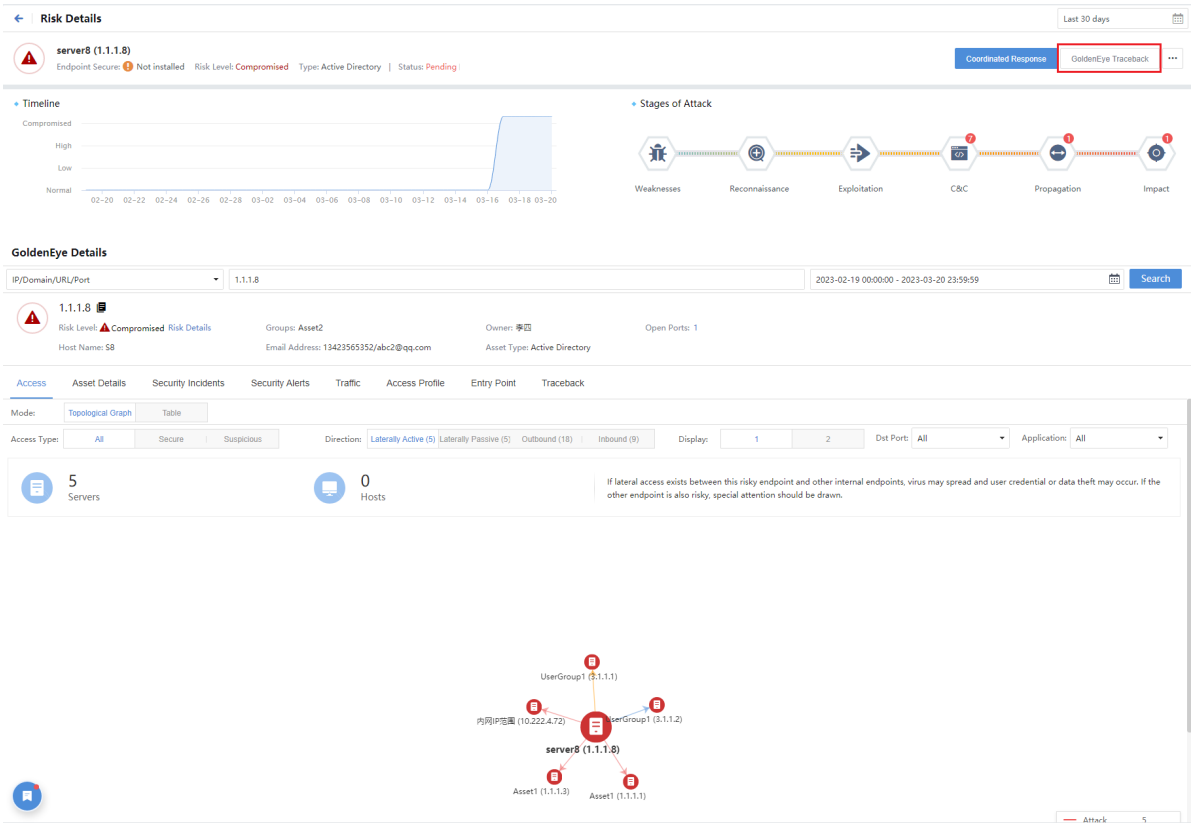
You can click the name of an incident to view its details, including hit rules, forensics (triggered by specific rules), and response recommendations, as shown in the figure below.


Incident Details
Custom threat intelligence indicators are hit.
Status: Pending
Threat Type: Bots
Severity: High
Detected By: SipDataPlatform(10.222.2.12...
Attack Stage: C&C
Incident ID: 1141000098
Integration
Threats
Hit Rules
Attacker Analysis
Forensics
Recommendations
All Targets (1)
Select
server8 (1.1.1.8)
Attacks: 3
Compromised
Last Detected: 2023-03-20 17:47:39
1 in all
Attacker
Victim
Attack Result
Last Detected
55.55.55.55(United States)
server8 (1.1.1.8)
Compromised
2023-03-20 17:47:39
Details
Original Logs
Details
Victim
Server
1.1.1.8
Asset2
Port: 14060
Attacks: 3
Attack Result: Compromised
Protocol: http
Attacker
Internet
55.55.55.55
United States
Port: 80
Latest Attack Details
GoldenEye Traceback
Threat Intelligence
indicator
gundam6.com/test
req_body_len
0
rsp_body_len
1163
http_status_code
404
Timeline
Data Packet
Code Converter
UTF-8
Hex
Request
Request Header
GET/userfiles/photos/small/imdex.asp?article_SUIb2HTTP/1.1
Host: www.gztenon.com
Connection: Keep-Alive
Accept-Encoding: gzip
CF-IPCountry: CN
CF-RAY: 392aa1c6409f43ef-SZV
Response
Response Header
HTTP/1.1404NotFound
Content-Type: text/html
Server: IIS
X-Powered-By: WAF/2.0
Date: Wed,23Aug201702: 23: 16GMT
Content-Length: 1163
1 in all
Per Page
10


Incident Details
Custom threat intelligence indicators are hit.
Status: Pending
Threat Type: Bots
Severity: High
High
Detected By: SipDataPlatform(10.222.2.12...
Attack Stage: C&C
Incident ID: 1141000098
Integration
Threats
Hit Rules
Attacker Analysis
Forensics
Recommendations
No.
Rule ID
Rule Name
Detection Engine
Threat Type
Severity
ATT&CK Attack Technique
1
141000098
Custom threat intelligence indi...
Custom Threat Intelligence Dat...
Bots
High
-
1 in all
Per Page
10

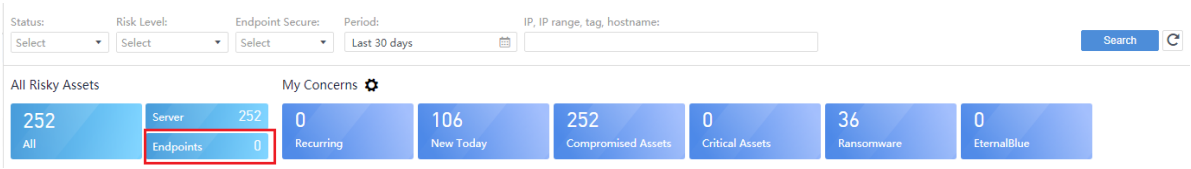


You can click <GoldenEye Traceback> on the risk details page to go to the GoldenEye Details page where the following tabs are displayed: Access, Asset Details, Security Incidents, Security Alerts, Traffic, Access Profile, Entry Point, and Traceback, as shown in the figure below.

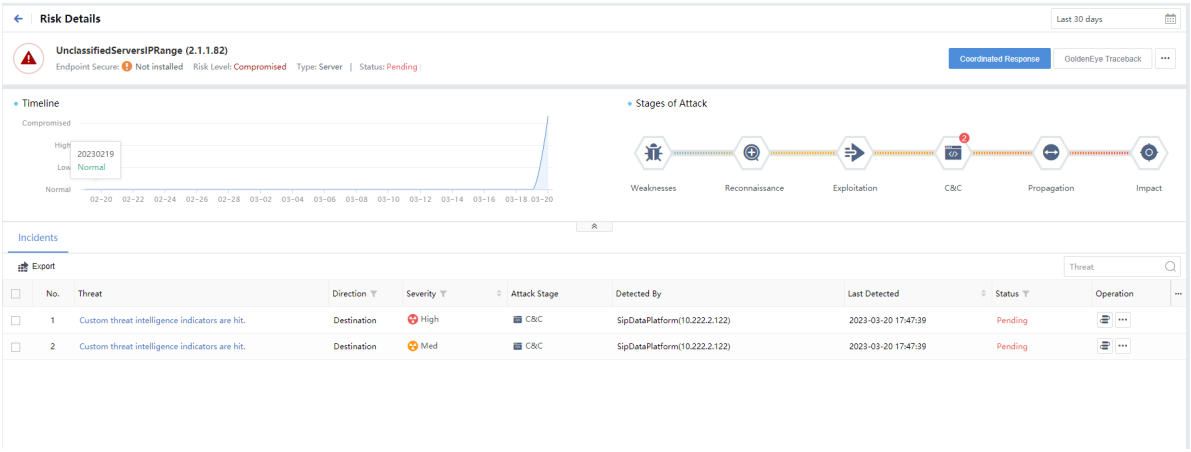


Risky hosts

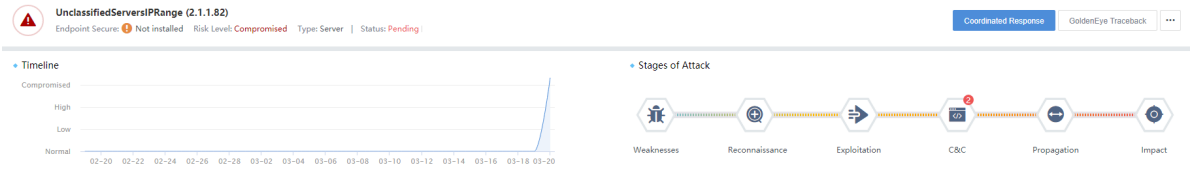
Under All Risky Assets, you can click <Host> to display only the risky assets of the host type in the risky assets list.



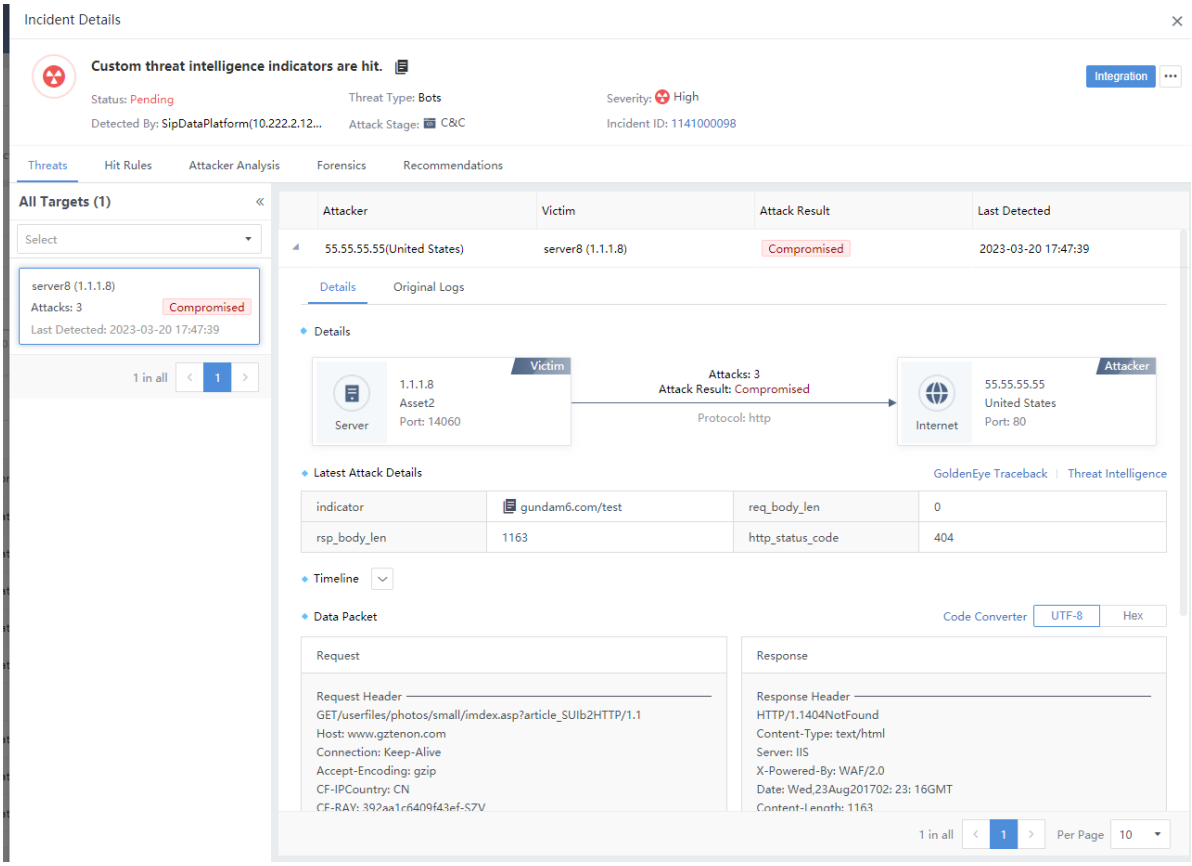
You can click an asset name to view the risk details of a risky host, including asset level trend, stages of attack, incident view, and threats, as shown in the figure below.

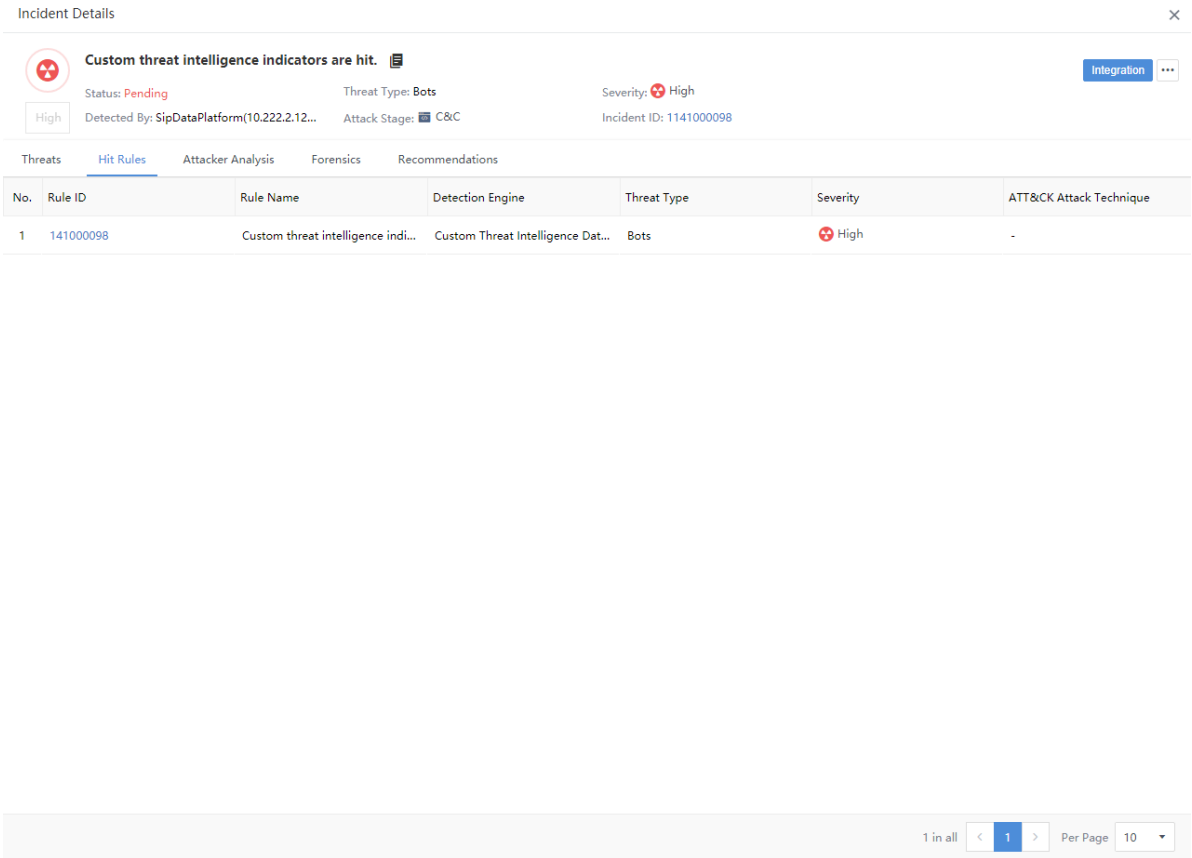


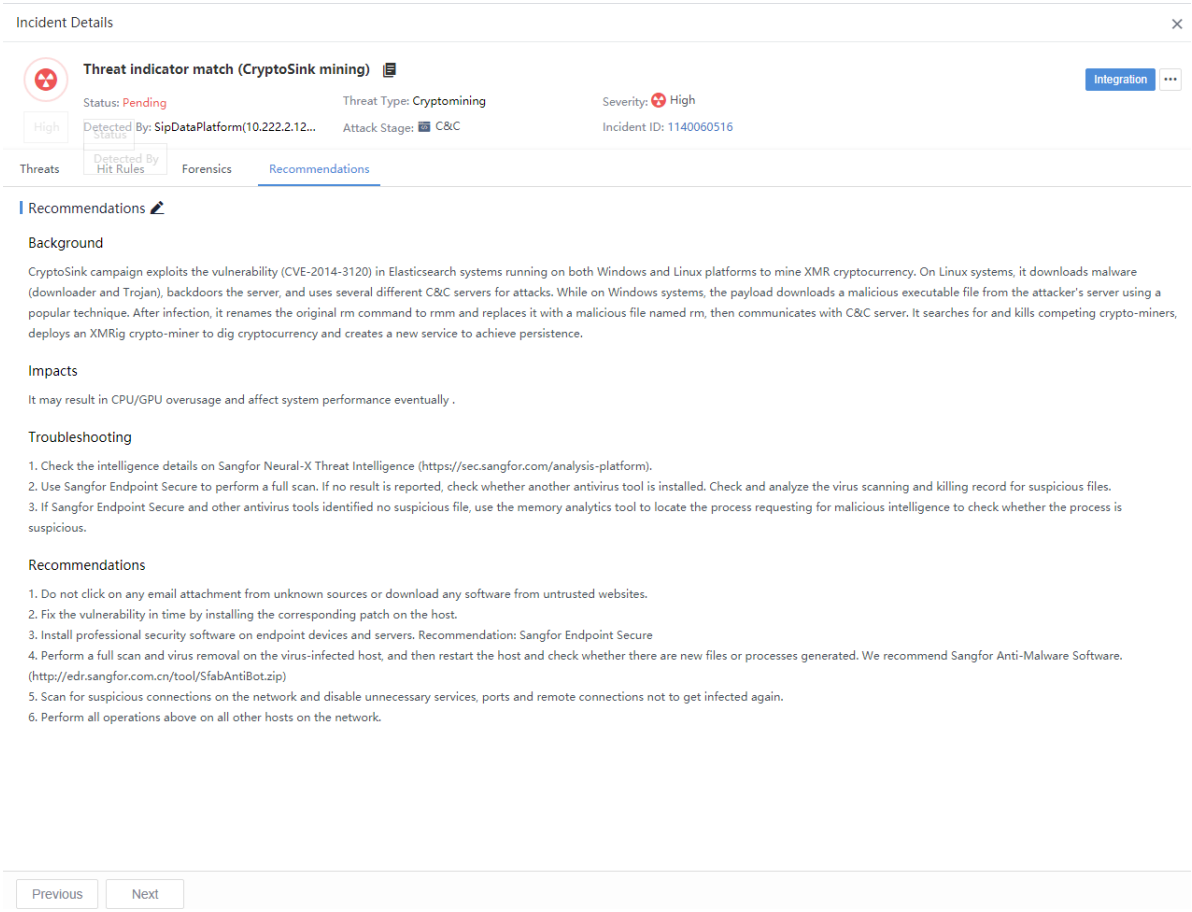
In the statistics zone, risk level trend and stages of attack are displayed by default, as shown in the figure below.



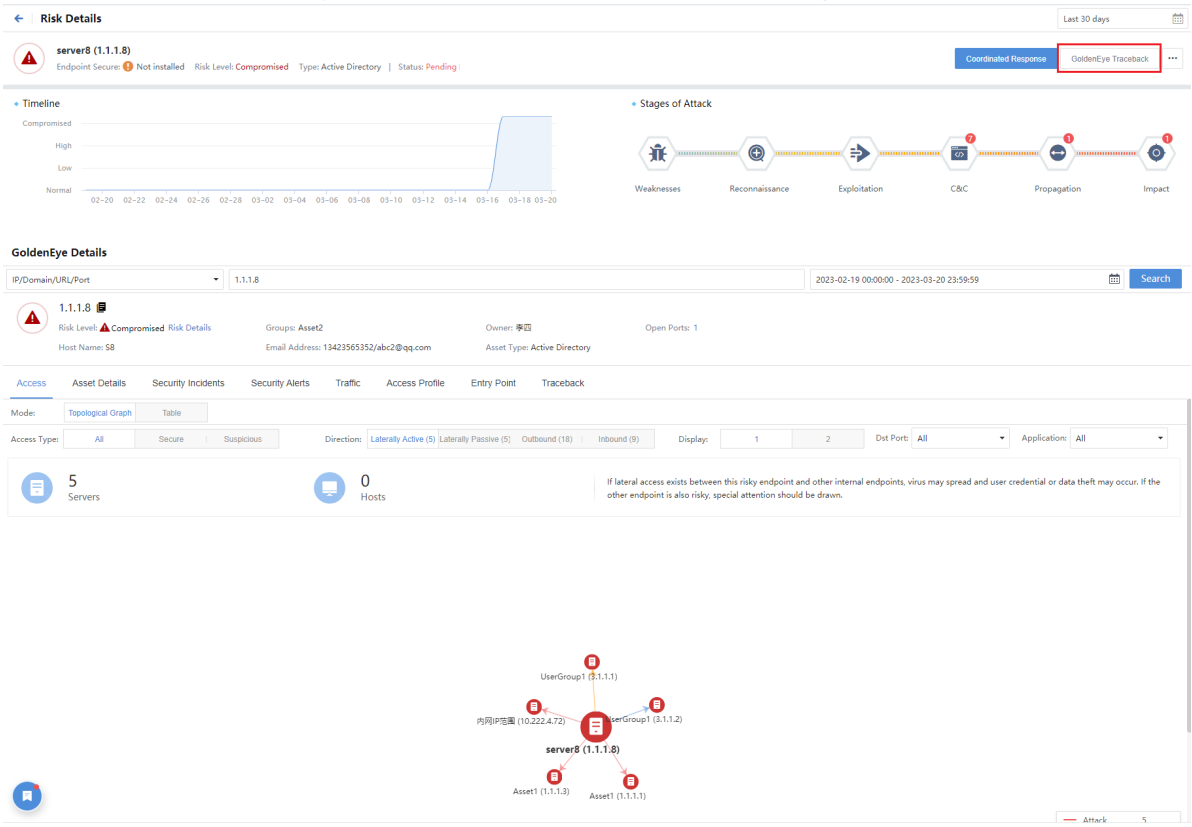
You can click the name of an incident to view its details, including hit rules, forensics (triggered by specific rules), and response recommendations, as shown in the figure below.


Incident Details
Custom threat intelligence indicators are hit.
Status: Pending
Threat Type: Bots
Severity: High
Detected By: SipDataPlatform(10.222.2.12...
Attack Stage: C&C
Incident ID: 1141000098
Integration
Threats
Hit Rules
Attacker Analysis
Forensics
Recommendations
All Targets (1)
Select
server8 (1.1.1.8)
Attacks: 3
Compromised
Last Detected: 2023-03-20 17:47:39
1 in all
Attacker
Victim
Attack Result
Last Detected
55.55.55.55(United States)
server8 (1.1.1.8)
Compromised
2023-03-20 17:47:39
Details
Original Logs
Details
Victim
Server
1.1.1.8
Asset2
Port: 14060
Attacks: 3
Attack Result: Compromised
Protocol: http
Attacker
Internet
55.55.55.55
United States
Port: 80
Latest Attack Details
GoldenEye Traceback
Threat Intelligence
indicator
gundam6.com/test
req_body_len
0
rsp_body_len
1163
http_status_code
404
Timeline
Data Packet
Code Converter
UTF-8
Hex
Request
Request Header
GET/userfiles/photos/small/imdex.asp?article_SUIb2HTTP/1.1
Host: www.gztenon.com
Connection: Keep-Alive
Accept-Encoding: gzip
CF-IPCountry: CN
CF-RAY: 392aa1c6409f43ef-SZV
Response
Response Header
HTTP/1.1404NotFound
Content-Type: text/html
Server: IIS
X-Powered-By: WAF/2.0
Date: Wed,23Aug201702: 23: 16GMT
Content-Length: 1163
1 in all
Per Page
10


Incident Details
Custom threat intelligence indicators are hit.
Status: Pending
Threat Type: Bots
Severity: High
High
Detected By: SipDataPlatform(10.222.2.12...
Attack Stage: C&C
Incident ID: 1141000098
Integration
Threats
Hit Rules
Attacker Analysis
Forensics
Recommendations
No.
Rule ID
Rule Name
Detection Engine
Threat Type
Severity
ATT&CK Attack Technique
1
141000098
Custom threat intelligence indi...
Custom Threat Intelligence Dat...
Bots
High
-
1 in all
Per Page
10



You can click <GoldenEye Traceback> on the risk details page to go to the GoldenEye Details page where the following tabs are displayed: Access, Asset Details, Security Incidents, Security Alerts, Traffic, Access Profile, Entry Point, and Traceback, as shown in the figure below.

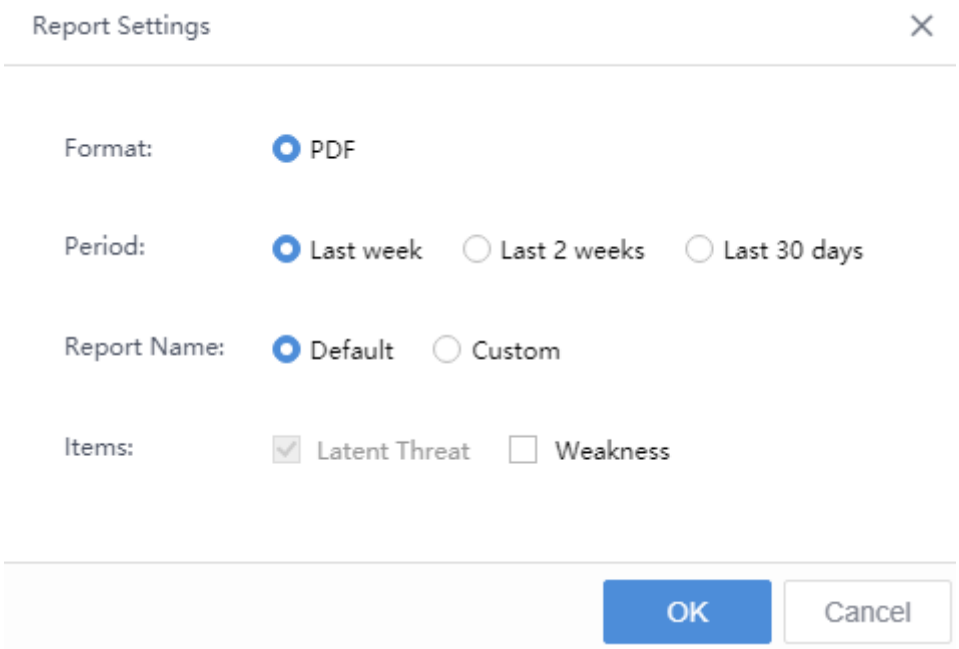


Export risky assets

The risky assets list and risk reports can be exported on the Risky Assets page. You can click <Export> to export all data of the current page in XLSX format by default. At the same time, by clicking the IP address of a risky asset, you can go to the Risk Details page to export the list of security incidents, inbound attacks, or data in another supported dimension, which will not be described in detail here.



By clicking <Export Report>, you can configure the report to export as needed. For example, you can specify the period, report name, and items, as shown in the figure below.

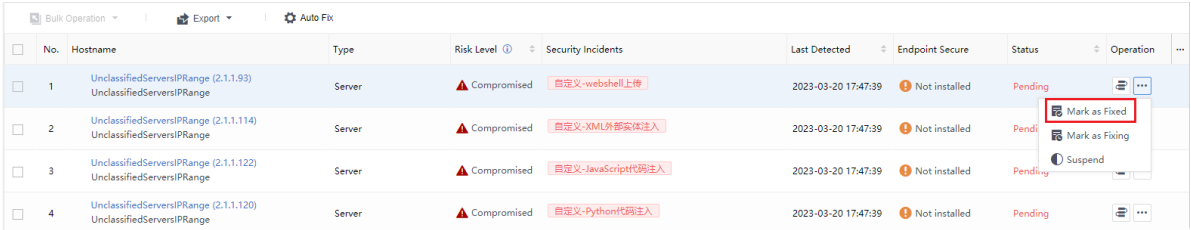


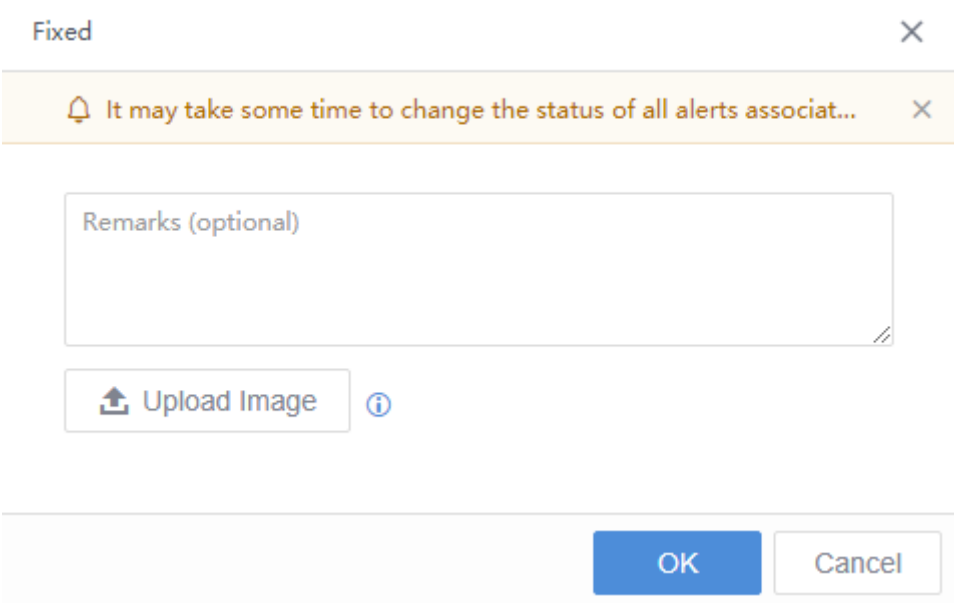
Response to Risky Assets

You can view and analyze risky assets, and make a response to them in the following ways:

1. Coordinated response: Respond to risky assets through corresponding policies.
2. Manual response: Perform the following operations on risky assets after multidimensional analysis:

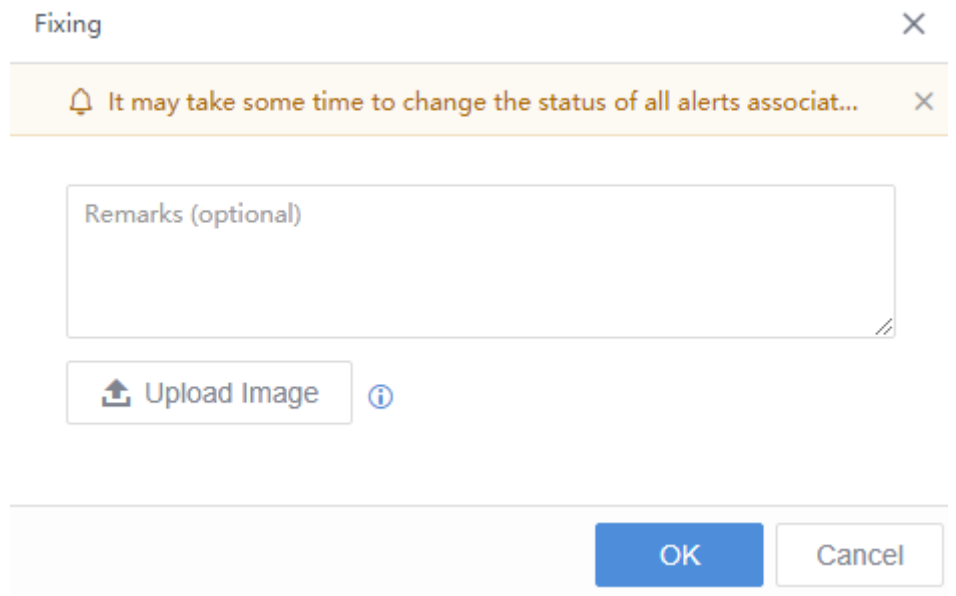
Mark as Fixed: It means the risk is fixed. You can add remarks and upload images for future tracing.





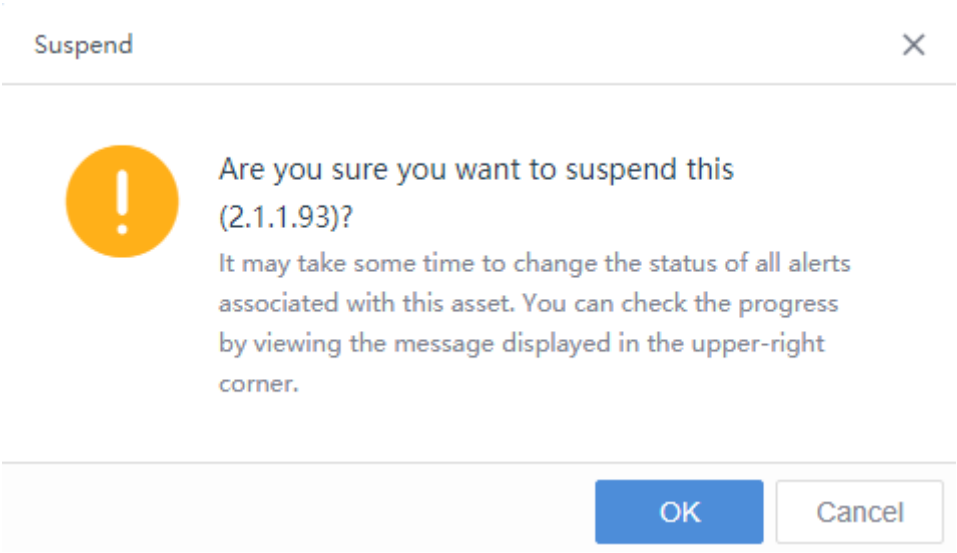
Mark as Fixing: It means the risk is being fixed and still requires attention.





Suspend: It means you understand the risk and will fix it later.





Bulk response

You can select several assets for manual response in a batch on the Risky Assets page.



Auto response

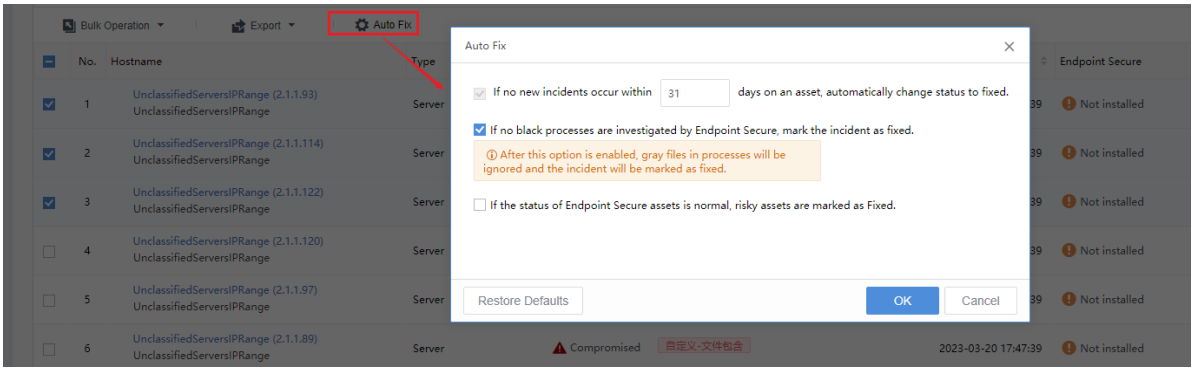
On the Risky Assets page, you can click <Auto Fix> to make auto response to risky assets in the following three cases.

If no new incidents occur within a certain number of days on an asset, the status of the asset automatically changes to Fixed. The time period can be customized.

If no black processes are investigated by NovaGuard, the incident is marked as Fixed.

If the status of risky assets in NovaGuard is normal, the risky assets are marked as Fixed.

The figure below shows the Auto Fix page.

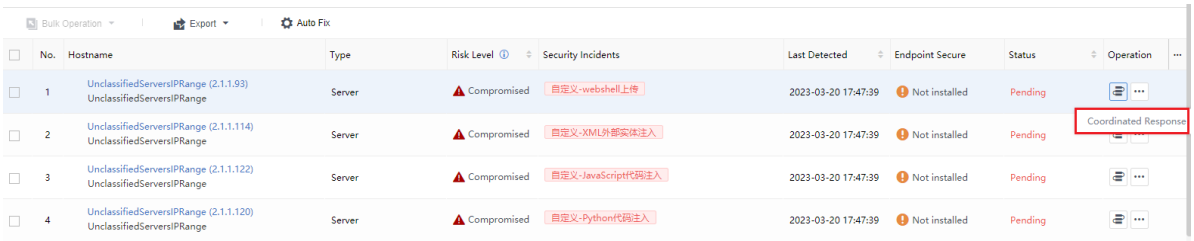


Coordinated response

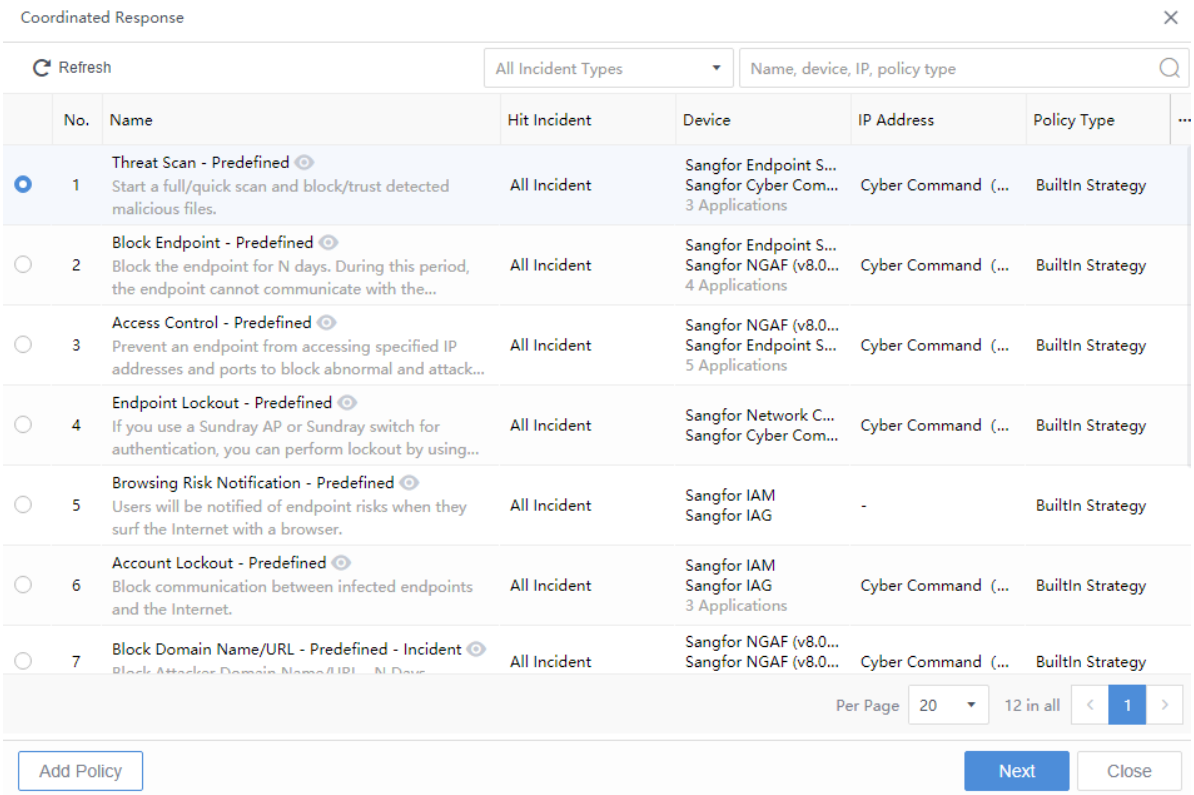
Nova Command can fix security incidents on assets such as botnets, exploits, and scanning & eavesdropping based on various response policies, to help you fix risks in a granular and efficient manner. To apply coordinated response, you need to perform the following steps:

Select an asset whose risks need to be fixed and then click " ".

The Coordinated Response page appears. You will be asked to select response policies, as shown in the figure below.

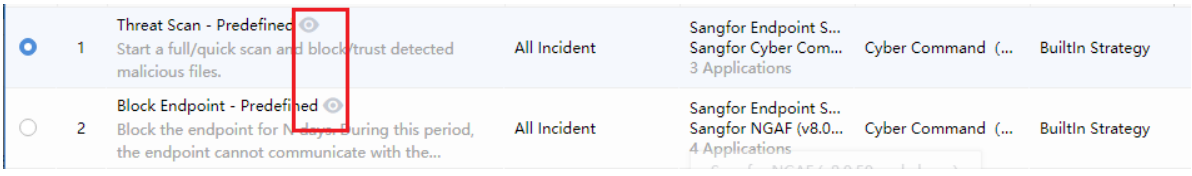


You can display available response policies by selecting Event or Alert from the drop-down list at the top. The platform provides some predefined policies, such as Threat Scan, Block Domain Name/URL, VM Suspend, Snapshot, VM Add, VM Shutdown, Block Endpoint, Account Lockout, Browsing Risk Notification, Endpoint Lockout, and Access Control. You can also clone or customize policies. The following figure shows the coordinated response settings page.

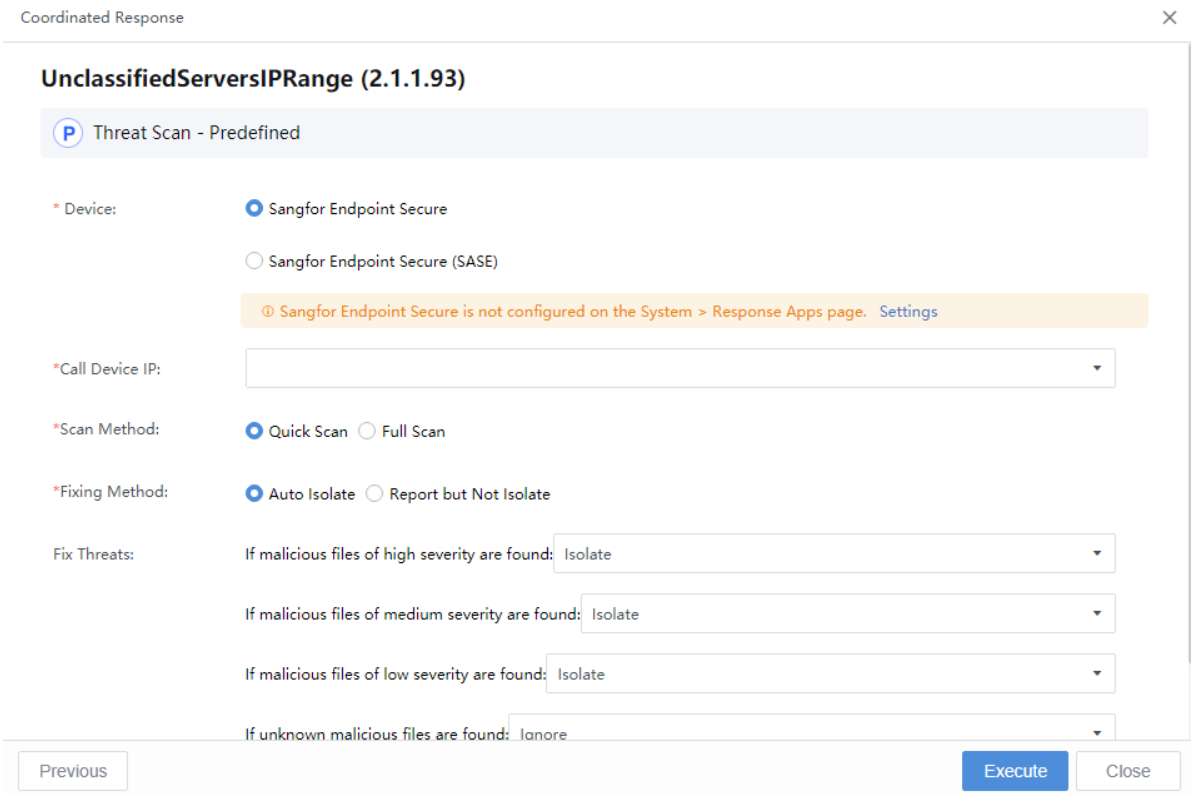


For endpoints with NovaGuard installed, when security incidents can be fixed in NovaGuard, the endpoints will automatically adopt actions such as "Threat Scan", "Access Control", "Block Endpoint", "Isolate Malicious Processes", and "Malicious File Fixing" depending on circumstances.

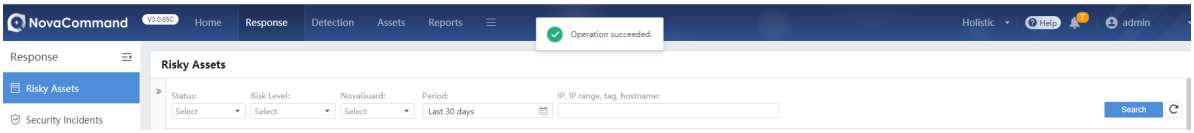
By clicking the < > sign next to a response policy, you will directly go to the canvas page of the policy, as shown in the figure below.



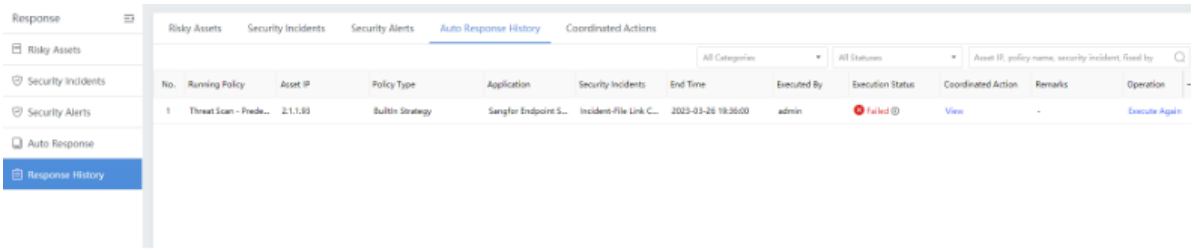
By clicking <Next>, you will go to the parameter settings page of the selected response policy, where you can configure the mapped device and options related to the response action, as shown in the figure below.



After you click <Execute>, the response action starts to be executed. The system prompts the message of <Executed> at the top of the page after the execution is completed.



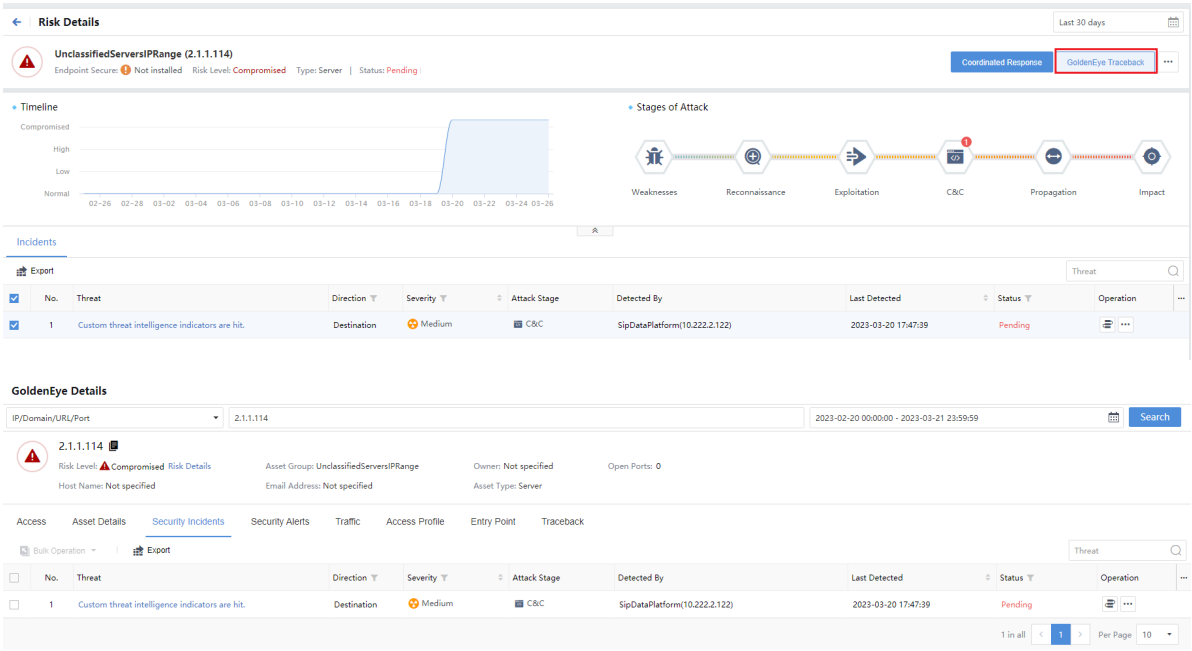
On the [Response/Response History/Auto Response History] page, you can view the response history, including the status, result, policy, and other related information, as shown in the figure below.



GoldenEye Traceback

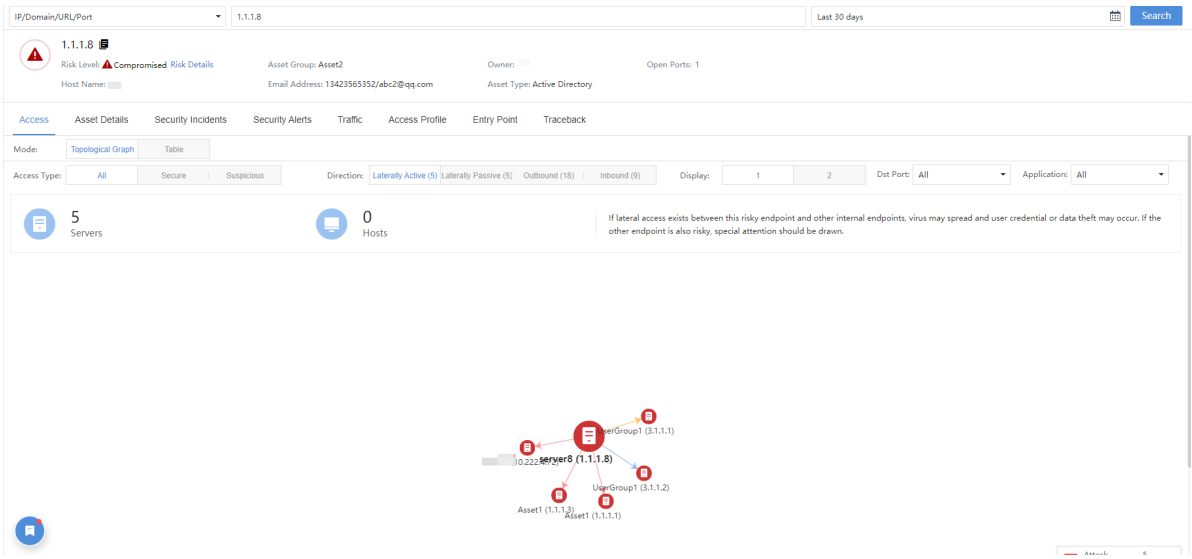
Channel 1

On the [Response/Risky Assets], you can click <GoldenEye Traceback> on the details page of a risk to go to the GoldenEye Details page where the following tabs are displayed: Access, Asset Details, Security Incidents, Security Alerts, Traffic, Access Profile, Entry Point, and Traceback, as shown in the figure below.



Fields:

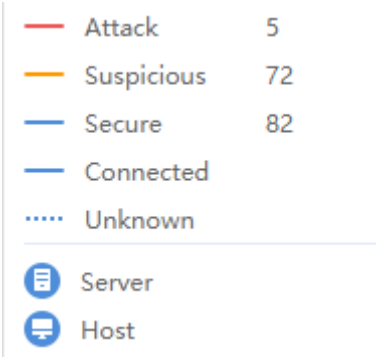
Access: It displays access information such as the access type and direction in table or topological graph mode, as shown in the figure below.



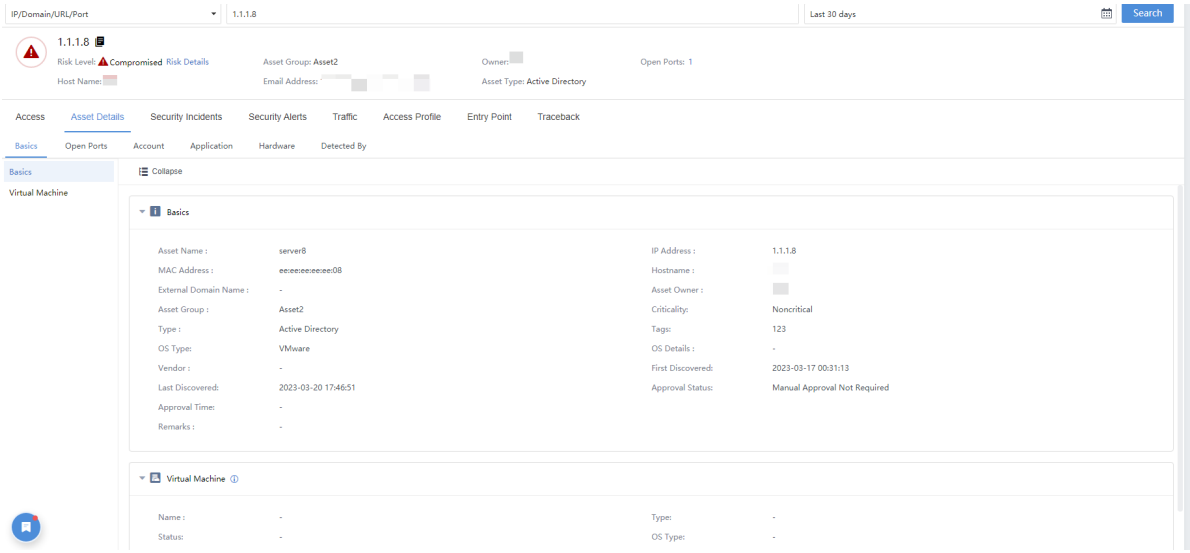
In two-level display mode, you can drill down to level 2 access to display a more complete access topology, as shown in the figure below.



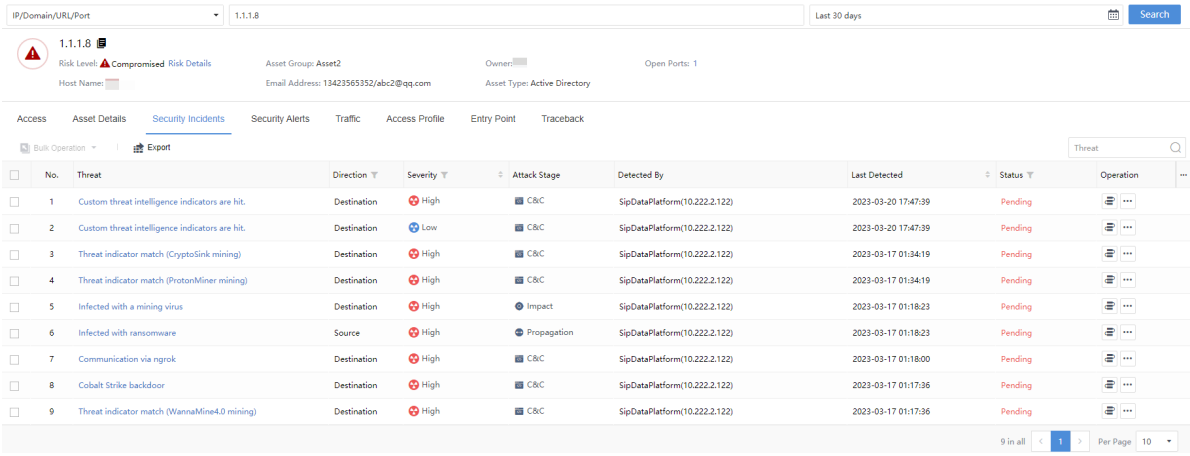
The description of each line or sign is given on the bottom right of the page, as shown in the figure below.



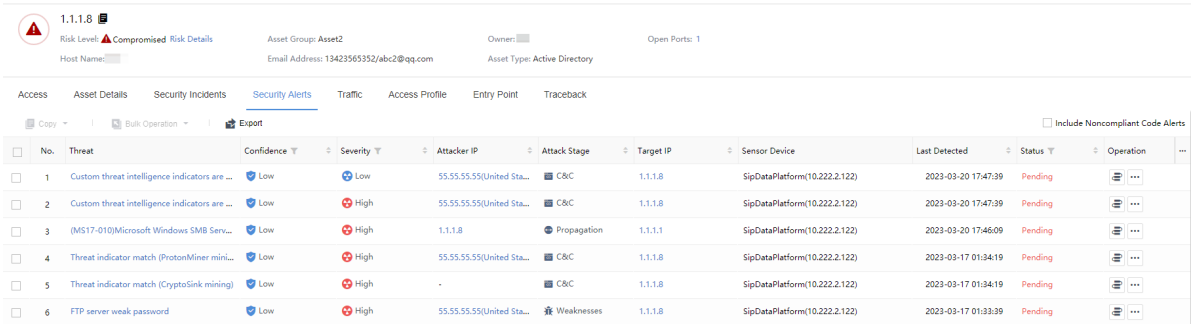
Asset Details: It displays the details of risky assets, as shown in the figure below. Information on this tab is the same as asset details in the Assets module.



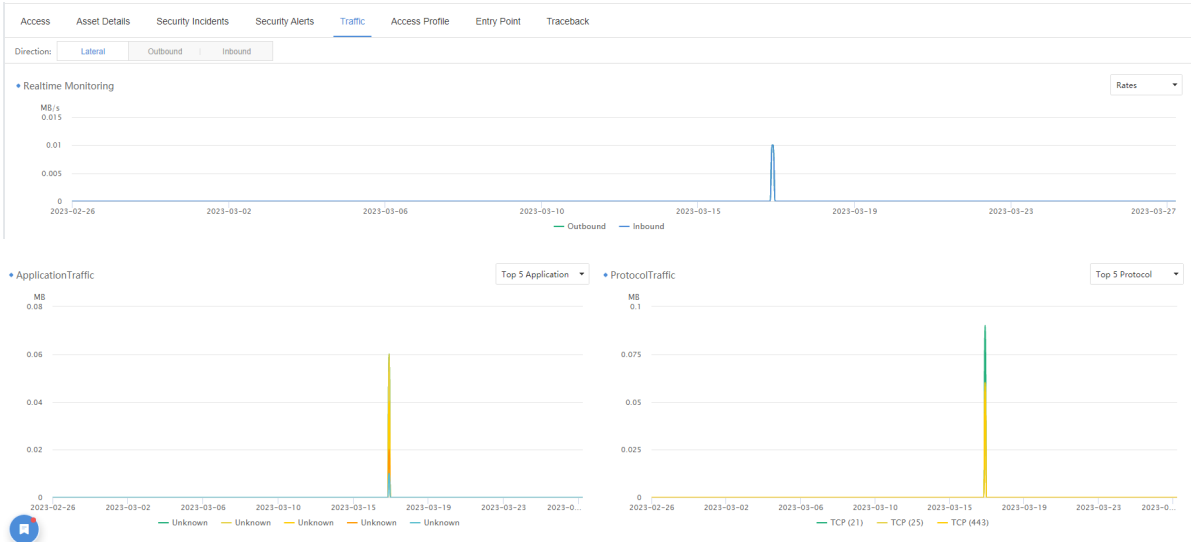
Security Incidents: It displays the security incidents associated with an asset, as shown in the figure below.



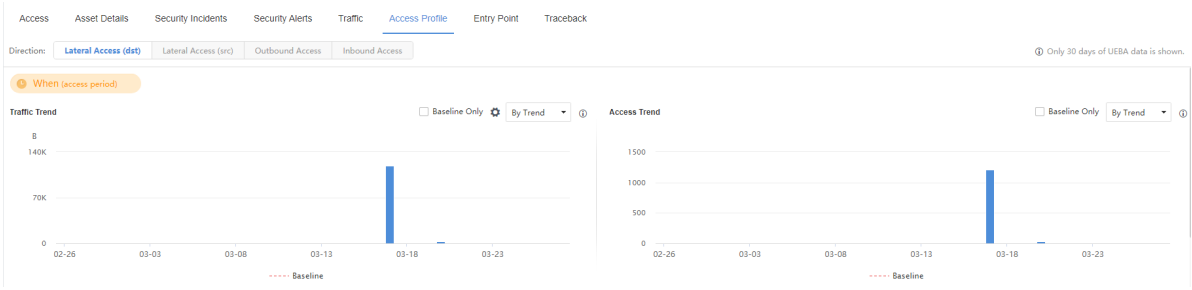
Security Alerts: It displays the security alerts associated with an asset, as shown in the figure below.

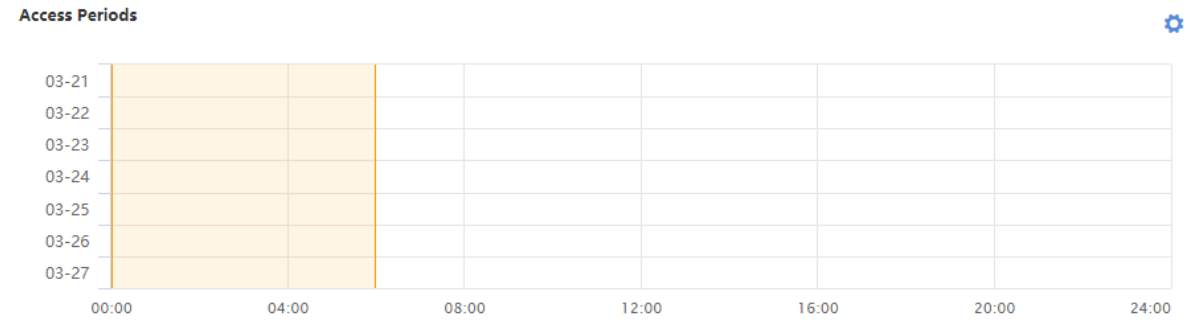


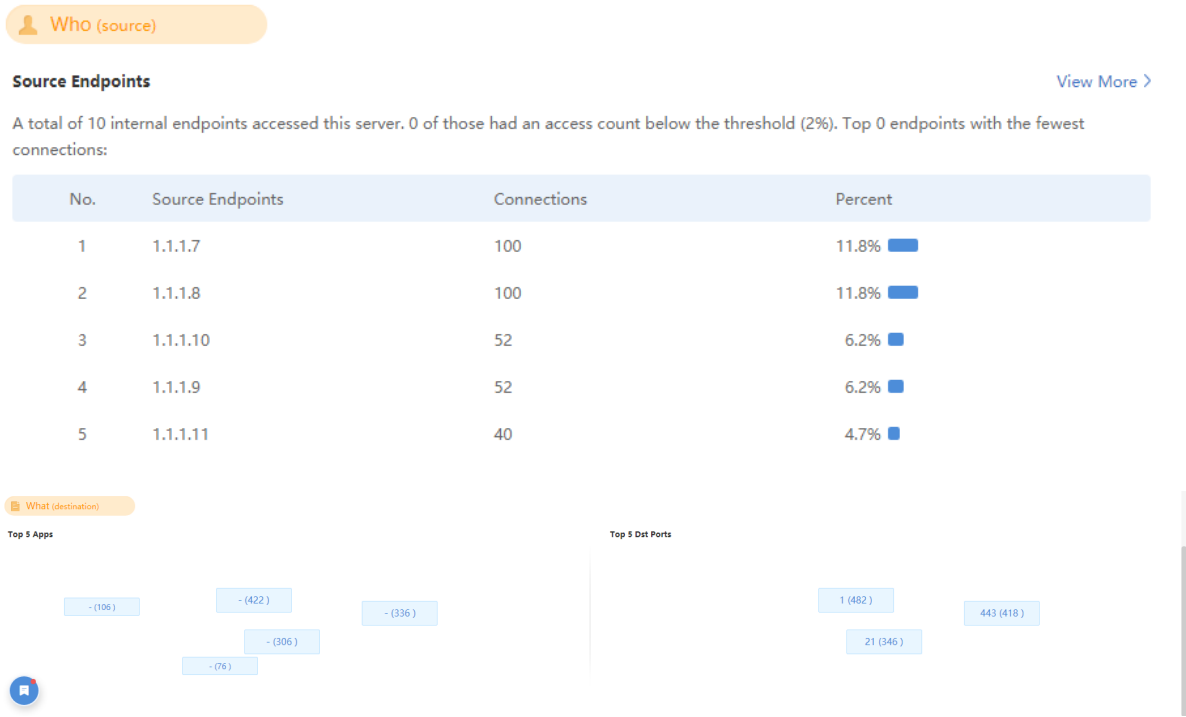
Traffic: It displays the statistics on traffic in three directions: lateral, outbound, and inbound. Information such as rates, top 5 applications, application traffic, top 5 protocols, and protocol traffic is collected, as shown in the figure below.



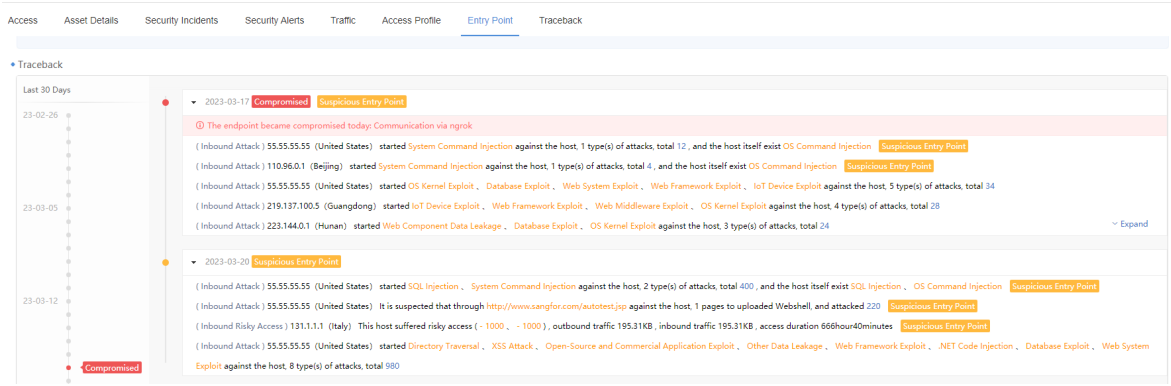
Access Profile: It displays the profile of lateral access (destination), lateral access (source), outbound access, and inbound access from the following aspects: traffic trend, access trend, access periods, usual source subnets, source endpoints, top 5 applications, and top 5 destination ports, as shown in the figure below.







Entry Point: It provides a summary of attacks against an endpoint and suggestions for tracing. The attack history is shown on a timeline where entry points are visualized. You can click a date on the timeline to locate the risk description on the right, as shown in the figure below.

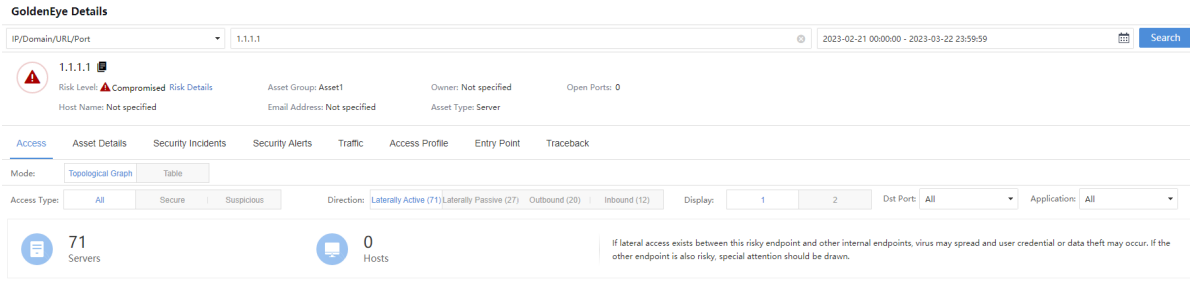


Traceback: It displays the attack network in a topological graph or table. The number at the top of Direct Sources represents the number of first-level attackers who launch attacks against an asset. The number at the top of indirect sources represents the number of second-level attackers. Both first-level and second-level attacks are further classified into LAN and WAN attacks, as shown in the figure below.

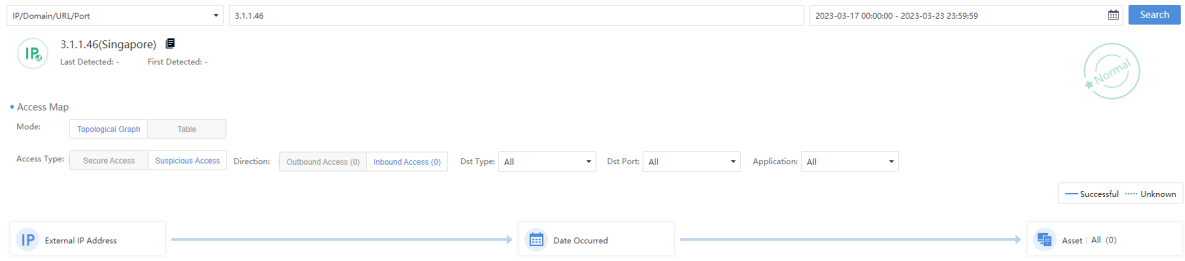


Note:

The GlodenEye Details page displayed when a LAN IP address is entered for search is different from that displayed when a WAN IP is entered for search. The following figure shows the page for LAN IP addresses.



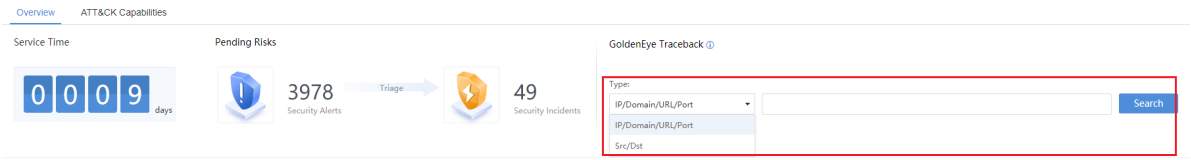
The following figure shows the page for WAN IP addresses.



You can also access GoldenEye Traceback in other ways.

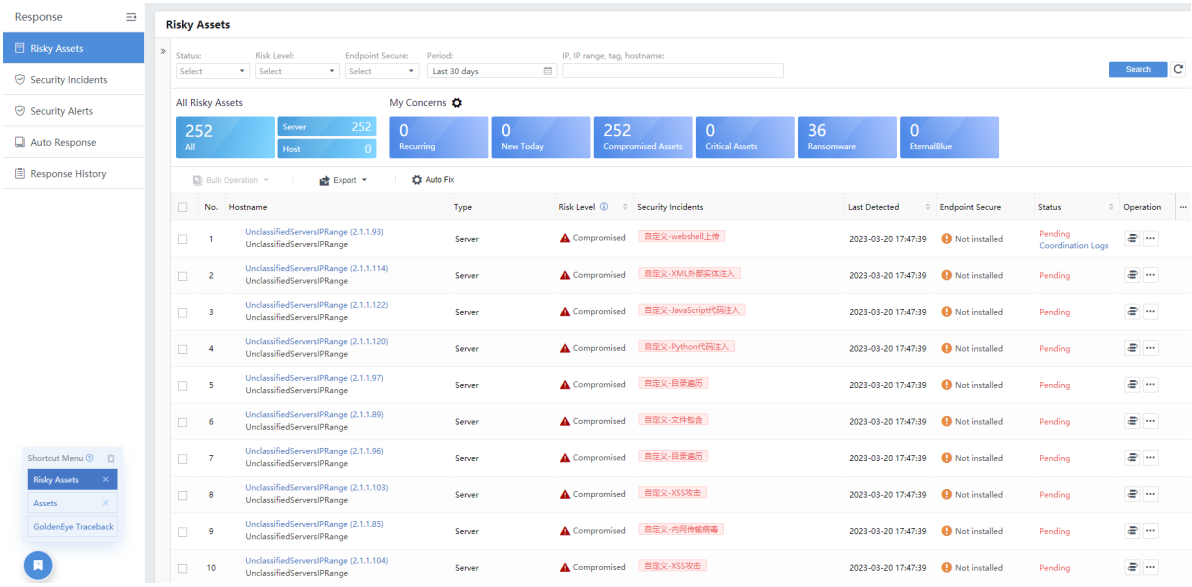
Channel 2

On the [Home/Overview] page, you can search for assets by IP address, domain name, URL, or port in the GoldenEye Traceback module to access GoldenEye Traceback, as shown in the figure below.



Channel 3

You can access GoldenEye Traceback by clicking the shortcut menu icon in the bottom left corner of the page.

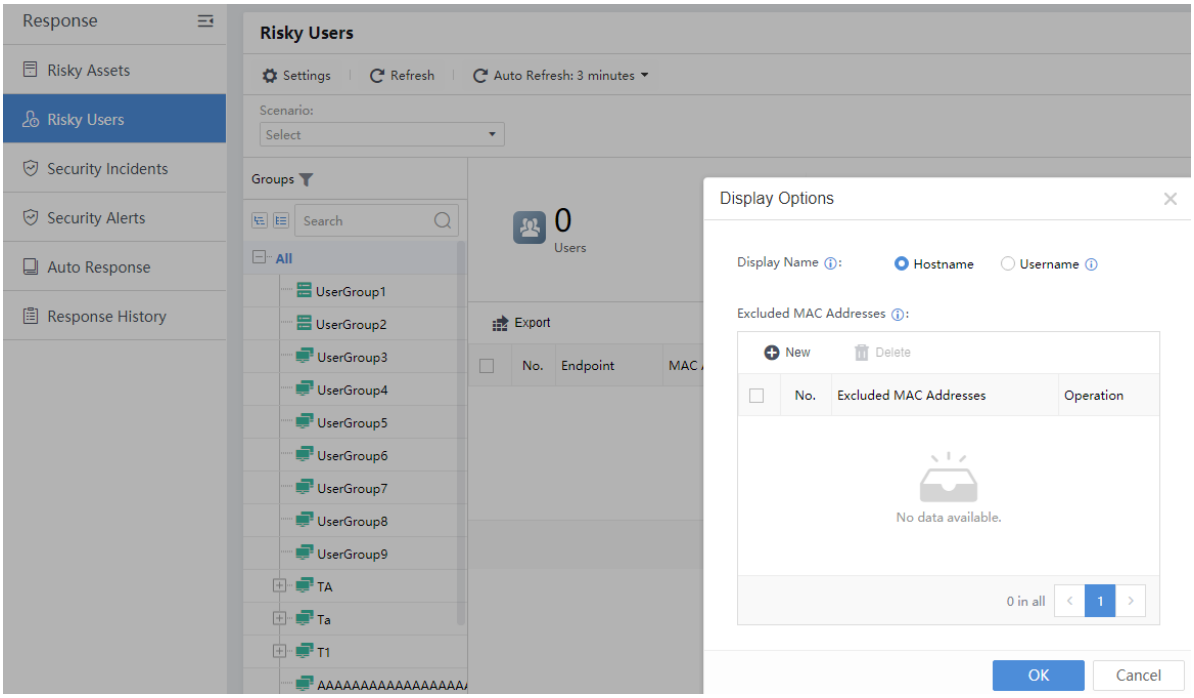


Risky Users

On the Risky Users page, security incidents are displayed by endpoint name or username. This module is available only when Nova Command is integrated with Internet Access Gateway (IAG), IDTrust, SSL VPN, Sundray NAC, and Dr.COM, and is not displayed by default.

Source of Risky Users

On the [Response/Risky Users] page, you can click <Settings> to specify the user view, which can be the endpoint name or username. Users can be synchronized from [Sundray NAC], [IAG], [VPN], [IDTrust], and [Dr.COM], as shown in the figure below.



Risky User Viewing

The page of risky users is refreshed every three minutes. You can select another interval from the drop-down list, as shown in the figure below.

// picture

Scenarios of risky users are [All] (default) and [New Today]. If you are concerned about only risky users added today, you can select the [New Today] scenario. The period is set in days and can be 30 days at most, as shown in the figure below.

// picture

Summary

Risky users are classified into normal users, high-risk users, and severe users. Asset groups with high-risk and severe users are marked in red. You can filter and export risky users by user type, as shown in the figure below.

// picture

Details

In the risky user list, risky users are displayed by endpoint name, real-time IP address, asset group, risk level, security incident, and when the incident was last detected, as shown in the figure below.

// picture

Note:

<Severe User: >A host asset associated with the user has been attacked or has security incidents that caused it to become compromised, such as remote access, lateral attacks, and APT. This asset has been or is about to be controlled and requires immediate attention.

High-risk User: A host asset associated with the user has been infected or is propagating a virus. This asset is at risk of being leveraged by an attacker and requires immediate attention.

When you select several risky users on the page, you can click <Export> to export them in XLSX format to local, as shown in the figure below.

// picture

You can click a specific risky user to drill down to its details page where you can see user information such as the risk level, asset group, and user source, as shown in the figure below.

// picture

You can view the risk level trend of each risky user. The default period is seven days, as shown in the figure below.

// picture

Risky users are displayed by incident. Based on security alerts, security incidents are mapped in various dimensions of the built-in algorithm, as shown in the figure below.

// picture

Incidents

Incidents

On the Incidents page, by clicking the <Threat> field, you can drill down to the forensics and view the incident details such as the alert summary, threat analysis, hit rules, attacker analysis, and response recommendations, as shown in the figure below.

// picture

// picture

On the [Threats] tab, attack targets, alert quantity, alert details, and original logs are displayed, as shown in the figure below.

// picture

You can scroll up and down in the [Details] section to view the data packet information, as shown in the figure below.

// picture

Hit rules

You can view the list of rules related to the event. Information such as the rule ID, rule name, detection engine, threat type, severity, and ATT&CK attack technique is displayed in the list, as shown in the figure below.

// picture

You can click a rule ID to go to [System/Security Capabilities/Detection Engines]. On the page that appears, you can view or edit the rule details, as shown in the figure below.

// picture

Attacker analysis

You can view the attacker IP address, region, attack count, attackers on the same subnet, target IP addresses, first attack time, last attack time, lockout status, and intelligence, as shown in the figure below.

// picture

You can click <Lockout> or the <// picture> icon in the [Operation] column to select the configured Next Generation Application Firewall (NGAF) for performing correlated block, as shown in the figure below.

// picture

You can click the <// picture> icon in the [Operation] column to view the threat intelligence or attacker profile, as shown in the figure below.

// picture

You can click the value in the "Attackers on the Same Subnet" or "Target IPs" column to view the attacker IP addresses or target IP addresses, as shown in the figure below.

// picture

// picture

If a lot of attacker IP addresses are associated with the event, you can click <Export> to export the attacker IP list in XLSX format.

Recommendations

Troubleshooting suggestions, fixing suggestions, and daily maintenance suggestions are provided based on the background and impact of the event, as shown in the figure below.

// picture

Response to Risky Users

Coordinated response

On the [Response/Risky Users] page, you can view the risky user list. By clicking a specific user, you can drill down to the user details page where you can view associated security incidents. By clicking the "// picture" icon of each incident, you can respond to the risky user according to its associated source, as shown in the figure below.

// picture

// picture

The Coordinated Response dialogue box appears. You can view available response policies by selecting Event or Alert from the drop-down list at the top. The platform provides some predefined policies, such as Threat Scan, Block Domain Name/URL, VM Suspend, Snapshot, VM Add, VM Shutdown, Block Endpoint, Account Lockout, Browsing Risk Notification, Endpoint Lockout, and Access Control. You can also clone or customize policies. The following figure shows the predefined threat scan policy.

// picture

By clicking <Next>, you will go to the parameter settings page of the selected response policy, where you can configure the mapped device and options related to the response action, as shown in the figure below.

// picture

After you click <Execute>, the response action starts to be executed. The system prompts the message of <Executed> at the top of the page after the execution is completed.

// picture

On the [Response/Response History/Auto Response History] page, you can view the response history, including the status, result, policy, and other related information, as shown in the figure below.

// picture

Manual operation

Besides coordinated response, you can also make manual responses to risky users. After manual response, the status of the risky users will change. Then you can select a risky user to drill down to the user details page, as shown in the figure below.

// picture

When you click the
"// picture" icon in the [Operation] column, you can see three options: [Mark as Fixed], [Mark as Fixing], and [Suspend], as shown in the figure below.

// picture

// picture

Mark as Fixed: It means the risk of this asset is fixed. You can add remarks and upload images for future tracing.

Mark as Fixing: It means the risk of this asset is being fixed and still requires attention.

Suspend: It means that you have known the risk of this asset and will fix it later.

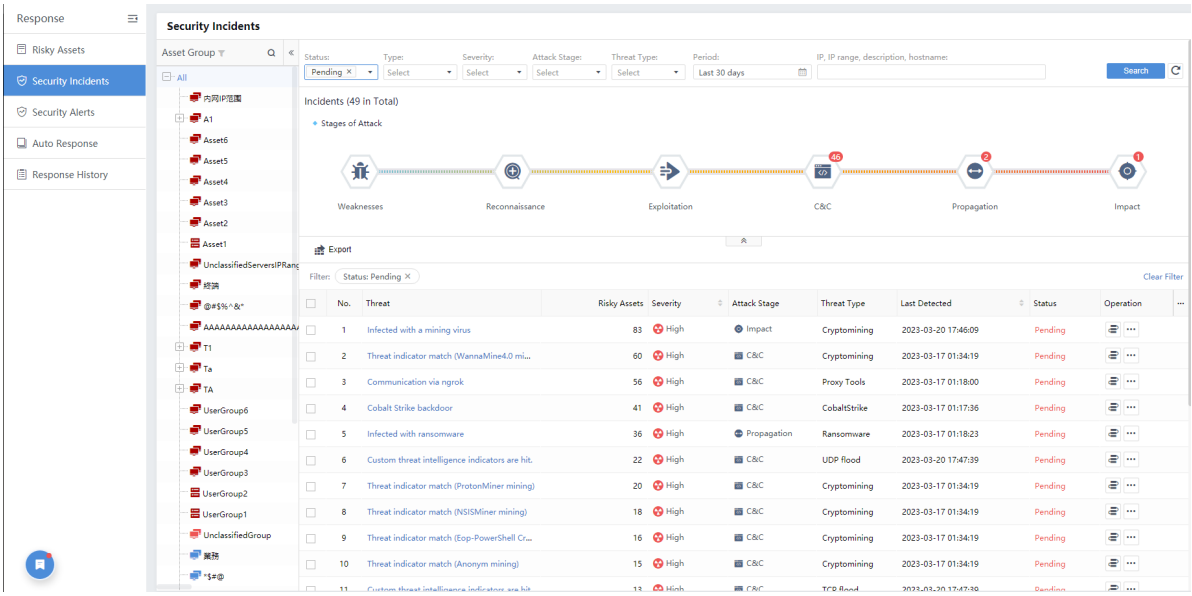
Security Incidents

The [Security Incidents] page provides the search, statistics, traceback, and forensics of security events and security alerts. This function is used frequently in security operations and receives a lot of attention. It includes two sublevels, namely security events and security alerts. A security event is the result of a security alert. When an endpoint is infected by malicious files or viruses or is controlled by attackers, a security event, such as C&C, backdoor, channel communication, brute-force attack on LAN, remote task execution, and virus infection, is generated from the corresponding security alert.

Security Incidents

Incident Filtering

On the [Response/Security Events/Security Incidents] page, you can view the distribution of security events and filter them by the following criteria, as shown in the figure below.



Parameters:

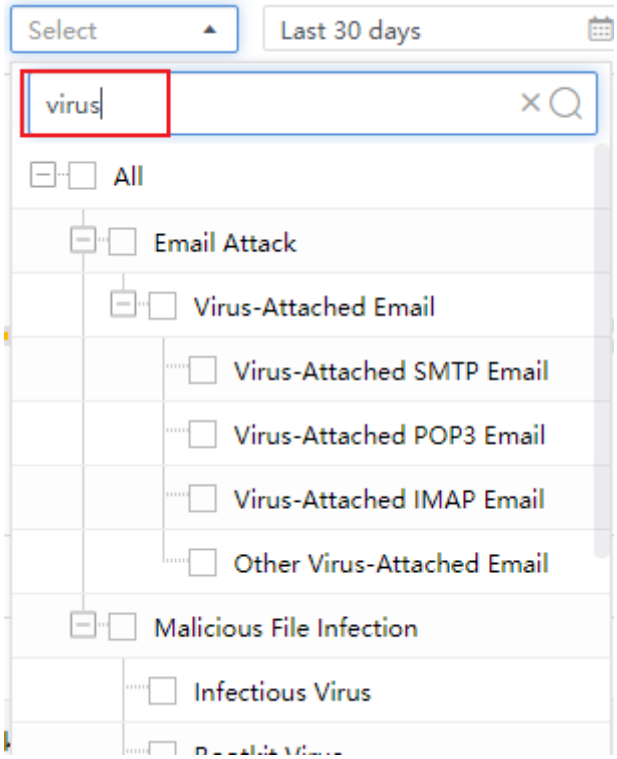
Status: Includes All, Pending, Suspended, Fixing, and Fixed.

<Type>: Includes All, Server, and Host.

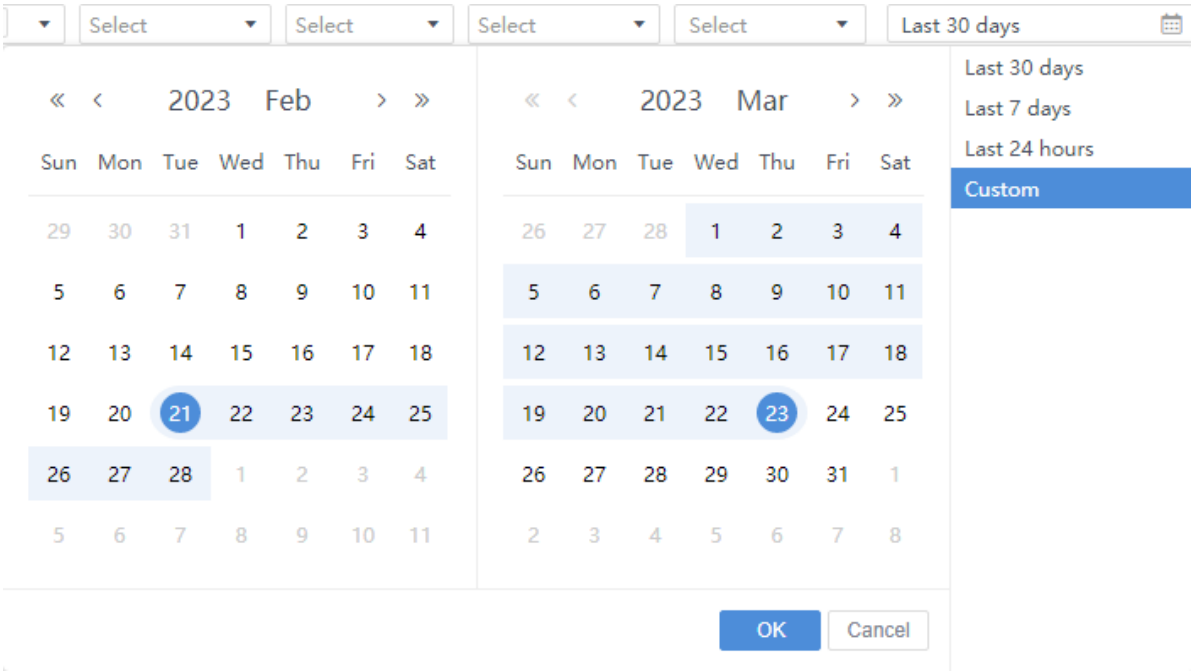
<Severity>: Includes All, High, Medium, and Low. The event severity is evaluated based on its impact scope and depth.

Attack Stage: Includes All, Weakness, Reconnaissance, Exploitation, C&C, Propagation, and Impact. The stage of a security event is determined based on the standard attack chain model of the industry.

Threat Type: A threat can be classified into three levels. You can filter events by the detailed threat type or keyword of the threat type for fuzzy search, as shown in the figure below.



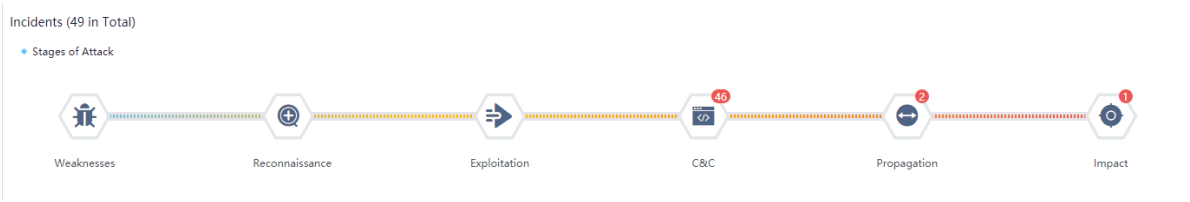
<Period>: You can search for security events by time period, including last 30 days, last 7 days, last 24 hours, and custom. To search for security events that occurred 30 days ago, you can select custom, as shown in the figure below.



Search: You can search for security events by IP, IP range, description, asset group, and endpoint name.

Incident Statistics

In the middle of the [Response/Security Events/Security Incidents] page, you can view the event statistics, which are classified into several parts, including weakness, reconnaissance, exploitation, C&C, propagation, and impact, according to the event attribute. Each part has its quantitative statistics, and the sum of events of each part is the same as that of all events, as shown in the figure below.



Incident Viewing

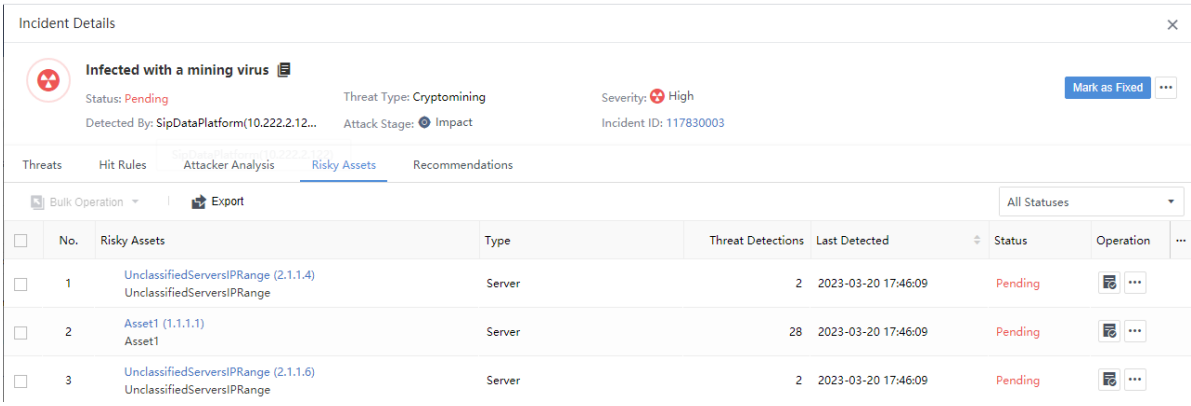
You can use the above conditions to search for specific security events and view the event details. Each event in the event list includes the content of the threat, incident attribute, risky assets, confidence, severity, tag, attack stage, threat type, engine, last detected time, status, and operation, as shown in the figure below.

No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Infected with a mining virus	83	High	Impact	Cryptomining	2023-03-20 17:46:09	Pending	
2	Threat indicator match (WannaMine4.0 mi...	60	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
3	Communication via ngrok	56	High	C&C	Proxy Tools	2023-03-17 01:18:00	Pending	
4	Cobalt Strike backdoor	41	High	C&C	CobaltStrike	2023-03-17 01:17:36	Pending	
5	Infected with ransomware	36	High	Propagation	Ransomware	2023-03-17 01:18:23	Pending	
6	Custom threat intelligence indicators are hit.	22	High	C&C	UDP flood	2023-03-20 17:47:39	Pending	
7	Threat indicator match (ProtonMiner mining)	20	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
8	Threat indicator match (NSISMiner mining)	18	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
9	Threat indicator match (Eop-PowerShell Cr...	16	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
10	Threat indicator match (Anonym mining)	15	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
11	Custom threat intelligence indicators are hit.	13	High	C&C	TCP flood	2023-03-20 17:47:39	Pending	
12	Access to malicious domain name (wanna...	11	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
13	Access to malicious domain name (bitcoin...	11	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
14	Threat indicator match (Fsysna mining)	10	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	

Parameters:

Risky Assets: The number of risky assets associated with the security event. You can click the event to go to the [Incident Details] page, where you can select [Risky Assets] to view the number of risky assets, as shown in the figures below.

No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Infected with a mining virus	83	High	Impact	Cryptomining	2023-03-20 17:46:09	Pending	
2	Threat indicator match (WannaMine4.0 mi...	60	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
3	Communication via ngrok	56	High	C&C	Proxy Tools	2023-03-17 01:18:00	Pending	



Status: Includes Pending, Fixing, and Suspended.

<Last Detected: >The last time when the event was detected, as shown in the figure below.

No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Infected with a mining virus	83	High	Impact	Cryptomining	2023-03-20 17:46:09	Pending	
2	Threat indicator match (WannaMine4.0 mi...	60	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
3	Communication via ngrok	56	High	C&C	Proxy Tools	2023-03-17 01:18:00	Pending	
4	Cobalt Strike backdoor	41	High	C&C	CobaltStrike	2023-03-17 01:17:36	Pending	

Engine: The built-in engine that detects the event, as shown in the figure below.

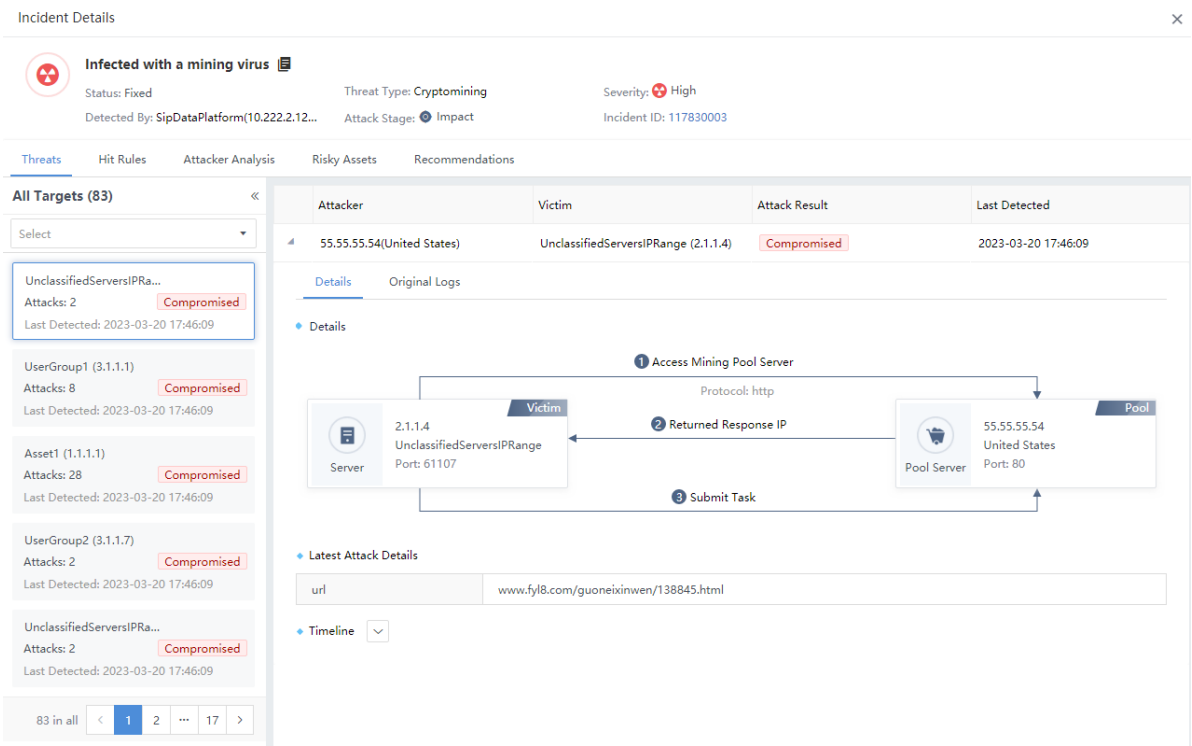
No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Infected with a mining virus	83	High	Impact	Cryptomining	2023-03-20 17:46:09	Pending	
2	Threat indicator match (WannaMine4.0 mi...	60	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	
3	Communication via ngrok	56	High	C&C	Proxy Tools	2023-03-17 01:18:00	Pending	
4	Cobalt Strike backdoor	41	High	C&C	CobaltStrike	2023-03-17 01:17:36	Pending	
5	Infected with ransomware	36	High	Propagation	Ransomware	2023-03-17 01:18:23	Pending	
6	Custom threat intelligence indicators are hit.	22	High	C&C	UDP flood	2023-03-20 17:47:39	Pending	
7	Threat indicator match (ProtonMiner mining)	20	High	C&C	Cryptomining	2023-03-17 01:34:19	Pending	

Status: The security status of the risky asset. When multiple risky assets exist and are all fixed, [Fixed] will be displayed. When one or more risky assets are pending, [Pending] will be displayed, as shown in the figure below.

No.	Threat	Risky Assets	Severity	Attack Stage	Threat Type	Last Detected	Status	Operation
1	Infected with a mining virus	83	High	Impact	Cryptomining	2023-03-20 17:46:09	Fixed	
2	Threat indicator match (WannaMine4.0 mi...	60	High	C&C	Cryptomining	2023-03-17 01:34:19	Fixed	
3	Communication via ngrok	56	High	C&C	Proxy Tools	2023-03-17 01:18:00	Pending	
4	Cobalt Strike backdoor	41	High	C&C	CobaltStrike	2023-03-17 01:17:36	Fixed	
5	Infected with ransomware	36	High	Propagation	Ransomware	2023-03-17 01:18:23	Pending	
6	Custom threat intelligence indicators are hit.	22	High	C&C	UDP flood	2023-03-20 17:47:39	Pending	

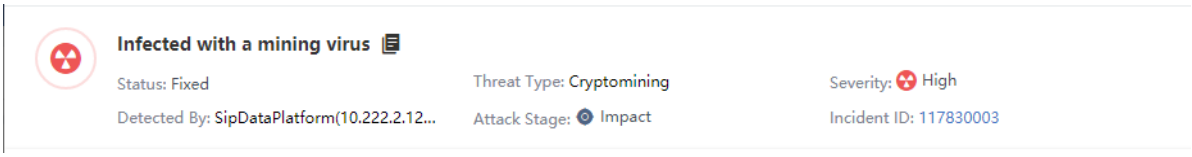
Incident Details

You can select a security event to go to the [Incident Details] page, where you can view the event overview, threat analysis, hit rules, attacker analysis, risky assets, and recommendations, as shown in the figure below.

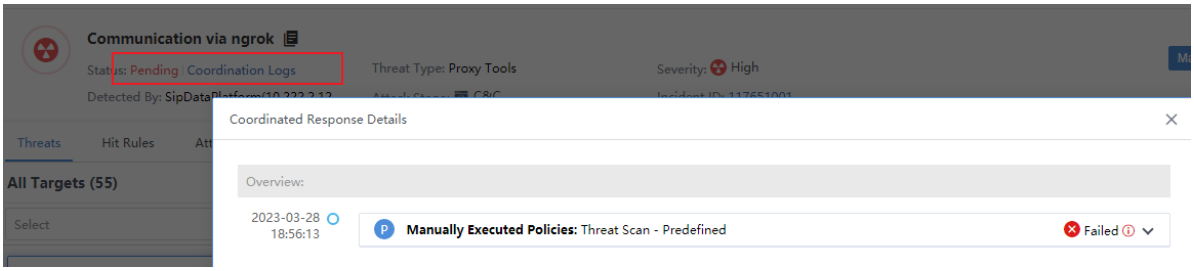


Incident details

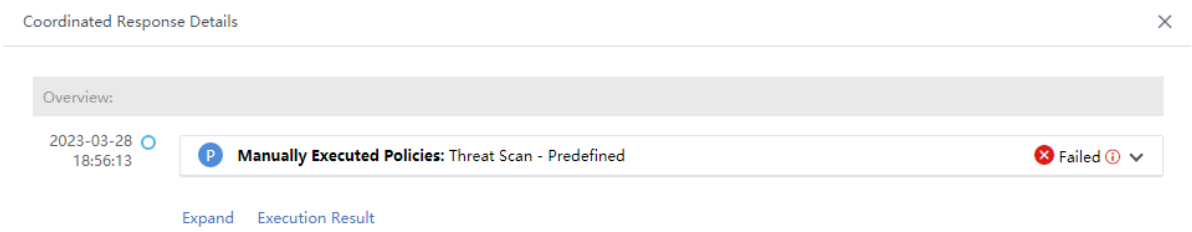
You can view the status, threat type, severity, data source, incident ID, and attack stage of the incident, as shown in the figure below.



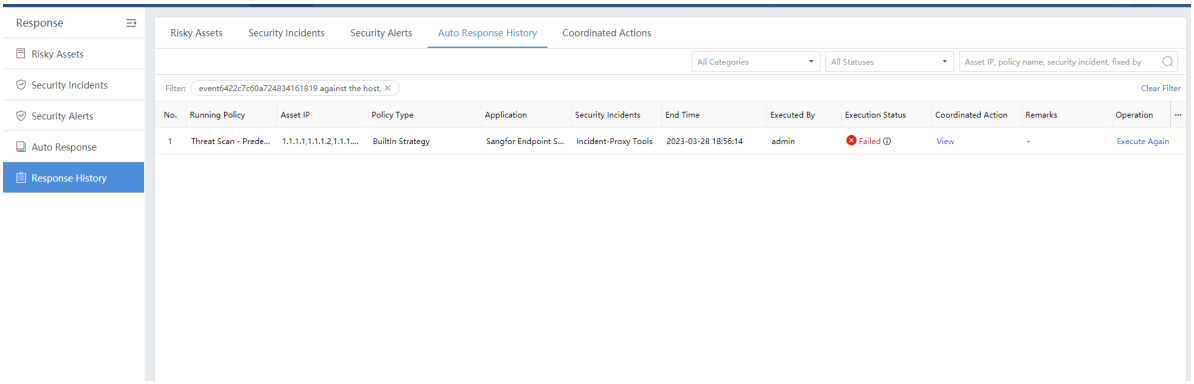
For events marked as fixing or fixed, you can click <Response History> to view the policy execution history, as shown in the figure below.



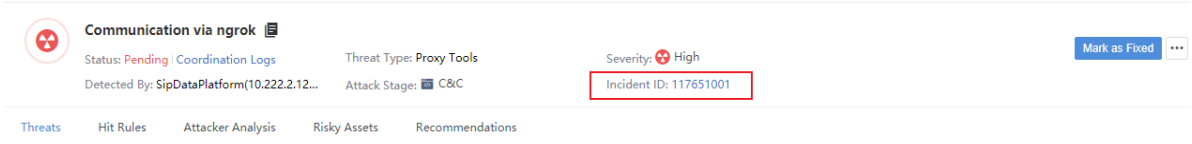
You can click ">" to view the policy execution process, as shown in the figure below.

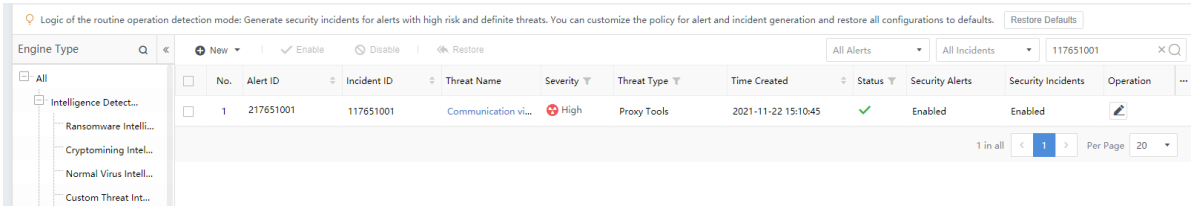


You can click <Expand> to go to the [Response/Response History/Auto Response History] page, as shown in the figure below.



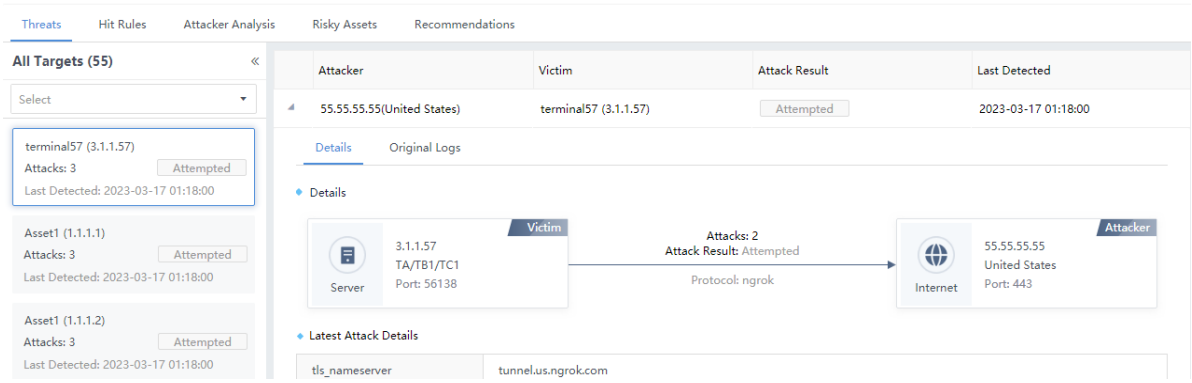
You can click the event ID to go to the [System/Security Capabilities] page and view the event details, as shown in the figure below.



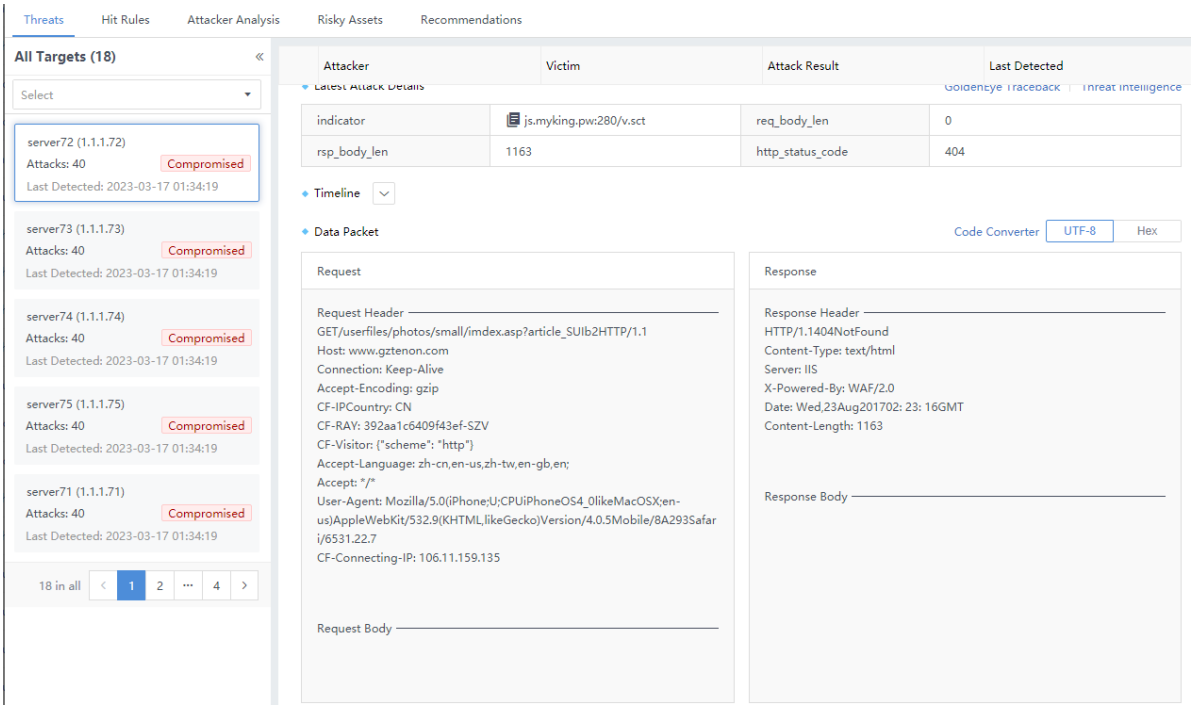


Threats

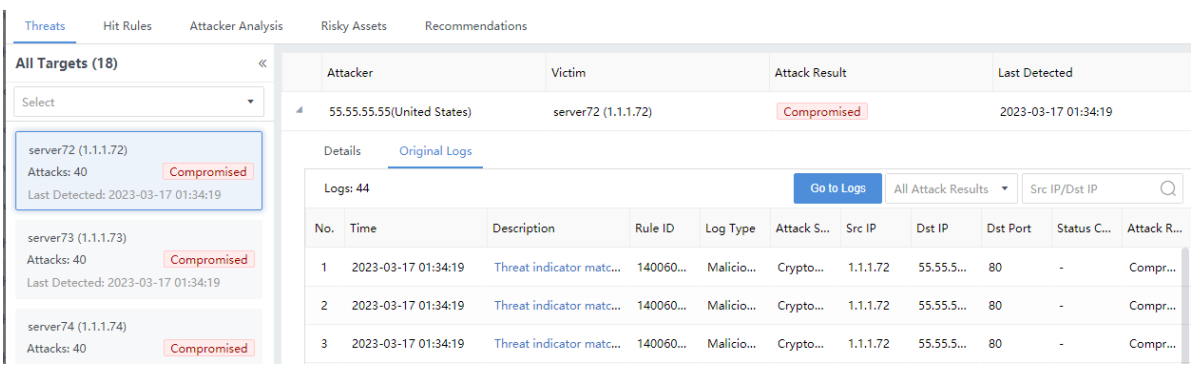
On the [Threats] tab, attack targets, alert quantity, alert details, and original logs are displayed, as shown in the figure below.



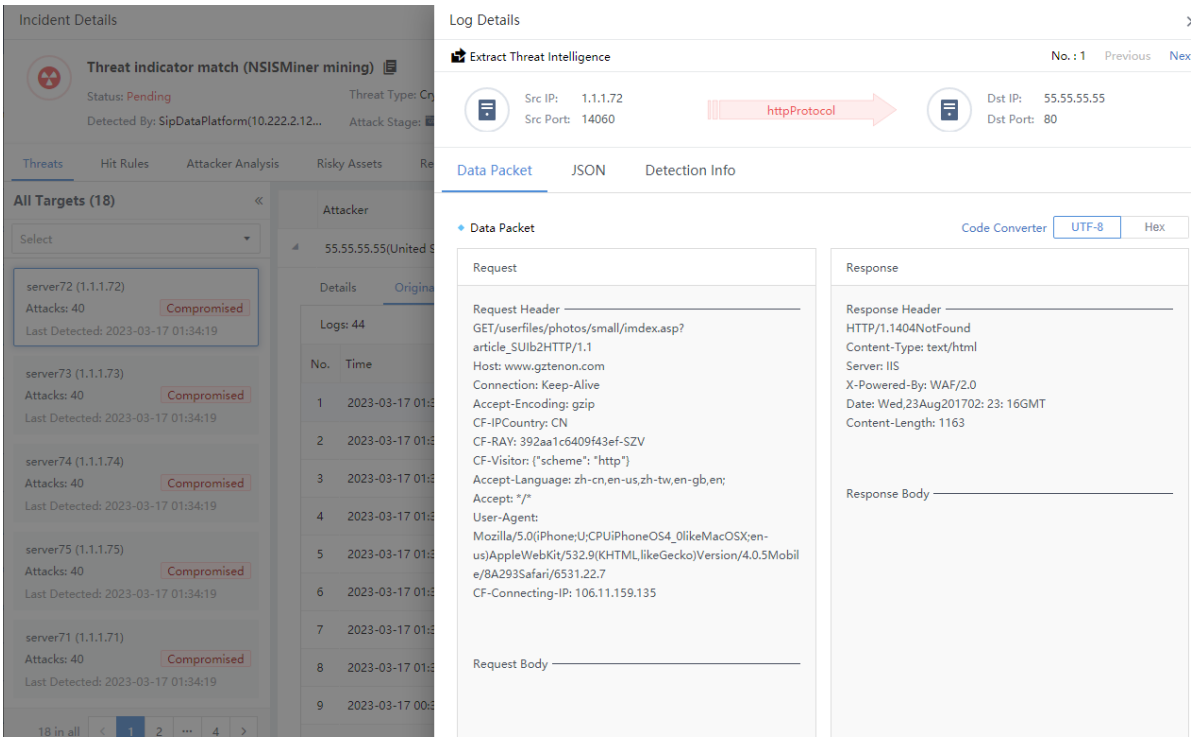
You can scroll up and down in the [Details] section to view the data packet information, as shown in the figure below.



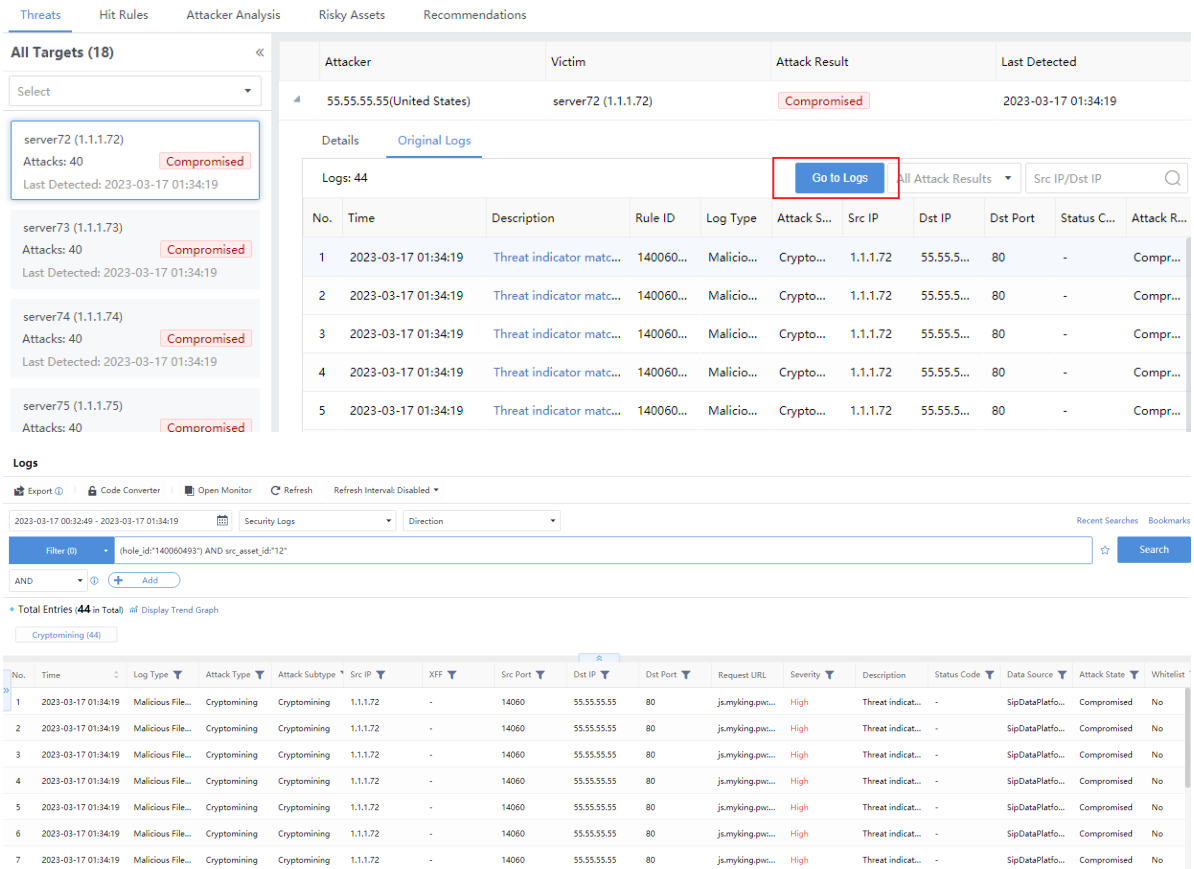
You can click the <Original Logs> tab to view the logs related to the alerts, as shown in the figure below.



You can click the content in the "Description" column to view the original log information for higher judging efficiency, as shown in the figure below.

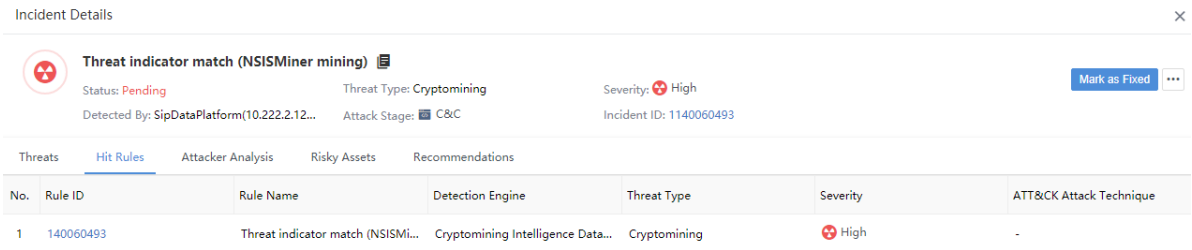


You can click <Go to Logs> to redirect to the <Logs> page and filter the logs related to this alert, as shown in the figure below.

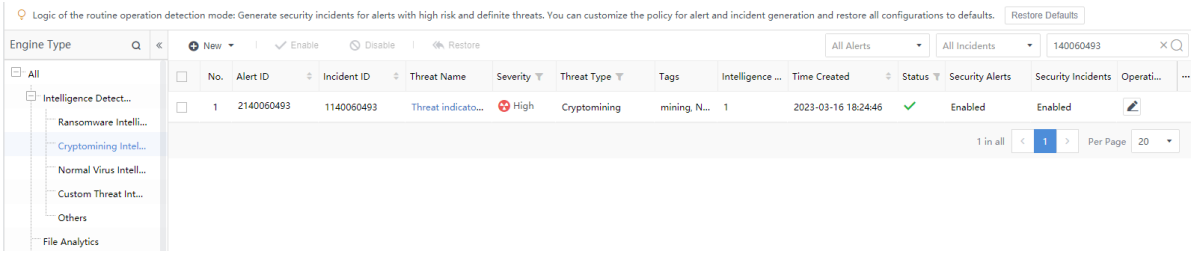


Hit rule

You can view the list of rules related to the event. Information such as the rule ID, rule name, detection engine, threat type, severity, and ATT&CK attack technique is displayed in the list, as shown in the figure below.

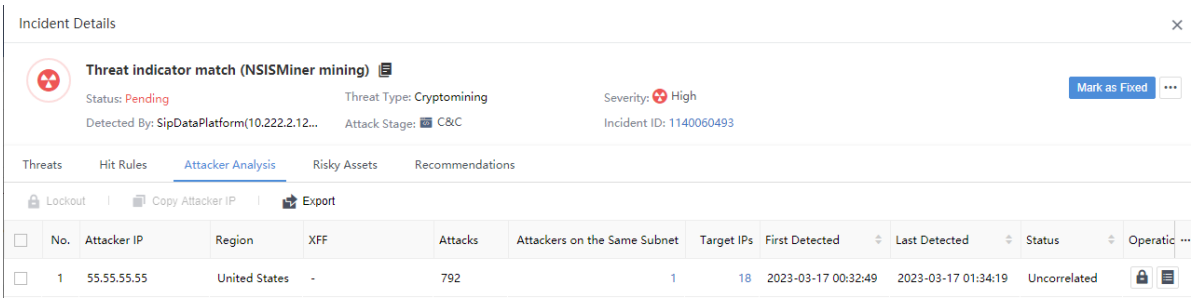


You can click a rule ID to go to [System/Security Capabilities/Detection Engines]. On the page that appears, you can view or edit the rule details, as shown in the figure below.

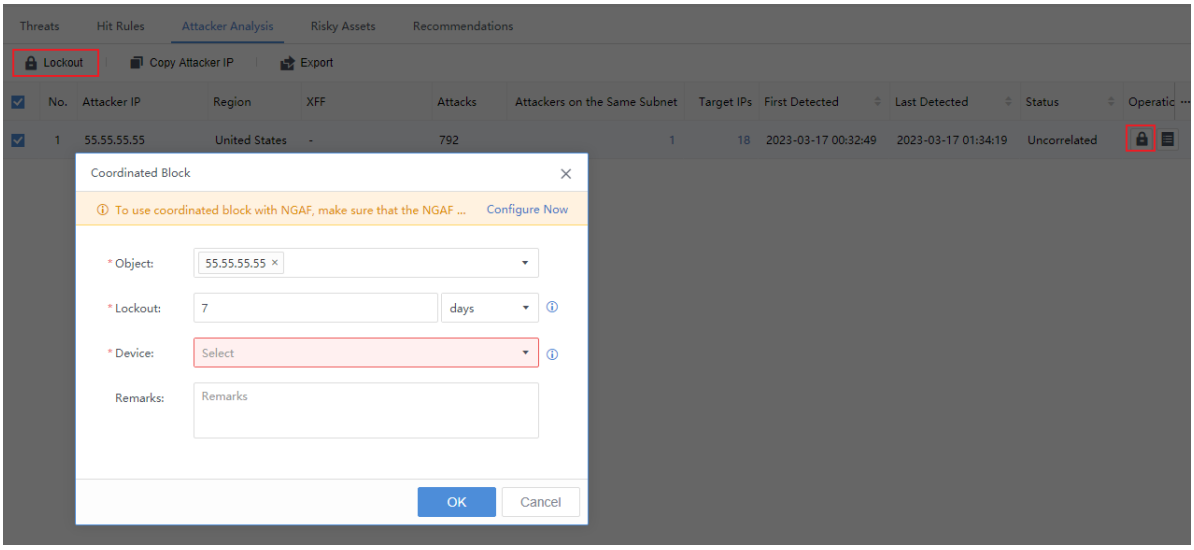


Attacker analysis

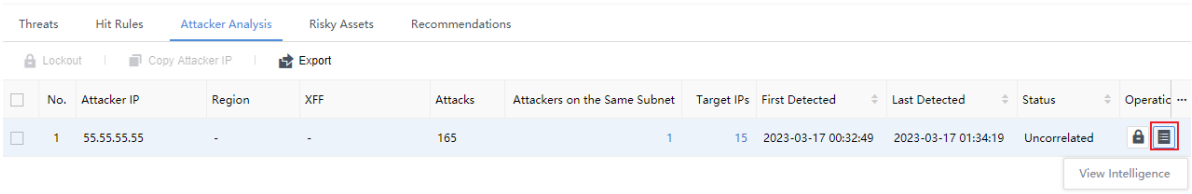
You can view the attacker IP address, region, attack count, attackers on the same subnet, target IP addresses, first attack time, last attack time, lockout status, threat intelligence, and attacker profile, as shown in the figure below.



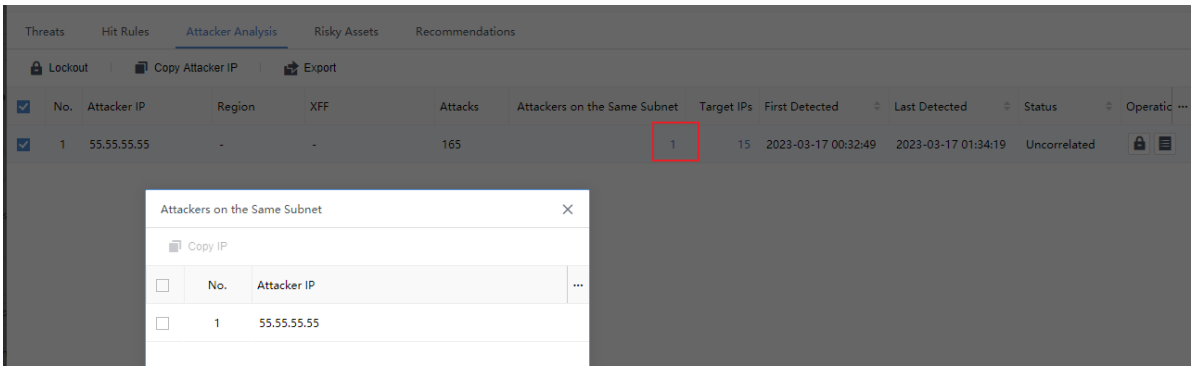
You can click <Lockout> or the < > icon in the [Operation] column to select the configured Next Generation Application Firewall (NGAF) for performing correlated block, as shown in the figure below.

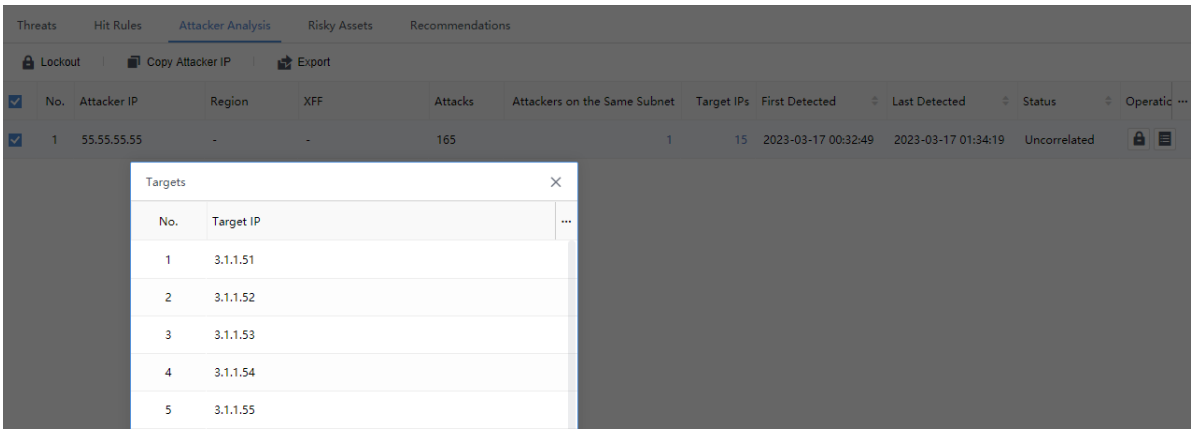


You can click the < > icon in the [Operation] column to view the threat intelligence, as shown in the figure below.



You can click the value in the "Attackers on the Same Subnet" or "Target IPs" column to view the attacker IP addresses or target IP addresses, as shown in the figure below.

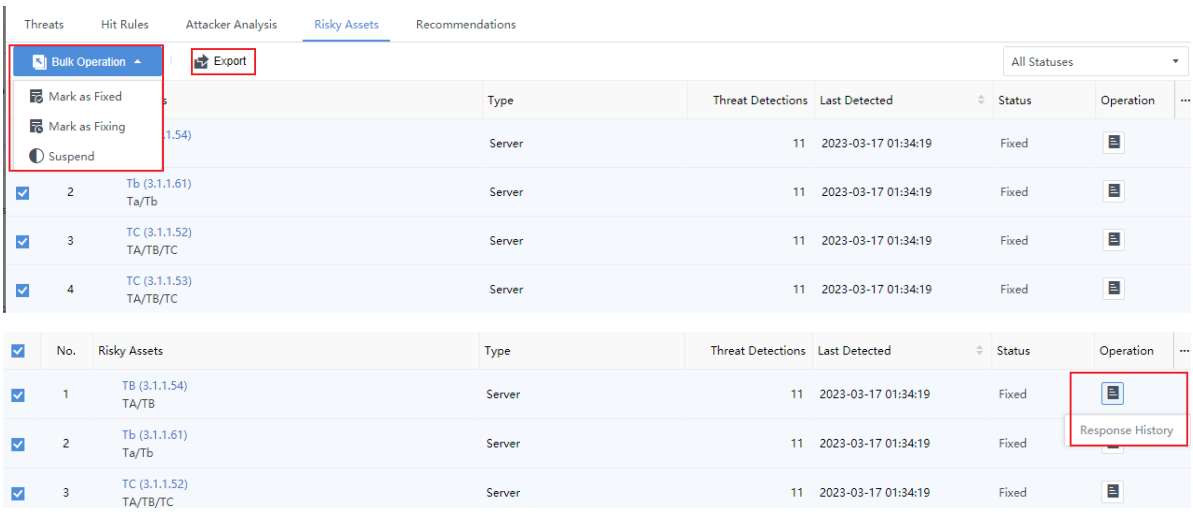




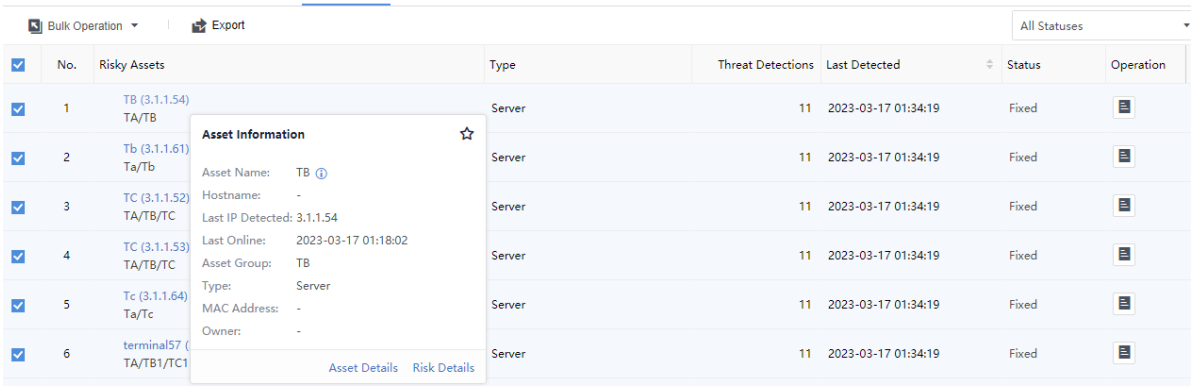
If a lot of attacker IP addresses are associated with the event, you can click <Export> to export the attacker IP list in XLSX format.

Risky assets

You can view the information about risky assets associated with the security event and perform operations such as export, bulk operation, and coordinated response of one event, as shown in the figure below.

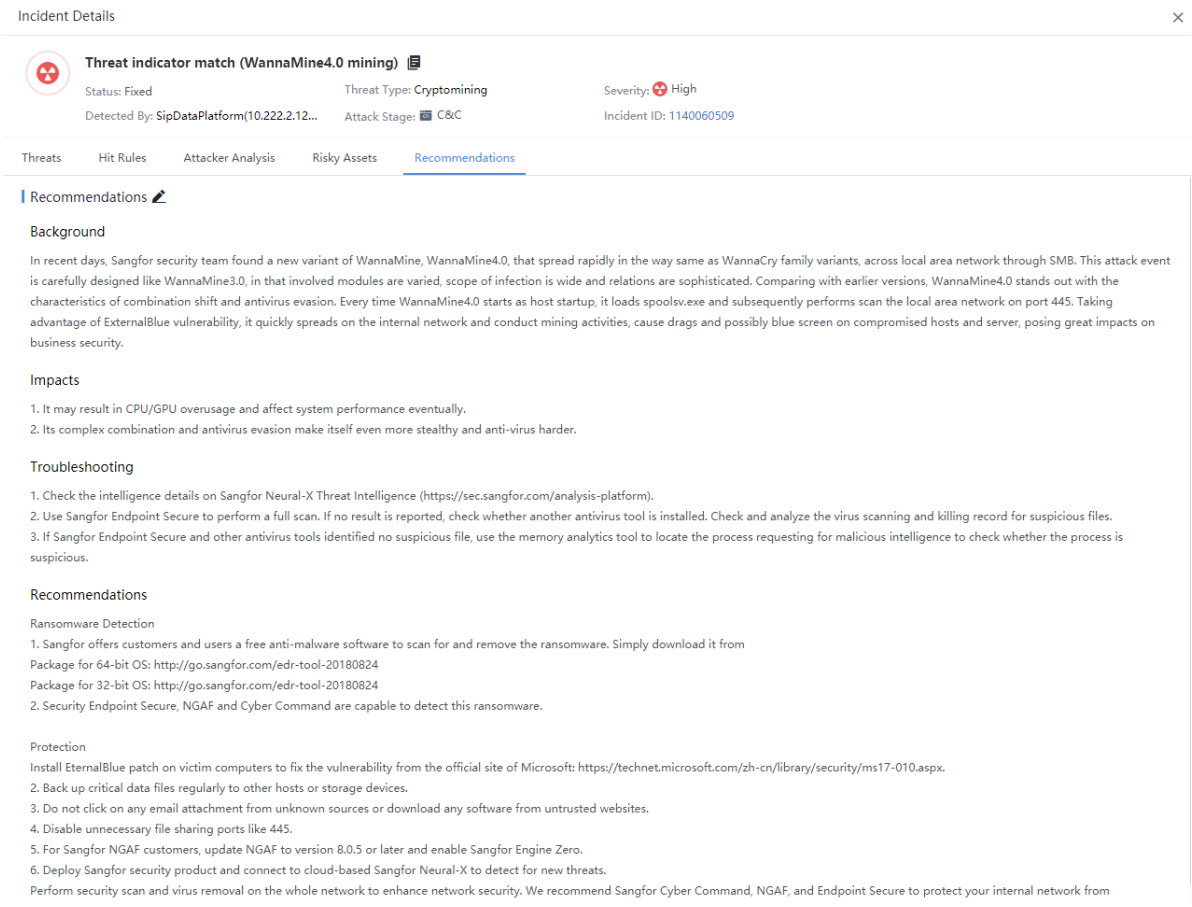


You can hover over a risky asset to view the asset details or risk details, as shown in the figure below.



Recommendations

Troubleshooting suggestions, fixing suggestions, and daily maintenance suggestions are provided based on the background and impact of the event, as shown in the figure below.

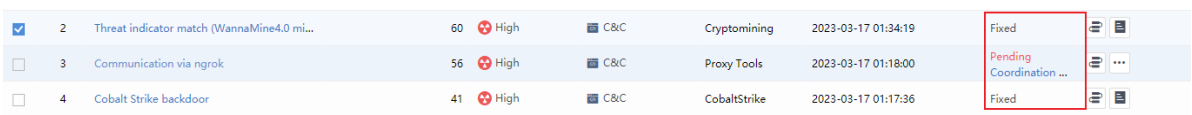


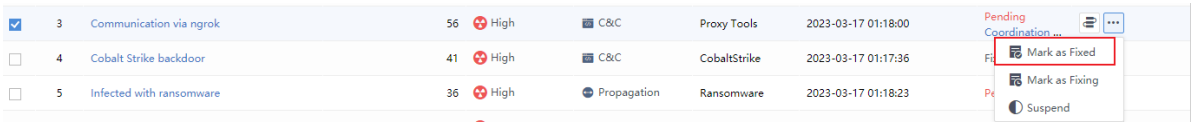
Incident Fixing

Security events can be fixed through manual operation and coordinated response. The status of a security event can be Fixed, Fixing, and Suspended after the manual operation. When the coordinated response operation is performed, the event is fixed automatically or manually according to the response policy.

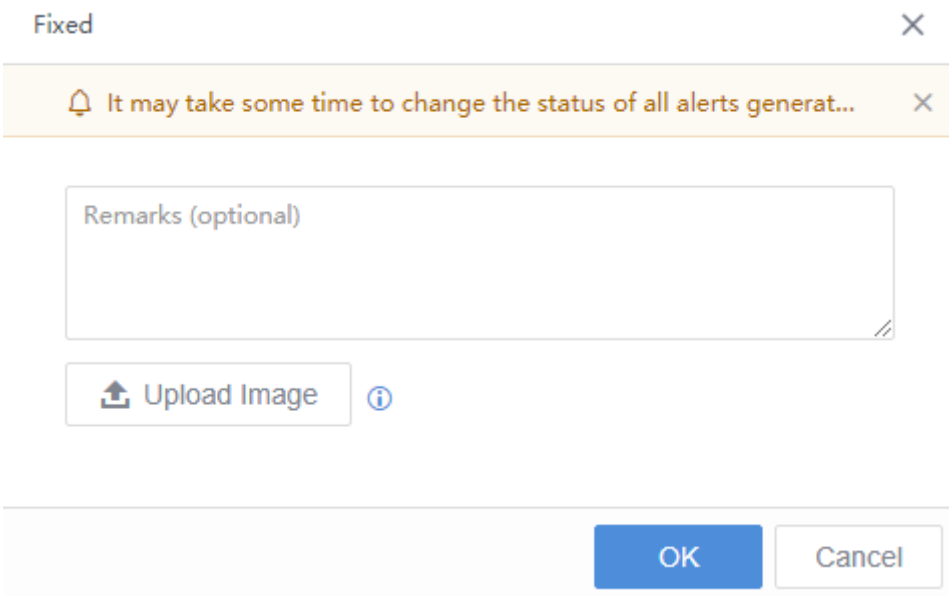
Manual operation

On the [Response/Security Events/Security Incidents] page, you can select an event and click the <•••>icon in the <Operation> column, as shown in the figure below.

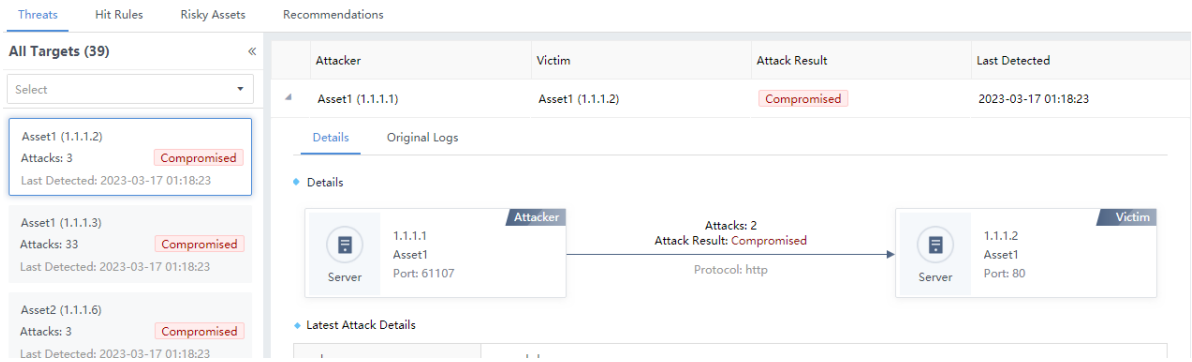




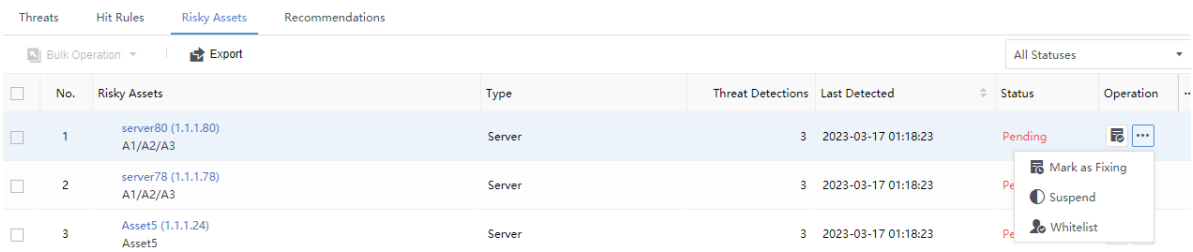
When you select <Mark as Fixed>, a pop-up box appears, where you can add remarks and upload images when needed. Then, the content in the <Status> column is changed to [Fixed], as shown in the figure below.



You can click an event to go to the [Incident Details] page to fix the event manually, as shown in the figure below.

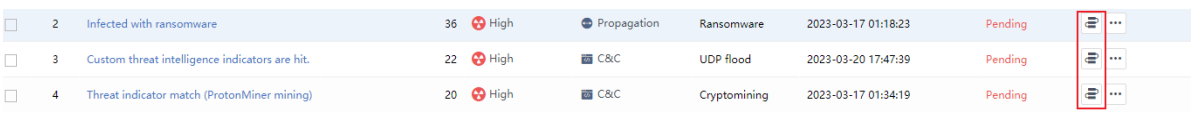


You can click the [Risky Assets] tab on the [Incident Details] page to fix risky assets manually as needed, as shown in the figure below.

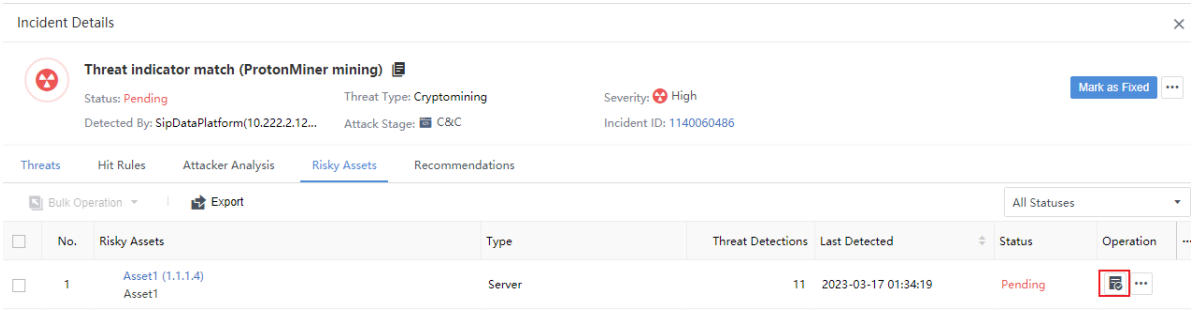


Coordinated response

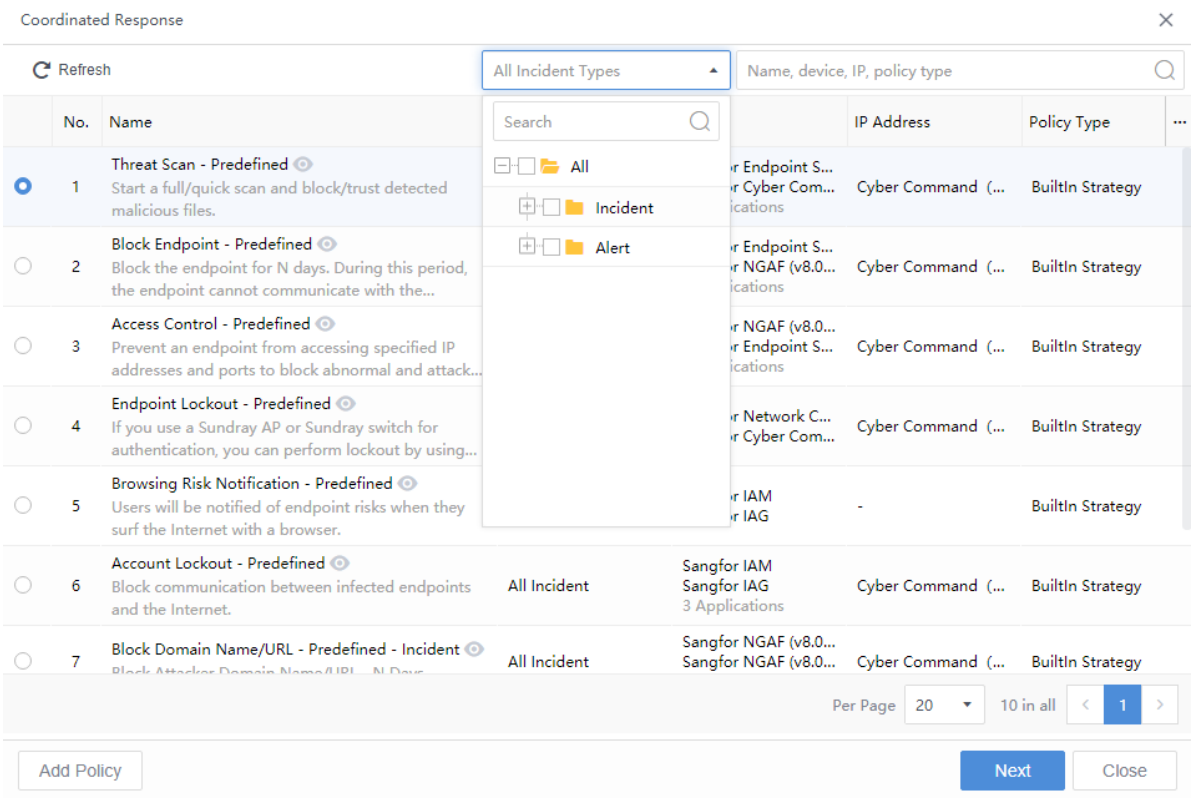
On the [Response/Security Events/Security Incidents] page, you can click the < > icon in the [Operation] column, and the [Coordinated Response] dialog box pops up. You can perform the coordinated response operation according to policies, as shown in the figure below.



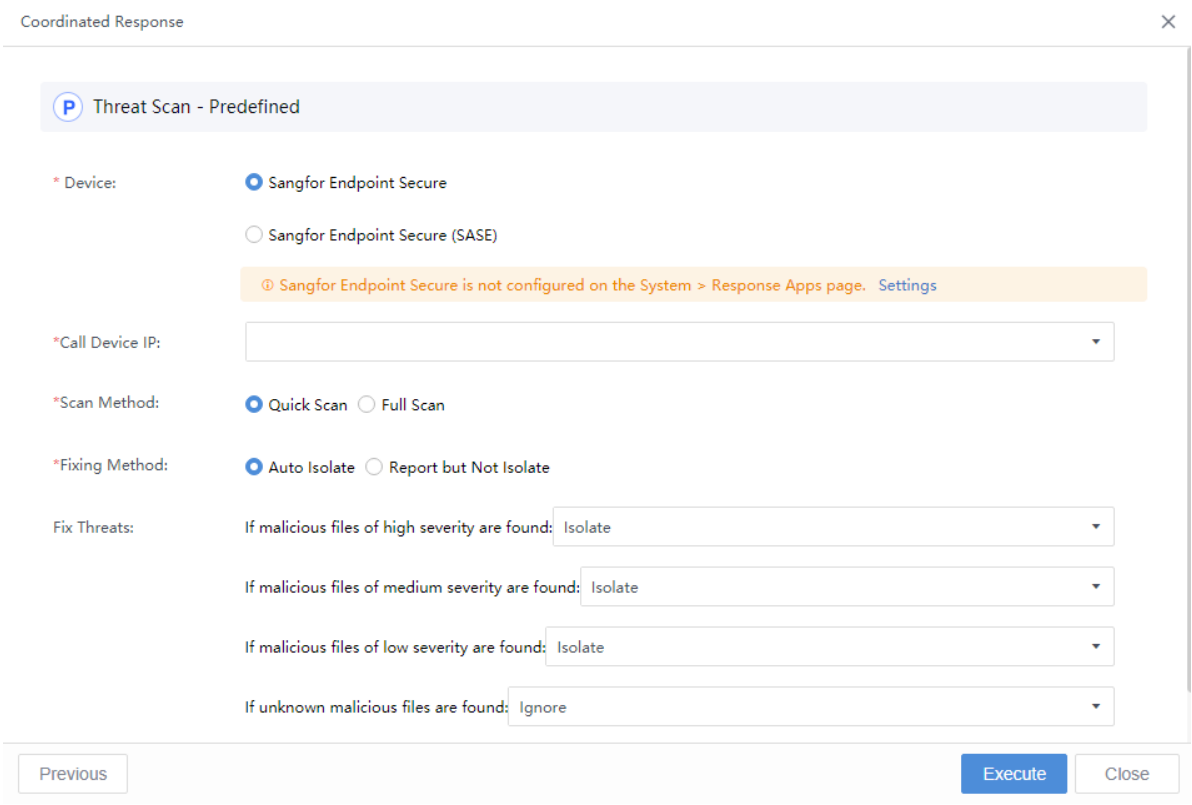
If you want to perform the coordinated response operation for the risky endpoint associated with the security event, click the < > icon in the [Operation] column on the [Risky Assets] tab of the [Incident Details] page.



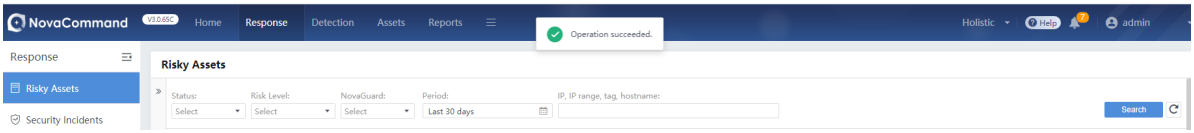
In this case, the [Coordinated Response] dialog box appears. You can select Event or Alert to filter out predefined policies, such as Threat Scan, Block Domain Name/URL, VM Suspend, Snapshot, VM Add, VM Shutdown, Block Endpoint, Account Lockout, Browsing Risk Notification, Endpoint Lockout, and Access Control. You can also add cloned or customized policies as required, as shown in the figure below.



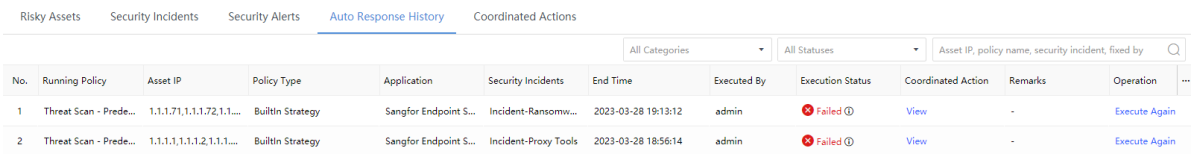
After you click <Next>, the [Coordinated Response] dialog box appears. You can configure parameters related to coordinated response, such as device. The parameters vary based on the policy. The figure below takes the policy for threat scan as an example.



After you click <Execute>, the response action starts to be executed. The system prompts the message of <Executed> at the top of the page after the execution is completed.

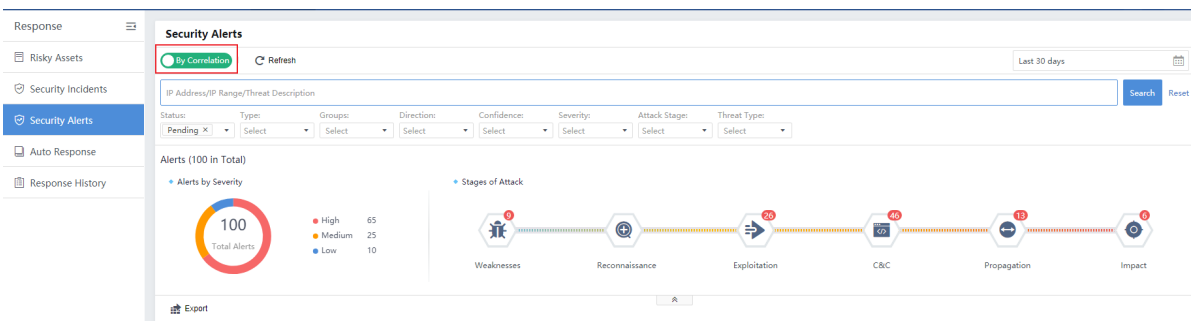


On the [Response/Response History/Auto Response History] page, you can view the response history, including the status, result, policy, and other related information, as shown in the figure below.



Security Alerts

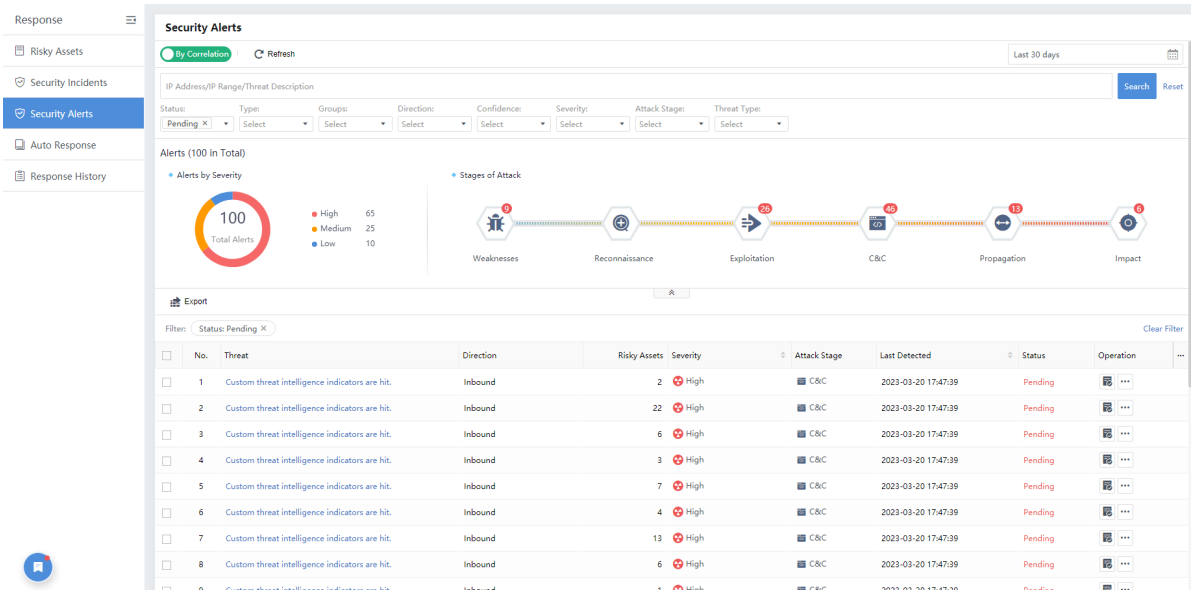
Like the [Security Incidents] module, the [Security Alerts] module is also frequently used by users and is indispensable for operations. In this module, security alerts can be displayed by correlation or by details. When alerts are displayed by correlation, the attacker IP and target IP have a many-to-many relationship; when alerts are displayed by details, the attacker IP and target IP have a one-to-one or one-to-many relationship. You can switch between the two modes with one click, as shown in the figure below.



Alert Filtering

By correlation

On the [Response/Security Events/Security Alerts] page, you can view the distribution of security alerts and filter them according to the following criteria, as shown in the figure below.



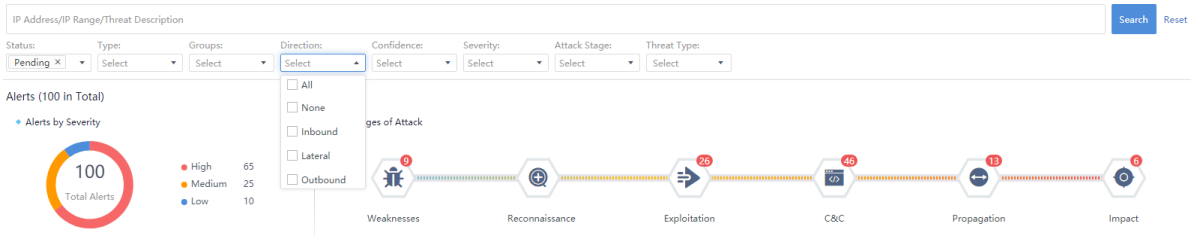
Parameters:

Status: Includes All, Pending, Suspended, Fixing, and Fixed.

<Type>: Includes All, Server, and Host.

<Asset Group>: You can select different asset groups from the drop-down list.

Direction: The data flow direction of a security alert, including none (local alerts), inbound (such as attacks launched from the outside), lateral (internal attacks), and outbound (such as malicious outbound access), as shown in the figure below.

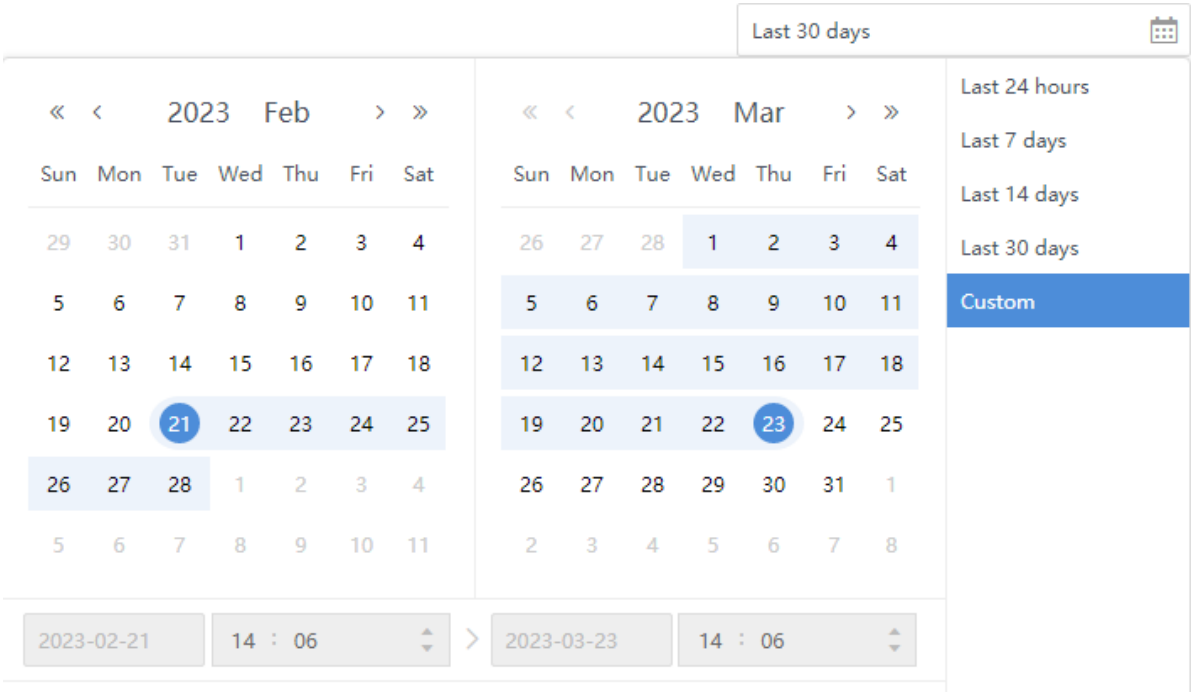


<Severity>: Includes All, High, Medium, and Low. The alert severity is evaluated based on its impact scope and depth.

Attack Stage: Includes All, Weakness, Reconnaissance, Exploitation, C&C, Propagation, and Impact. The stage of a security alert is determined based on the standard attack chain model of the industry.

Threat Type: A threat can be classified into three levels.

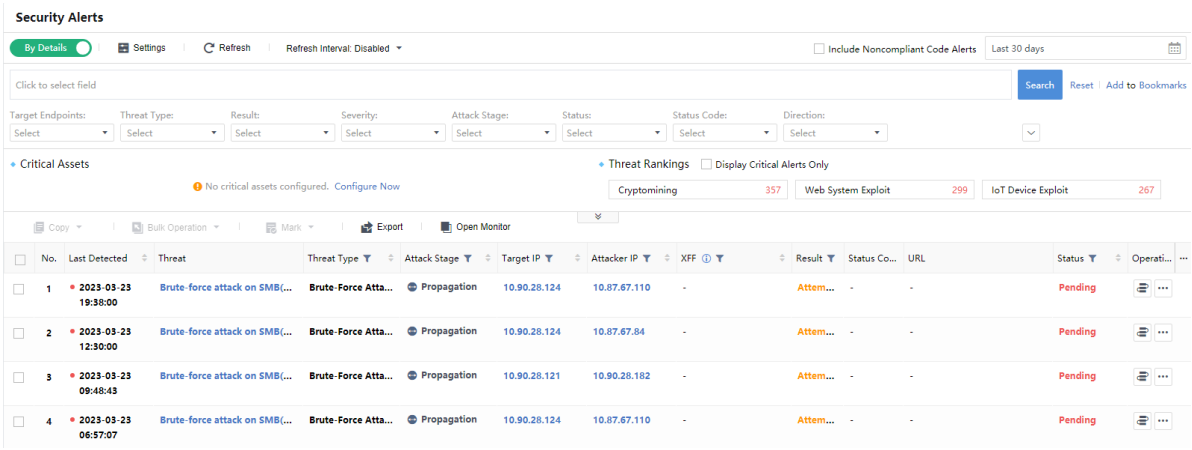
<Period>: You can search for security alerts by time period, including last 30 days, last 7 days, last 24 hours, and custom. To search for security alerts that occurred 30 days ago, you can select custom, as shown in the figure below.



Search: You can perform a fuzzy search of security alerts by IP, IP range, description, asset group, and endpoint name.

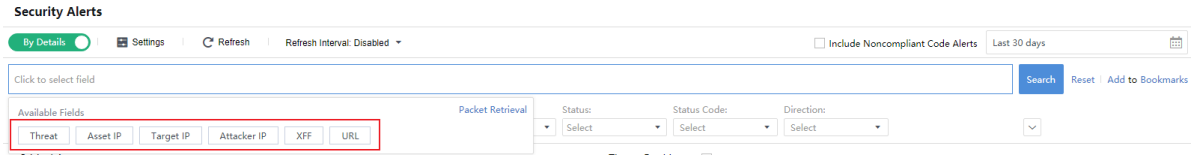
By details

When security alerts are displayed by details, more criteria can be used for alert search, as shown in the figure below.



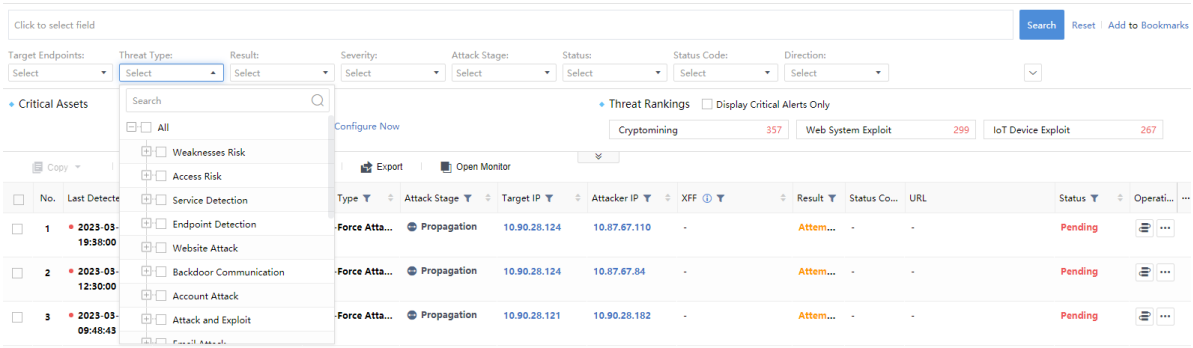
Parameters:

<Search box>: You can search alerts by threat, asset IP, target IP, attacker IP, proxy server IP, and URL, as shown in the figure below.



<Target Endpoints>: Includes Server and Host.

<Threat Type>: A threat can be classified into three levels. You can expand each threat level by clicking <⊞>, or filter alerts by entering keywords in the search box for fuzzy search, as shown in the figure below.



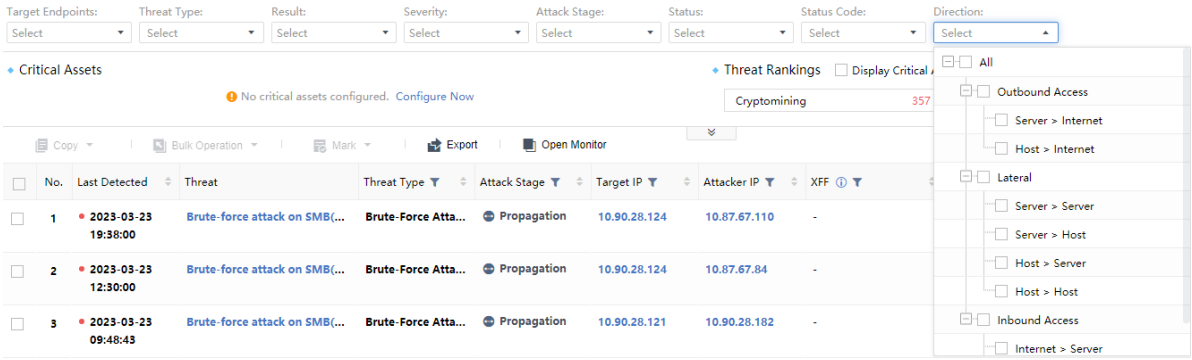
<Result>: Includes Compromised, Succeed, Attempted, and Failed. Compromised indicates further destruction after a successful attack.

<Severity>: Includes High, Medium, and Low.

<Status>: Includes Pending, Suspended, Fixing, and Fixed.

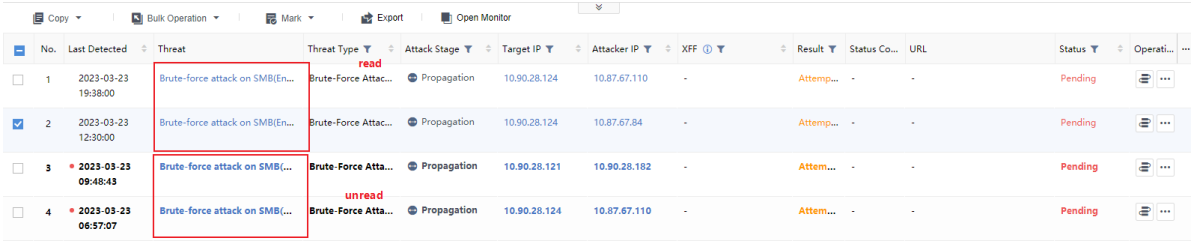
<Status Code>: The status codes are classified into 1XX, 2XX, 3XX, 4XX, and 5XX.

<Direction>: Includes Outbound Access, Lateral, and Inbound Access. Each direction has different access directions between asset types, as shown in the figure below.



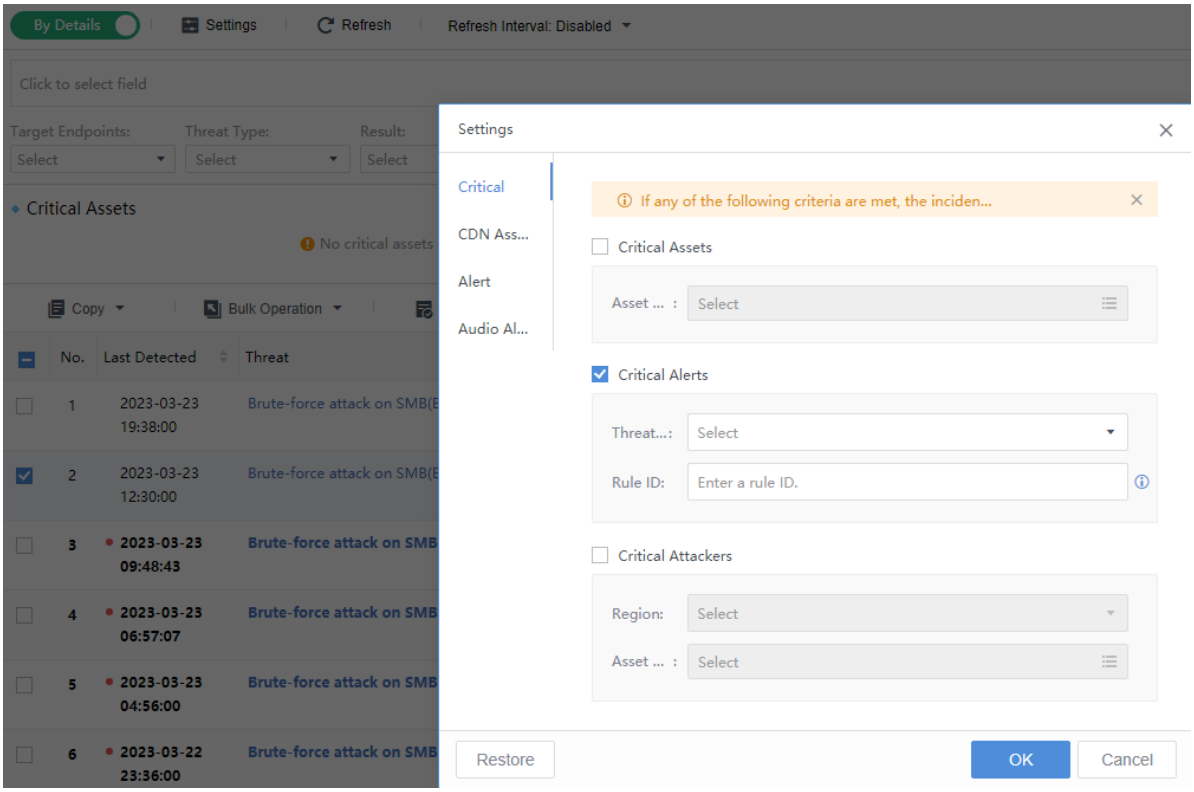
<Groups>: You can select a group from the drop-down list.

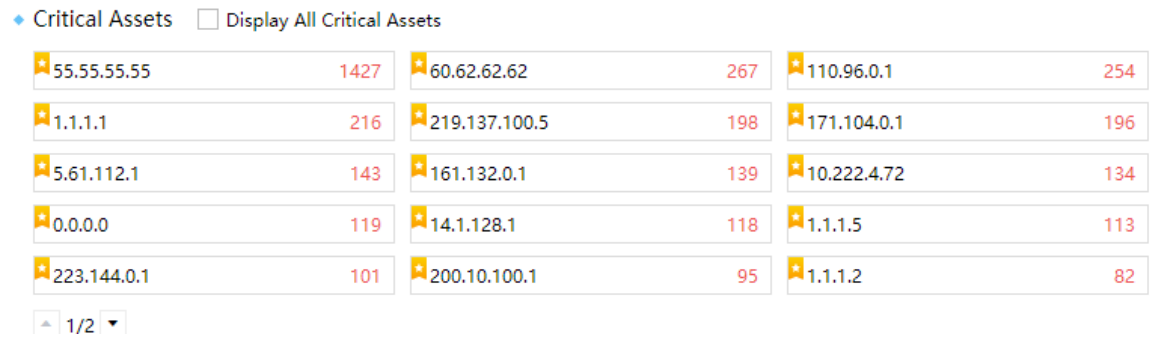
<Read>: Includes Read and Unread. When the <By Details> mode is selected, alerts are constantly refreshed in chronological order, with those that are read displayed in normal text and those that are unread displayed in bold text, as shown in the following figure.



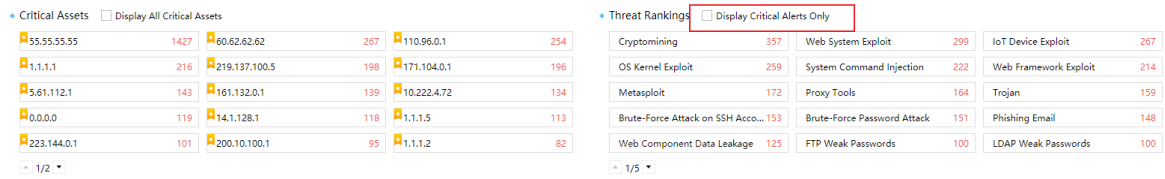
Critical assets

When the <By Details> mode is selected, you can set the criteria for critical items, including critical assets, critical alerts, and critical attackers. These criteria have an "OR" relationship, which means the items will be highlighted in the statistics and list if any of these criteria are met, as shown in the following figure.



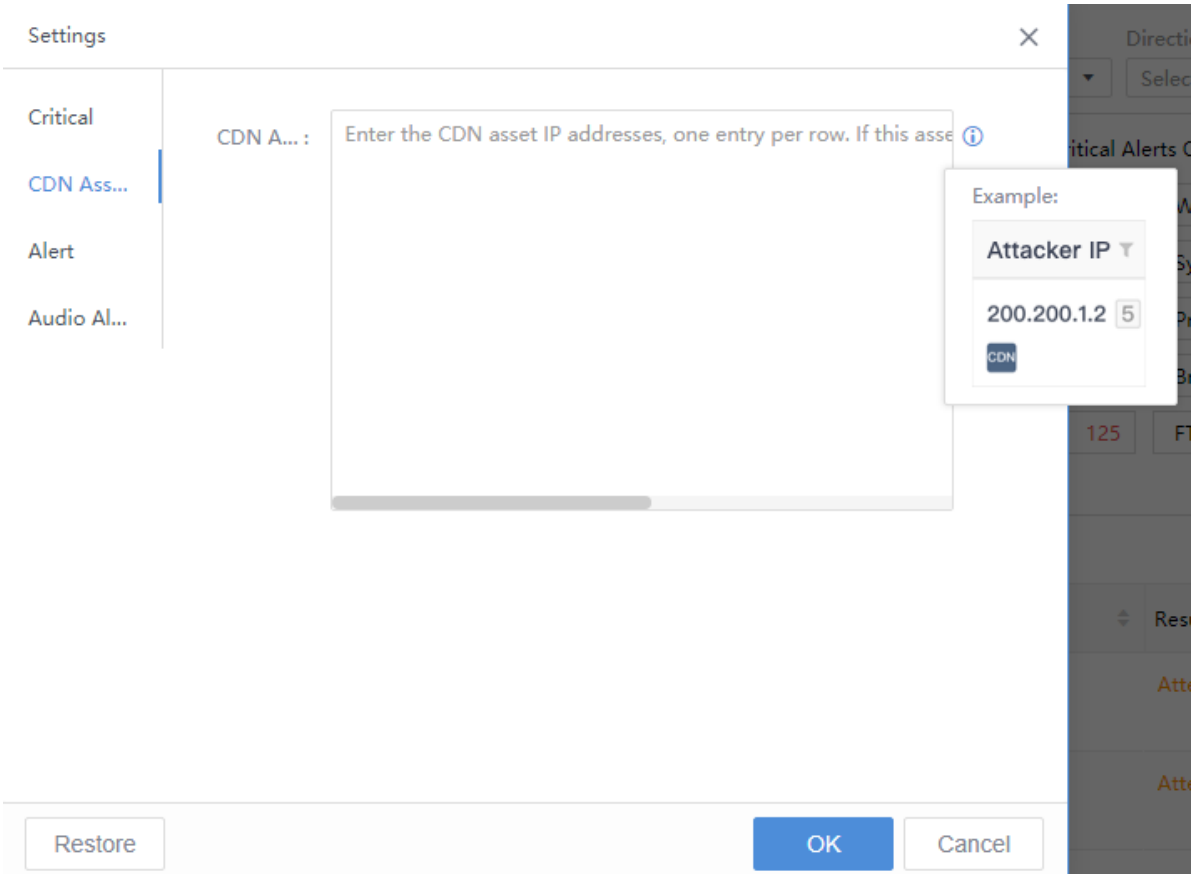


After the criteria are set, you can select the <Display Critical Assets Only> check box to display the critical items. This check box is not selected by default, and all security alerts are displayed, as shown in the following figure.



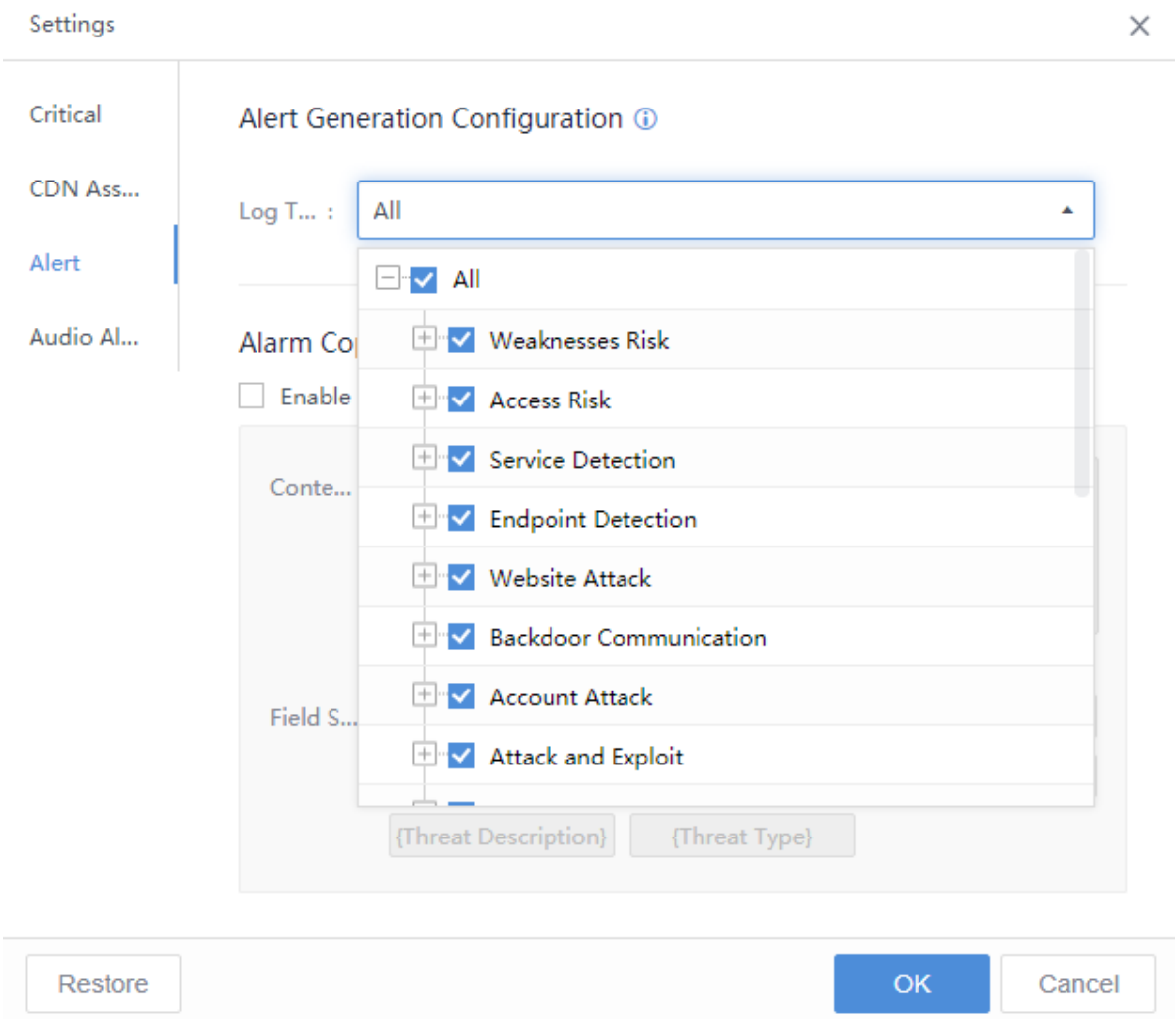
CDN assets

If you are using CDN, you can mark CDN assets separately to ensure they can be identified in real-time alerts, in order to facilitate tracing and analysis. You can enter the information about one asset per row, as shown in the following figure.

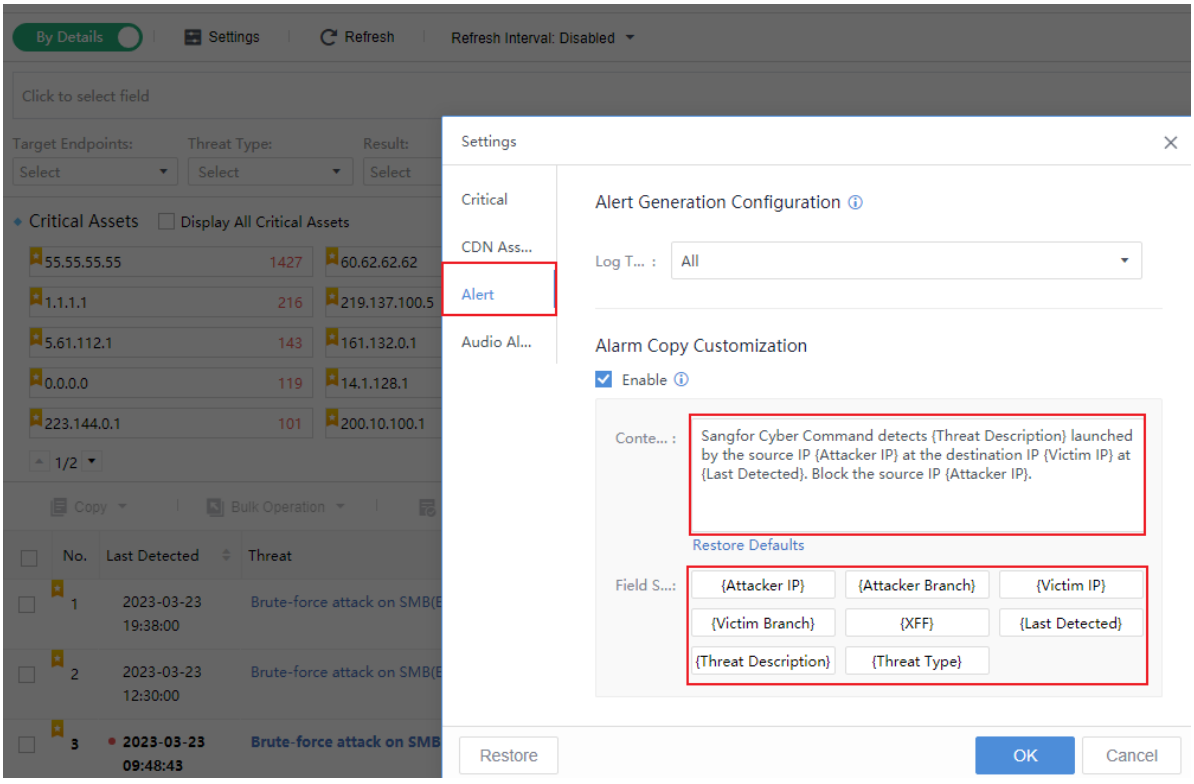


Alert

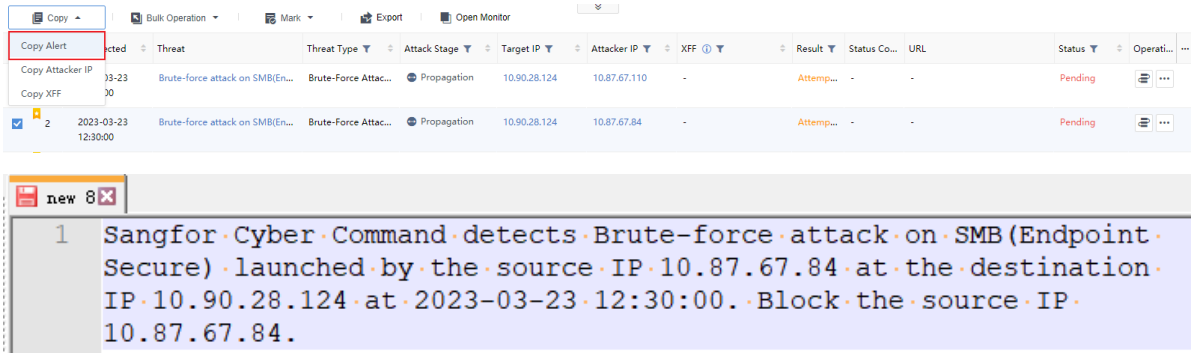
You can specify the log types for which you want to generate alerts. By default, all log types are selected, or you can specify the log types as needed, as shown in the following figure.



You can also customize the <Copy> action by selecting the <Enable> check box. In the Content Preview box, you can specify the content and fill in common parameters with the constants in Field Settings, as shown in the following figure.

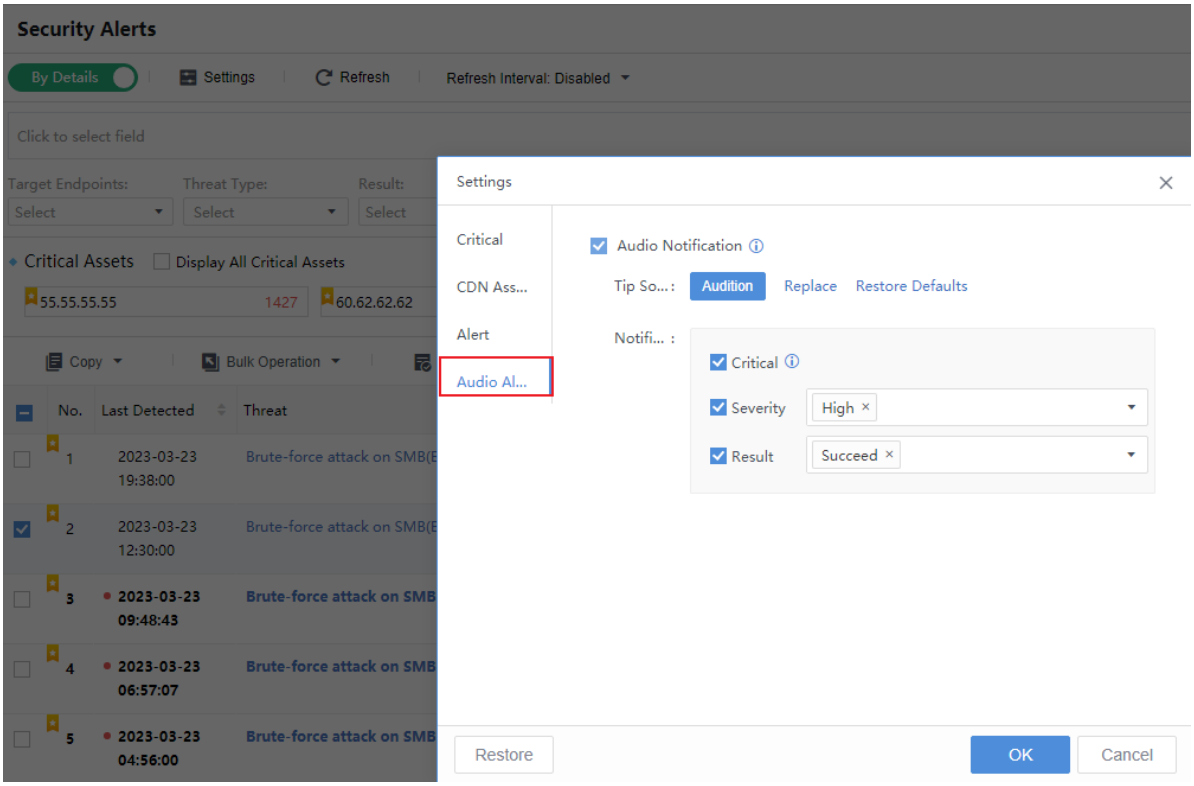


After you click <OK>, you can select an alert in the alert list and click \Copy Alert>. The content that you have copied is the same as that you have just edited, as shown in the following figure.



Audio alert

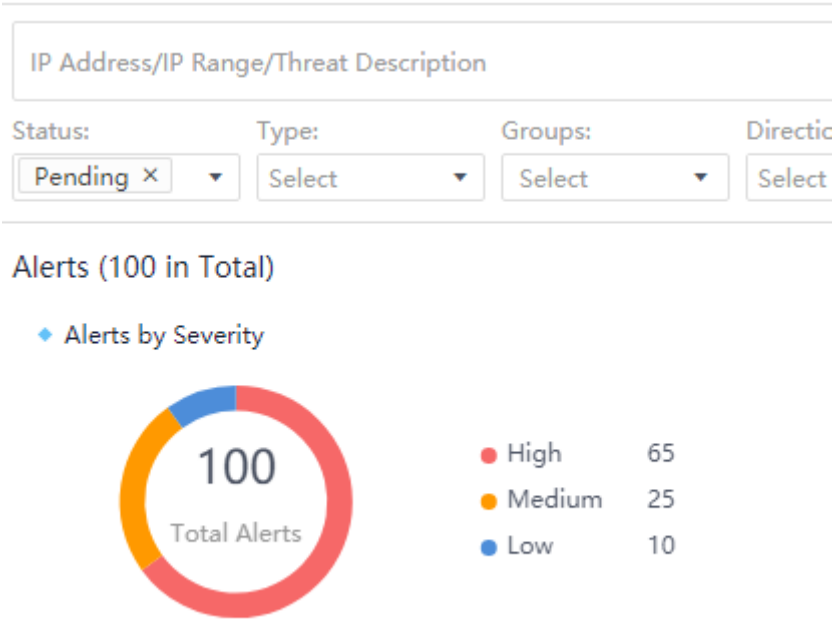
When security alerts are displayed by details, you can set audio alerts. For new security alerts that meet the conditions for audio notifications (the refresh interval is one minute by default), you will hear a tip sound. For those that do not meet the conditions or when there are no new security alerts, you cannot hear the tip sound even when the audio notification is enabled, as shown in the following figure.



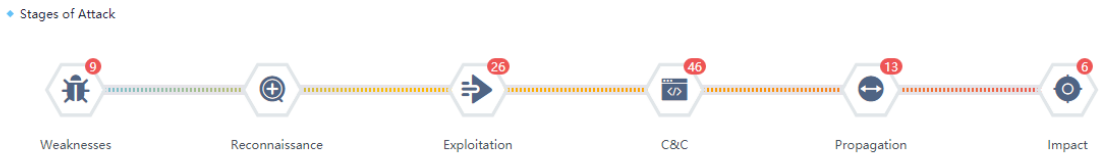
You can click <Replace> to replace the default tip sound. The audio file in MP3 format is supported. You can click <Audition> to listen to the audio. By editing the notification content, you can specify the conditions for audio notification. The options (Critical, Severity, and Result) are in an "AND" relationship.

Alert Statistics

When security alerts are displayed by correlation, the alert statistics are displayed in the middle of the [Response/Threats/Security Alerts] page and classified into three parts by severity (high, medium, and low). The number of alerts is displayed for each part, as shown in the following figure.



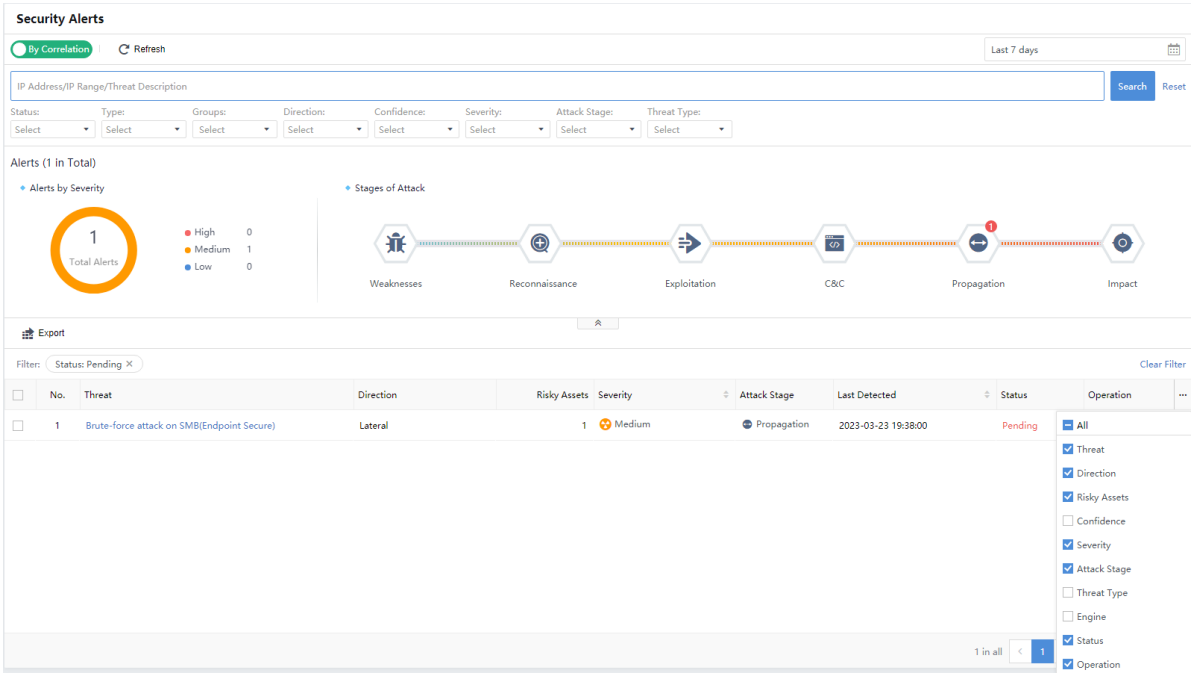
The number of security alerts in each stage of attack is displayed. The total number of security alerts is the same as the sum of alerts classified by severity, as shown in the following figure.



Alert Viewing

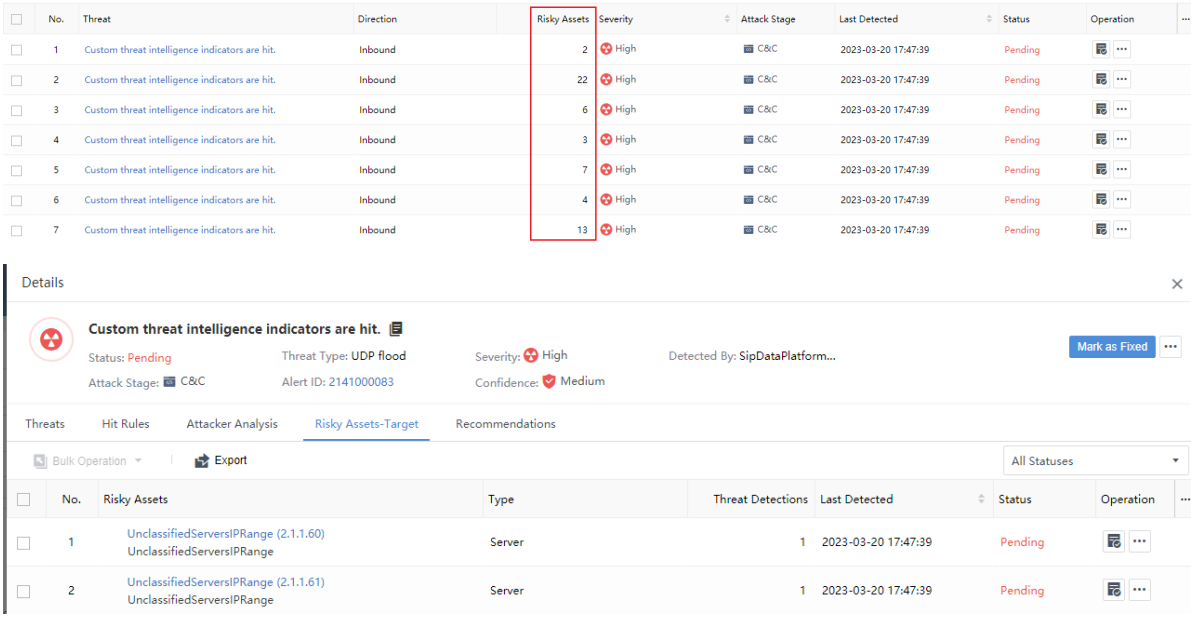
By correlation

You can search for specific security alerts by the conditions below the search box. Fields for each alert in the list include threat, direction, risky assets, confidence, severity, attack stage, threat type, engine, last detection time, status, and operation, as shown in the figure below.

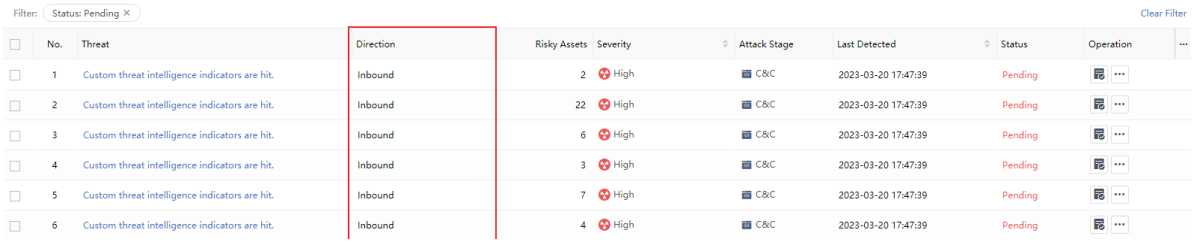


Fields:

Risky Assets: Represents the number of risky assets associated with the alert. You can view the number in the Risky Assets column on the Risky Assets - Targets tab after you click a threat, as shown in the figure below.

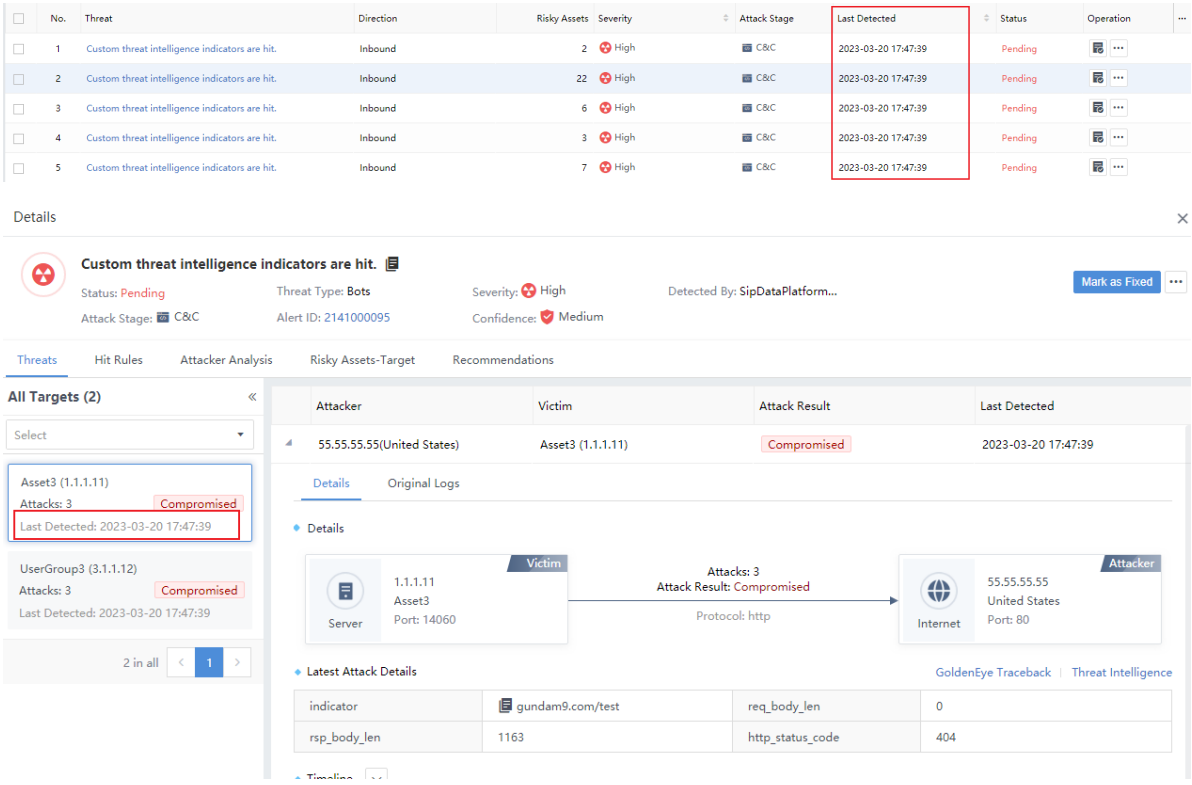


Direction: Represents the data flow direction of a security alert. Available options include None, Inbound (attacks launched from the outside), Lateral (lateral attacks), and Outbound (malicious outbound access), as shown in the figure below.



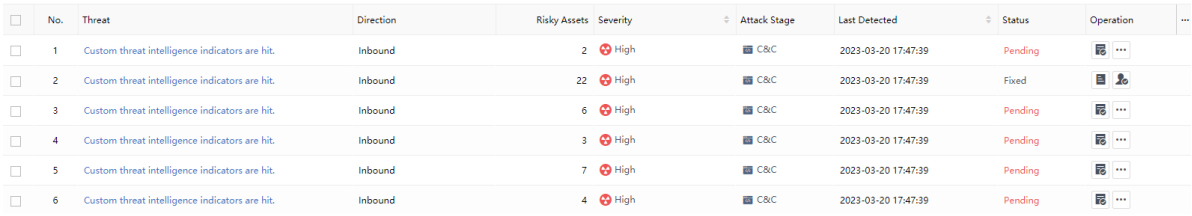
Status: Includes Pending, Fixing, and Suspended.

<Last Detected: >The last time when the alert was generated, as shown in the figure below.



Engine: Represents the built-in engine that detects the incident.

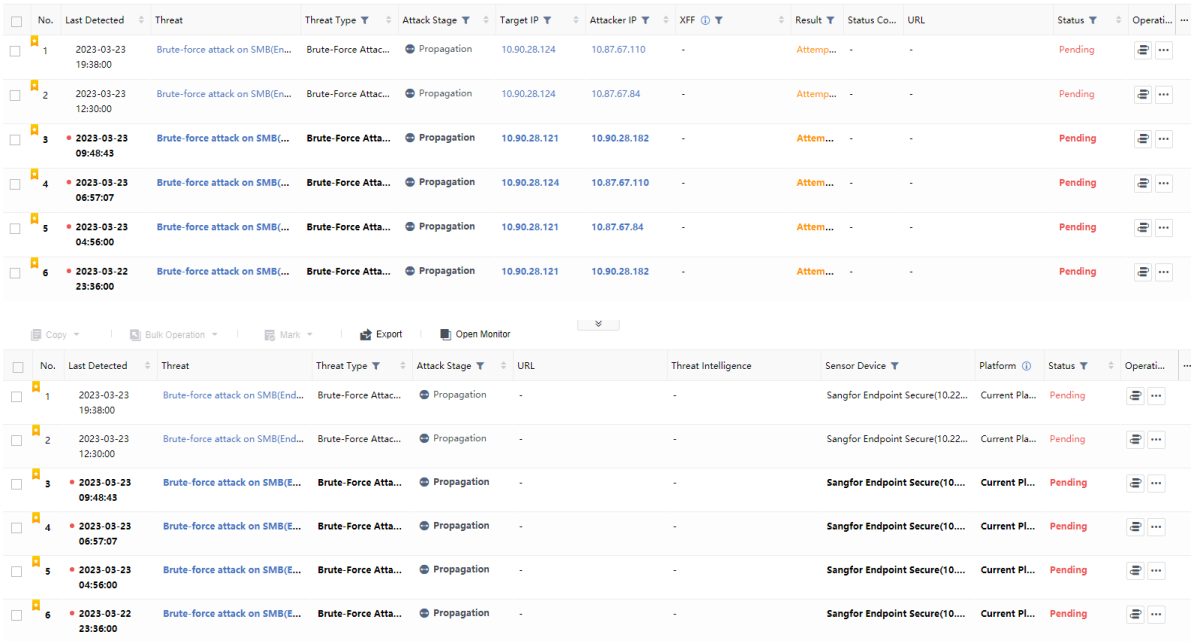
Status: Represents the fixing status of the alert. If the alert involves several risky assets that are all fixed, [Fixed] will be displayed. If one or more risky assets are pending fixing, [Pending] will be displayed, as shown in the figure below.



No.	Threat	Direction	Risky Assets	Severity	Attack Stage	Last Detected	Status	Operation
1	Custom threat intelligence indicators are hit.	Inbound	2	High	C&C	2023-03-20 17:47:39	Pending	
2	Custom threat intelligence indicators are hit.	Inbound	22	High	C&C	2023-03-20 17:47:39	Fixed	
3	Custom threat intelligence indicators are hit.	Inbound	6	High	C&C	2023-03-20 17:47:39	Pending	
4	Custom threat intelligence indicators are hit.	Inbound	3	High	C&C	2023-03-20 17:47:39	Pending	
5	Custom threat intelligence indicators are hit.	Inbound	7	High	C&C	2023-03-20 17:47:39	Pending	
6	Custom threat intelligence indicators are hit.	Inbound	4	High	C&C	2023-03-20 17:47:39	Pending	

By details

When security alerts are displayed by details, fields for each alert include last detection time, threat, threat type, attack stage, severity, target IP, target group, attacker IP, asset of attacker, proxy server IP, result, status code, attacks, URL, threat intelligence, device, data source, status, and operation, as shown in the figure below.



No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Co...	URL	Status	Operati...
1	2023-03-23 19:38:00	Brute-force attack on SMB(En...	Brute-Force Attac...	Propagation	10.90.28.124	10.87.67.110	-	Attemp...	-	-	Pending	
2	2023-03-23 12:30:00	Brute-force attack on SMB(En...	Brute-Force Attac...	Propagation	10.90.28.124	10.87.67.84	-	Attemp...	-	-	Pending	
3	2023-03-23 09:48:43	Brute-force attack on SMB(...	Brute-Force Atta...	Propagation	10.90.28.121	10.90.28.182	-	Attem...	-	-	Pending	
4	2023-03-23 06:57:07	Brute-force attack on SMB(...	Brute-Force Atta...	Propagation	10.90.28.124	10.87.67.110	-	Attem...	-	-	Pending	
5	2023-03-23 04:56:00	Brute-force attack on SMB(...	Brute-Force Atta...	Propagation	10.90.28.121	10.87.67.84	-	Attem...	-	-	Pending	
6	2023-03-22 23:36:00	Brute-force attack on SMB(...	Brute-Force Atta...	Propagation	10.90.28.121	10.90.28.182	-	Attem...	-	-	Pending	

Copy | Bulk Operation | Mark | Export | Open Monitor

No.	Last Detected	Threat	Threat Type	Attack Stage	URL	Threat Intelligence	Sensor Device	Platform	Status	Operati...
1	2023-03-23 19:38:00	Brute-force attack on SMB(End...	Brute-Force Attac...	Propagation	-	-	Sangfor Endpoint Secure(10.22...	Current Pla...	Pending	
2	2023-03-23 12:30:00	Brute-force attack on SMB(End...	Brute-Force Attac...	Propagation	-	-	Sangfor Endpoint Secure(10.22...	Current Pla...	Pending	
3	2023-03-23 09:48:43	Brute-force attack on SMB(E...	Brute-Force Atta...	Propagation	-	-	Sangfor Endpoint Secure(10....	Current Pl...	Pending	
4	2023-03-23 06:57:07	Brute-force attack on SMB(E...	Brute-Force Atta...	Propagation	-	-	Sangfor Endpoint Secure(10....	Current Pl...	Pending	
5	2023-03-23 04:56:00	Brute-force attack on SMB(E...	Brute-Force Atta...	Propagation	-	-	Sangfor Endpoint Secure(10....	Current Pl...	Pending	
6	2023-03-22 23:36:00	Brute-force attack on SMB(E...	Brute-Force Atta...	Propagation	-	-	Sangfor Endpoint Secure(10....	Current Pl...	Pending	

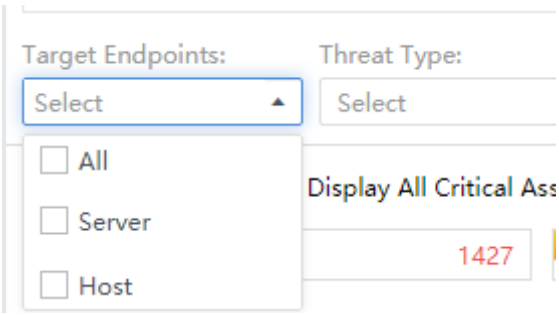
Fields:

<Threat Type: >Represents the threat subcategory of the alert.

<Severity:> Includes High, Medium, and Low.

<Target Group: >Represents the asset group to which the target belongs.

<Asset of attacker: >Includes Internet assets and LAN assets, as shown in the figure below.



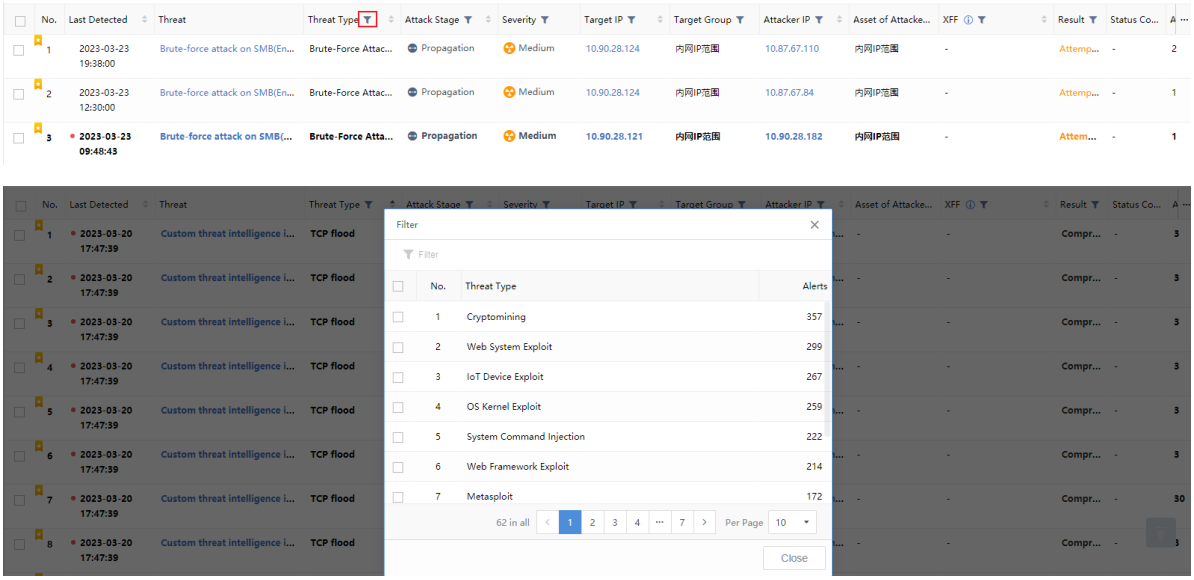
<Proxy Server IP: >Records the proxy information about Cdn-Src-Ip, X-Forwarded-For, X-Real-IP, and Clienttip.

<URL: >Represents the URL involved in the alert details.

<Data Source: >Nova Command or a lower-level platform.

<Operation: >Includes manual operations and coordinated response.

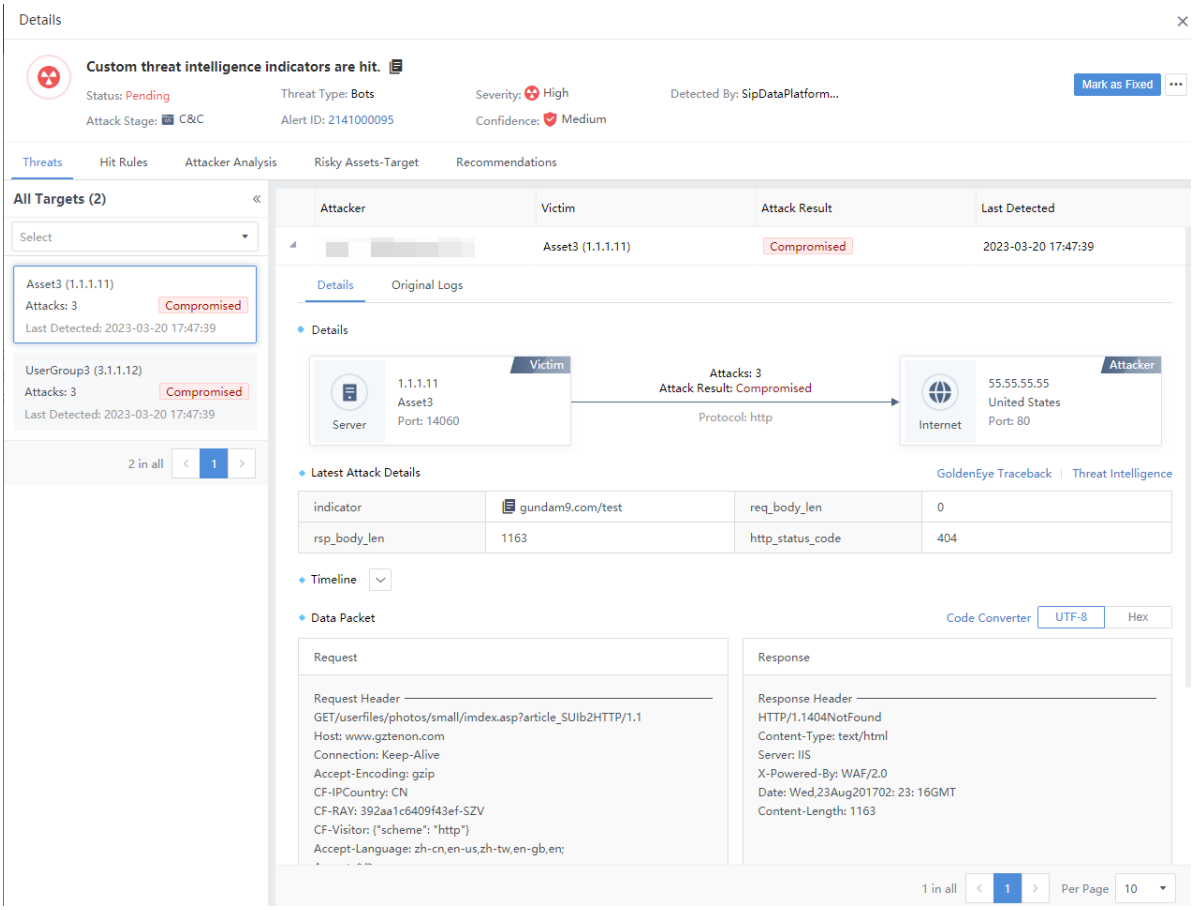
You can click the < > icon of some fields to further filter alerts, including threat, attack stage, severity, target IP, target group, attacker IP, asset of attacker, result, status code, device, and status, as shown in the following figure.



Alert Details

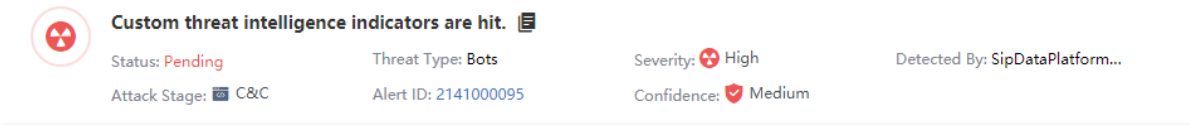
By correlation

You can select a security alert to go to the Details page, where you can see the basic alert information, threat information, hit rules, attacker analysis, risky assets (target), and recommendations, as shown in the figure below.

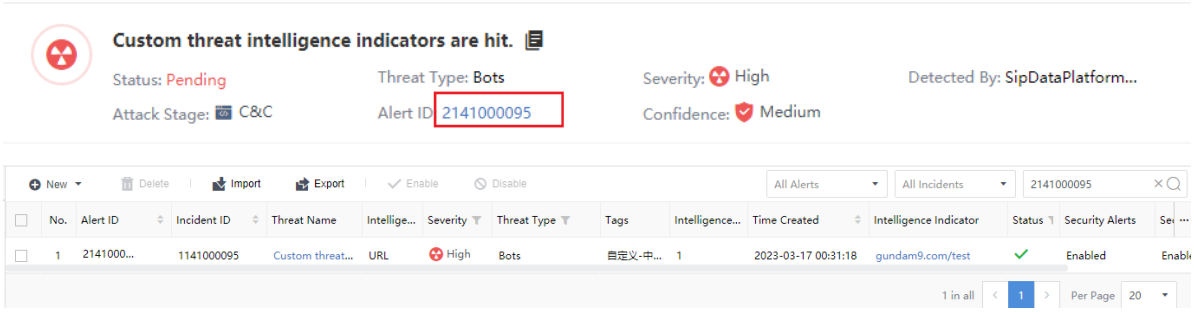


Basic information

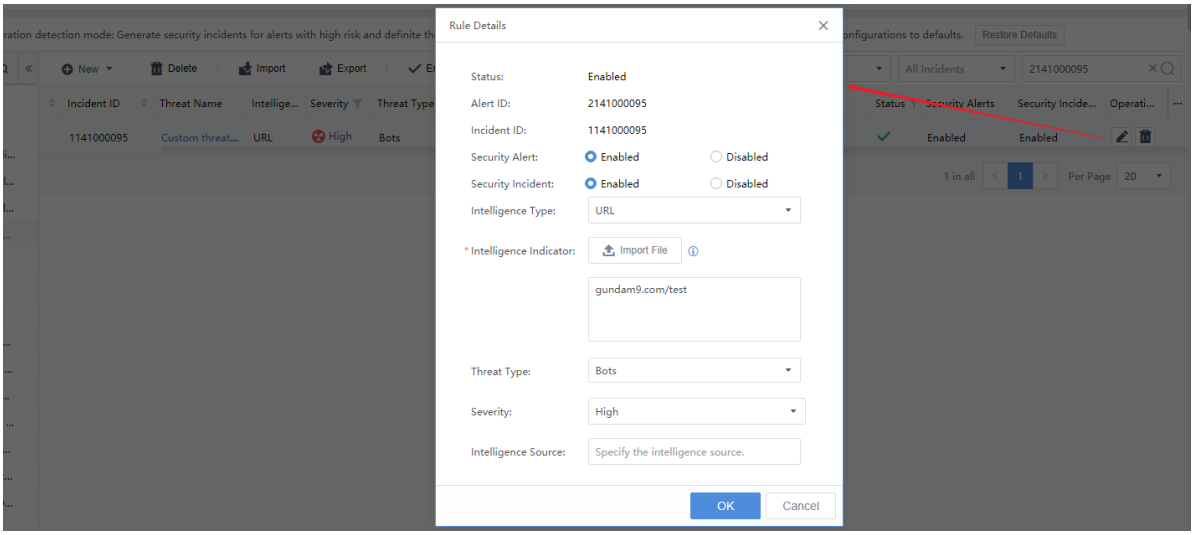
You can view the status, threat type, severity, data source, attack stage, and alert ID of the alert, as shown in the following figure.



You can click the alert ID to go to the [System/Security Capabilities/Detection Engines] page, where you can view the details, as shown in the figure below.

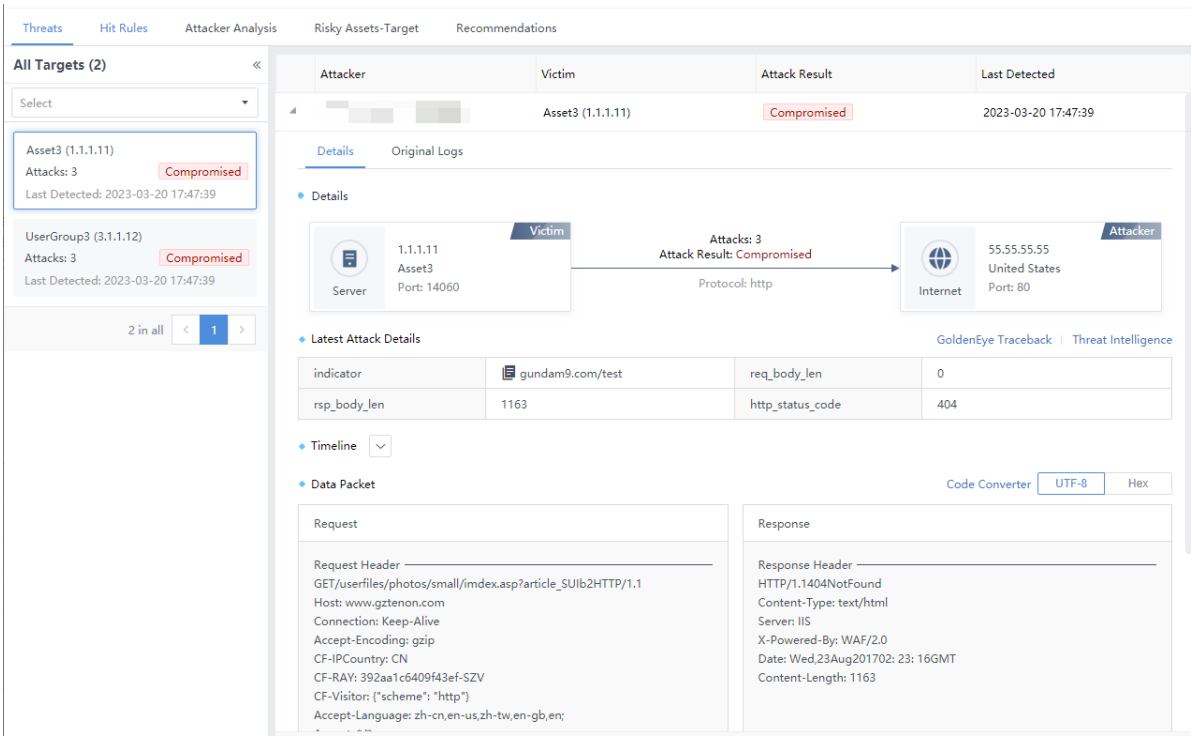


On the Detection Engines page, you can also click >to edit the alert information, including enabling or disabling security alert or security incident, changing the severity, and specifying the background, impacts, and recommendations, as shown in the following figure.

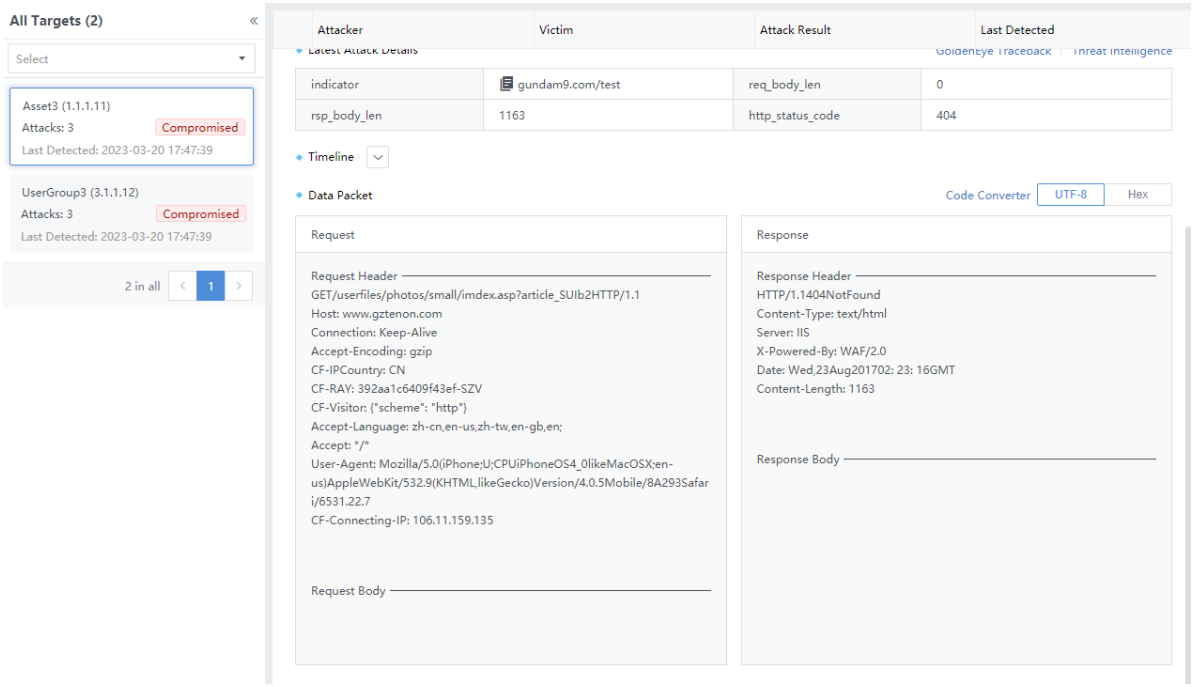


Threats

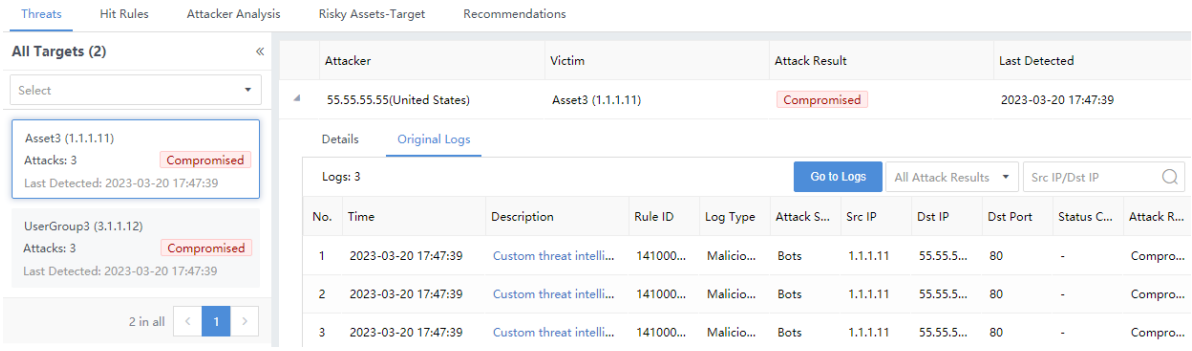
On the [Threats] tab, attack targets, alert quantity, alert details, and original logs are displayed, as shown in the figure below.



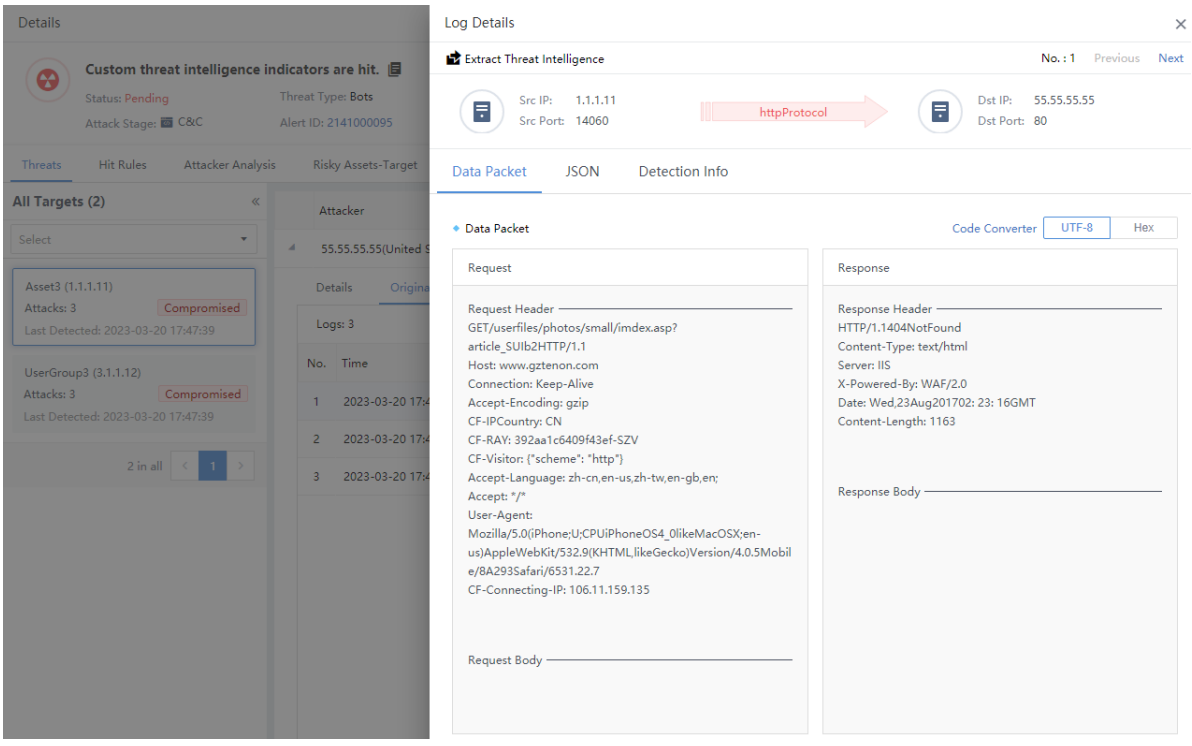
You can scroll up and down in the [Details] section to view the data packet information, as shown in the figure below.



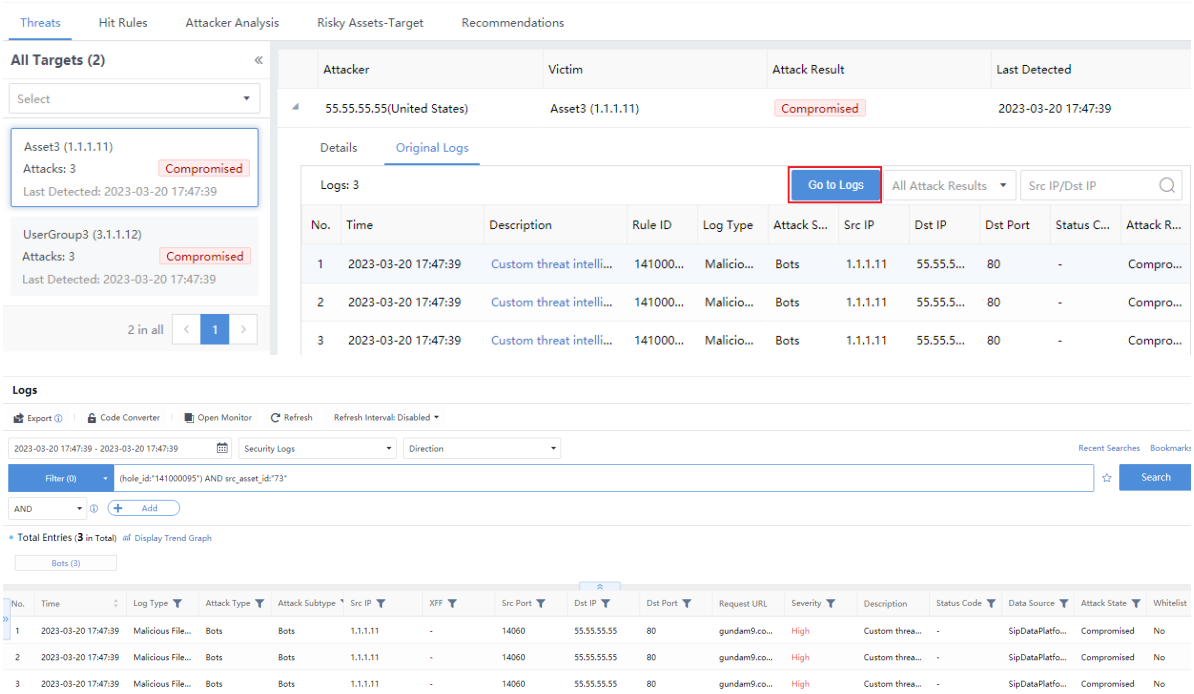
You can click the <Original Logs> tab to view the logs related to the alert, as shown in the figure below.



You can click the content in the "Description" column to view the original log information for higher judging efficiency, as shown in the figure below.

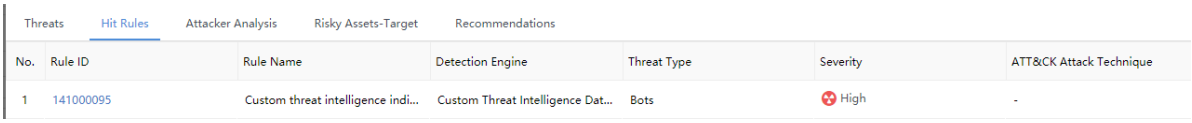


You can click <Go to Logs> to redirect to the <Logs> page and filter the logs related to this alert, as shown in the figure below.

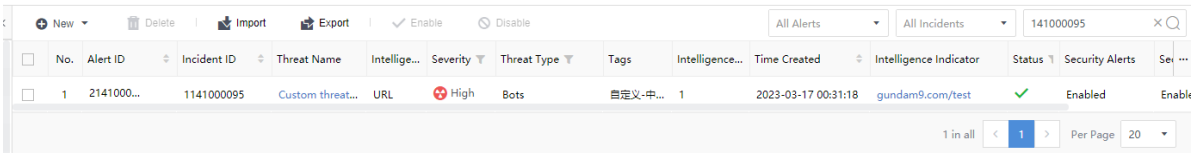


Hit rules

You can view the rule ID list related to the alert, containing information such as rule ID, rule name, detection engine, threat type, severity, and ATT&CK attack technique, as shown in the figure below.

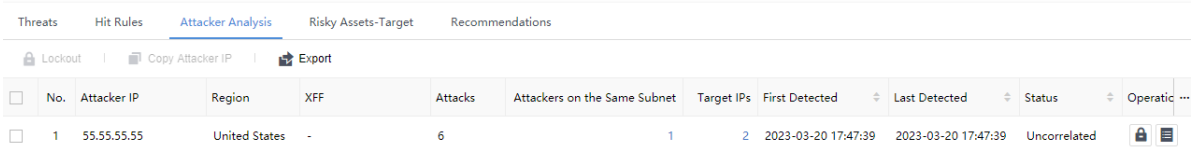


You can click a rule ID to go to [System/Security Capabilities/Detection Engines]. On the page that appears, you can view or edit the rule details, as shown in the figure below.

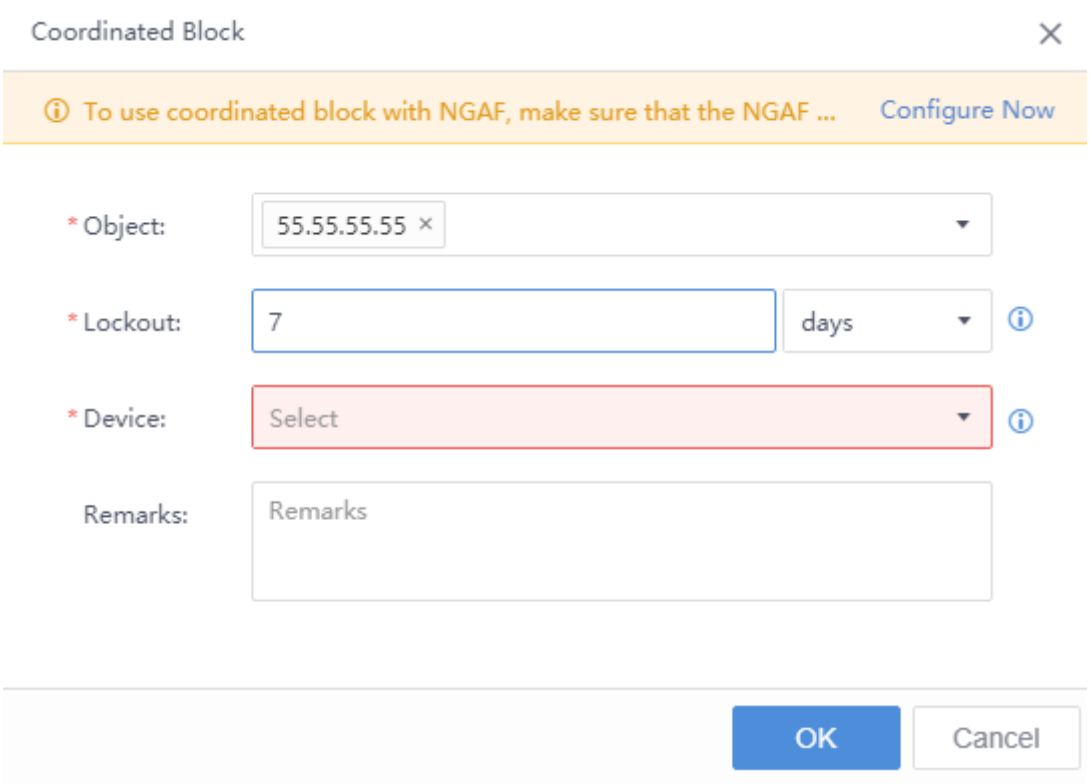


Attacker analysis

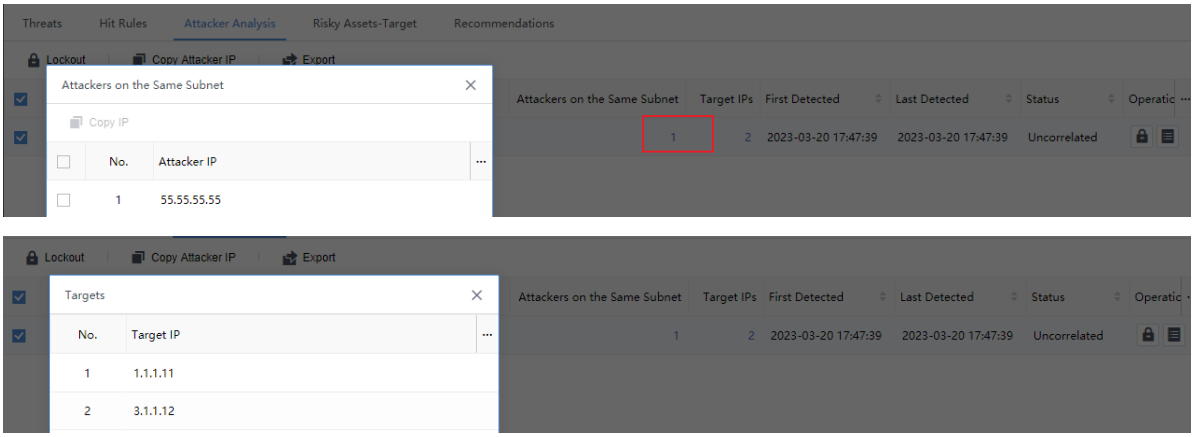
You can view the attacker IP address, region, attack count, attackers on the same subnet, target IP addresses, first attack time, last attack time, lockout status, and intelligence, as shown in the figure below.



You can click the <  > icon in the [Operation] column to select the configured Next Generation Application Firewall (NGAF) for performing correlated block, as shown in the figure below.



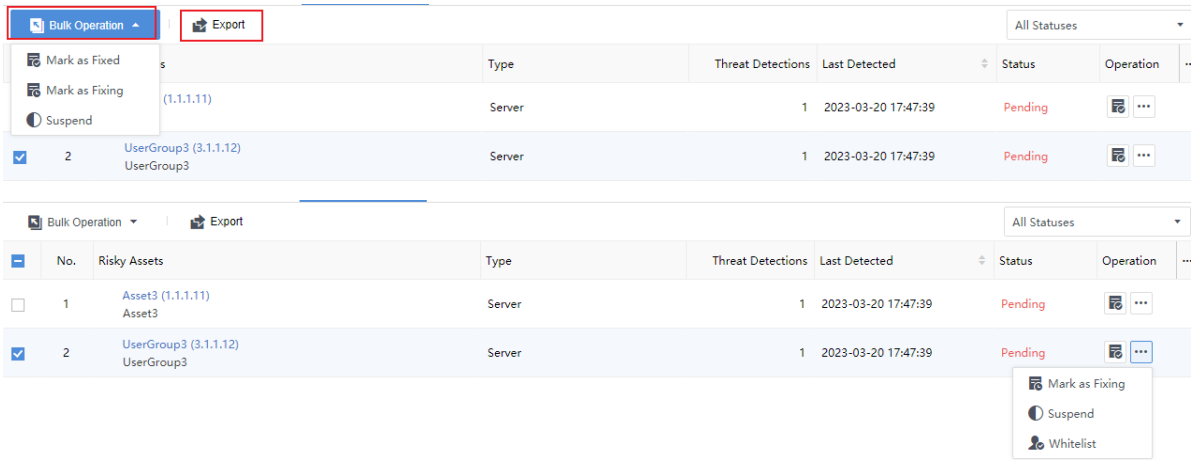
You can click the value in the "Attackers on the Same Subnet" or "Target IPs" column to view the attacker IP addresses or target IP addresses, as shown in the figure below.



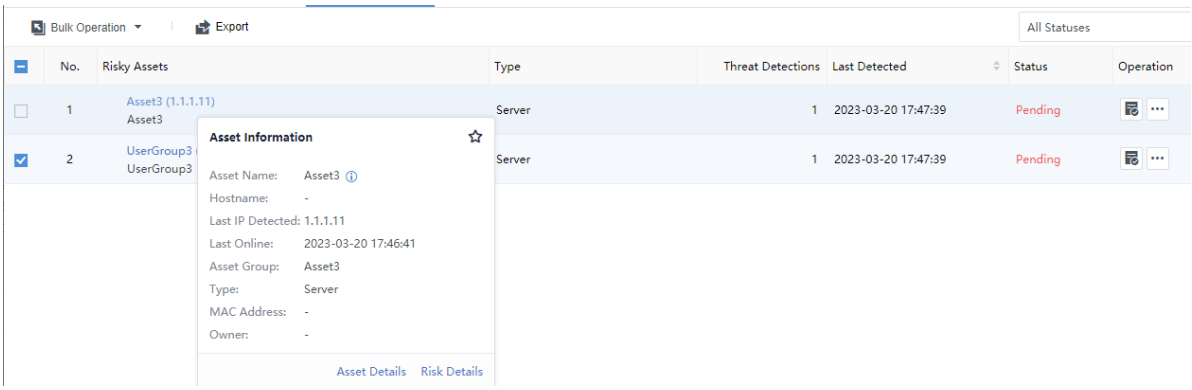
If multiple attacker IPs are associated with the alert, you can click <Export> to export the attacker IP list in the XLSX format.

Risky assets - target

You can view the information about risky assets associated with the security alert and perform operations such as export, bulk operation, and manual operation, as shown in the figure below.

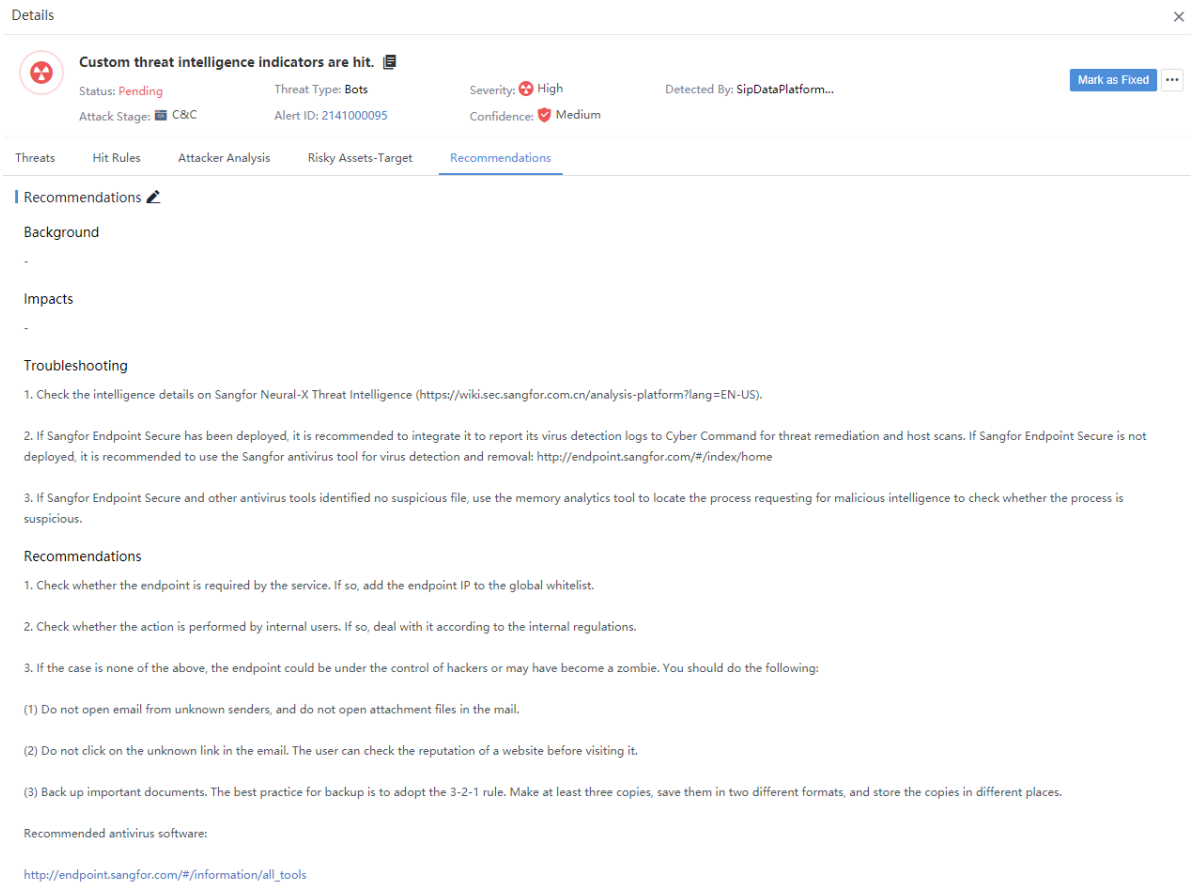


You can hover over a risky asset to view the asset details or risk details, as shown in the figure below.



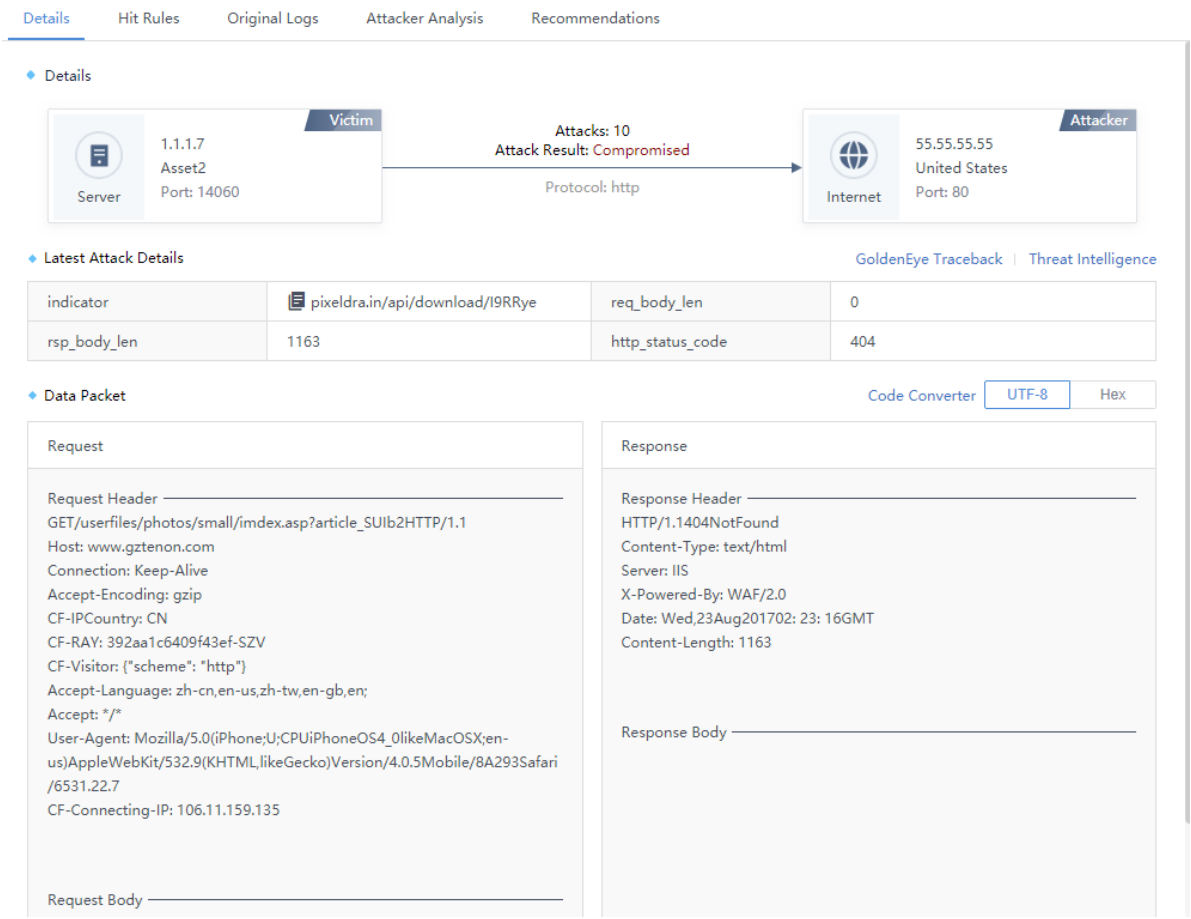
Recommendations

Troubleshooting and fixing suggestions are provided based on the alert background and impact, as shown in the figure below.



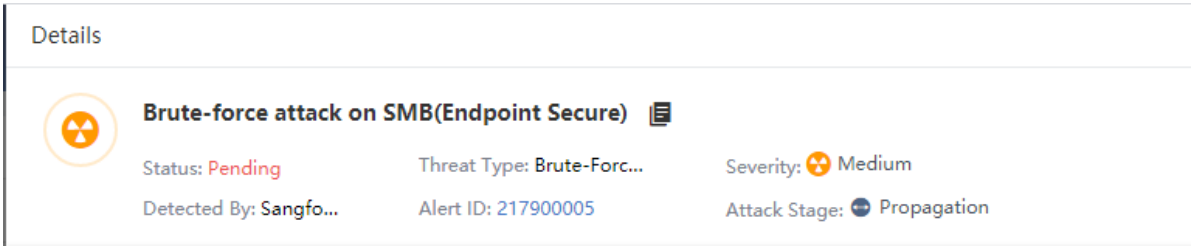
By details

After you click a threat in the list, the Details page appears, which displays basic alert information, alert details, hit rules, original logs, attacker analysis, and recommendations, as shown in the figure below.



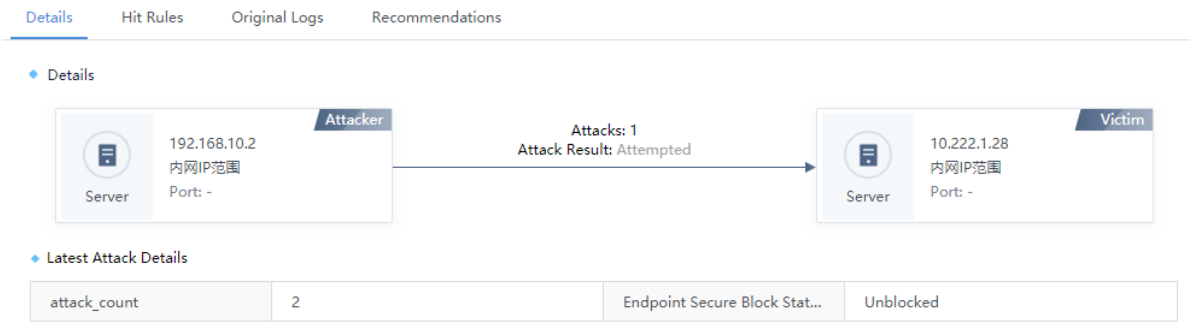
Basic information

You can view the status, threat type, severity, data source, attack stage, and alert ID of the alert, as shown in the following figure. You can click the ID to view details on the System/Security Capabilities/Detection Engines page.



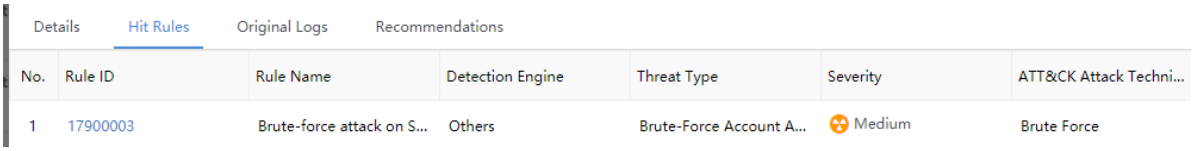
Details

You can view the attack direction, source IP, destination IP, and protocol on the <Details> tab. The latest alert details and data packet information are also displayed, as shown in the figure below.

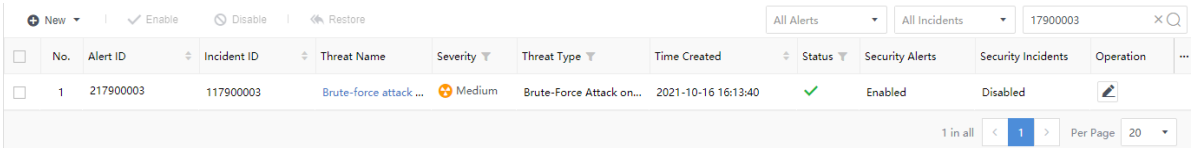


Hit rules

You can view the rule ID list related to the incident, containing information about the rule ID, rule name, detection engine, threat type, severity, and ATT&CK attack technique, as shown in the figure below.

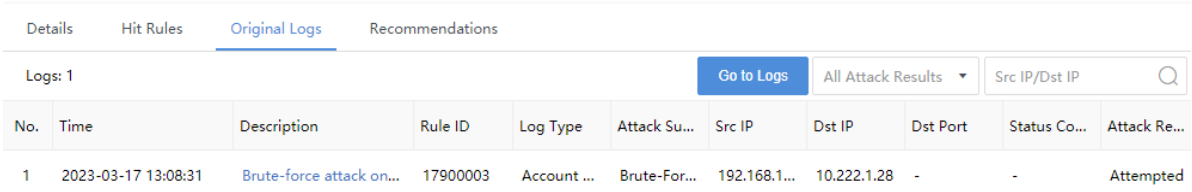


You can click a rule ID to go to [System/Security Capabilities/Detection Engines]. On the page that appears, you can view or edit the rule details, as shown in the figure below.

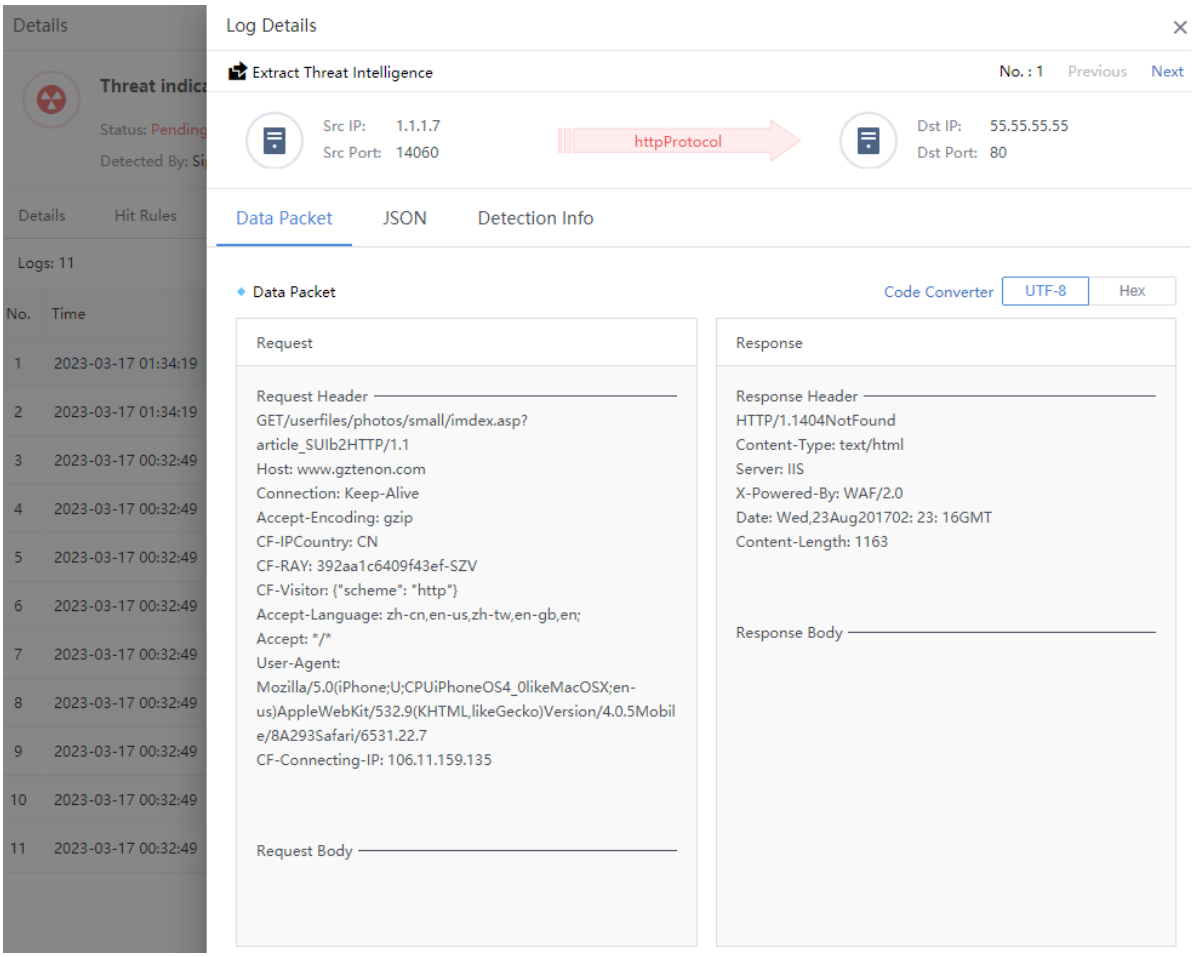


Original logs

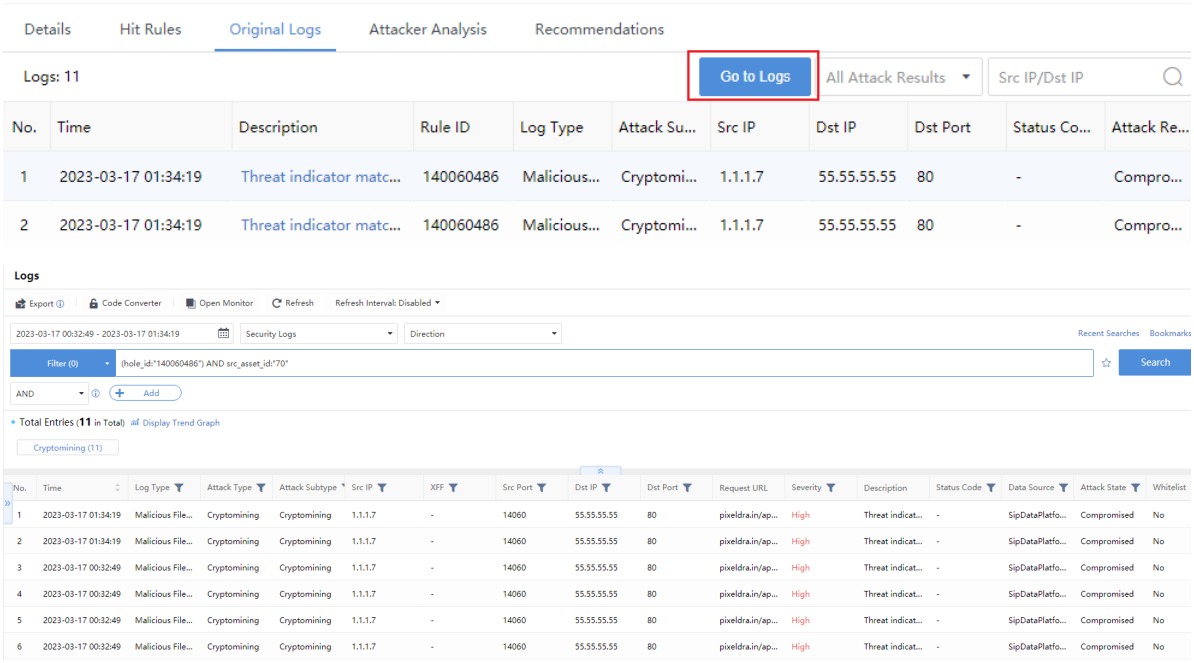
You can view the logs related to the alert, as shown in the figure below.



You can click the content in the "Description" column to view the original log information for higher judging efficiency, as shown in the figure below.

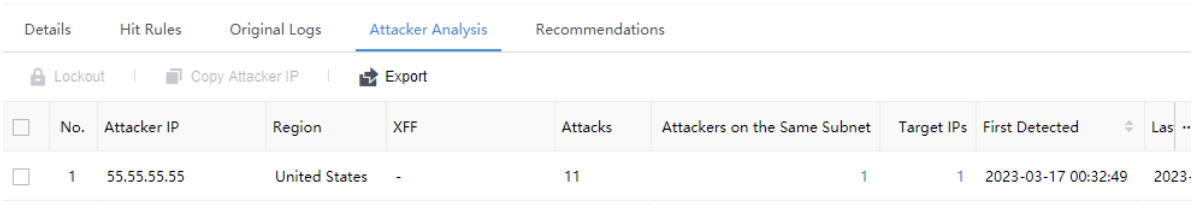


You can click <Go to Logs> to redirect to the <Logs> page and filter the logs related to this alert, as shown in the figure below.

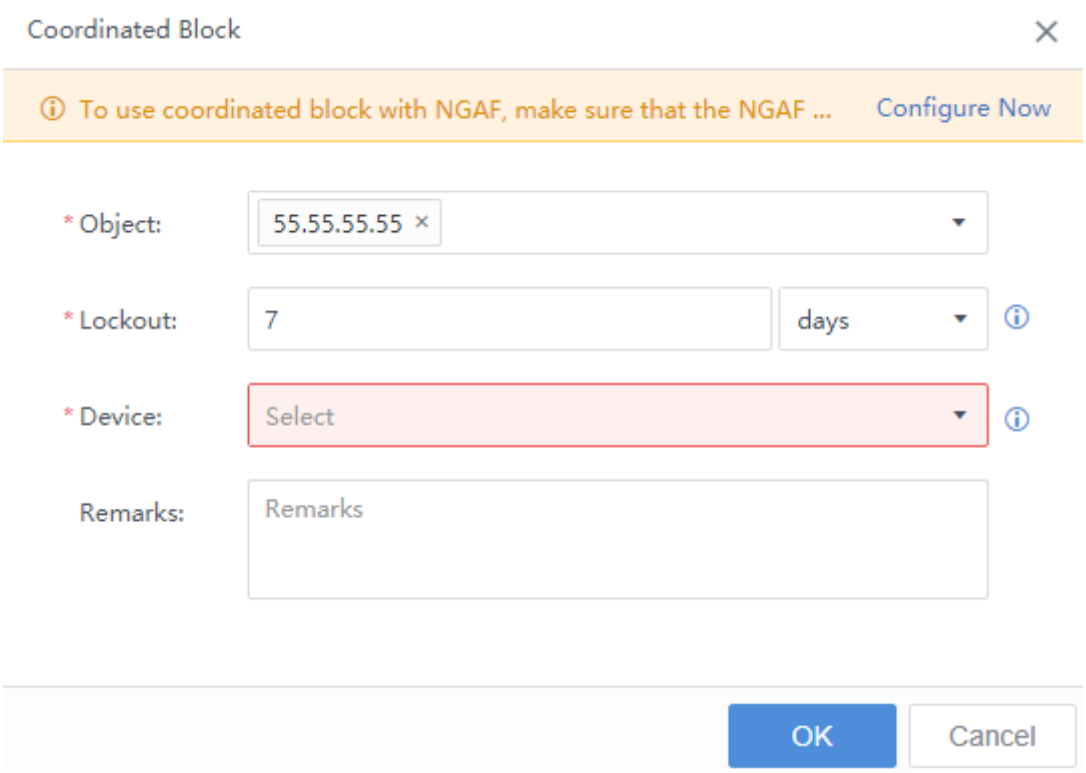


Attacker analysis

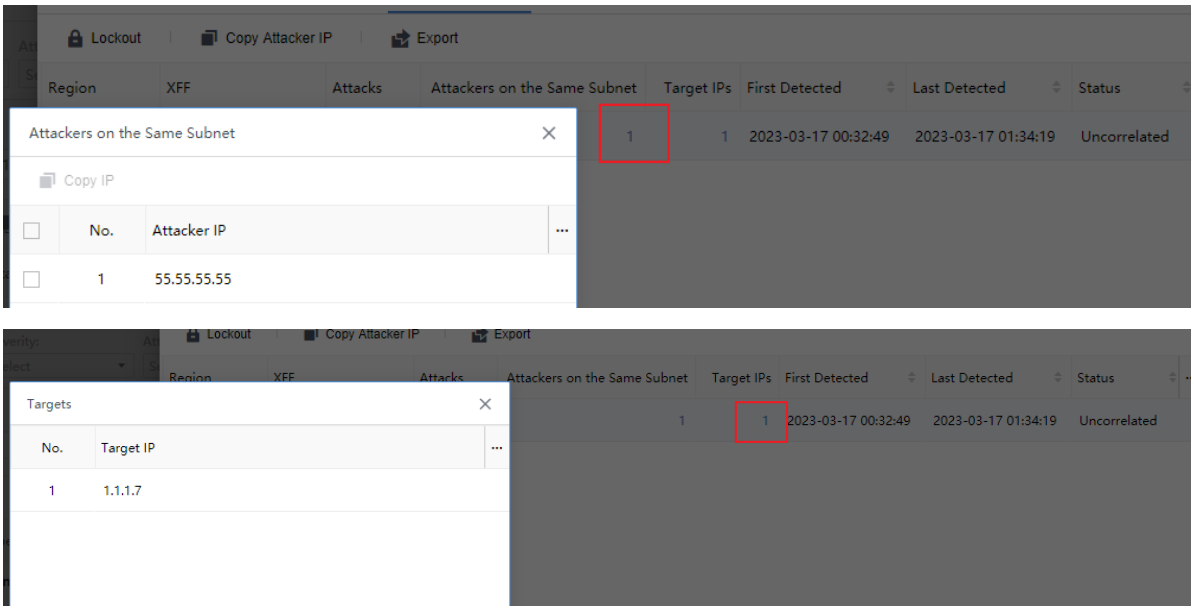
You can view the attacker IP address, region, attack count, attackers on the same subnet, target IP addresses, first attack time, last attack time, lockout status, and intelligence, as shown in the figure below.



You can click <Lockout> or the < > icon in the [Operation] column to select the configured Next Generation Application Firewall (NGAF) for performing correlated block, as shown in the figure below.



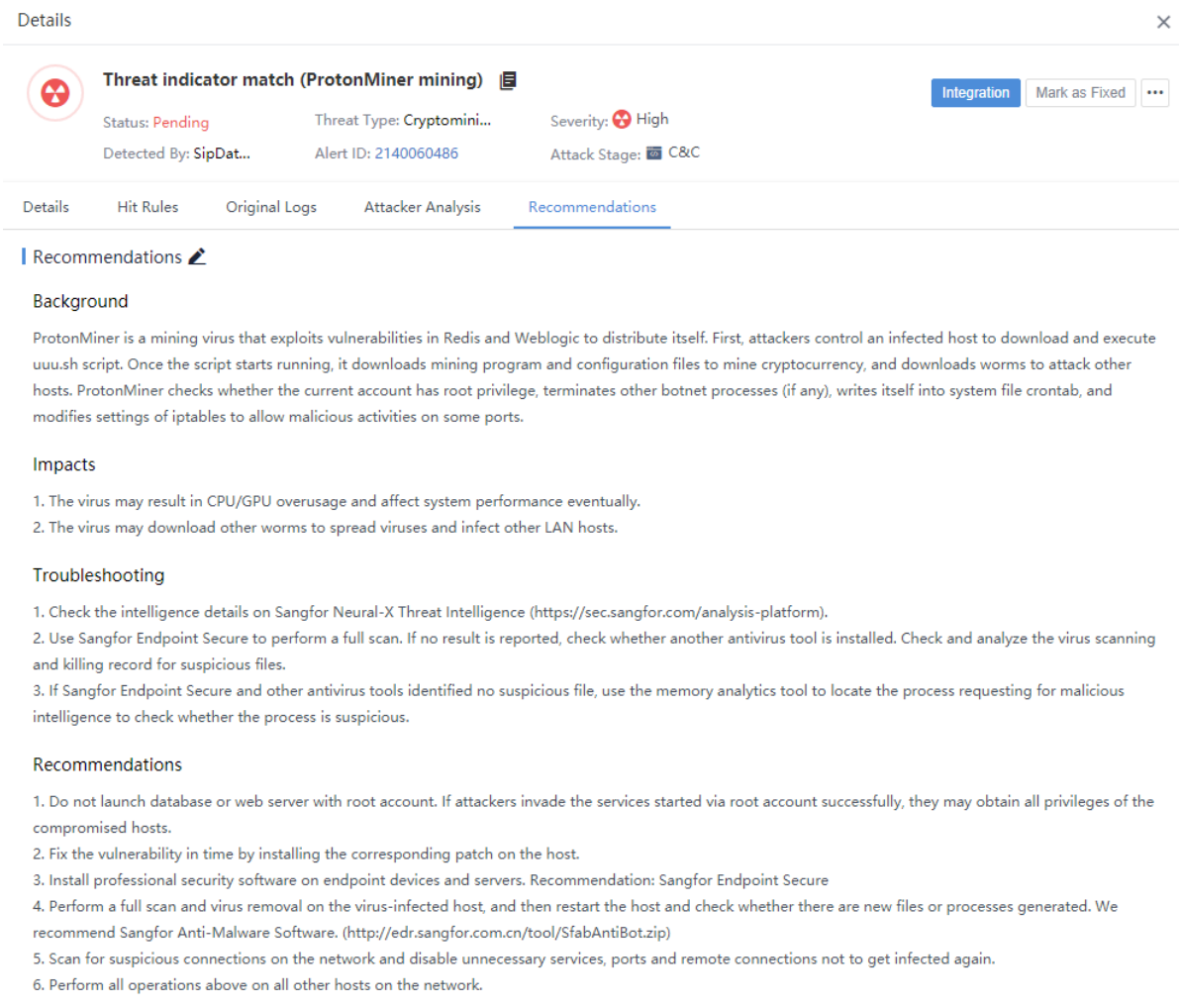
You can click the value in the "Attackers on the Same Subnet" or "Target IPs" column to view the attacker IP addresses or target IP addresses, as shown in the figure below.



If multiple attacker IPs are associated with the alert, you can click <Export> to export the attacker IP list in the XLSX format.

Recommendations

Troubleshooting and fixing suggestions are provided based on the alert background and impact, as shown in the figure below.



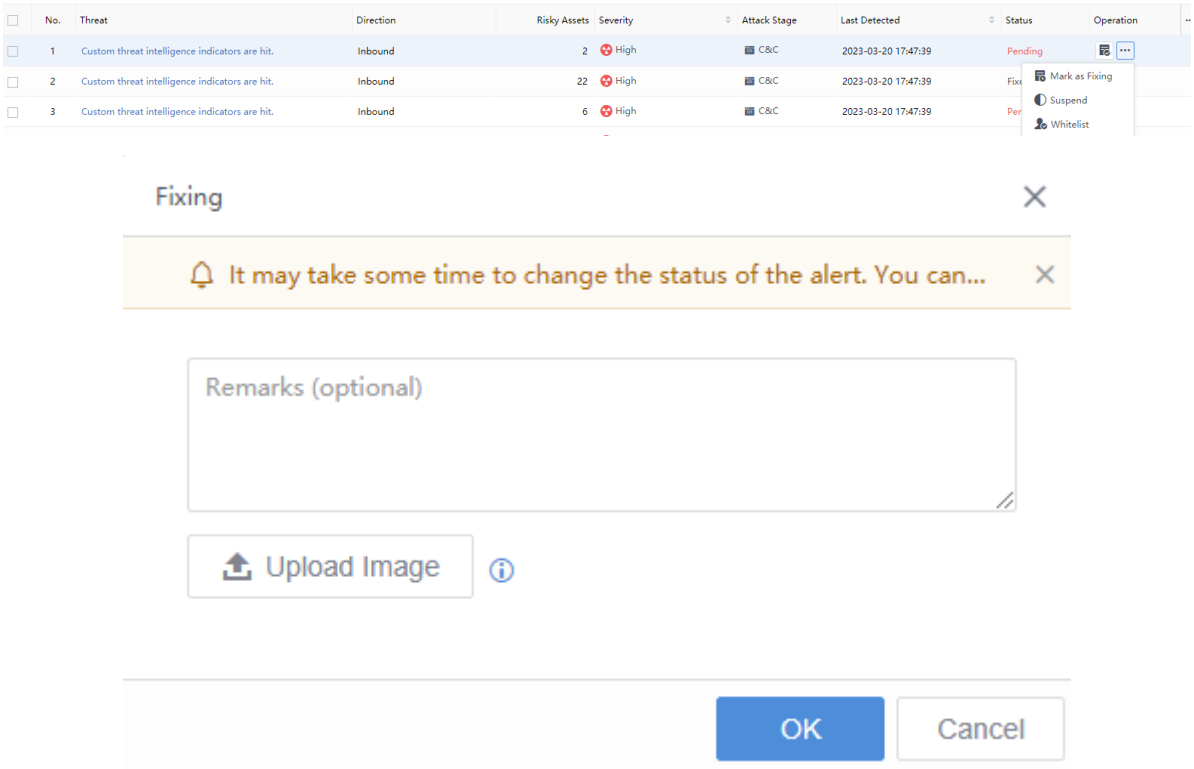
Alert Action

Only manual operation is supported when security alerts are displayed by correlation, while both manual operation and coordinated response are supported when security alerts are displayed by details.

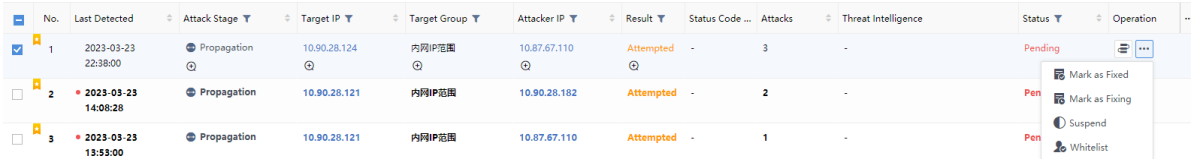
Manual operation

Method 1: Direct operation

When security alerts are displayed by correlation, you can choose a security alert and select an operation such as <Mark as Fixed>, <Mark as Fixing>, and <Suspend>. The page will be refreshed when the status changes, as shown in the figure below.

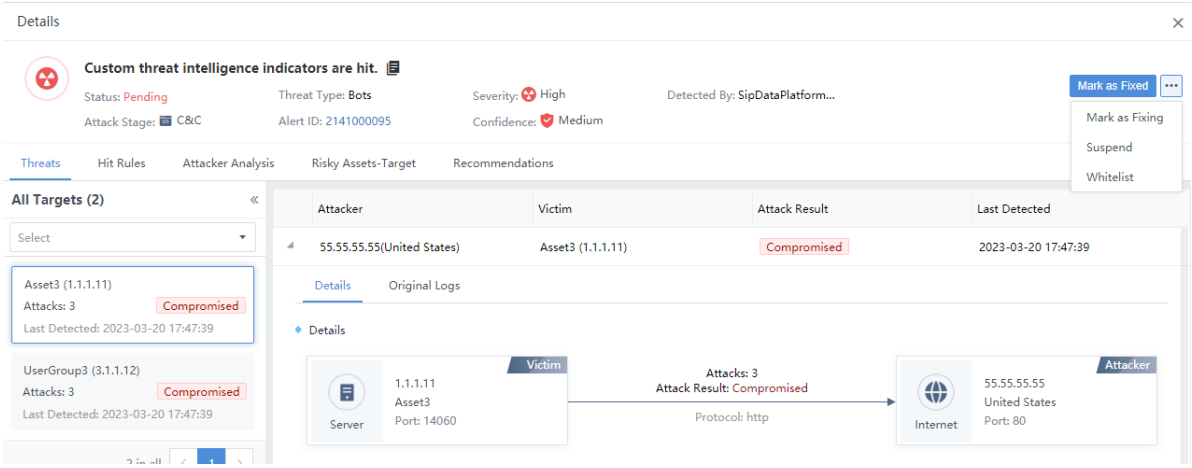


When security alerts are displayed by details, you can choose a security alert and select an operation such as <Mark as Fixed>, <Mark as Fixing>, <Suspend>, and <Whitelist>, as shown in the figure below.



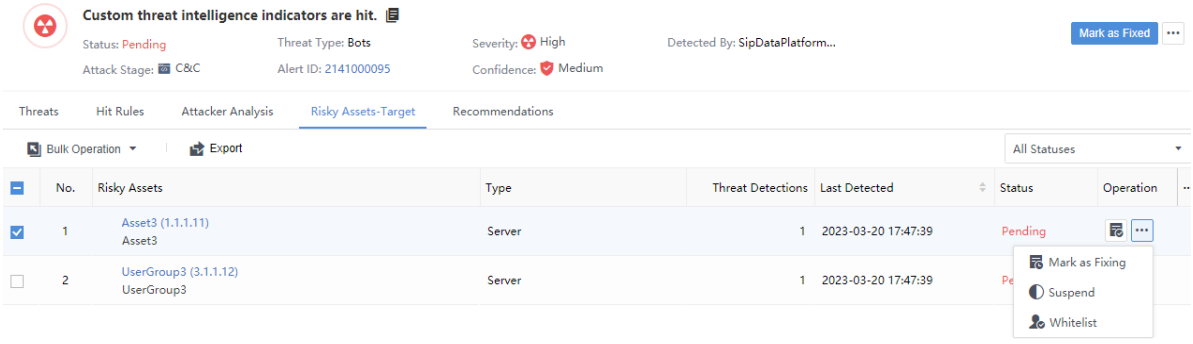
Method 2: Operation on the Details page

When security alerts are displayed by correlation, you can click a security alert to go to the details page, and then click the ··· icon in the top right corner to select an operation, as shown in the following figure.



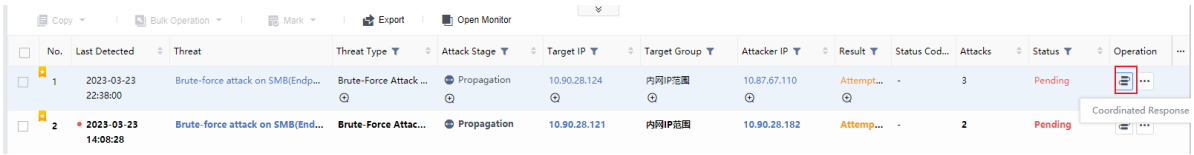
Method 3: Operation on the Risky Assets -Target tab

When security alerts are displayed by correlation, you can select an operation on the Risky Assets - Target tab of the Details page, as shown in the following figure.

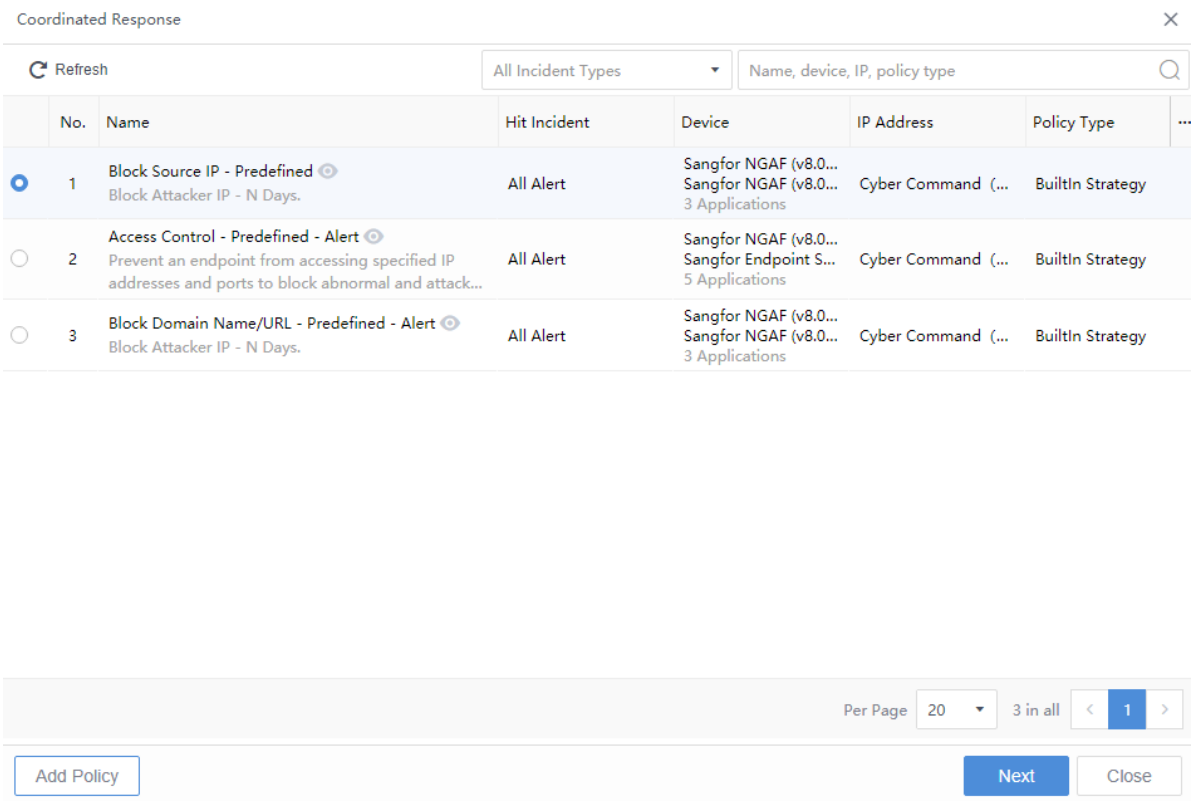


Coordinated response

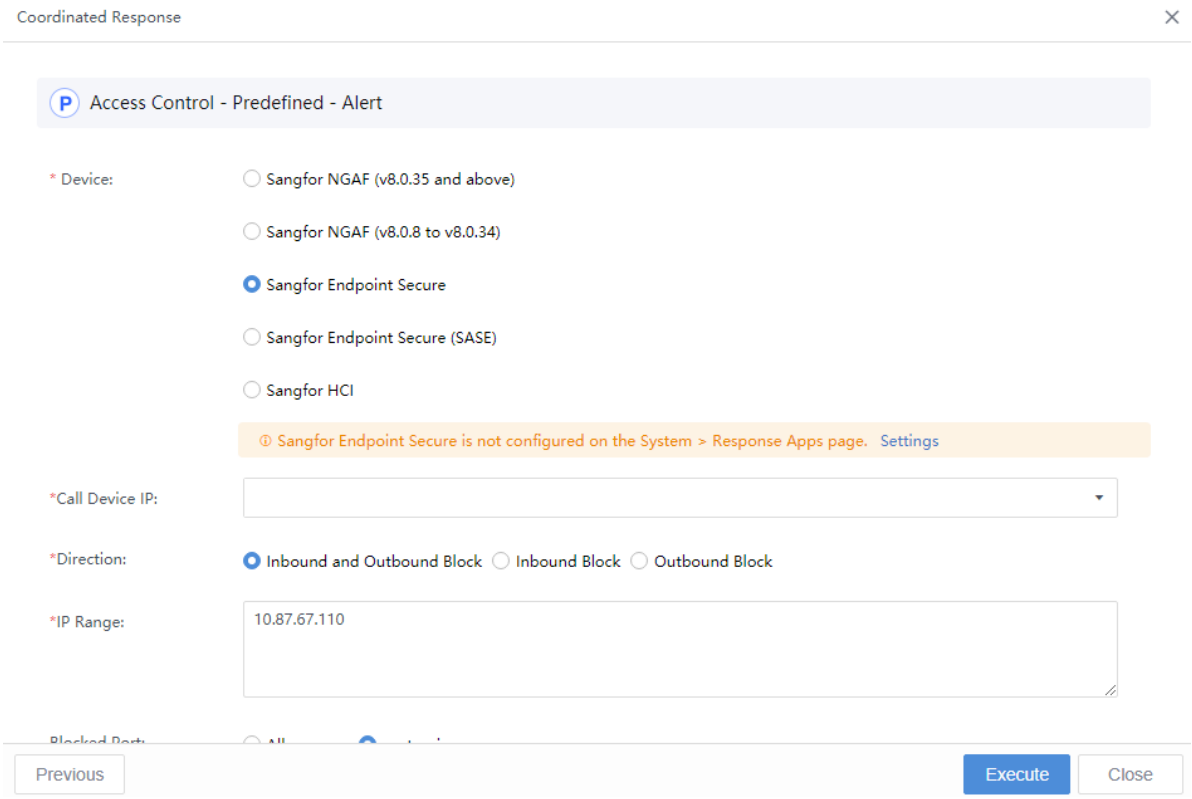
When security alerts are displayed by details, you can click the< > icon to pop up the Coordinated Response dialog box, as shown in the following figure.



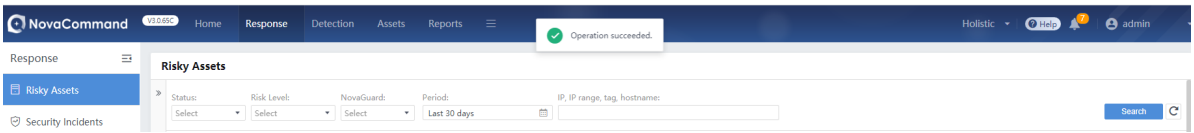
In the dialog box, you can view various policies by event type, including predefined policies, such as Threat Scan, Block Domain Name/URL, VM Suspend, Snapshot, VM Add, VM Shutdown, Block Endpoint, Account Lockout, Browsing Risk Notification, Endpoint Lockout, and Access Control. You can also clone or customize policies, as shown in the figure below.



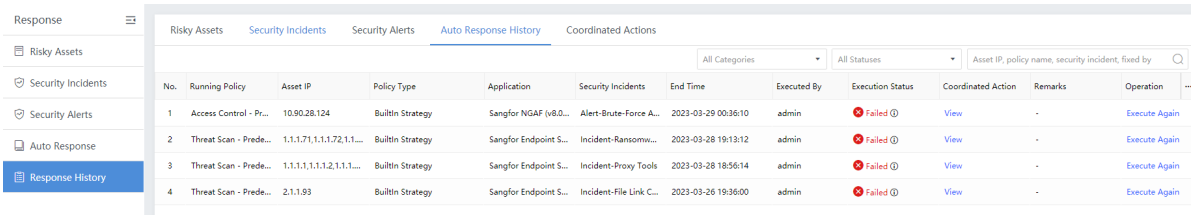
After clicking <Next>, you will go to the parameter settings page of coordinated response based on the policy you selected., You can set the device, call device IP, source IP, and block duration. The figure below takes the policy for blocking source IP as an example.



After you click <Execute>, the response action starts to be executed. The system prompts the message of <Executed> at the top of the page after the execution is completed.

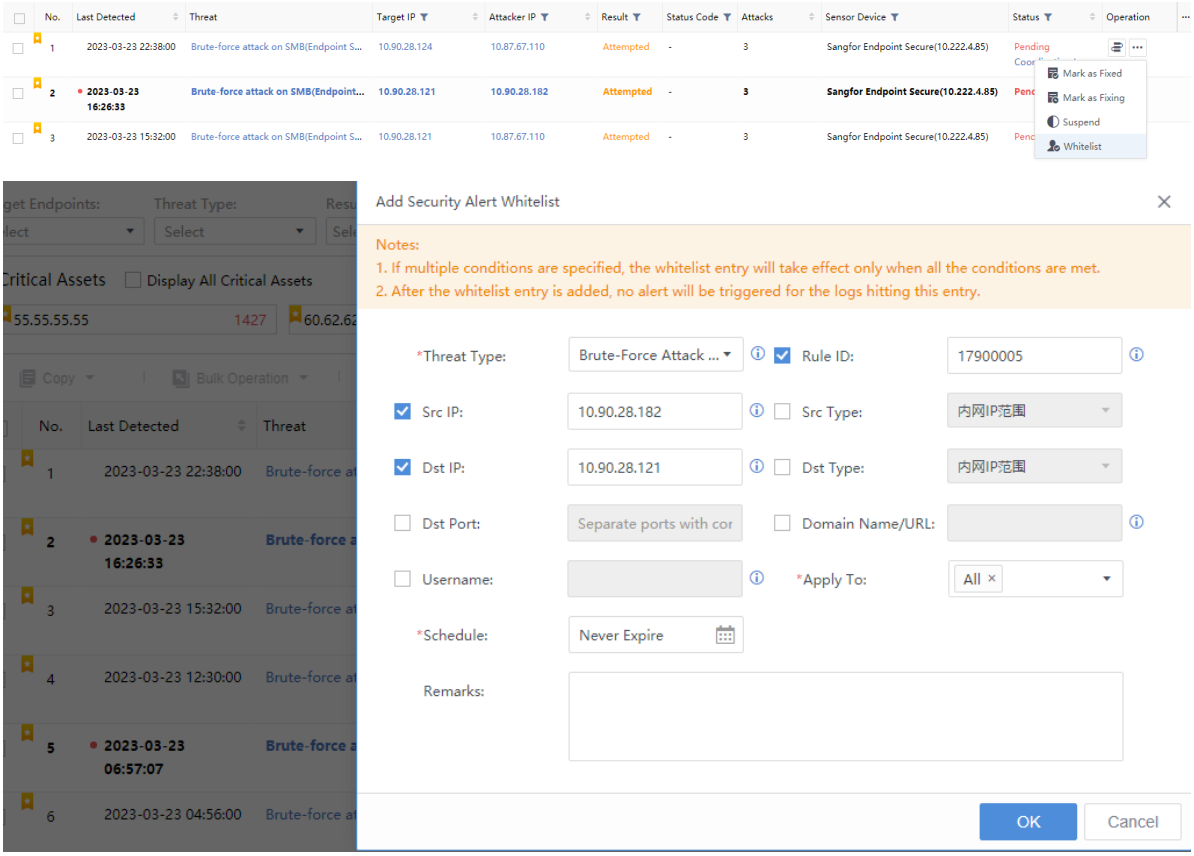


On the [Response/Response History/Auto Response History] page, you can view the response history, including the status, result, policy, and other related information, as shown in the figure below.



Whitelist

In addition to above operations, you can also whitelist security alerts. First, select an alert, and click the < ••• > icon. Then, select <Whitelist>. The [Add Security Alert Whitelist] window automatically appears. The source IP, destination IP, and rule ID are filled in by default. You need to specify and check other fields such as the applicable device and validity period.



Note:

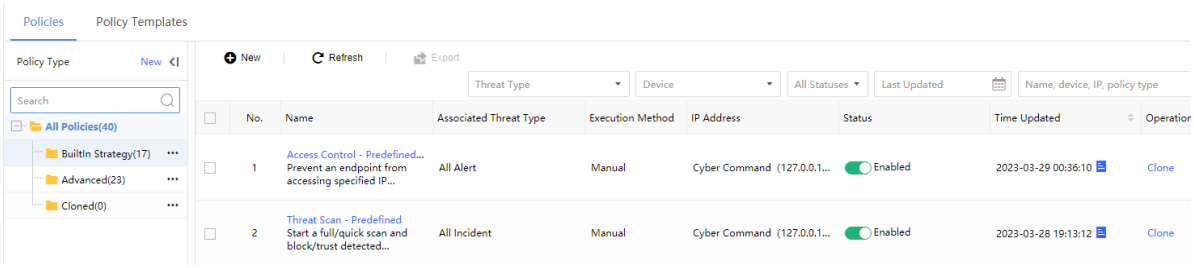
The whitelisting function is applicable to security alerts only.

Auto Response

This module aims to help you build standard response processes for security incidents through built-in or orchestrated custom response policies. By doing so, you can respond to threats and attacks in time and efficiently, build a security defense system, and reduce security operation cost. You can classify, manage, add, and edit policies in this module.

Policy Type

Policies are classified into three types by default: built-in, advanced, and cloned policies. You can also add policy types, as shown in the following figure.

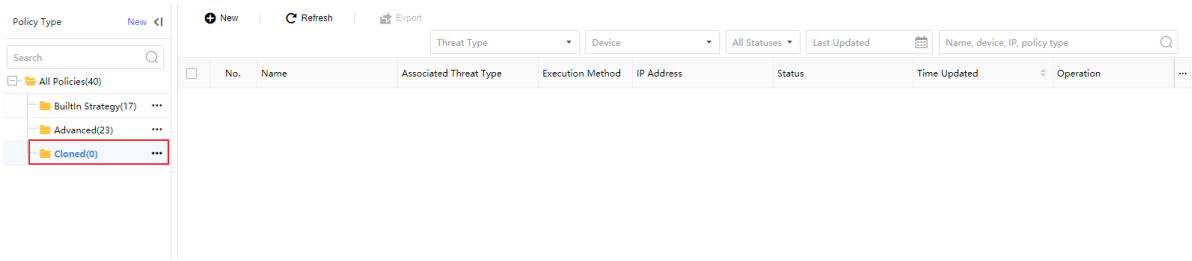


Types:

BuiltIn Strategy: Policies that are built in when Nova Command is released. They may change together with the update of Nova Command.

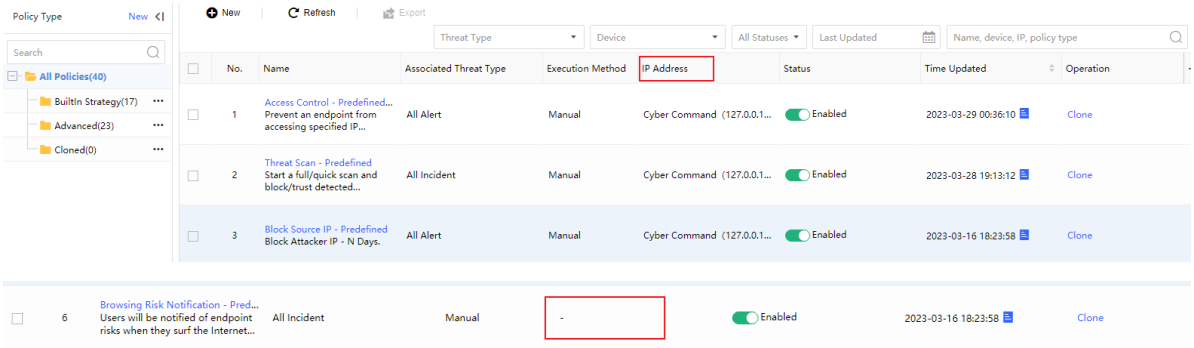
Advanced: Default auto response policies (excluding cloned policies) of the previous version of Nova Command. They are updated and translated to advanced policies when Nova Command is updated.

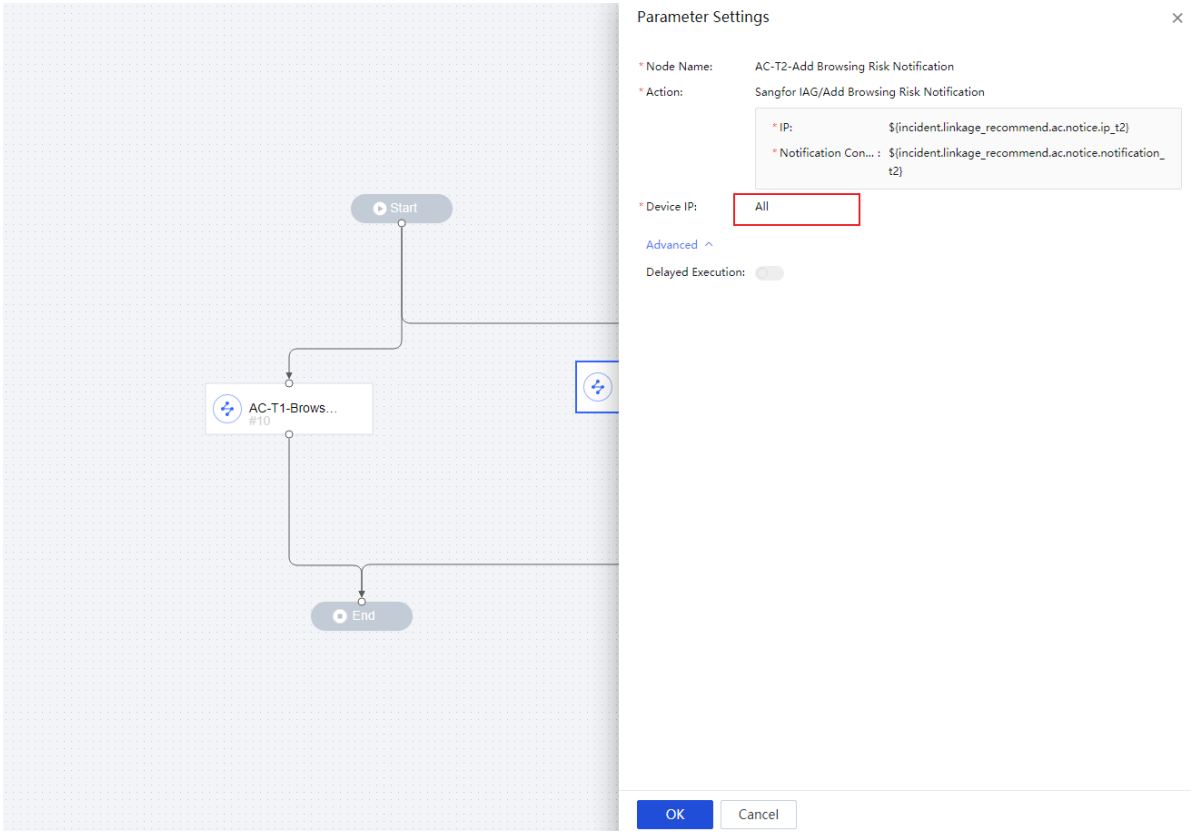
Cloned: Customized policies. You can add a policy type here by clicking <New> in the [Policies/Policy Type] area. You can also delete/edit this type, as shown in the following figure.



Note:

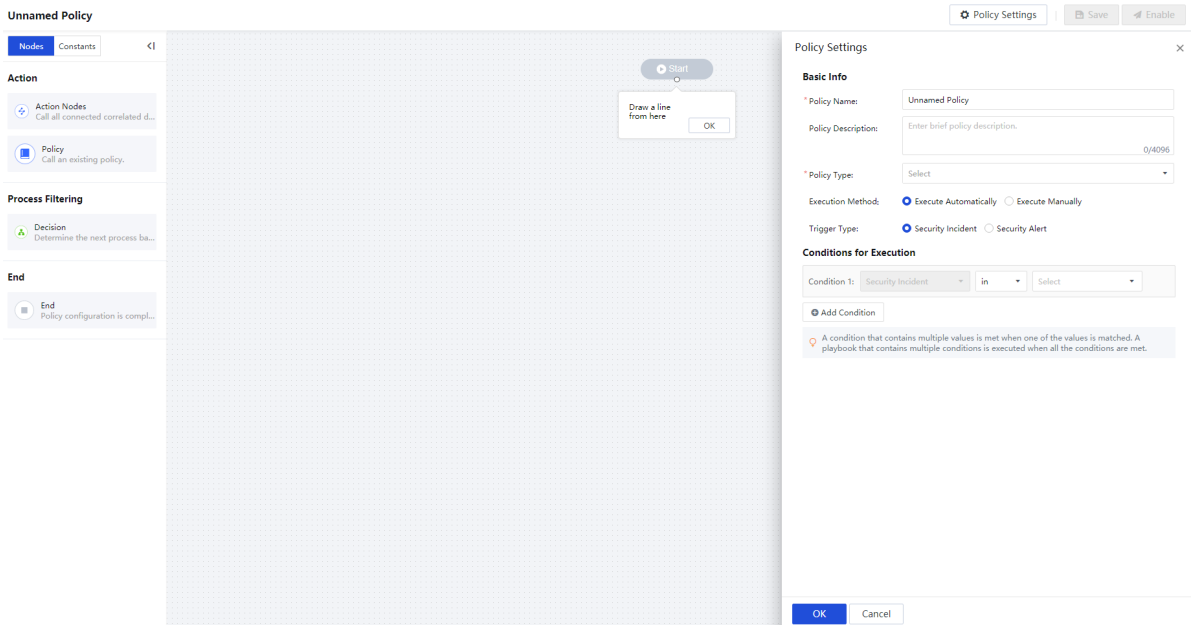
The IP addresses in the list are the instance request IP addresses of applications, which can be found in applications on the [System/Devices/Response Apps] page. However, the IP addresses on the Response Apps page may not be found in the "IP Address" column on the [Response/Auto Response] page. This is because All is selected for the Device IP field in "Action Nodes" of this policy, as shown in the following figure.





Policy Addition

On the [Response/Auto Response/Policies] page, you can click <New> to go to the policy orchestration canvas page, as shown in the following figure.



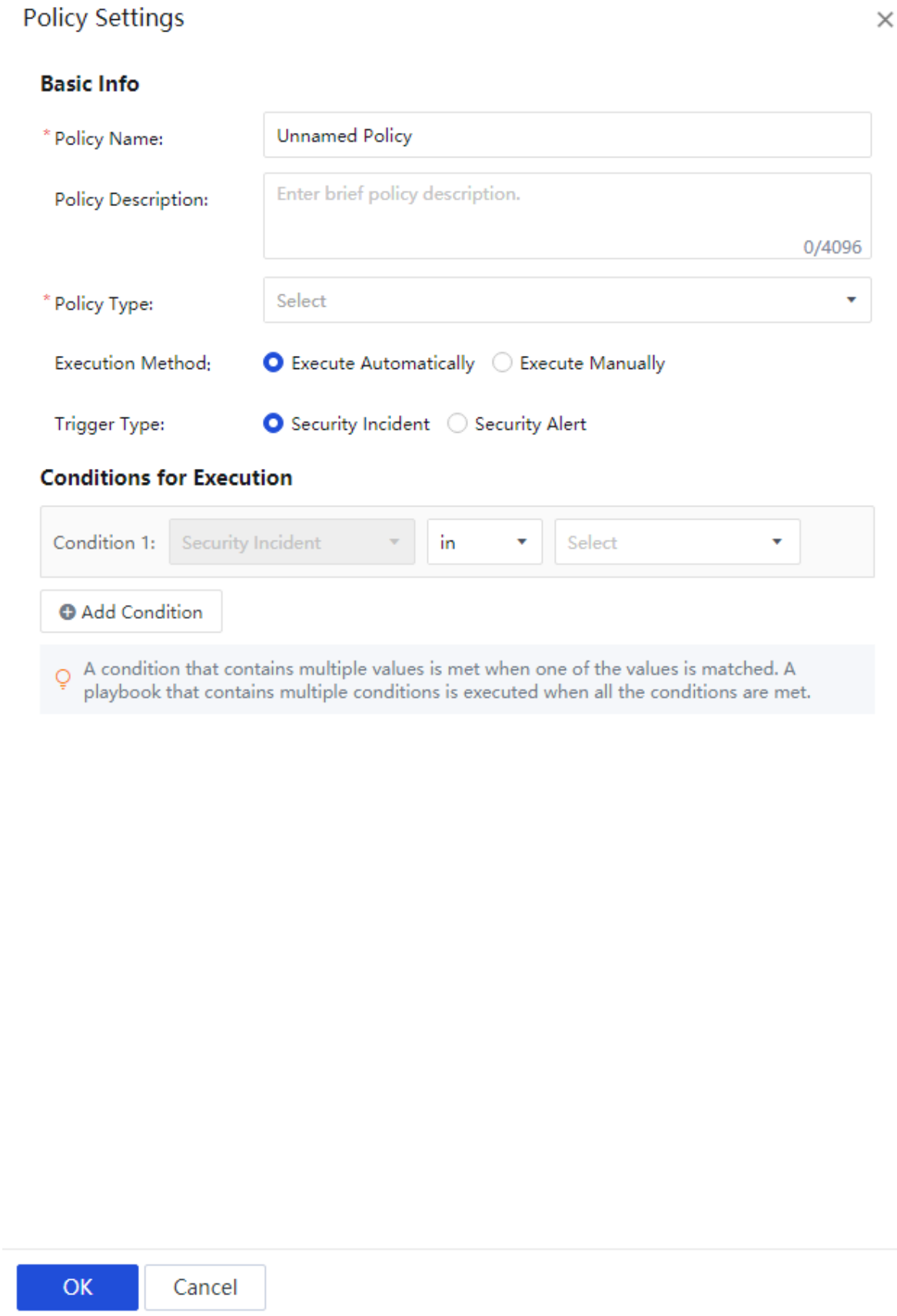
Nodes and constants are located in the left navigation pane, and their functions are described in the following table.

Table 1 Policy Elements

Type	Name	Function
Nodes	Action Nodes	The corresponding response action according to the type of the application.
Policy	The whole response process, including execution node, process filtering node, and end node. It is used to call an existing policy.	
Decision	Decisions are used for logical judgment between nodes. The "if-else" statement is commonly used for judgment.	
End	The end of the whole policy process.	
Constants		Parameters can be marked as constants. For example, you can add an IP address, IP range business group name, or organization name as a constant. With these constants, you can identify the corresponding parameters quickly and call them during policy orchestration. You can define all types of resources as constants except network IP resources.

Policy Settings

In the Policy Settings window, you can specify the policy name and policy description, select the policy type from the drop-down list, select the execution method check box, and specify the conditions for execution, as shown in the following figure.

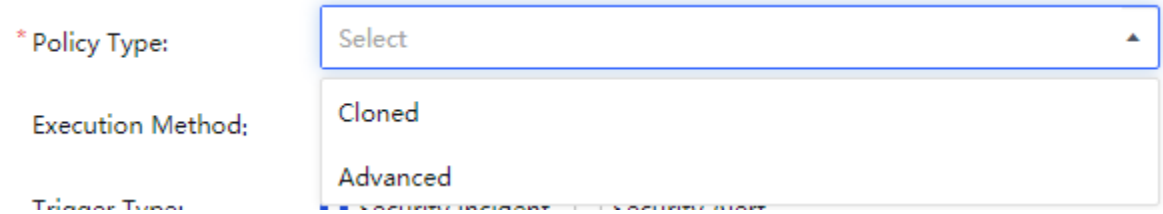


Fields:

Policy Name: Required. You can specify the name.

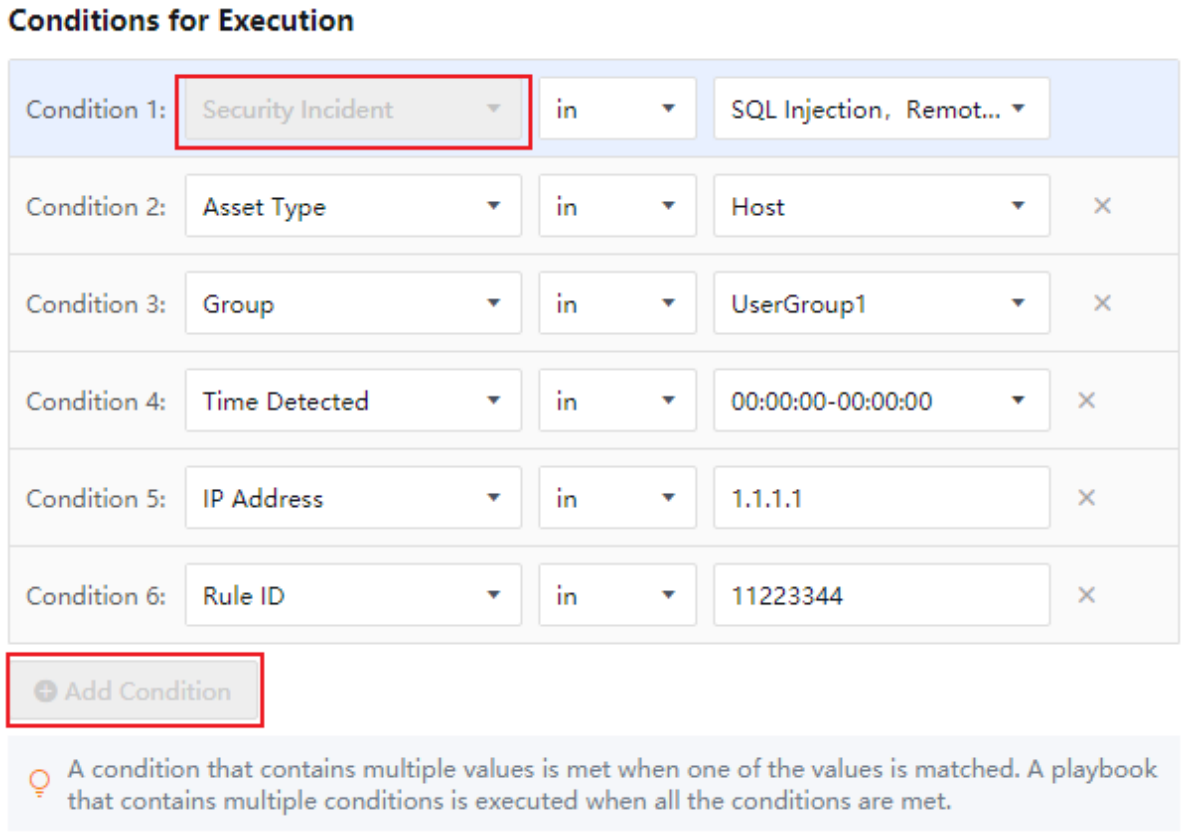
Policy Description; Optional. You can enter the description according to the actual condition.

Policy Type: Available types include Advanced and Cloned, as shown in the following figure.

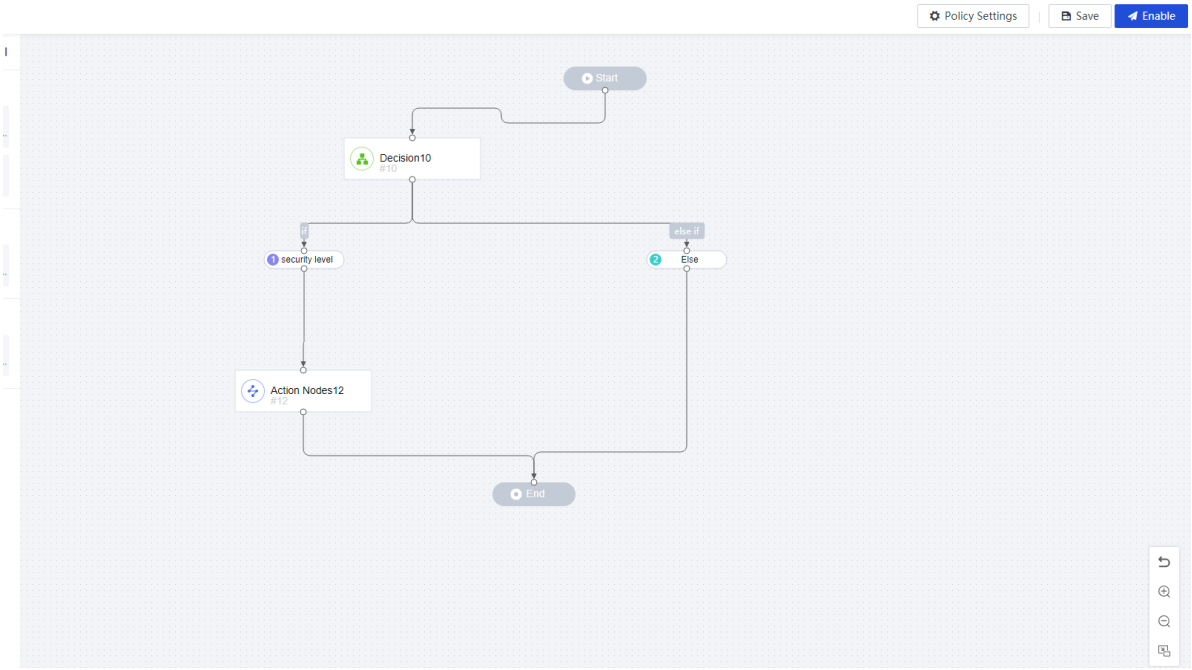


Execution Method: You can select [Execute Automatically] or [Execute Manually]. Polices that are set to be executed automatically will be matched when the corresponding security incidents/security alerts occur, and then coordinated response will be automatically executed. Policies that are set to be executed manually will not be executed automatically.

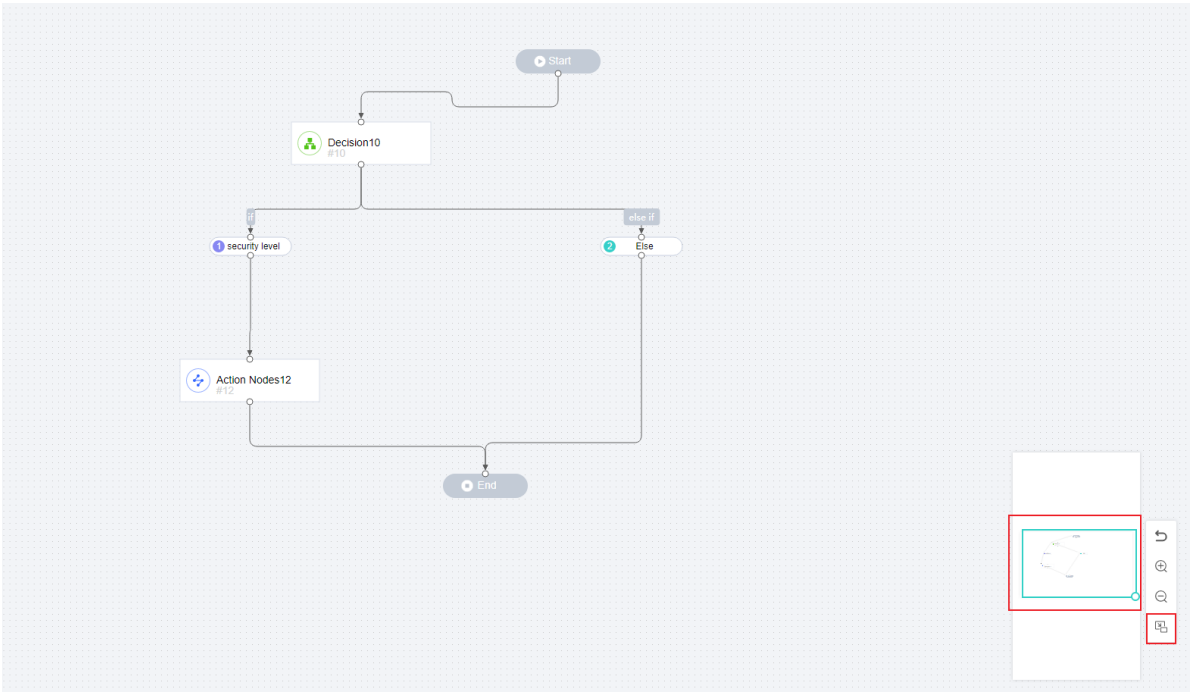
Conditions for Execution: You can determine the conditions for execution of a policy based on dimensions of asset type, asset group, detection time, IP address, rule ID, and security incident. Each dimension can contain one condition only. If one dimension contains multiple conditions, the conditions must be met at the same time. If one condition contains multiple values, the values do not need to be met at the same time. By default, a condition in the dimension of security incident must be set, as shown in the following figure.



As shown in the above figure, a security incident condition is required by default and cannot be changed to conditions in other dimensions. Each dimension applies to only one condition. When all dimensions are used by conditions, the \Add Condition> button will turn gray, which means that you cannot add more conditions. After completing policy settings, you can click <OK> to return to the canvas page. You can then click <Save> or <Enable>, as shown in the following figure.



As shown in the above figure, you can click < > on the canvas to undo the policy orchestration and go back to the previous step, click < > to zoom in the canvas, click < > to zoom out the canvas, and click < > to display the thumbnail. You can also click and drag to adjust the position of the policy on the canvas, as shown in the following figure.

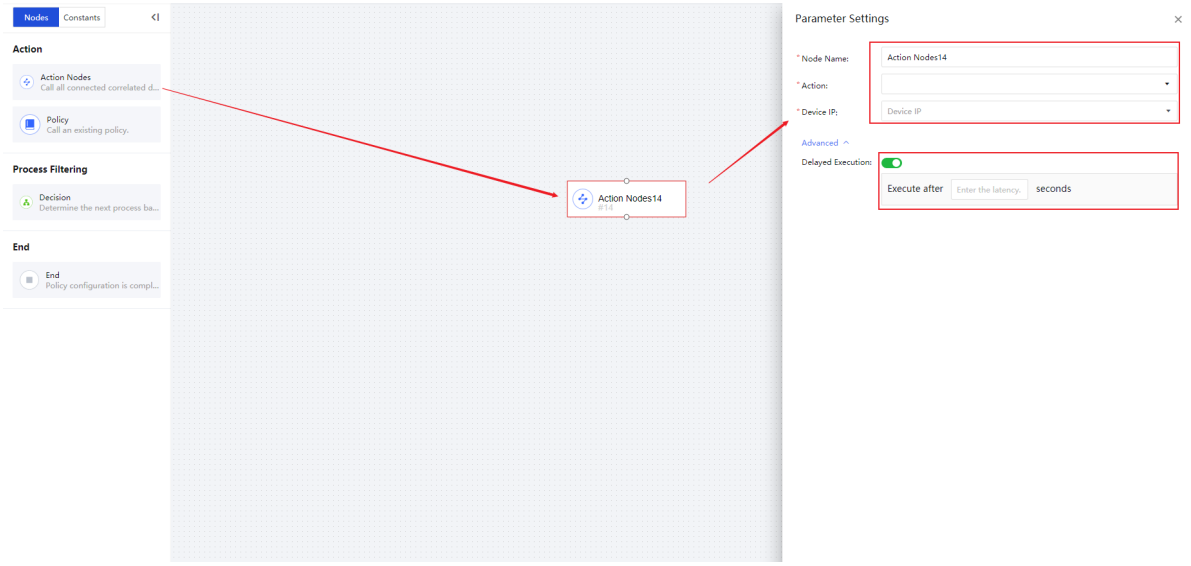


Node Addition

On the [Policies] page, you can choose a policy type and click <New> at the top of the list to go to the canvas page. Then, you can click and drag the action node icon in the left navigation pane and then drop it on the canvas.

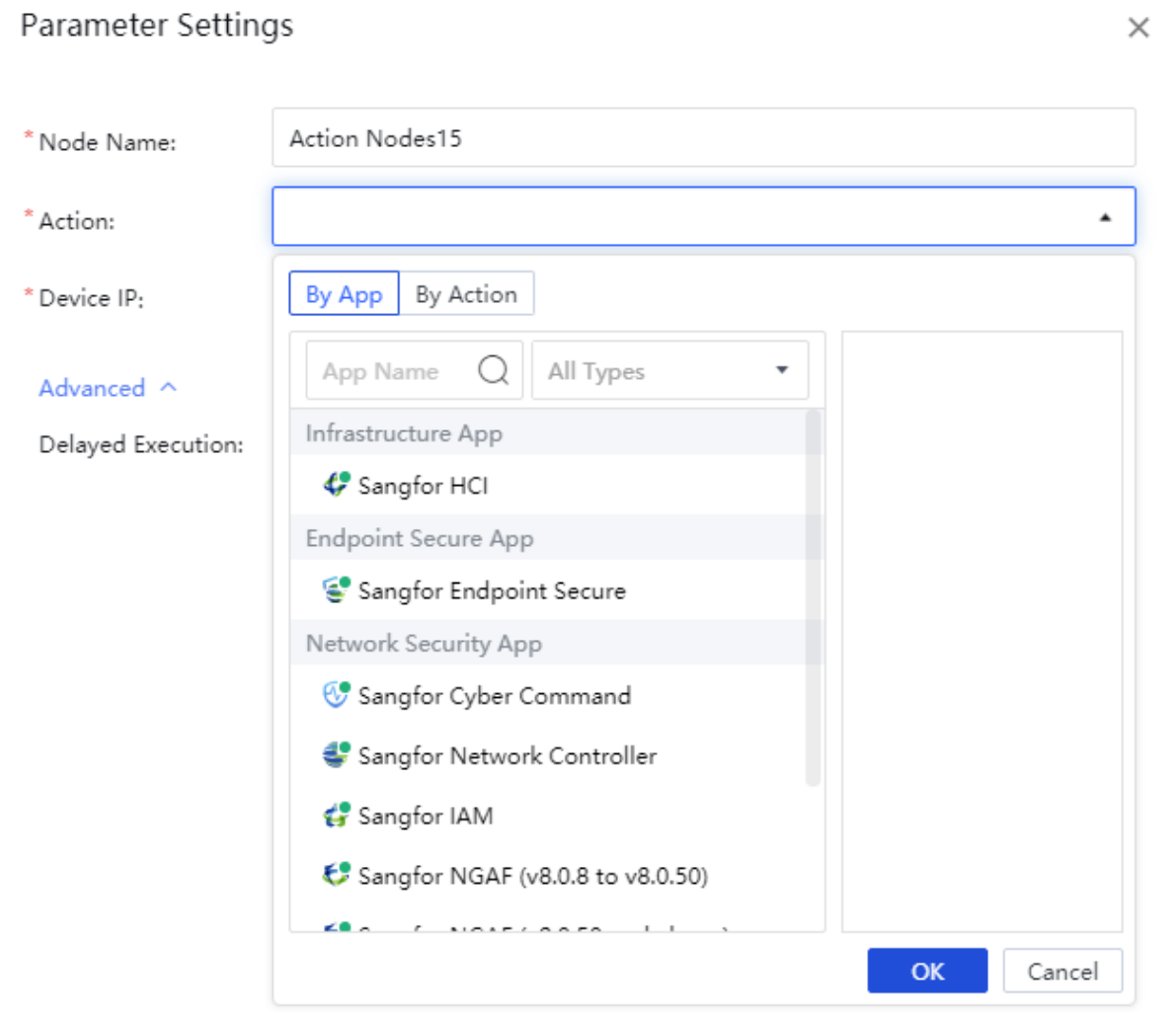
Action - action nodes

After you drag and drop the action node to the canvas, you can click it to pop up the Parameter Settings dialog box. You can specify the node name, select an action and device IP from the drop-down list, and click <Advanced> to manually enable or disable delayed execution.



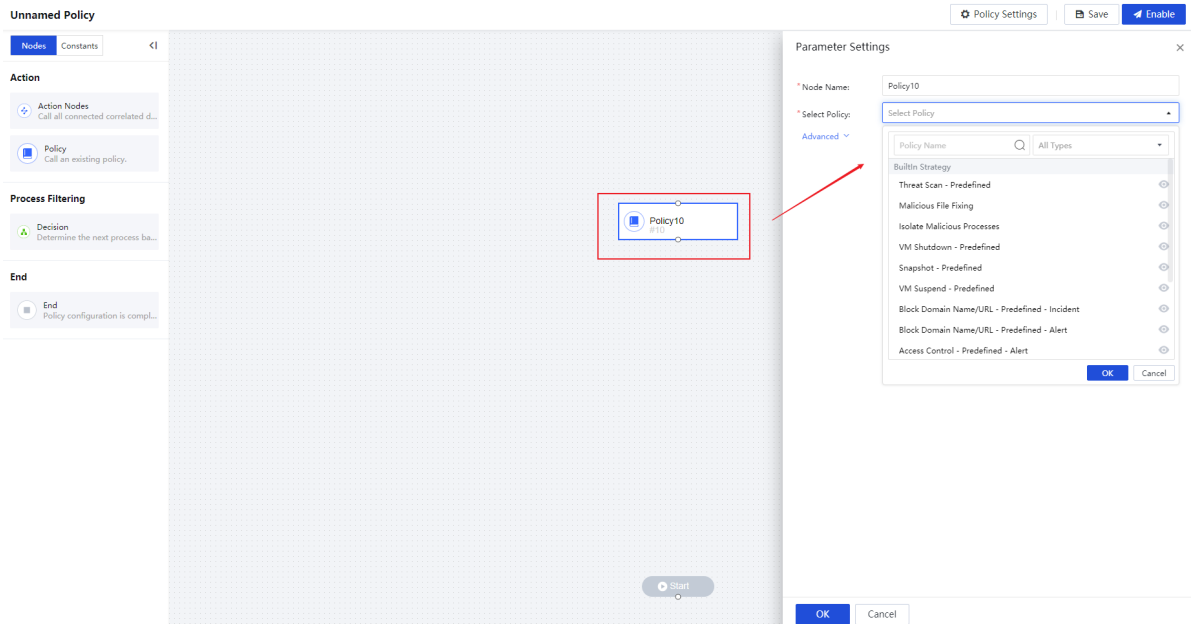
Fields:

Action: You can select the action by application or by action. Actions vary by application. You can select an action in the drop-down list or enter keywords to perform fuzzy search by application/action, as shown in the following figure.



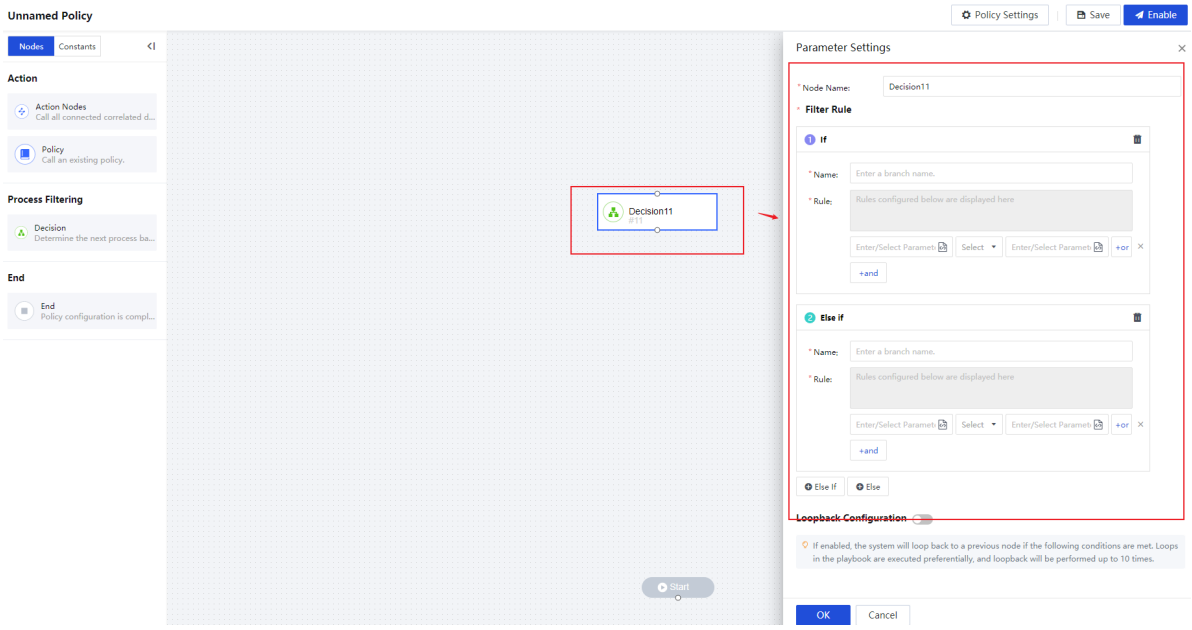
Action - policy

[Node/Policy] in the left navigation pane allows you to call an existing policy when a new policy is added. You can drag and drop it to the canvas and then double click it to set parameters. The Parameter Settings dialog box appears. You can specify [Node Name], select a policy from the drop-down list of [Select Policy], and enable/disable delayed execution (disabled by default) in Advanced Settings. After parameters are set, you can click <OK>, as shown in the following figure.

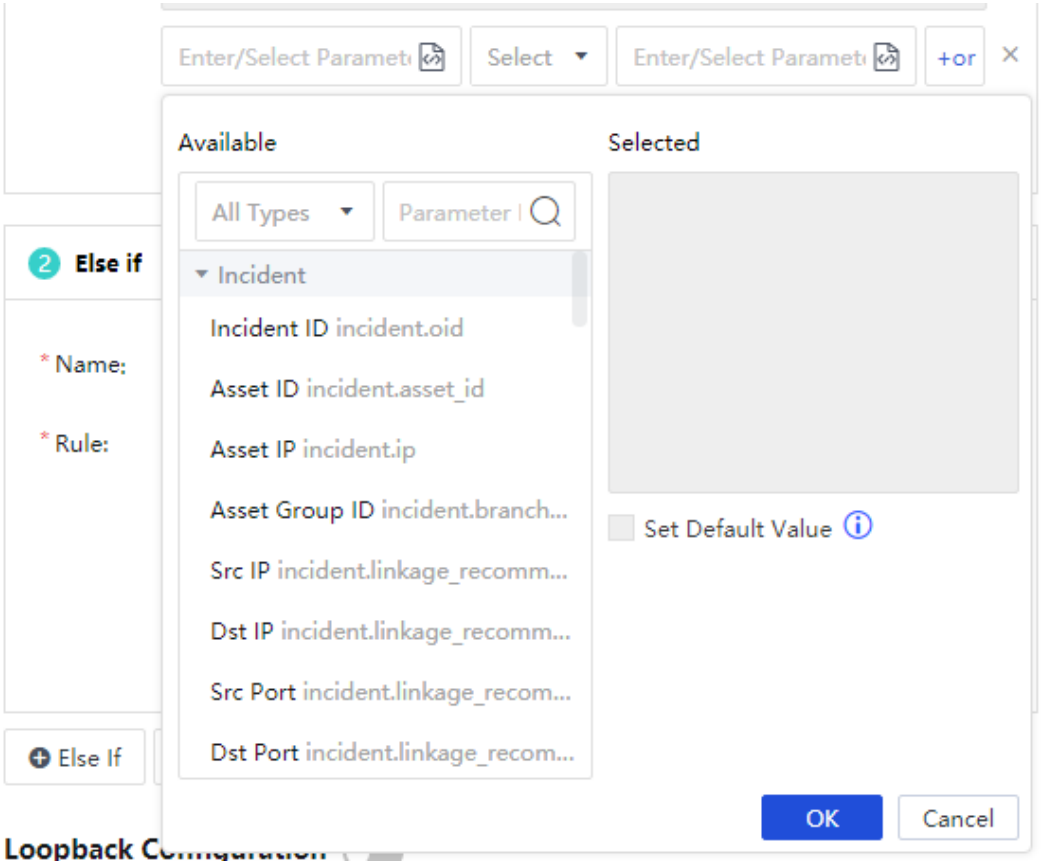


Process filtering - decision

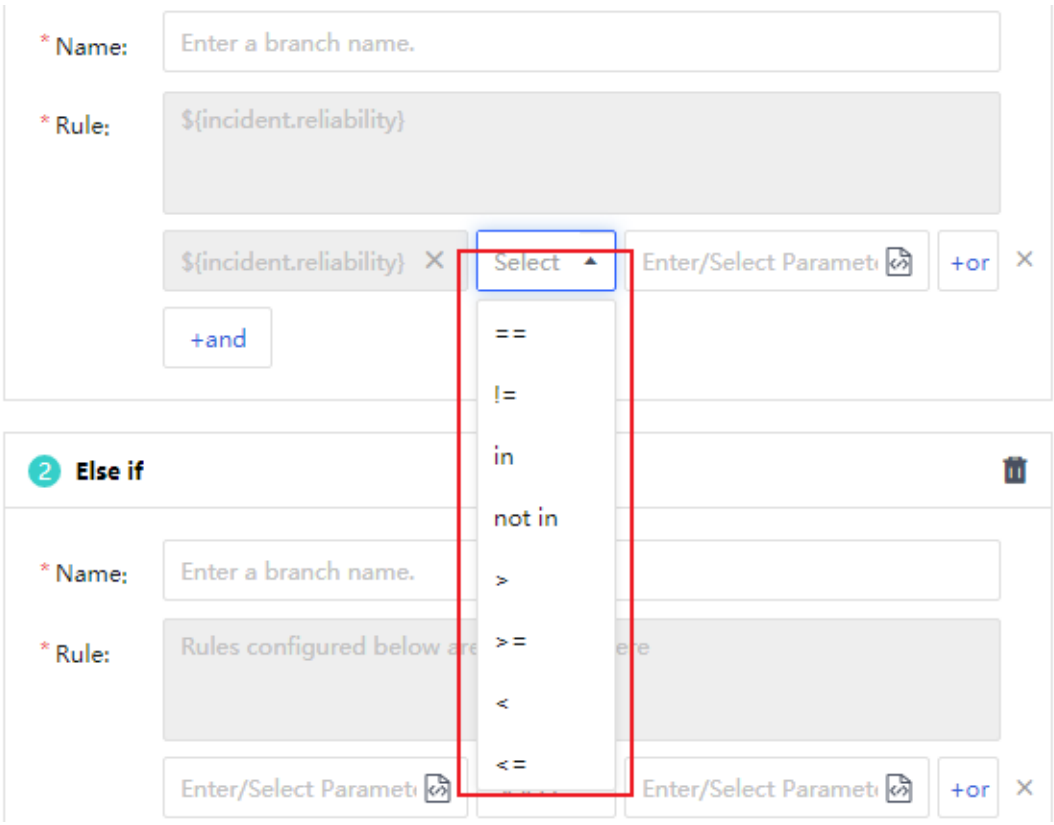
[Process Filtering/Decision] in the left navigation pane allows you to add conditions to determine the next process. You can drag and drop it to the canvas and then double click it to set parameters. The Parameter Settings window appears. You can specify [Node Name], create filter rules using the "if-else", "if-else", and "if-...-else" statements, and enable or disable [Loopback Configuration], as shown in the following figure.



Filter Rule: You need to click the < > icon first to pop up the parameter selection window. You can select a parameter from the drop-down list by event/alert and click <OK>, as shown in the following figure.



Logical Relationship: You can select the logical relationship from the drop-down list, including "==", "! =", "in", "not
in", ">", ">=", "<", and "<=", as shown in the following figure.



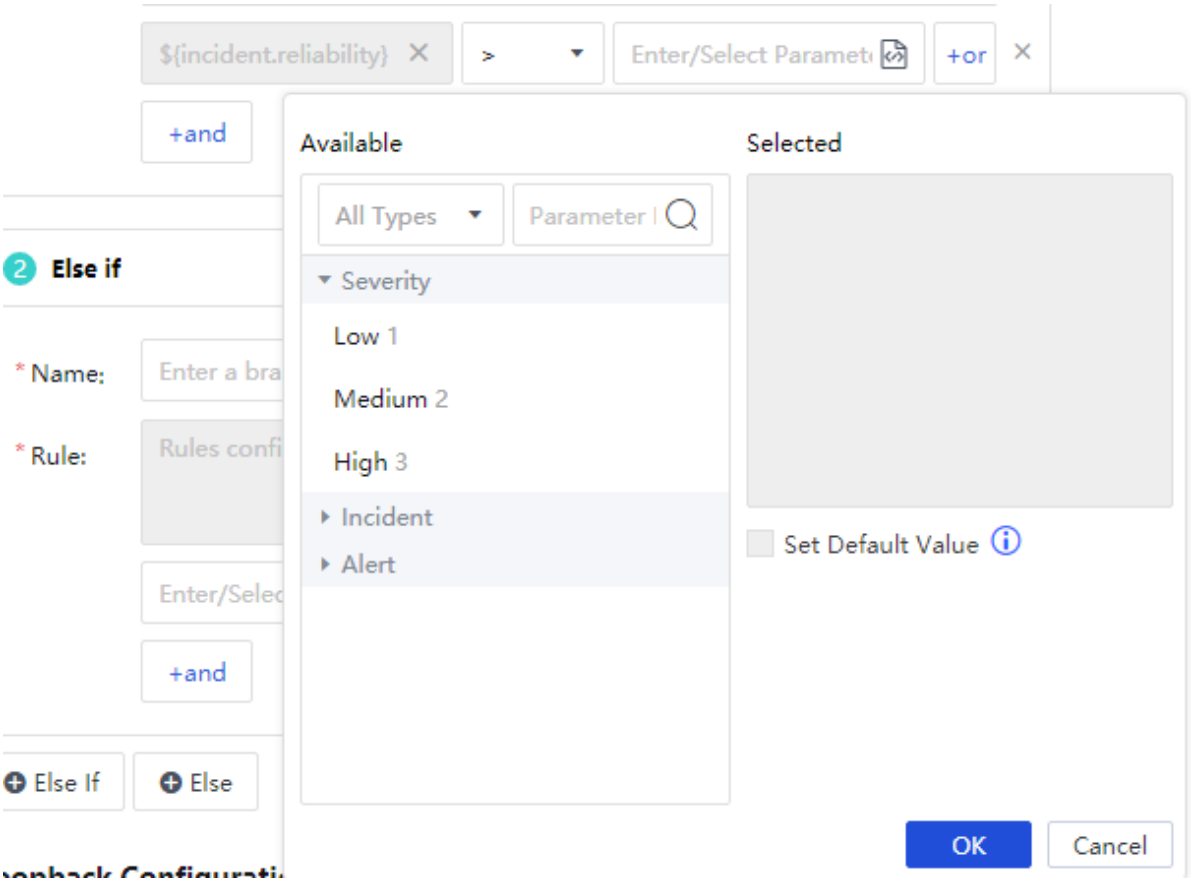
Note:

in and not in: Arrays and other types are supported in the left field, and values in the right field are automatically converted to arrays.

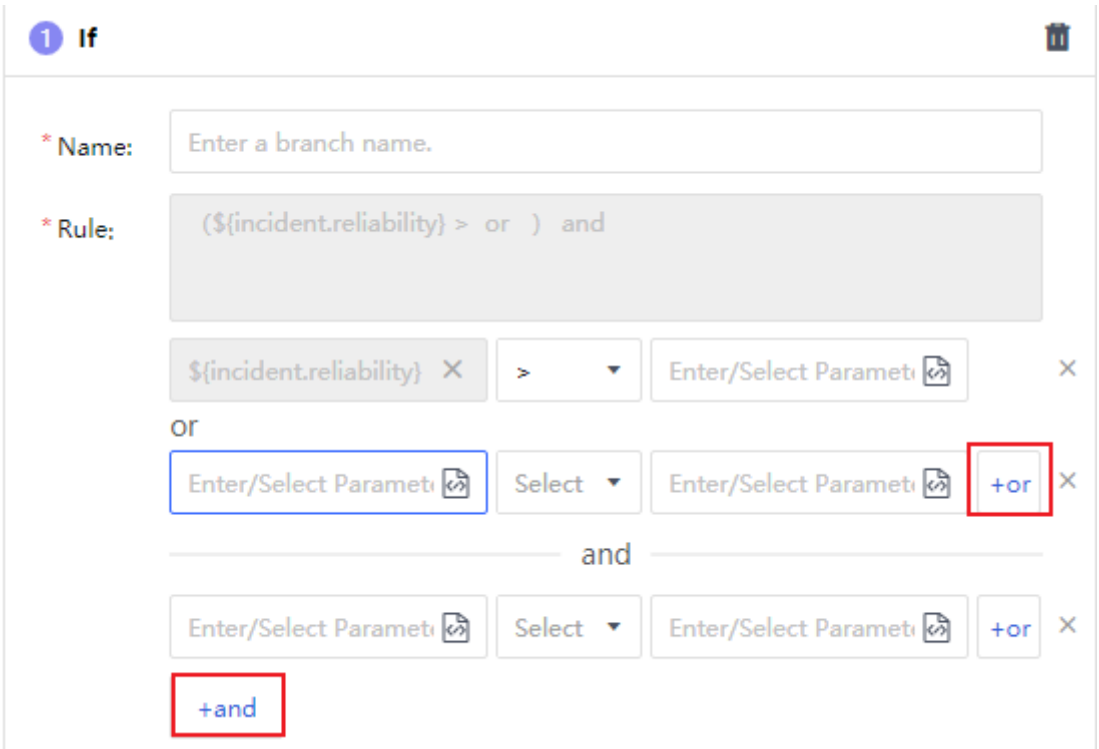
== and !=: Strings and digits are supported both in the left and right fields.

<, <=, >=, and >: Digits are supported both in the left and right fields.

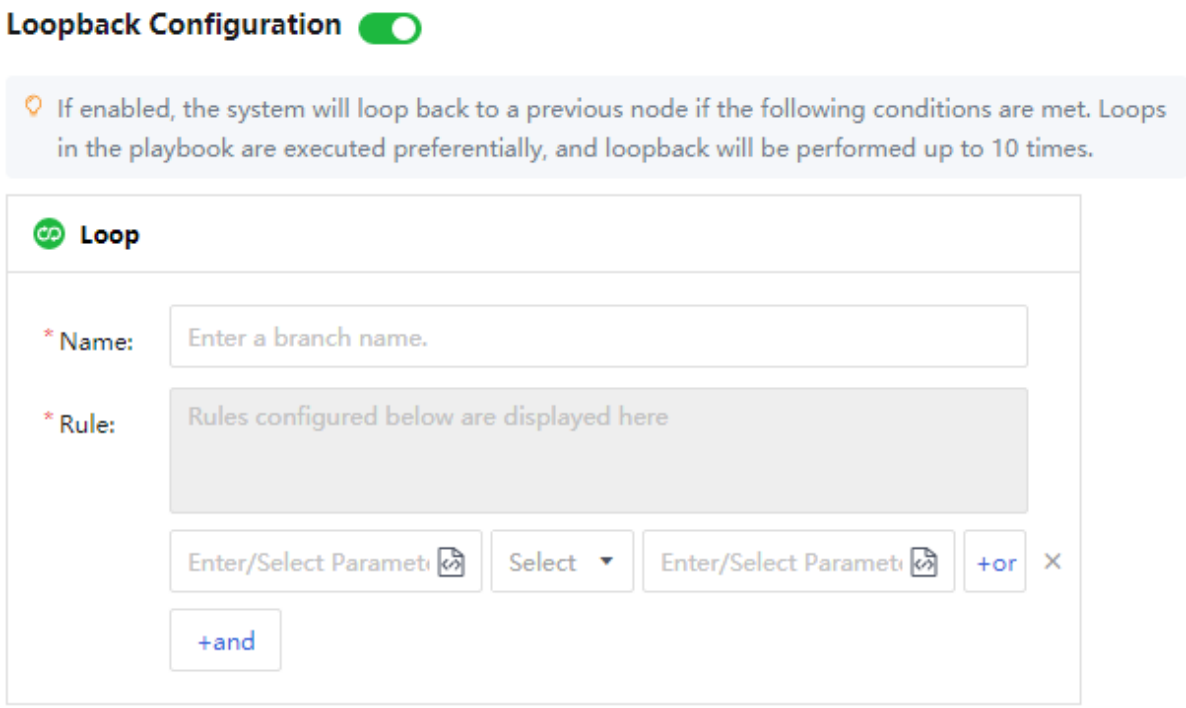
Attribute Value: You can enter the attribute value of the selected attribute corresponding to the logical relationship, or select a parameter according to the actual condition.



You can also add several rules for one "if" condition and select "and" or "or" relationship for these rules by clicking < +or > or < +and >, as shown in the following figure.



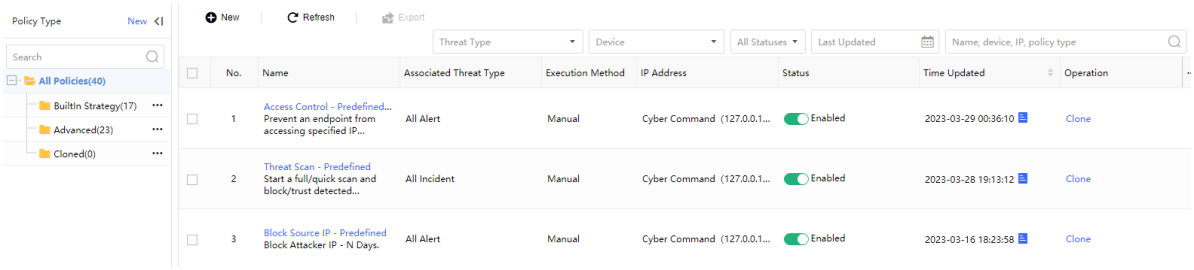
Loopback Configuration: If enabled, the system will loop back to a previous node if the configured conditions are met. Loops in the playbook are executed preferentially and loopback will be performed up to 200 times, as shown in the following figure.



Policy Editing

Policy attributes

After you have orchestrated a policy, you can view all attributes of the policy on the [Response/Auto Response/Policies] page, as shown in the following figure.



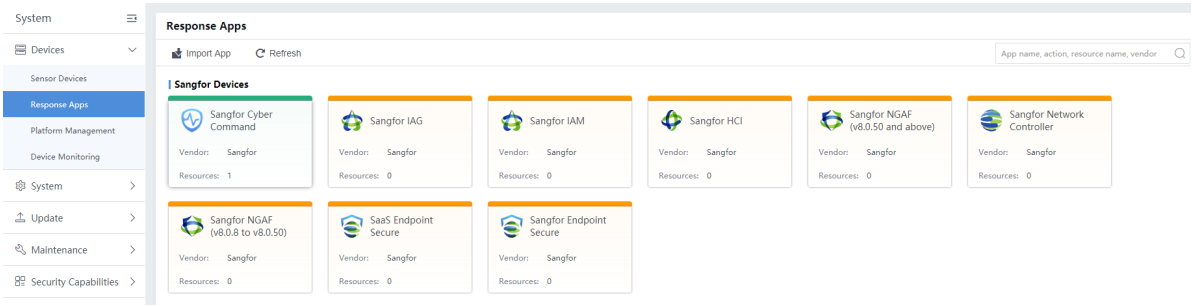
Attributes:

Associated Threat Type: Indicates the threat type selected during policy settings.

Execution Method: Includes automatic execution and manual execution.

Policy Type: Includes built-in, advanced, and cloned policies.

Device: Indicates the application name cited by all action nodes involved in a policy. You can view all application names on the [System/Response Apps] page, as shown in the following figure.

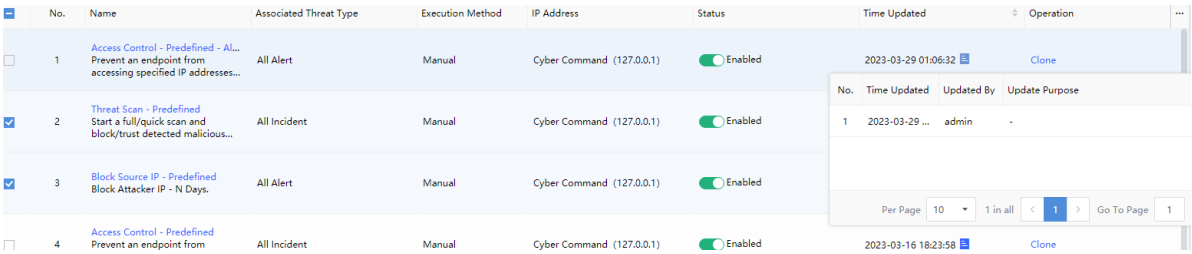


Policies

You can edit, clone, delete, and enable/disable a policy, as shown in the following figure.



You can click the < > icon to view the policy update history, including the update time, operator, and purpose, as shown in the following figure.



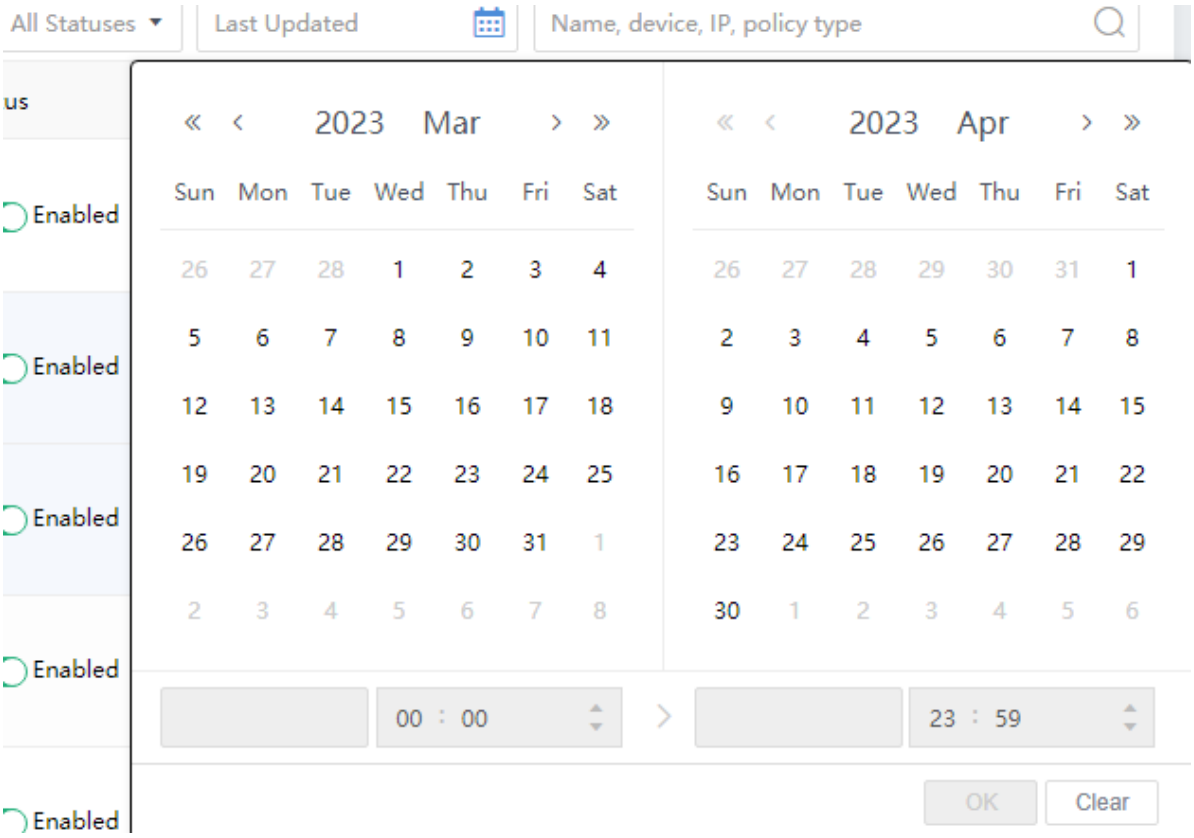
You can click <Edit> to go to the policy canvas and edit the policy. You can also click <Clone> to clone the policy. The cloned policy will be saved to the [Cloned] policy type.

Policy exporting

You can select one or multiple policies in the policy list and export them as PNG images.

Quick search

When the number of policies reaches a certain amount, you can search for polices by status and last update time. You can also perform a fuzzy search by policy name, creator, and operator of last update, as shown in the following figure.

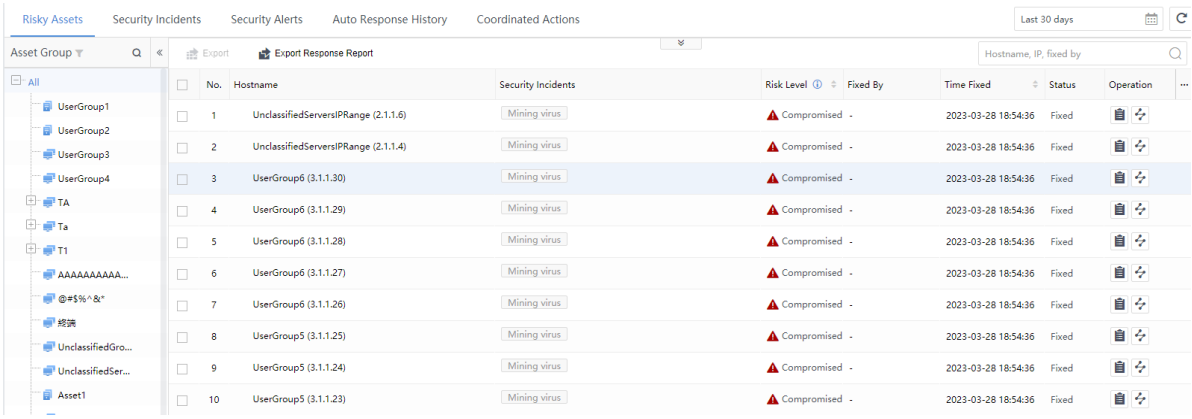


Response History

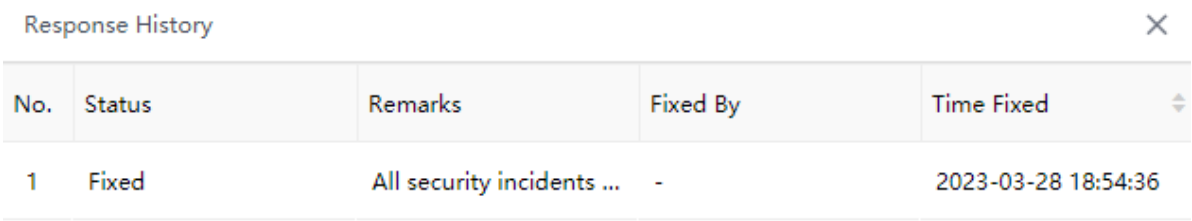
This page contains five tabs: Risky Assets, Security Incidents, Security Alerts, Auto Response History, and Coordinated Actions. The [Response/Risky Assets] page corresponds to the [Response History\Risky Assets] tab. The [Response/Security Incidents] page corresponds to the [Response History\Security Incidents] tab. The [Response/Security Alerts] page corresponds to the [Response History/Security Alerts] tab.

Risky Assets

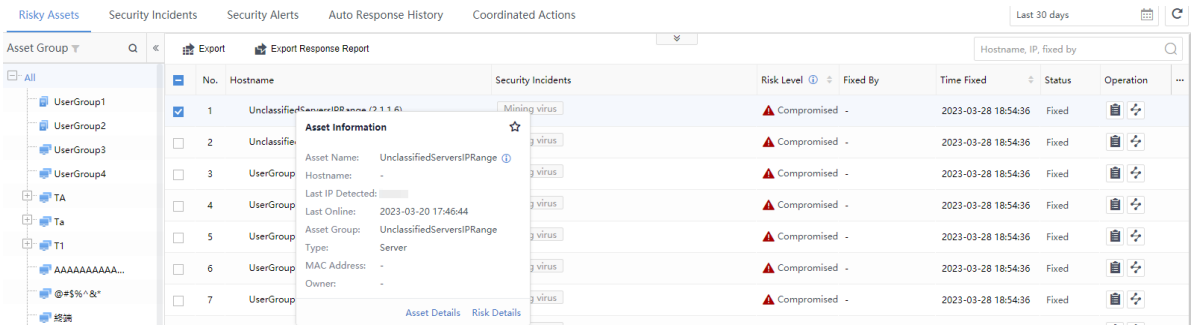
On the [Risky Assets] tab, you can view the details of fixed risky assets, asset groups, trends, and a list.



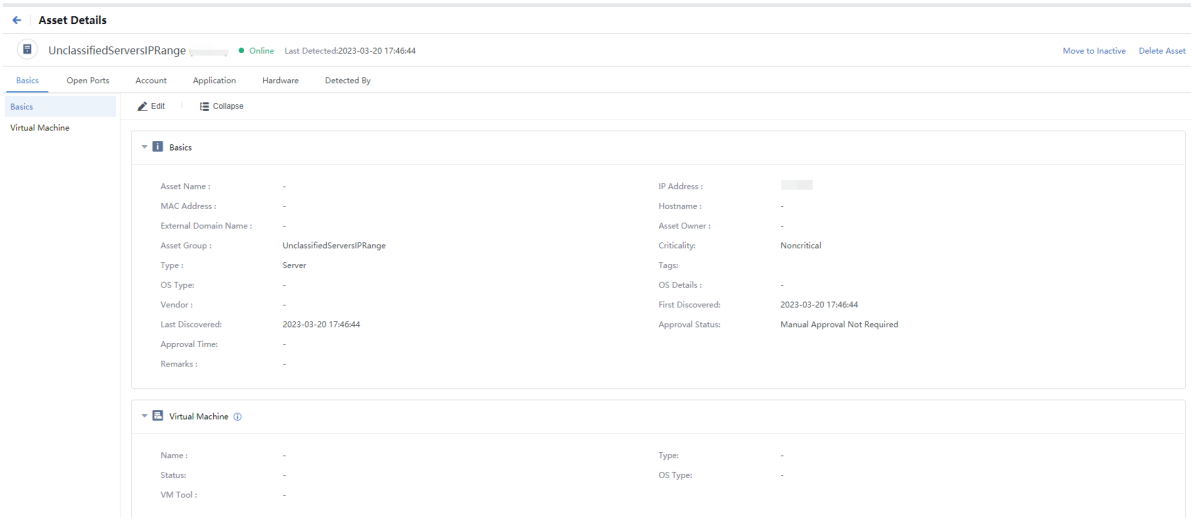
You can click the response history icon in the operation column to view the remarks, fixing person, and fixing time.



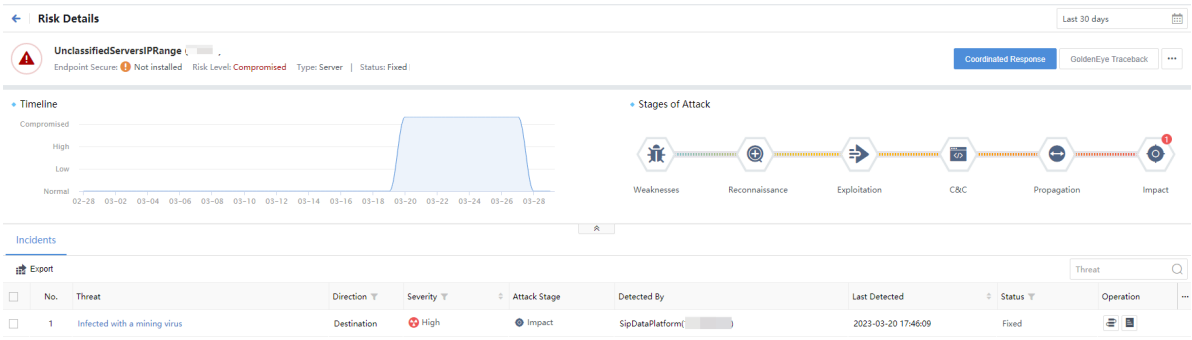
If you want to view the details, you can hover the mouse over the name in the Hostname column, as shown in the following figure.



You can click [Asset Details] in the pop-up box to go to the details page of an asset. Then, you can go back to the original page by clicking the return arrow, as shown in the following figure.

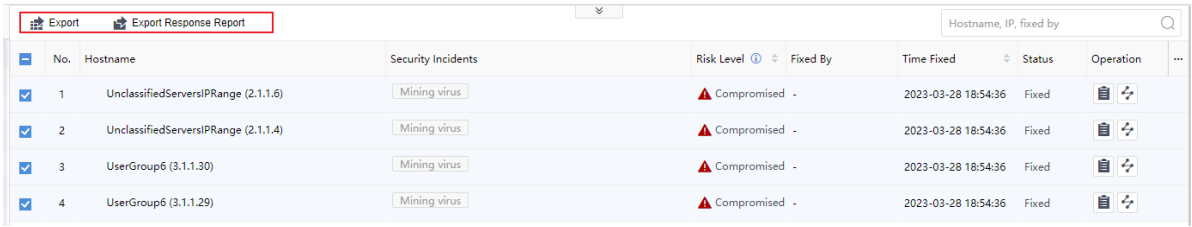


You can click [Risk Details] in the pop-up box to go to the risk details page of an asset. Then, you can go back to the original page by clicking the return arrow, as shown in the following figure.



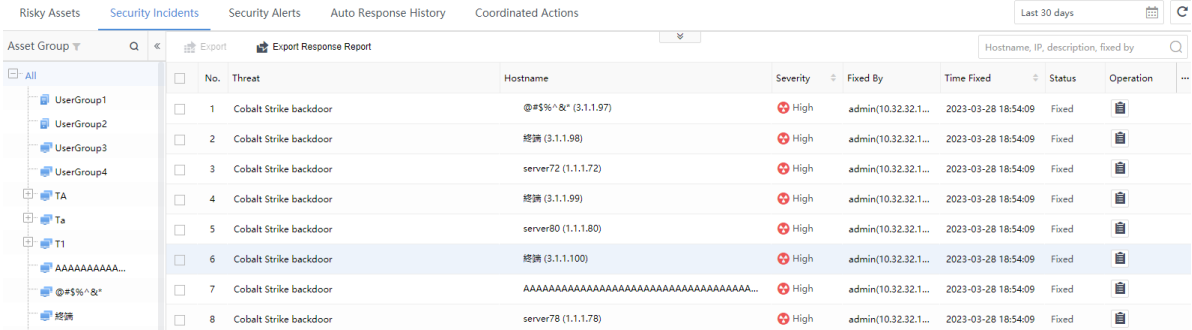
You can filter risky assets by time and asset group, or search for risky assets by asset group, hostname, IP address, tag, and fixing person.

You can export the list and response reports as needed, as shown in the following figure.



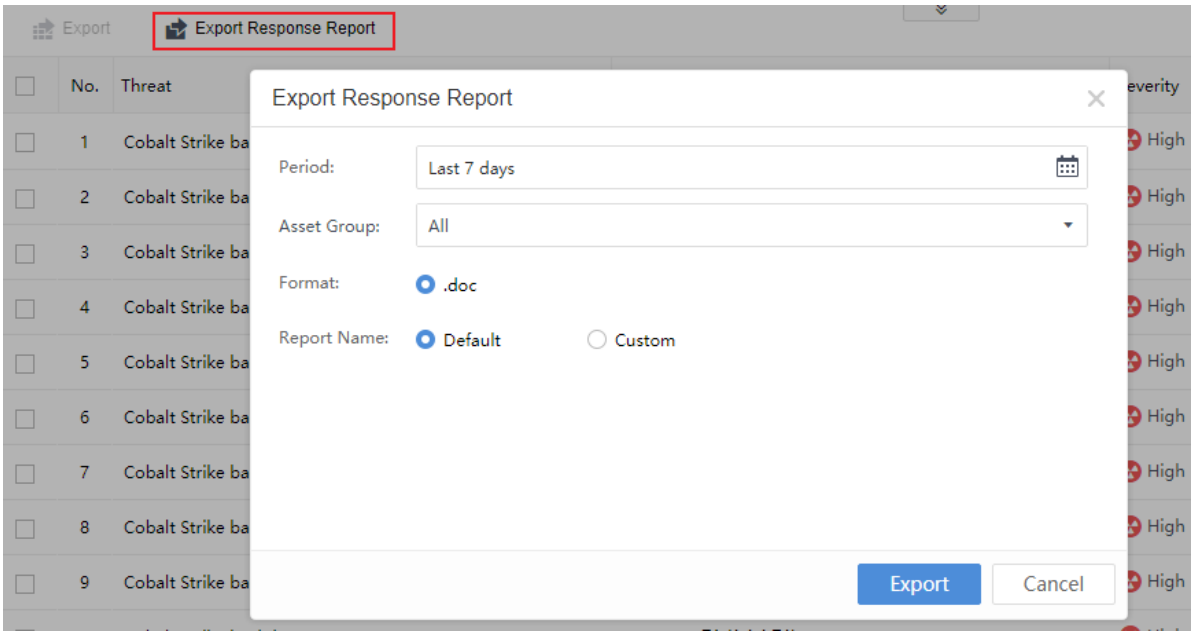
Security Incidents

On the [Response History/Security Incidents] tab, you can filter, search for, and view the fixed incidents, as well as exporting response reports. This tab displays asset groups, the number of fixed incidents, trend, and a security incident list, as shown in the following figure.

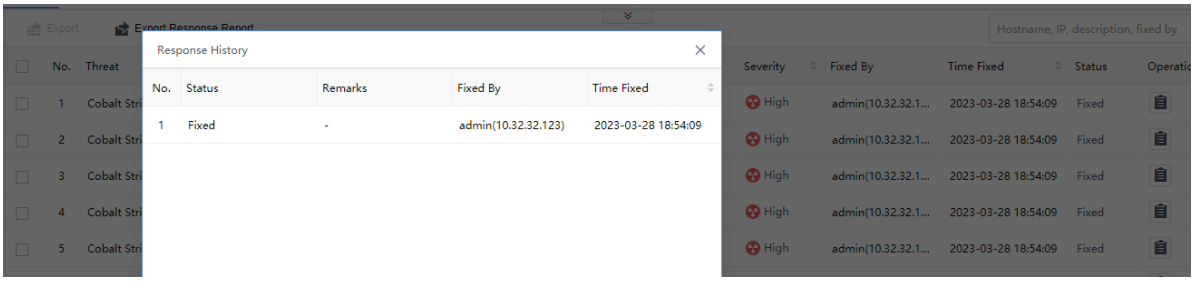


<Export: >You can select security incidents and export them.

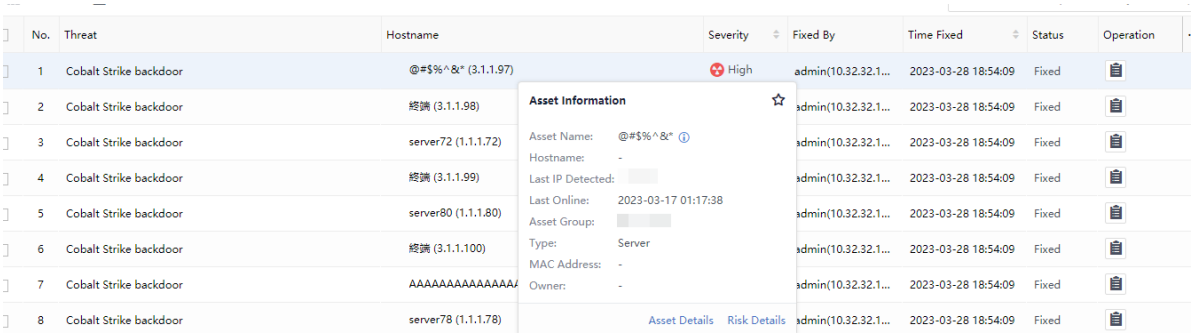
<Export Response Report: >You can click this button to specify parameters for exporting response reports as needed, as shown in the following figure.



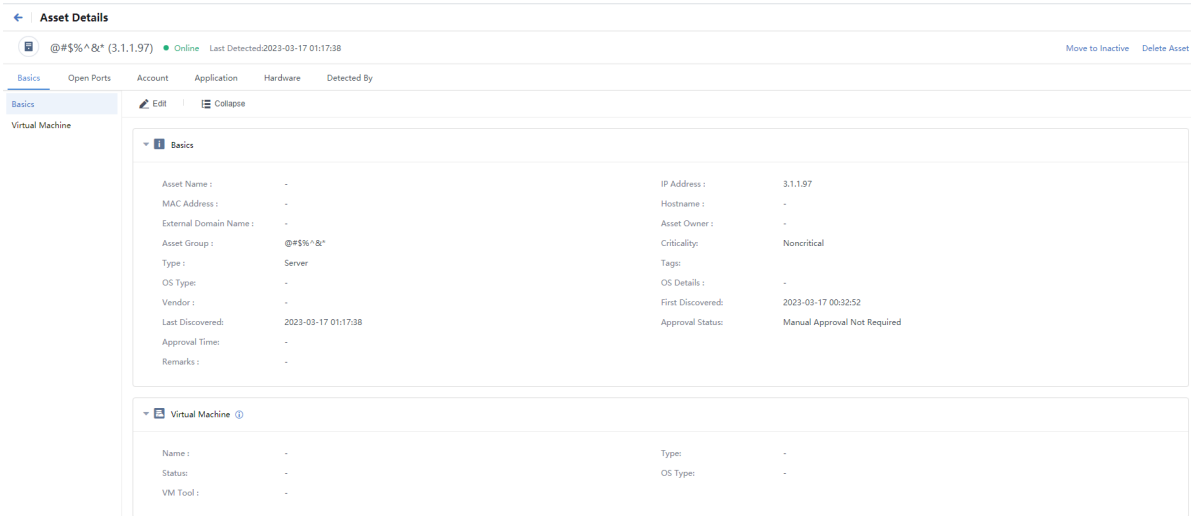
<View History: >You can click the < > icon in the Operation column to view the remarks, fixing person, and fixing time.



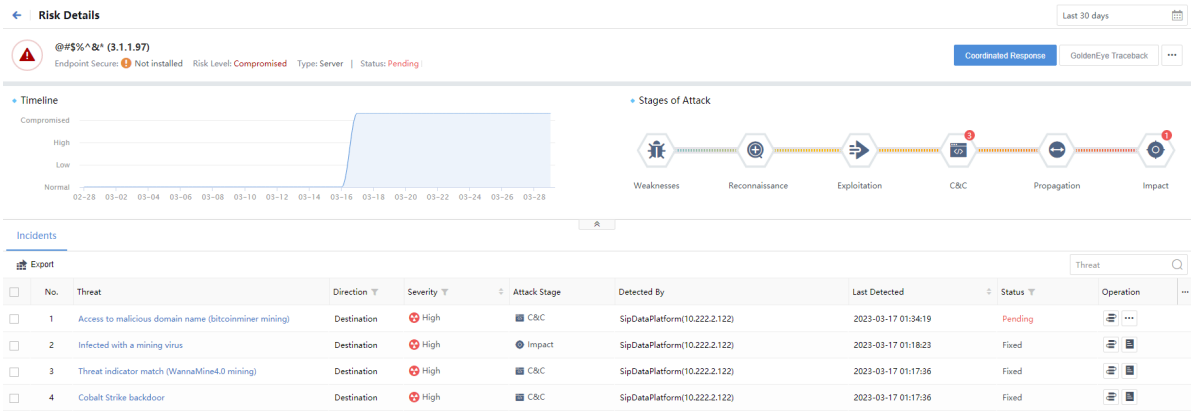
If you want to view the incident details, you can hover the mouse over the content in the Hostname column to view the details.



You can click [Asset Details] in the pop-up box to go to the details page of an asset. Then, you can go back to the original page by clicking the return arrow, as shown in the following figure.

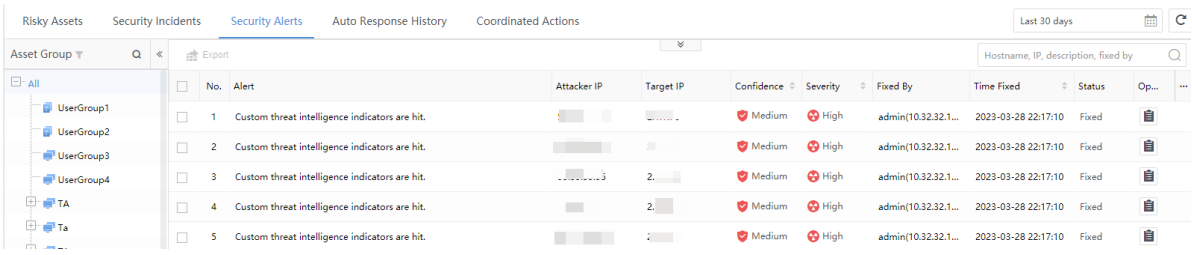


You can click [Risk Details] in the pop-up box to go to the risk details page of an asset. Then, you can go back to the original page by clicking the return arrow, as shown in the following figure.

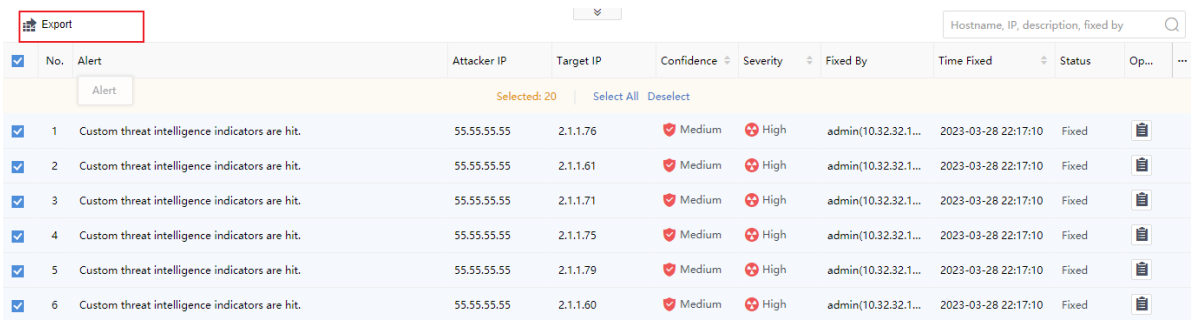


Security Alerts

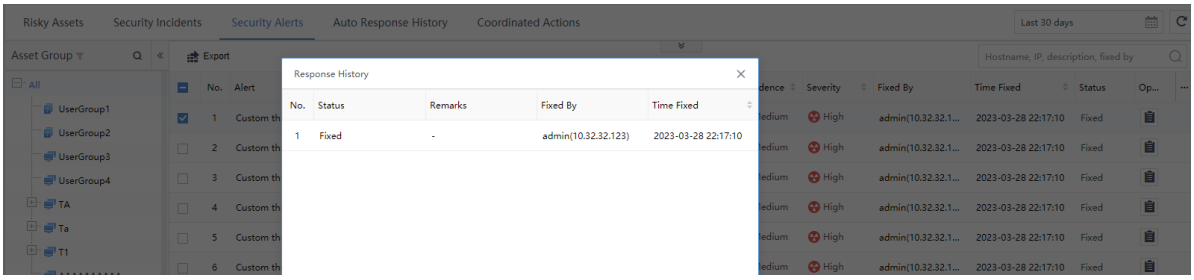
On the [Response History/Security Alerts] tab, you can filter, search for, and view the fixed alerts, as well as exporting response reports. This tab displays asset groups, the number of fixed alerts, trend, and a security alert list, as shown in the following figure.



<Export: >You can select security alerts and export them.

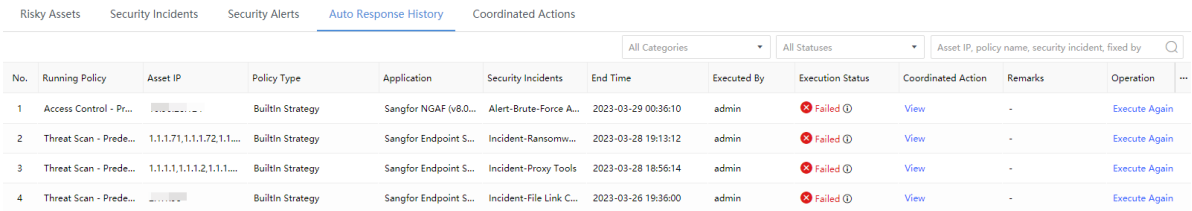


<View History: >You can click the < > icon in the Operation column to view the remarks, fixing person, and fixing time.



Auto Response History

This tab mainly displays the history of policies that are called, including the history from [Response/Risky Assets], [Response/Security Incidents], and [Response/Security Alerts]. This tab contains information such as the name of running policy, policy type, application, security incidents, start time, end time, duration, execution operator, execution status, coordinated action, and operation, as shown in the following figure.



Fields:

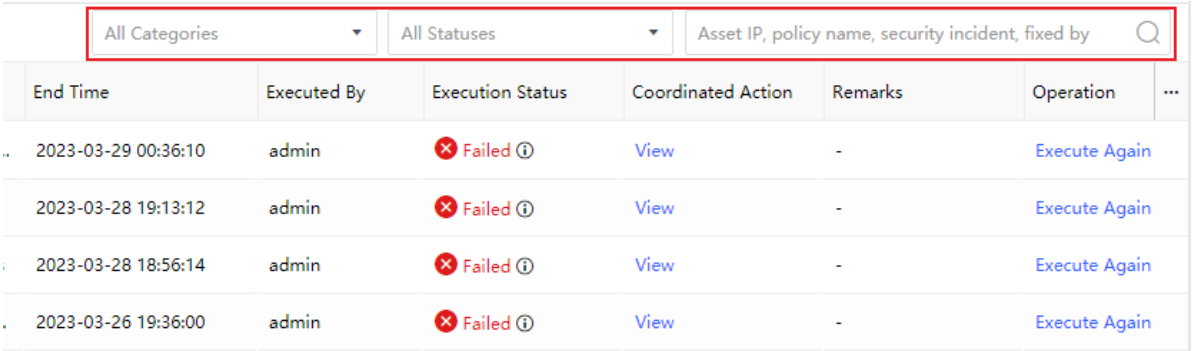
Execution Status: Includes "In Progress", "Executed", and "Failed".

Operation: You can click <Execute Again> to execute the policy again.

<Coordinated Action: >You can click <View> to go to the [Response/Response History/Coordinated Actions] page to view the details.

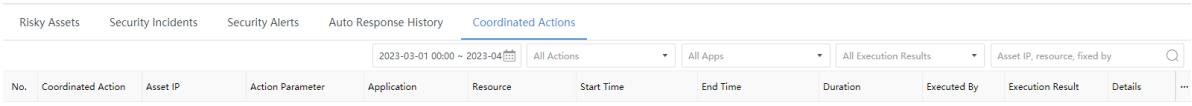
Search

You can filter the response history of policies by policy type and execution status. You can also search by policy name, security incident, and execution operator, as shown in the following figure.



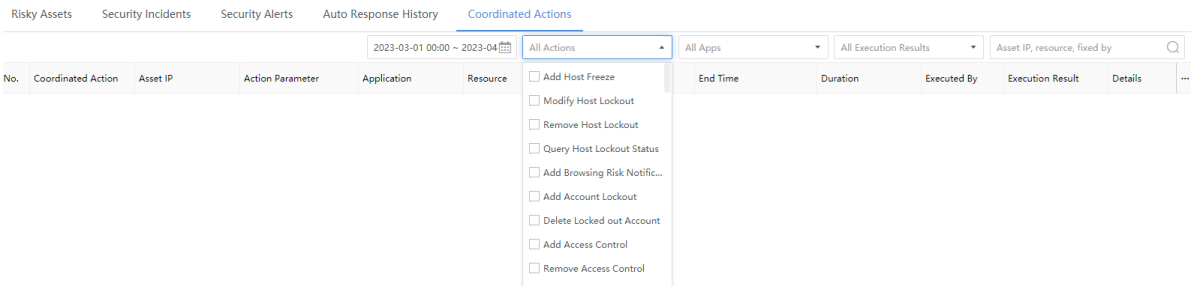
Coordinated Actions

This tab mainly displays the execution history of actions generated on [Response/Risky Assets], [Response/Security Incidents], [Response/Security Alerts], and [Critical Protection Center]. Fields on this tab include coordinated action, action parameter, application, resource, start time, end time, duration, execution operator, execution result, and details, as shown in the following figure.



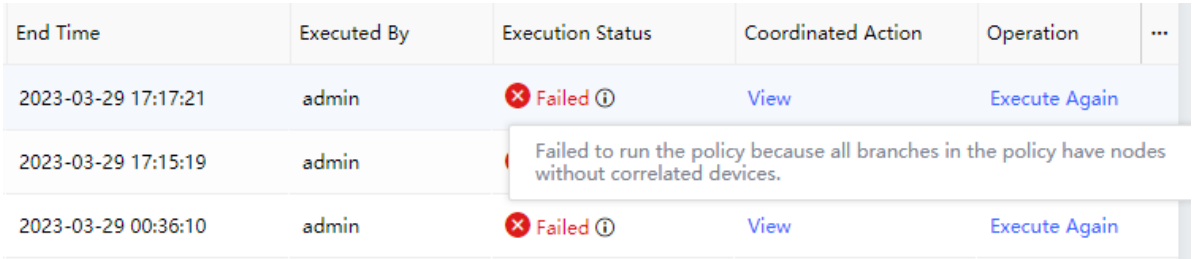
Fields:

Coordinated Action: All actions supported by Nova Command, as shown in the following figure.

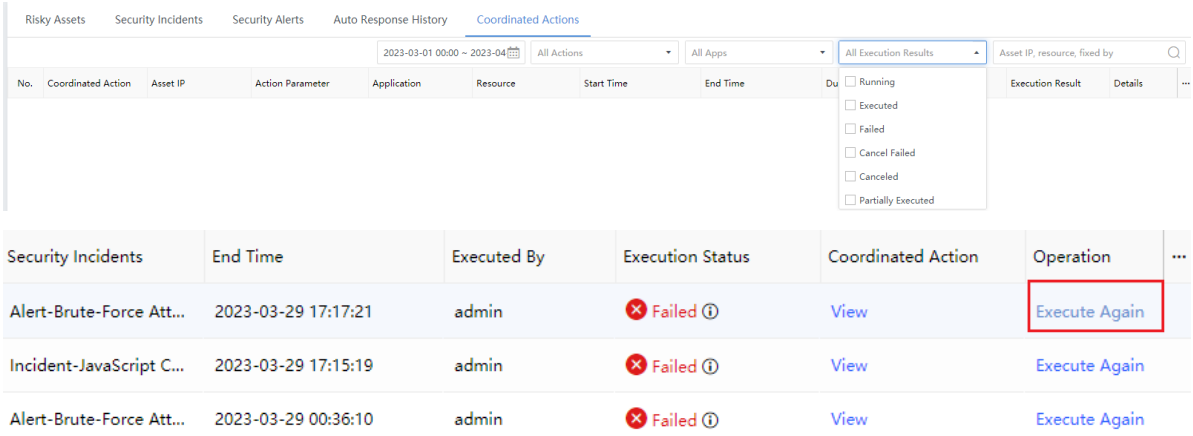


Executed By: The role that called the policy.

Execution Result: If the action has failed, you can hover the mouse over ⓘ to view the reason, as shown in the following figure.



Execution Result: Includes "Running", "Executed", "Failed", "Cancel Failed", "Canceled", and "Partially Executed". You can click <View> to view the details of executed actions. You can view the reasons for failed actions and make corrections accordingly. After correction, you can click <Execute Again> to execute the action again, as shown in the following figure.



You can click <View> to view the details of an executed action.

Detection

Similar to the Response module, the Detection module also provides important functions of Nova Command, such as organizing and displaying data after processing and analysis. It is frequently used in security operations and contains child modules such as Logs, Threats, Anomalies, Traffic, and SIEM.

Logs

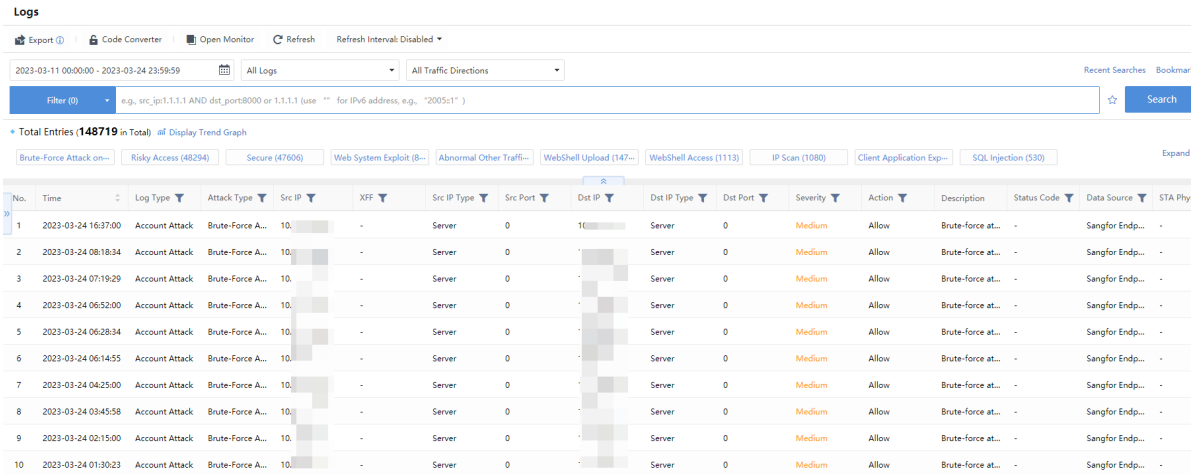
On the [Detection/Logs] page, you can search for security logs, audit logs, and third-party logs to facilitate further analysis of security issues.

Log Search

On the Logs page, you can search for specific logs by specifying the log type and using keywords in the search box.

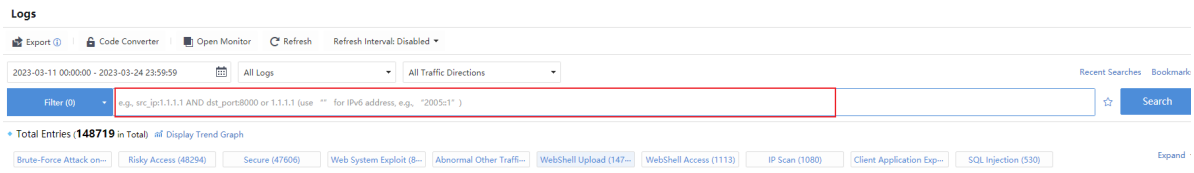
Search by type

On the [Logs] page, you can filter logs by log type, traffic direction, and key fields. You can also search for logs by key field, as shown in the following figure.



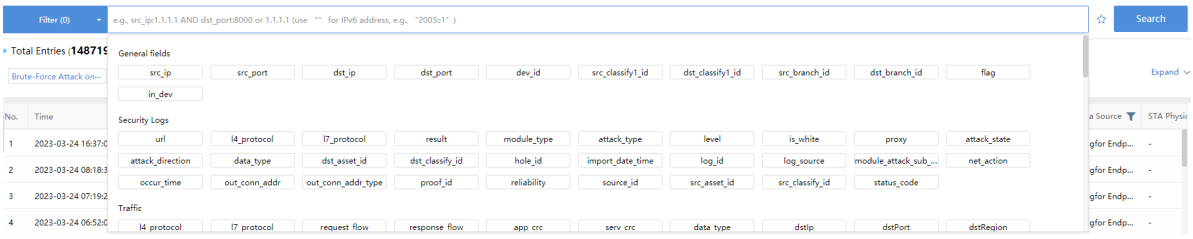
Search by keyword

On the [Logs] page, you can search for logs by field. You can use a specific field for accurate search or any field for fuzzy search. At the same time, you can also search for logs by specifying several filters at one time, as shown in the following figure.

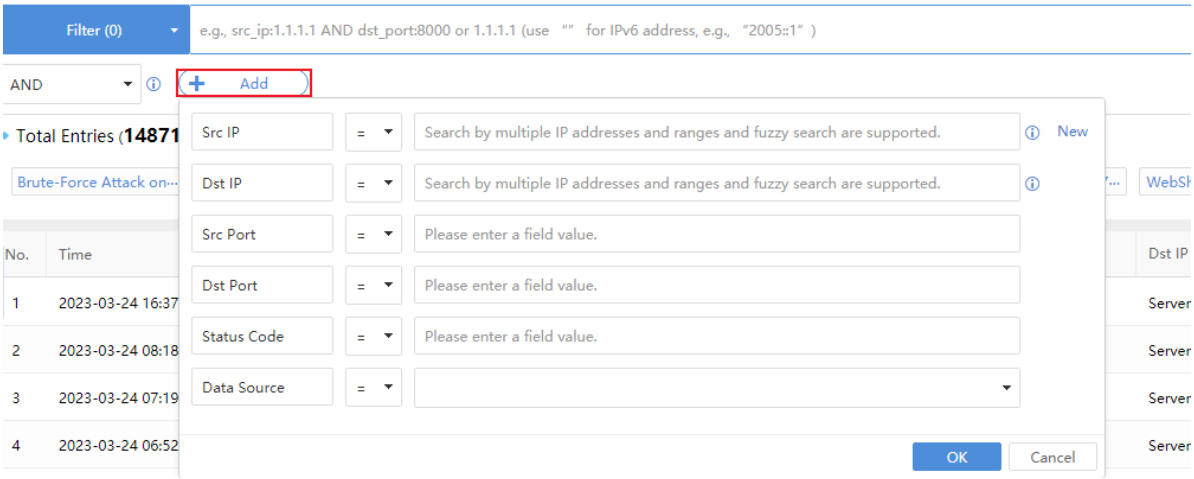


<Search by any fields: >Fuzzy search by IP address, data packet, and combination of multiple fields is supported.

<Search by specific fields: >Search by combination of multiple fields and fuzzy search by specific fields are supported, as shown in the following figure.

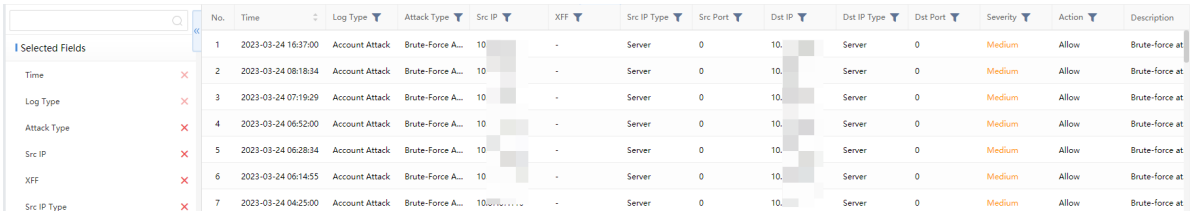


<Search with filter: >Search with specified filters, such as IP address, port, status code, and data source, is supported, as shown in the following figure.



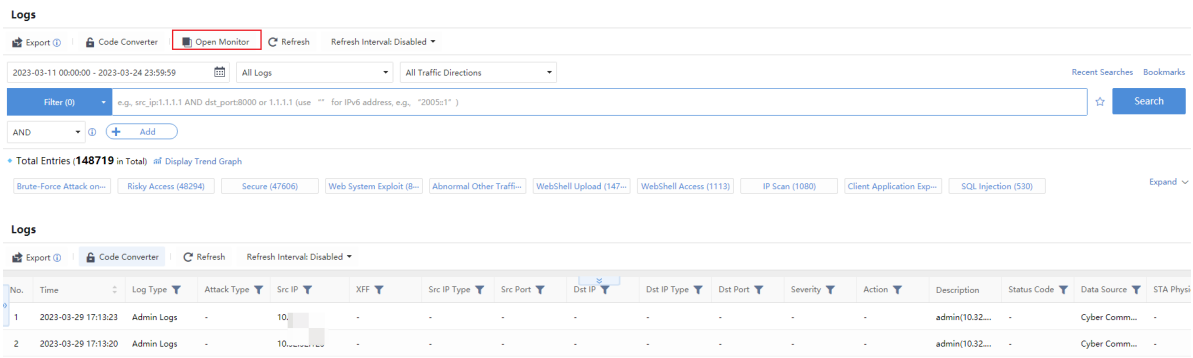
Search results

The search results contain information such as time, log type, source/destination IP address, source/destination port, and data source. You can click a log to view the details, as shown in the following figure.



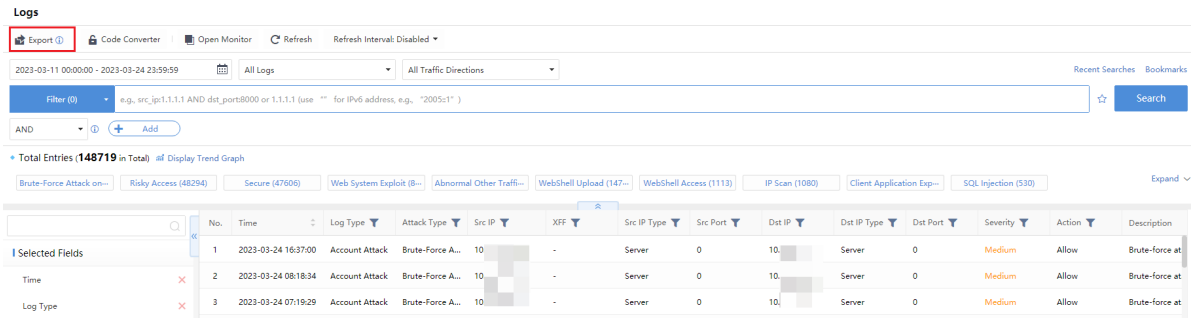
Open Monitor

On the [Logs] page, you click <Open Monitor> to pop up a new page that does not have the menu bar of Nova Command. It provides you with a better view of the logs, as shown in the following figures.

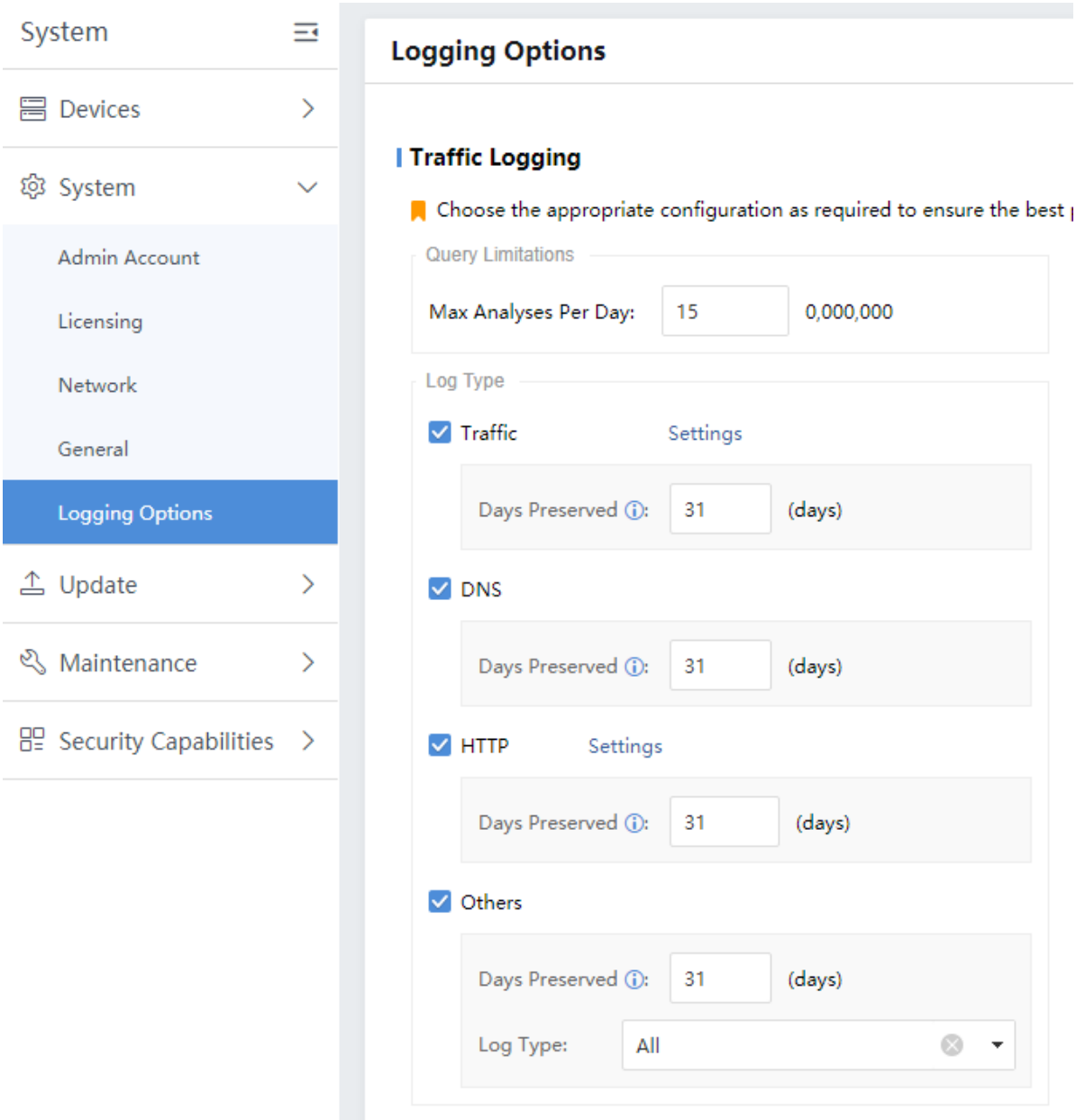


Log Export

You can export all searched logs by clicking the <Export> button in the top left corner, as shown in the following figure.



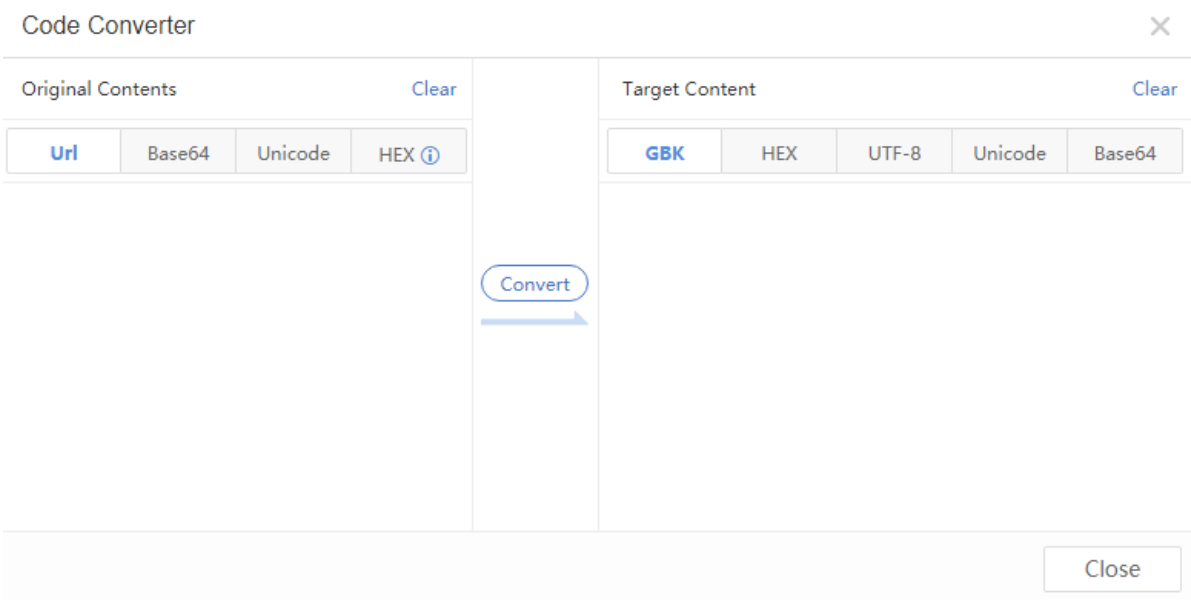
10,000 logs can be exported at one time by default. If you want to adjust the number of logs for a single export, you can click <Advanced>\ on the [System\Logging Options] page, as shown in the following figure.



Code Converter

Code converter is used to convert data packets to readable content and supports decoding of URL-, Base64-, Unicode-, and HEX-encoded strings.

If logs are encoded data packets, you can copy the packets to Code Converter, which converts packets to readable content, as shown in the following figure.



Threats

Detected threats are organized according to business scenarios and hot incidents, including ransomware, cryptomining, file threats, email threats, inbound attacks, and evasive attacks

Ransomware

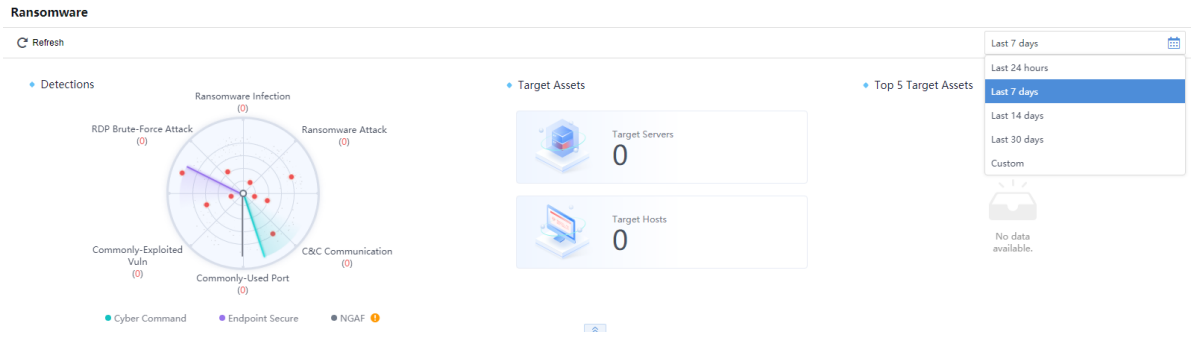
On the Ransomware page, security alerts associated with ransomware are displayed and managed. The data is mainly from correlated NovaGuard and NGAF, which detect traffic/processes with ransomware characteristics through traffic learning and endpoint security monitoring. A small part of data comes from Nova Command by identifying and determining traffic payloads. Currently, ransomware-related attacks are classified into ransomware infection, weak passwords, commonly-used ports, commonly-exploited vulnerabilities, access from overseas IPs, ransomware attacks, RDP brute-force attacks, and C&C communication.

Alert Display

On the [Ransomware] page, you can filter alerts by time period, view information in Detections and Target Assets sections, and use the auto response feature.

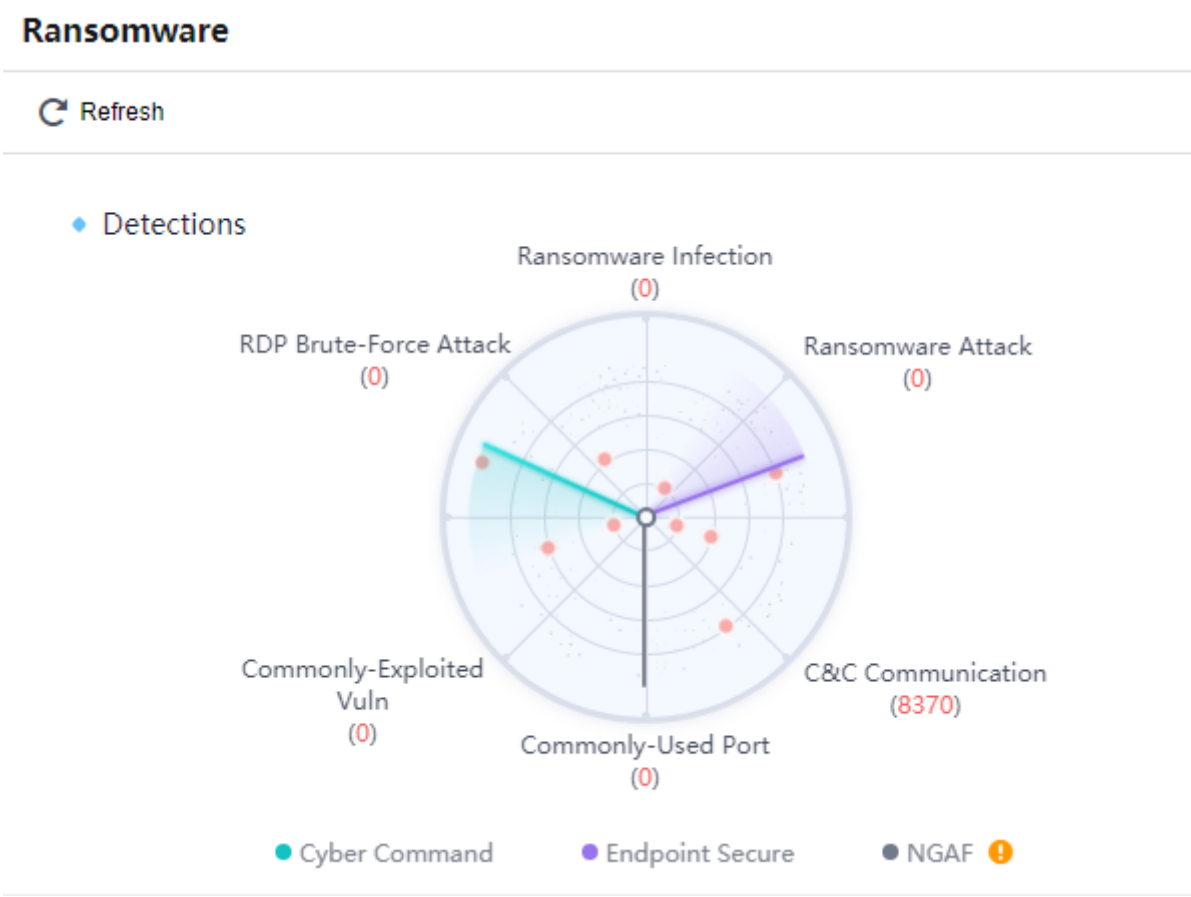
Filtration by time

You can select Last 30 days, Last 7 days, Last 24 hours, or Custom from the drop-down list to filter records, as shown in the figure below. If you select Custom, no limits are set for the time period.

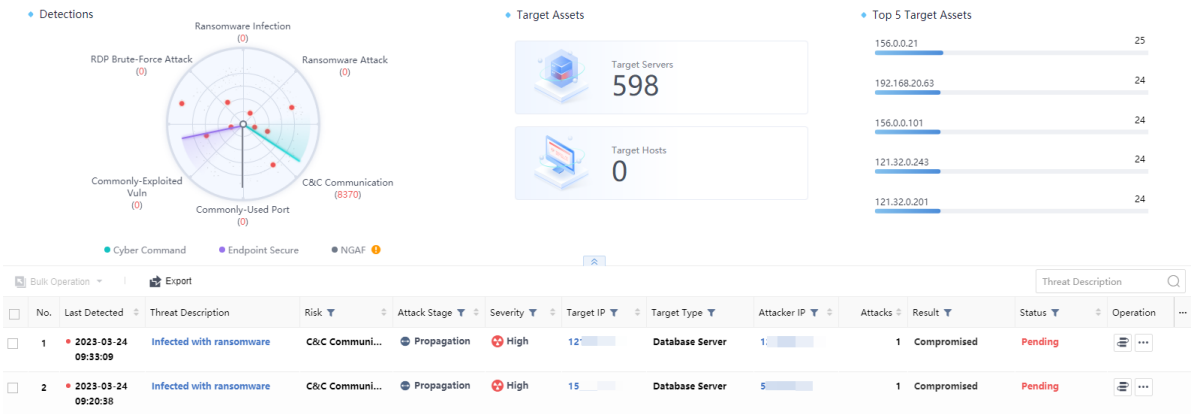


Detections

The data displayed in this section is collected by Nova Command, NovaGuard, and NGAF. It is classified based on the ransomware infection method, including C&C Communication, Ransomware Infection, Weak Password, Commonly-Used Port, Commonly-Exploited Vuln, Access from Overseas IP, Ransomware Attack, and RDP Brute-Force Attack, as shown in the figure below.

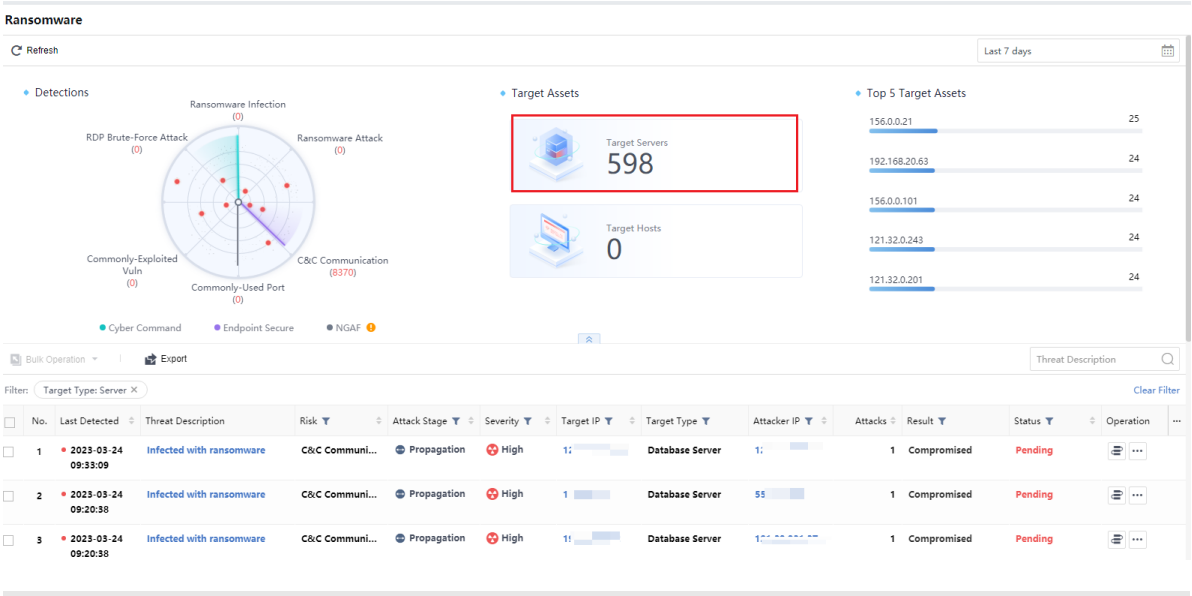


The numbers in red indicate the times of attacks that all ransomware risk assets suffer by the corresponding method. The three pointers associated with the source device are normally in blue during periodic scanning, as shown in the figure below.



Target assets

Two target asset types, namely target servers and target hosts, are displayed in this section. You can click either type to view the related event list, as shown in the figure below.



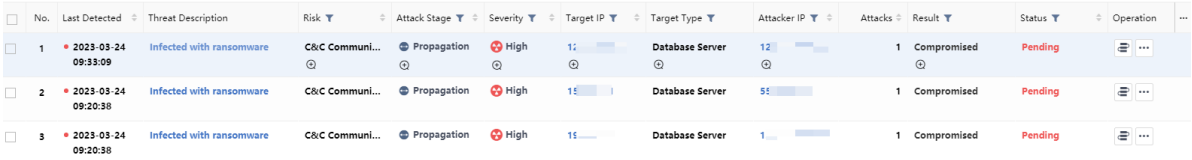
Note:

The data records displayed in the list are not aggregated. If you want to view the records of a specific target IP, click < > in the [Target IP] column.

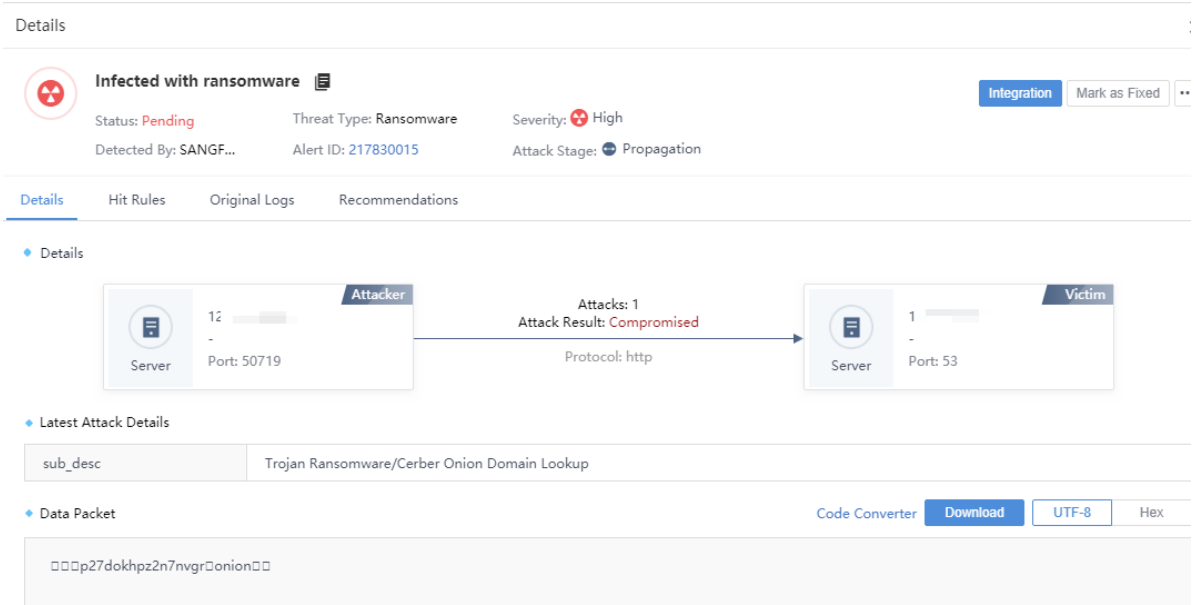
Alert Viewing

Event list

The event list includes fields such as Threat Description, Risk, Attack Stage, Severity, Target IP, Target Type, Attacker IP, Attacks, and Status, as shown in the figure below.

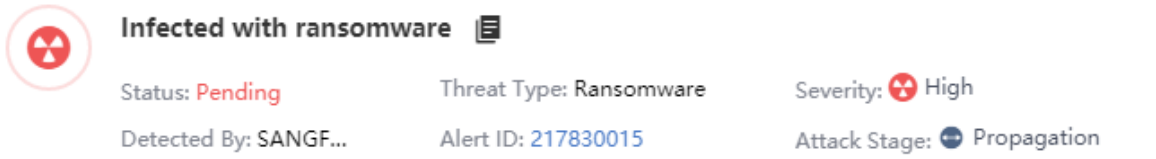


You can select a ransomware alert and click the content in the <Threat Description> column to go to the <Details> page. The <Details> page has a basic information section and several tabs, including Details, Hit Rules, Original Logs, and Recommendations. The basic information section shows information such as the status, severity, data source, hit rule, and attack stage, as shown in the figure below.



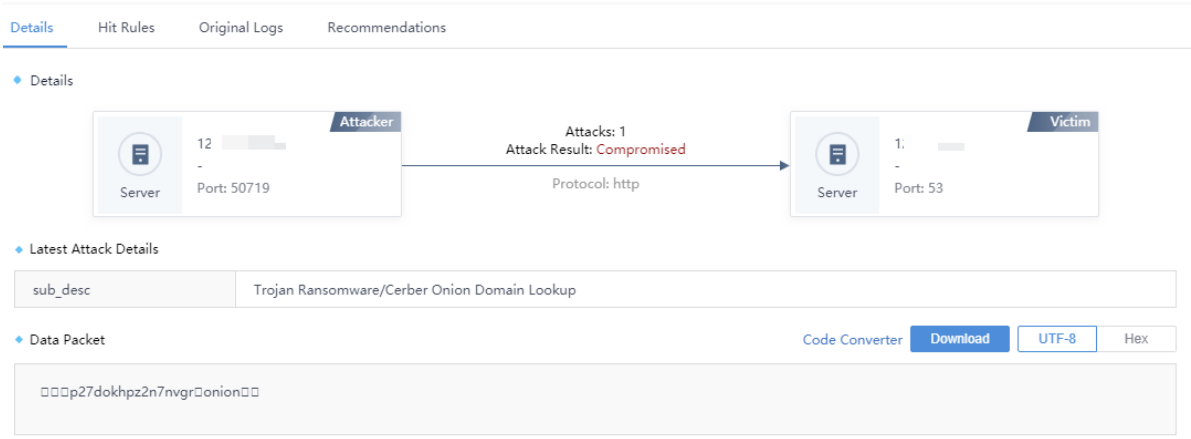
Basic information

You can view the status, threat type, severity, data source, and attack stage of the alert, as shown in the figure below.



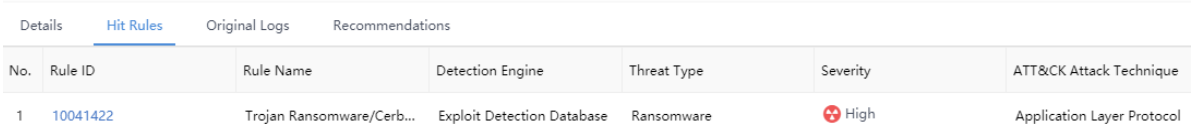
Details

You can view the attack direction, source IP, destination IP, and protocol on the <Details> tab. The latest alert details and data packet information are also displayed, as shown in the figure below.

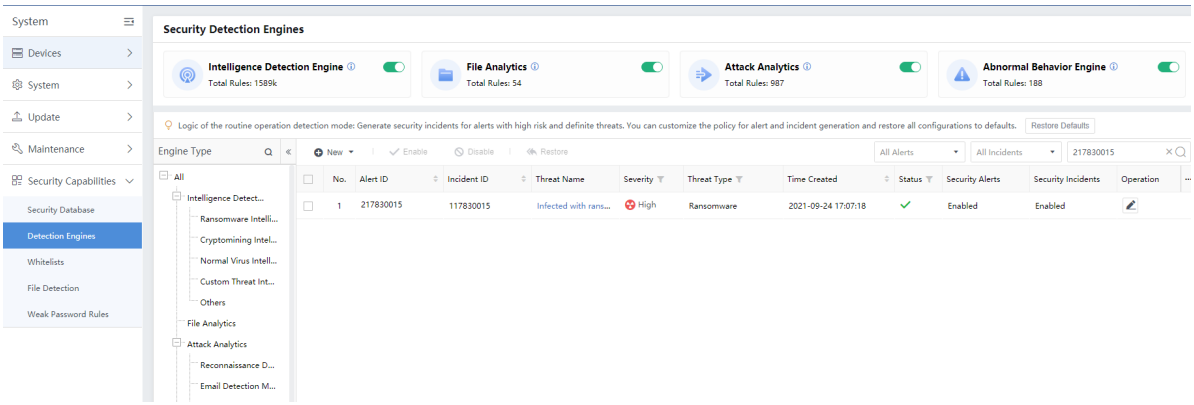


Hit rules

You can view the list of rules related to the event. Information such as the rule ID, rule name, detection engine, threat type, severity, and ATT&CK attack technique is displayed in the list, as shown in the figure below.

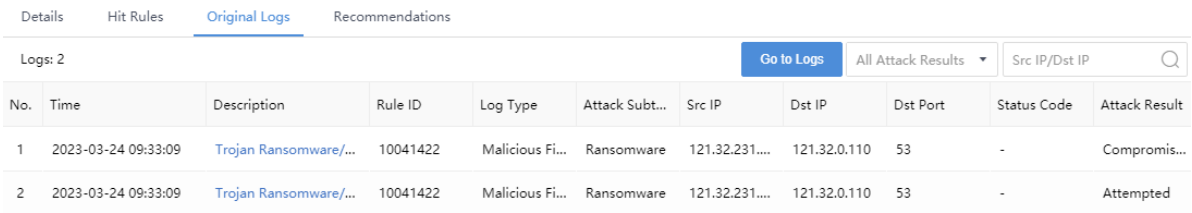


You can click a rule ID to go to [System/Security Capabilities/Detection Engines]. On the page that appears, you can view or edit the rule details, as shown in the figure below.

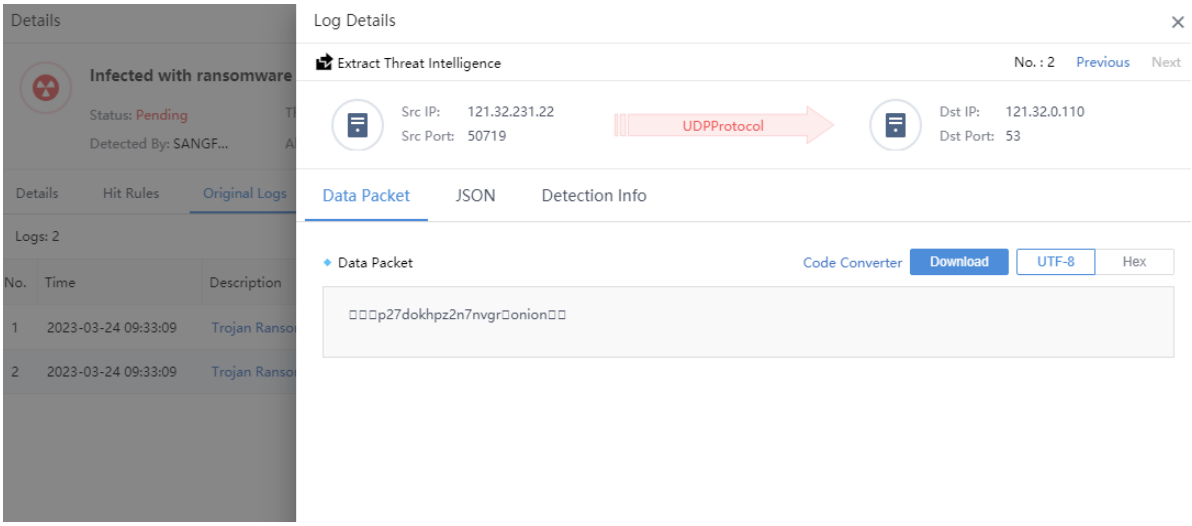


Original logs

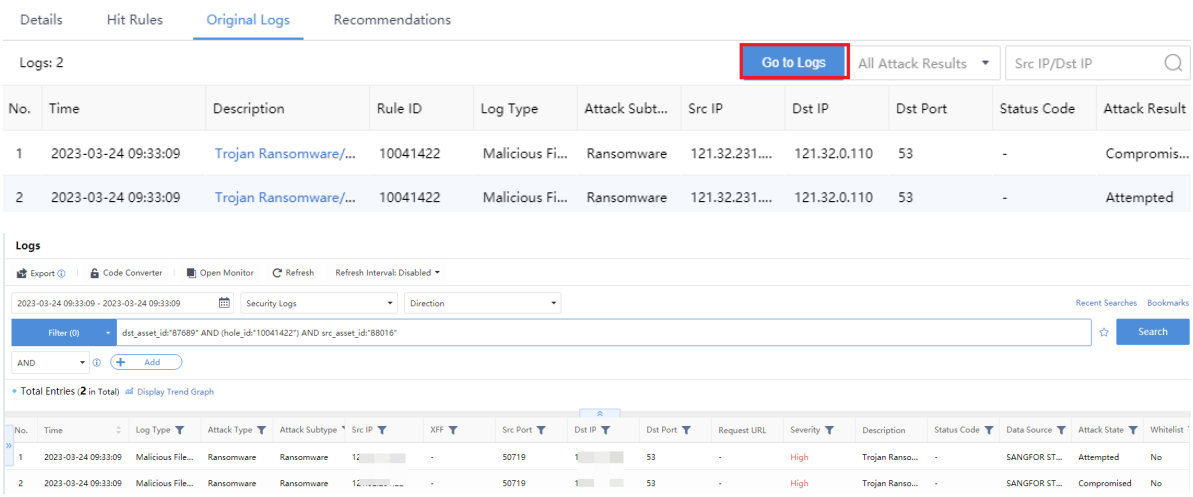
You can view the logs related to the alert, as shown in the figure below.



You can click the content in the "Description" column to view the original log information for higher judging efficiency, as shown in the figure below.

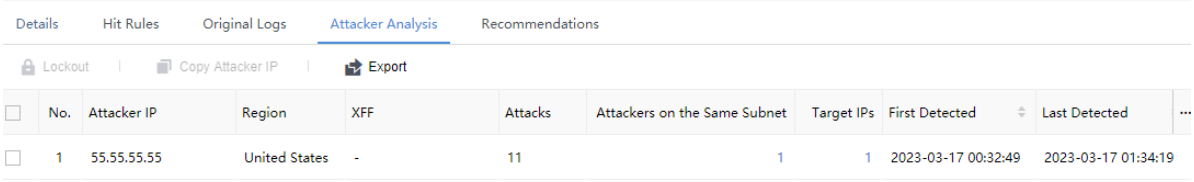


You can click <Go to Logs> to redirect to the <Logs> page and filter the logs related to this alert, as shown in the figure below.

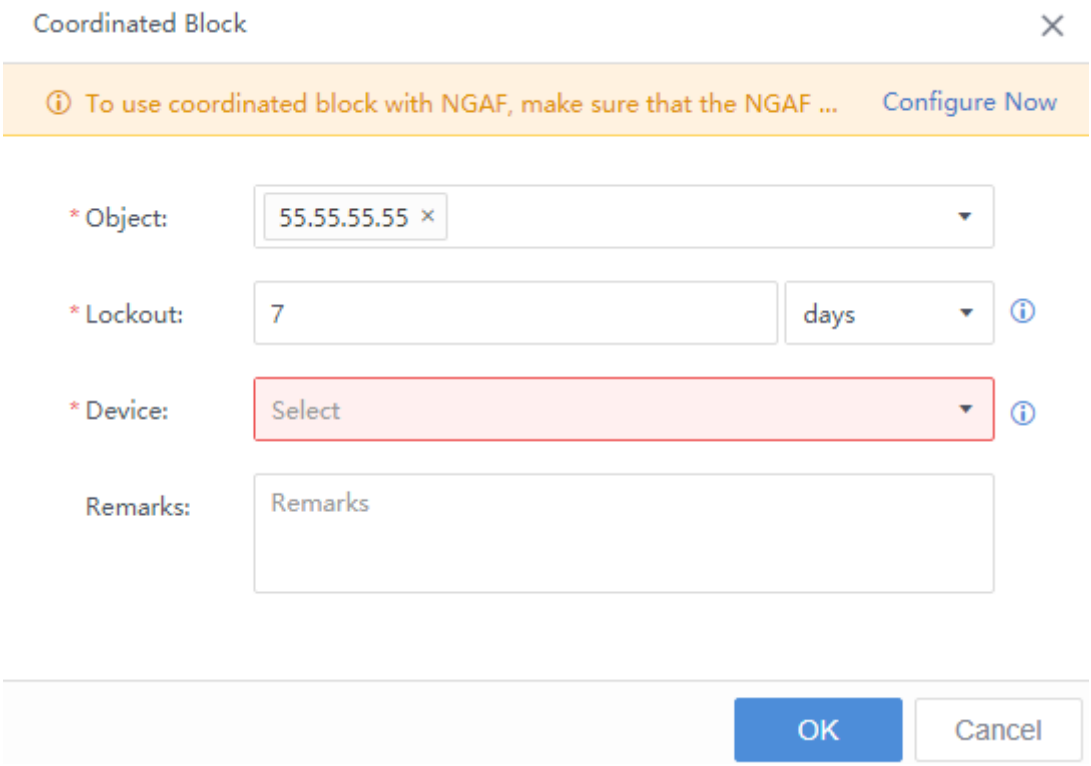


Attacker analysis

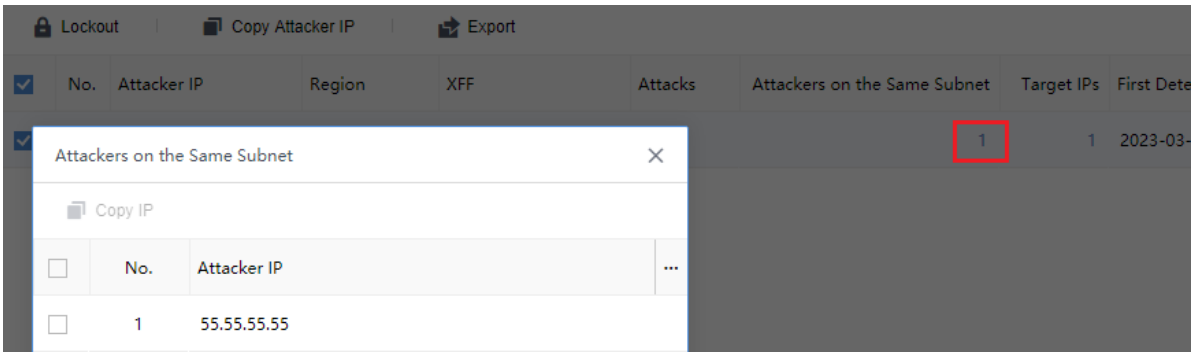
You can view the attacker IP address, region, attack count, attackers on the same subnet, target IP addresses, first attack time, last attack time, lockout status, and intelligence, as shown in the figure below.

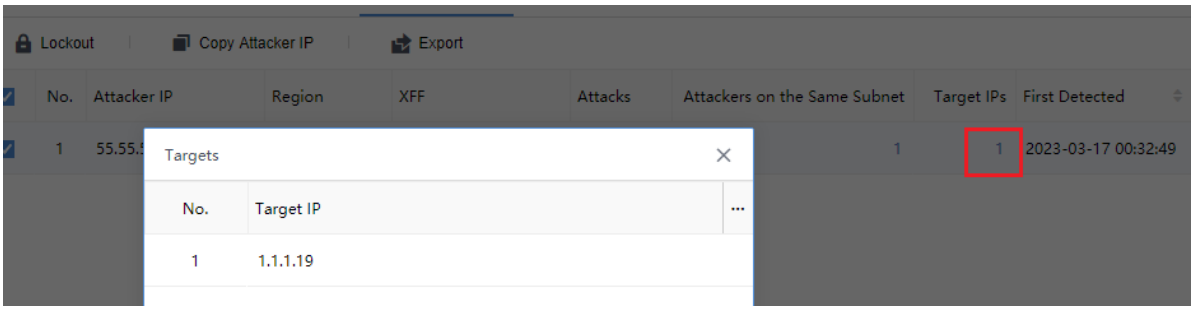


You can click <Lockout> or the < > icon in the [Operation] column to select the configured Next Generation Application Firewall (NGAF) for performing correlated block, as shown in the figure below.



You can click the value in the "Attackers on the Same Subnet" or "Target IPs" column to view the attacker IP addresses or target IP addresses, as shown in the figure below.

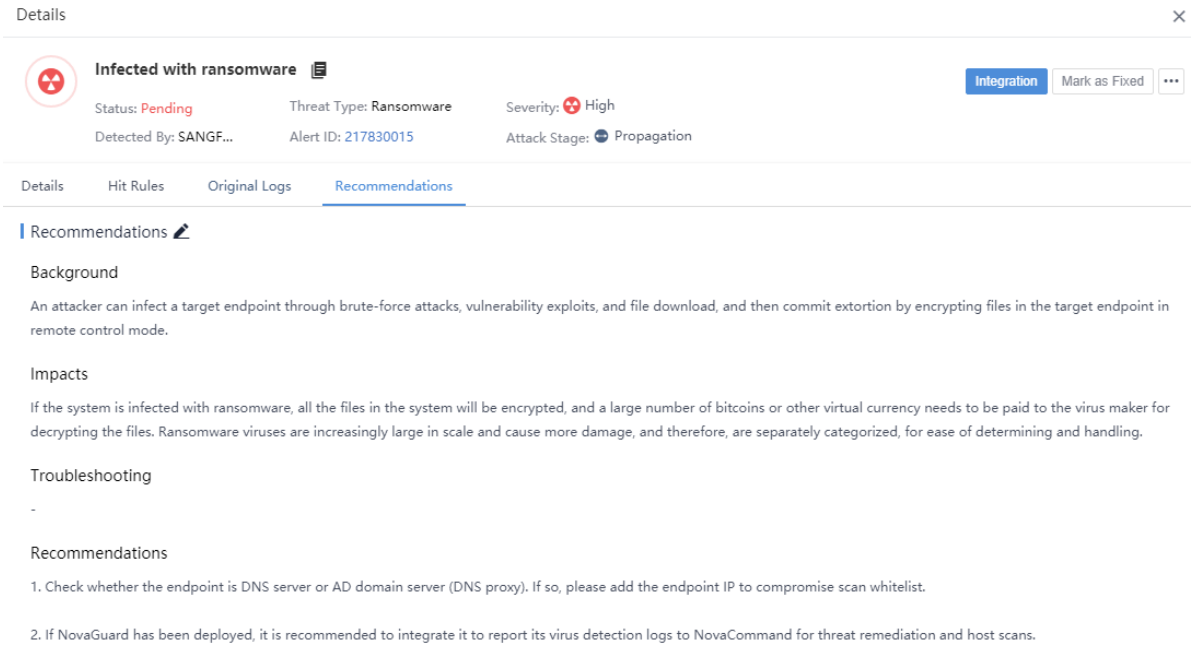




If multiple attacker IPs are associated with the alert, you can click <Export> to export the attacker IP list in the XLSX format.

Recommendations

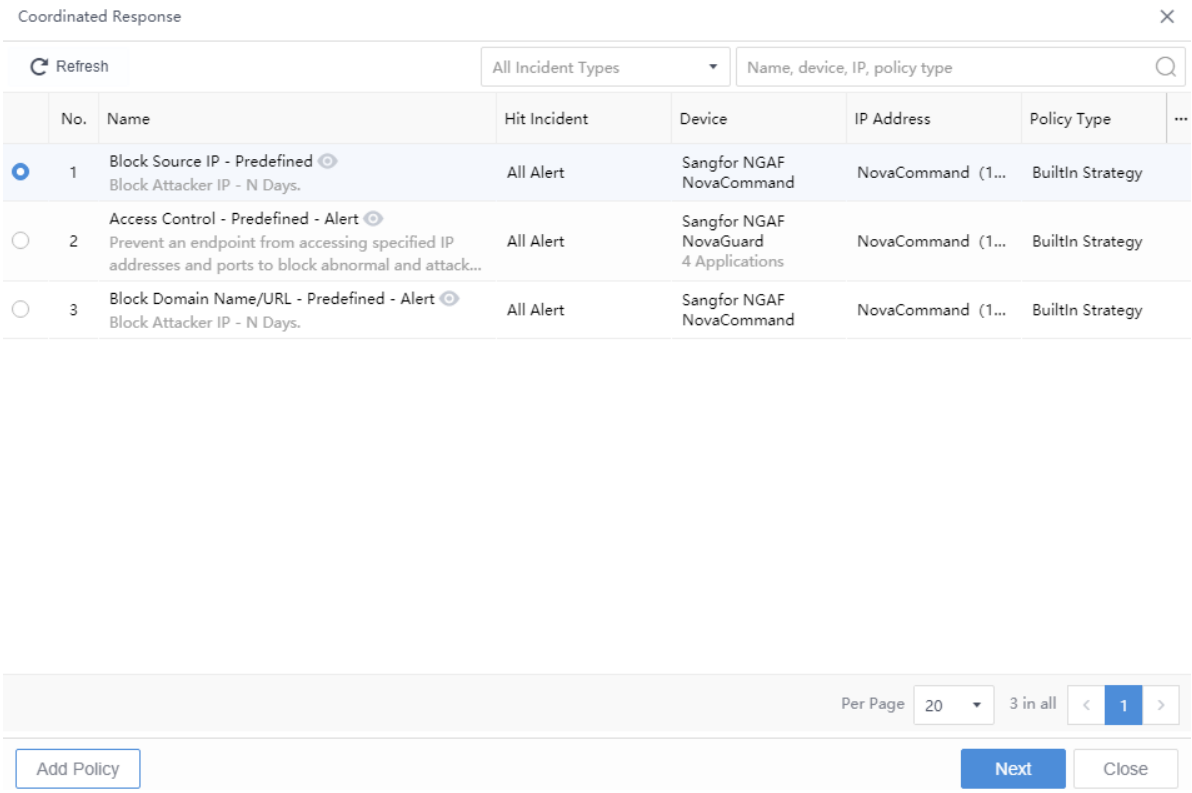
Troubleshooting and fixing suggestions are provided based on the alert background and impact, as shown in the figure below.



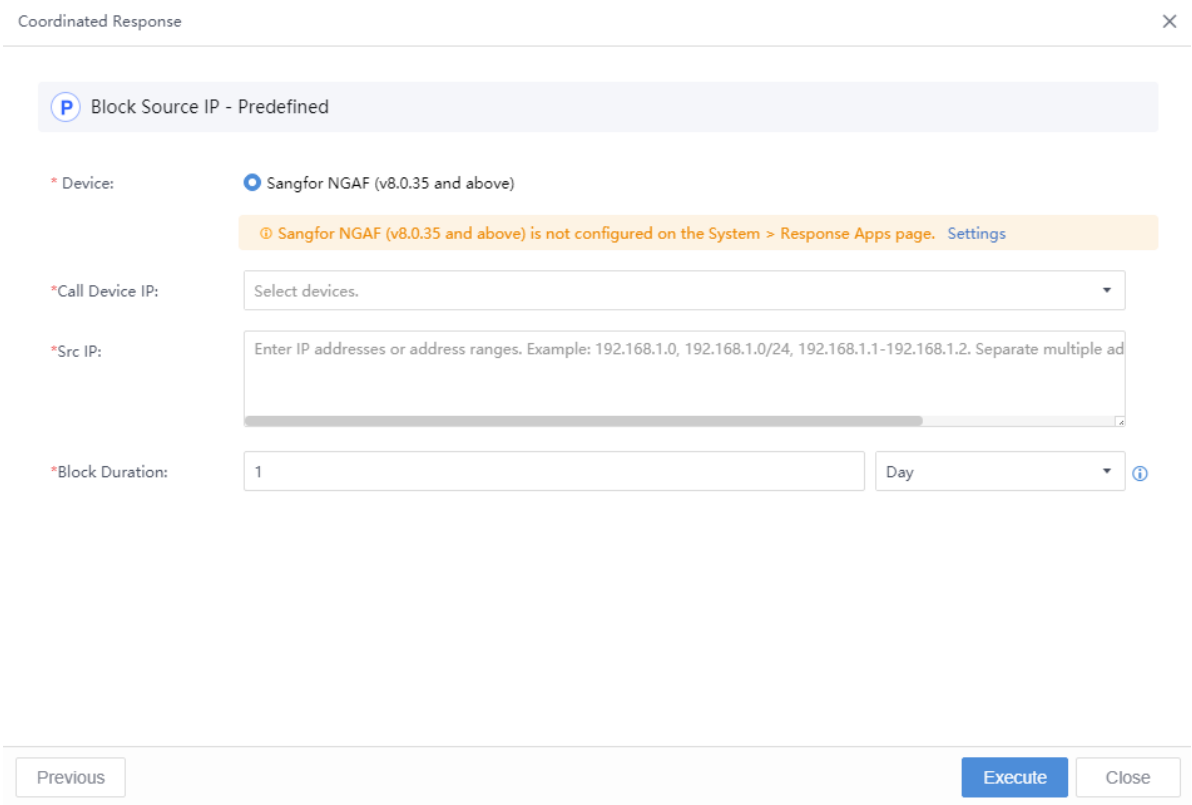
Alert Action

Coordinated response

On the <Ransomware> page,
you can click the <> icon in the [Operation] column to go to the Coordinated Response dialog box. You can fix the alert based on the coordinated response policy, as shown in the figure below.



You can click <Next> to select the correlated device and configure the block duration and other parameters. Then, you can click <Execute>. The figure below takes the policy for blocking source IP as an example.



Fields:

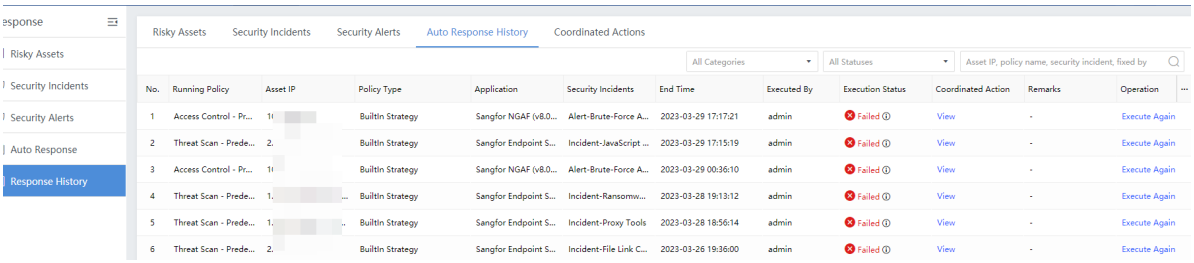
Call Device IP: The specific instance name and IP address. You can select the specific device IPs based on your requirements. All device IPs are selected by default. The instances correspond to the information on the [System/Devices/Response Apps] page.

Src IP: The source IP to be blocked. This field will be specified automatically.

Block Duration: You can set different values and select different units, such as day, hour, or minute, from the drop-down list.

The system prompts a message of <Executed> after execution.

You can go to [Response/Response History] and click the "Auto Response History" tab to view the execution history of corresponding policies, as shown in the figure below.

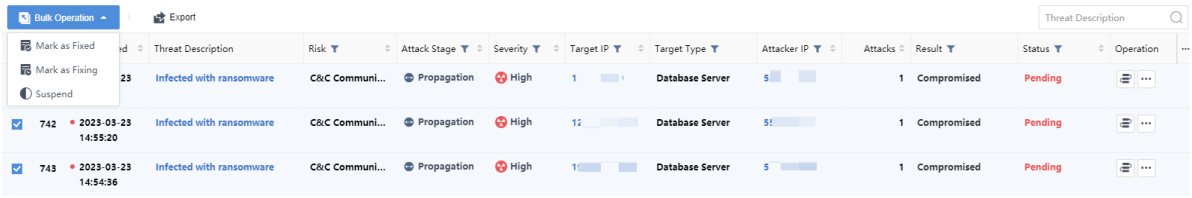


Manual operation

You can operate a single alert or multiple alerts in bulk.

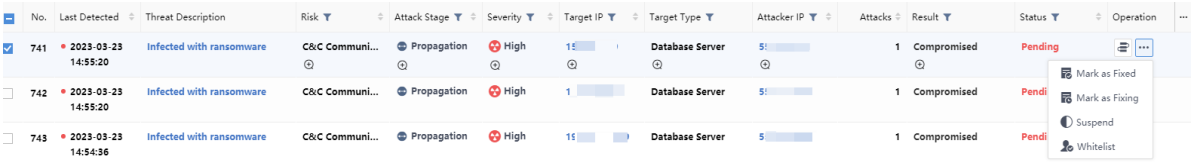
1. **Bulk**

You can click <Bulk Operation> for alert filtration based on the options in the drop-down list or select multiple alerts from the alert list directly to perform the bulk operation.



2. **Single**

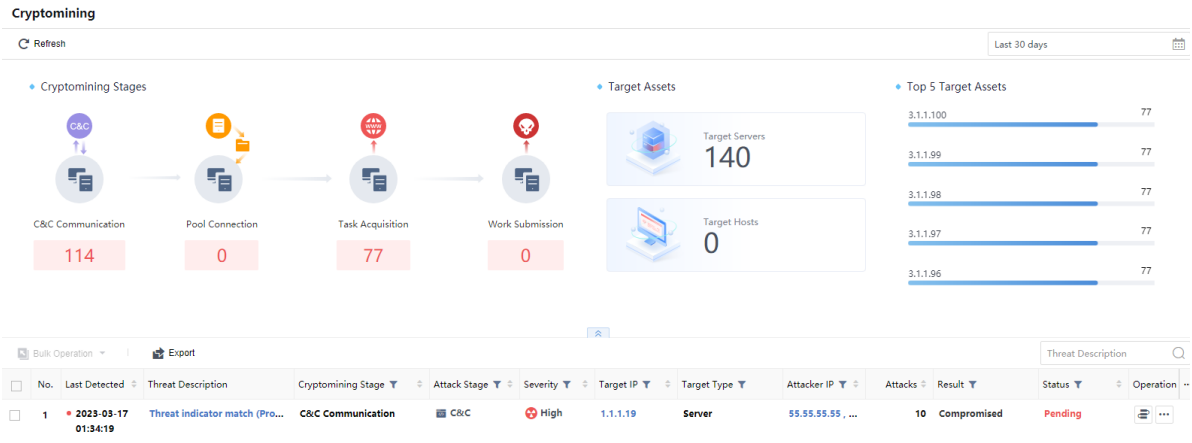
You can select one alert and click the <•••> icon in the [Operation] column. Available options include Mark as Fixed, Mark as Fixing, Suspend, and Whitelist, as shown in the figure below.



Cryptomining

Alert Display

Cryptomining detection can be used to analyze LAN cryptomining events. Cryptomining involves four stages, namely C&C communication, pool connection, task acquisition, and work submission, as shown in the figure below.



Alert Viewing

The alert list displays information such as cryptomining stage, attack stage, severity, target IP, target type, attacker IP, attacks, and result.

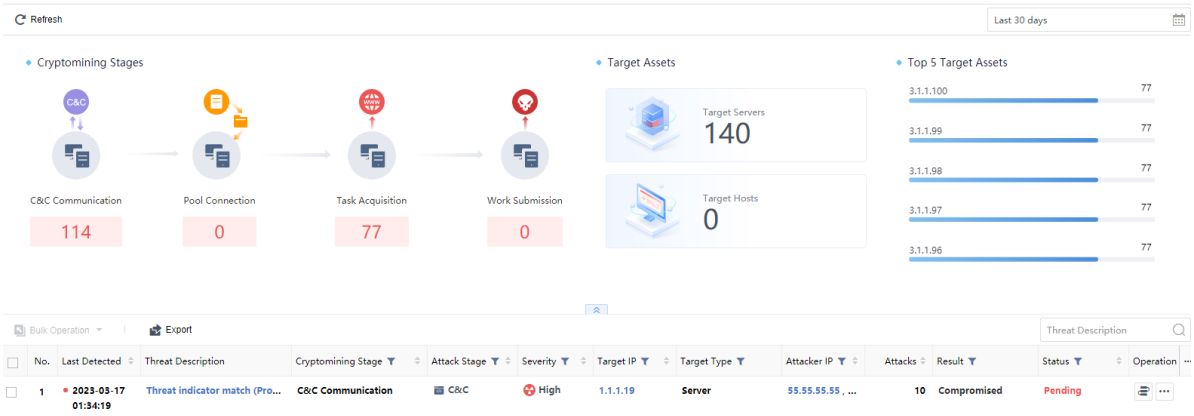
Cryptomining Stage: Includes C&C Communication, Pool Connection, Task Acquisition, and Work Submission.

Severity: Includes High, Medium, and Low.

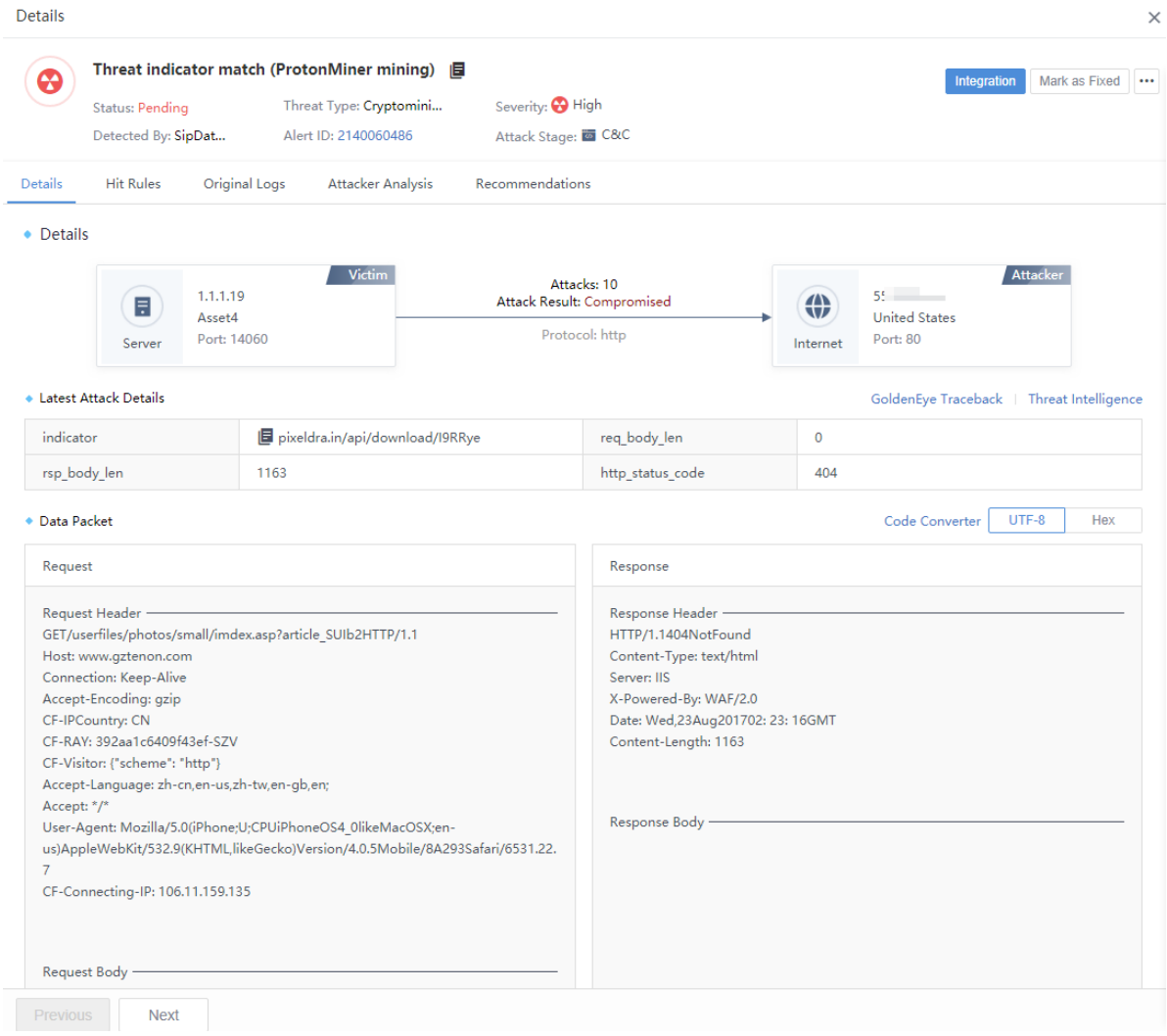
Target Type: Includes server asset and host asset.

Result: Includes Compromised, Succeeded, Failed, and To be Judged.

See the figure below.

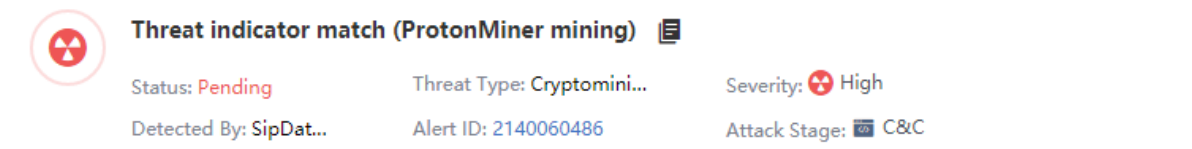


You can select a cryptomining alert and click the content in the <Threat Description> column to go to the <Details> page. The <Details> page has a basic information section and several tabs, including Details, Hit Rules, Original Logs, and Recommendations. The basic information section shows information such as the status, severity, data source, hit rule, and attack stage, as shown in the figure below.



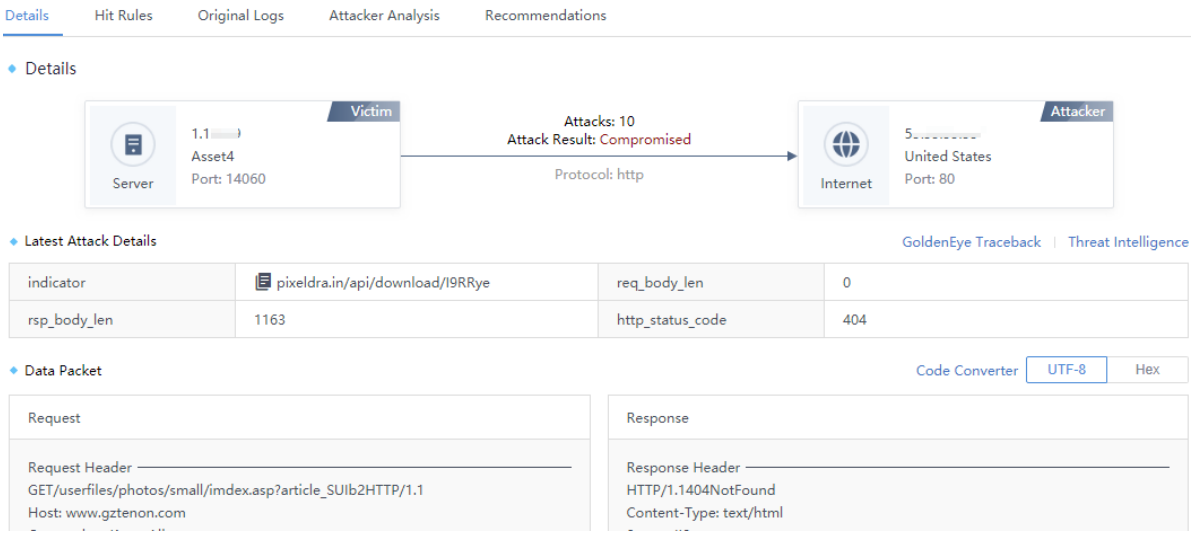
Basic information

You can view the status, threat type, severity, data source, and attack stage of the alert, as shown in the figure below.



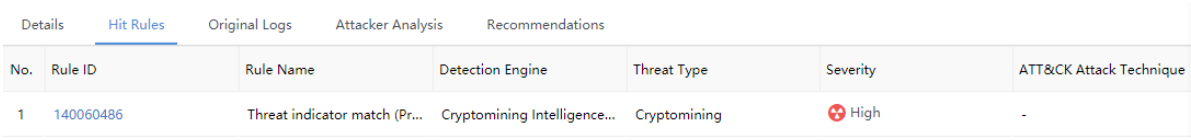
Details

You can view the attack direction, source IP, destination IP, and protocol in the <Details> tab. The latest alert details and data packet information are also displayed, as shown in the figure below.

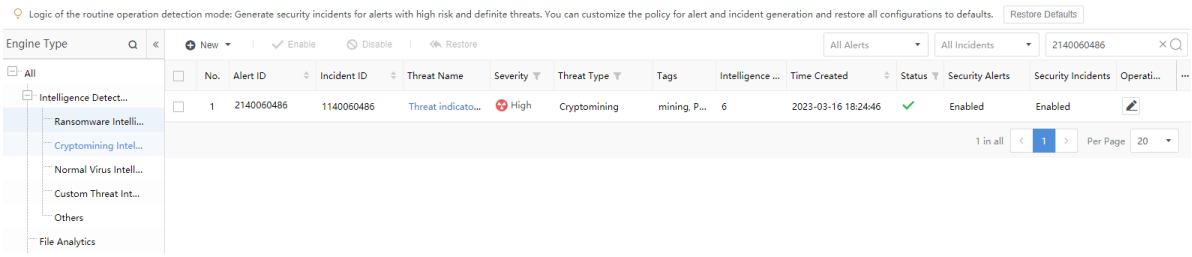


Hit rules

You can view the list of rules related to the event. Information such as the rule ID, rule name, detection engine, threat type, severity, and ATT&CK attack technique is displayed in the list, as shown in the figure below.

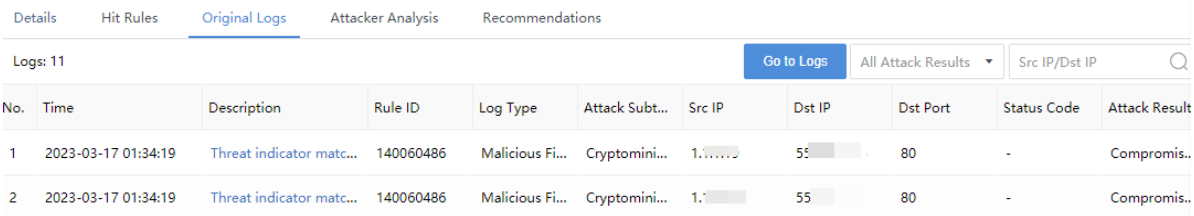


You can click a rule ID to go to [System/Security Capabilities/Detection Engines]. On the page that appears, you can view or edit the rule details, as shown in the figure below.

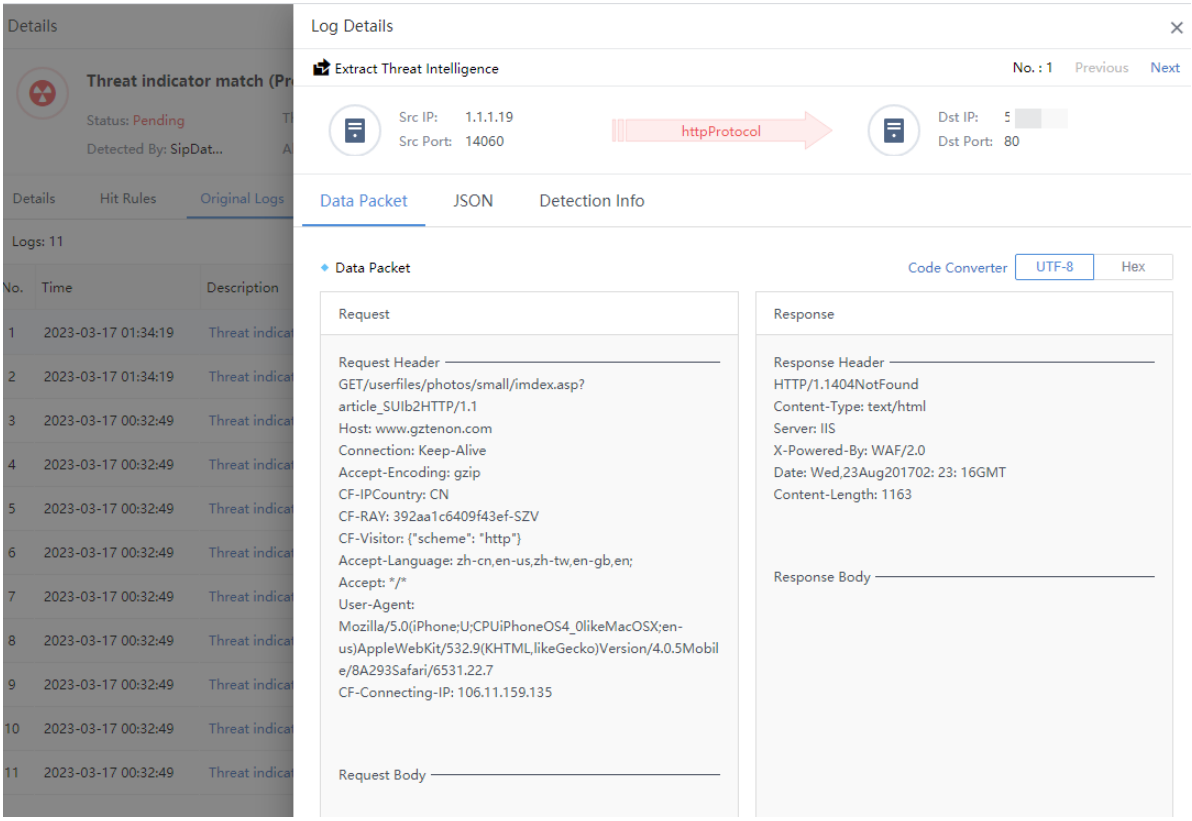


Original logs

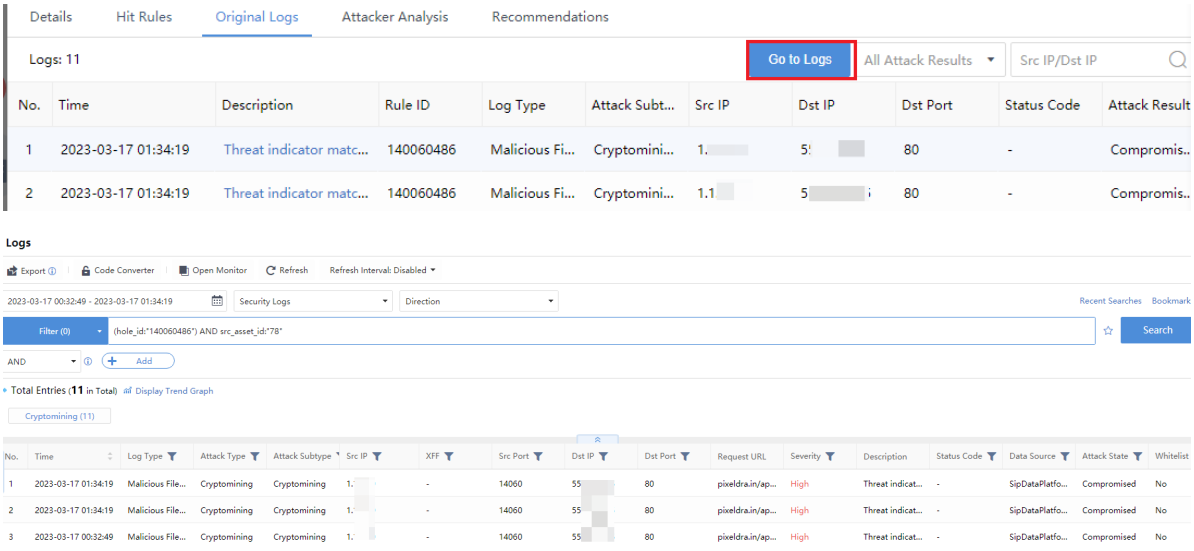
You can view the logs related to the alert, as shown in the figure below.



You can click the content in the "Description" column to view the original log information for higher judging efficiency, as shown in the figure below.

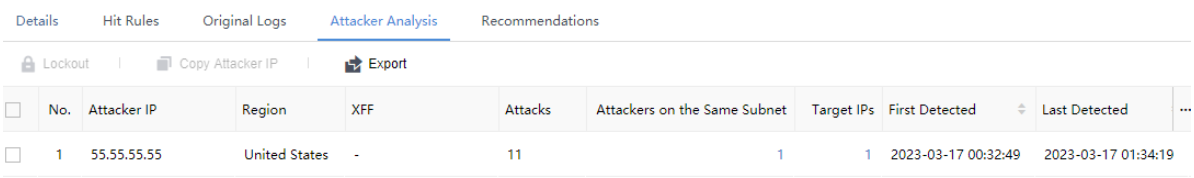


You can click <Go to Logs> to redirect to the <Logs> page and filter the logs related to this alert, as shown in the figure below.

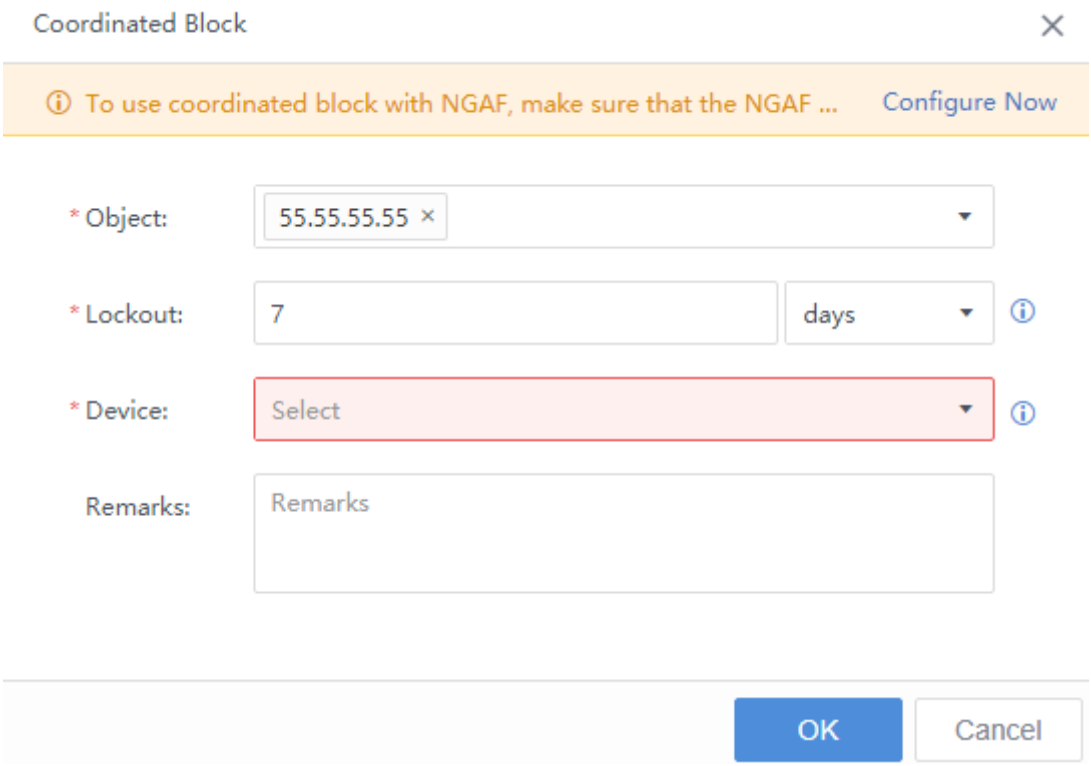


Attacker analysis

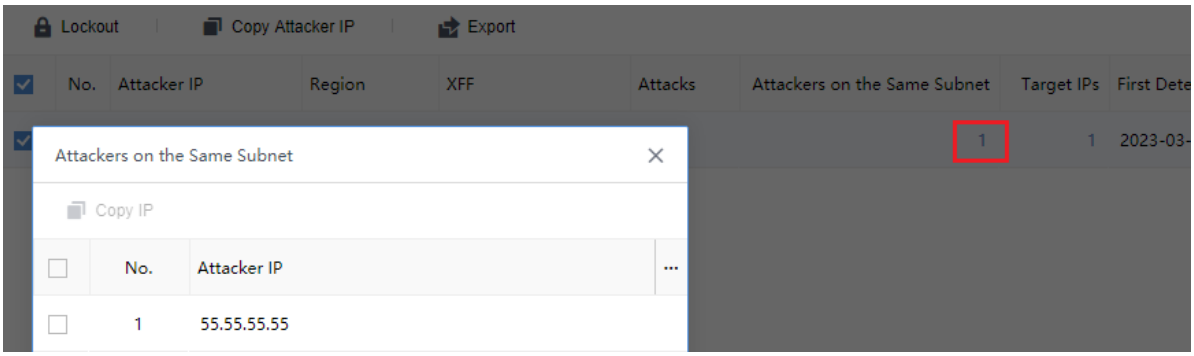
You can view the attacker IP address, region, attack count, attackers on the same subnet, target IP addresses, first attack time, last attack time, lockout status, and intelligence, as shown in the figure below.

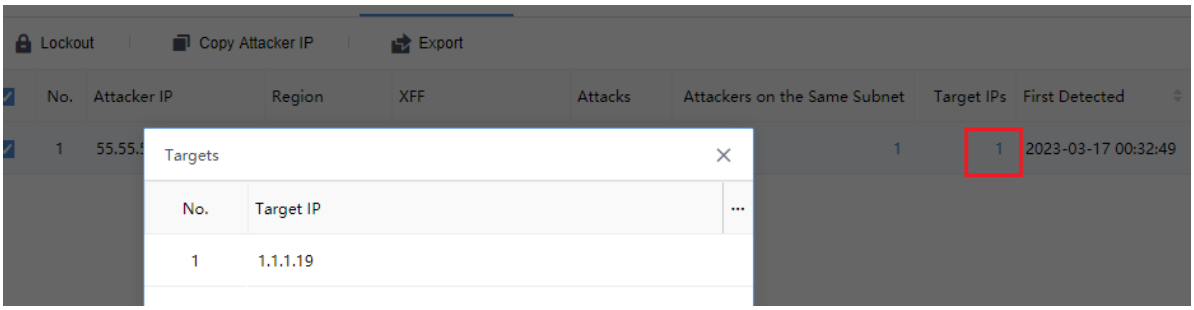


You can click <Lockout> or the < 🔒 > icon in the [Operation] column to select the configured Next Generation Application Firewall (NGAF) for performing correlated block, as shown in the figure below.



You can click the value in the "Attackers on the Same Subnet" or "Target IPs" column to view the attacker IP addresses or target IP addresses, as shown in the figure below.

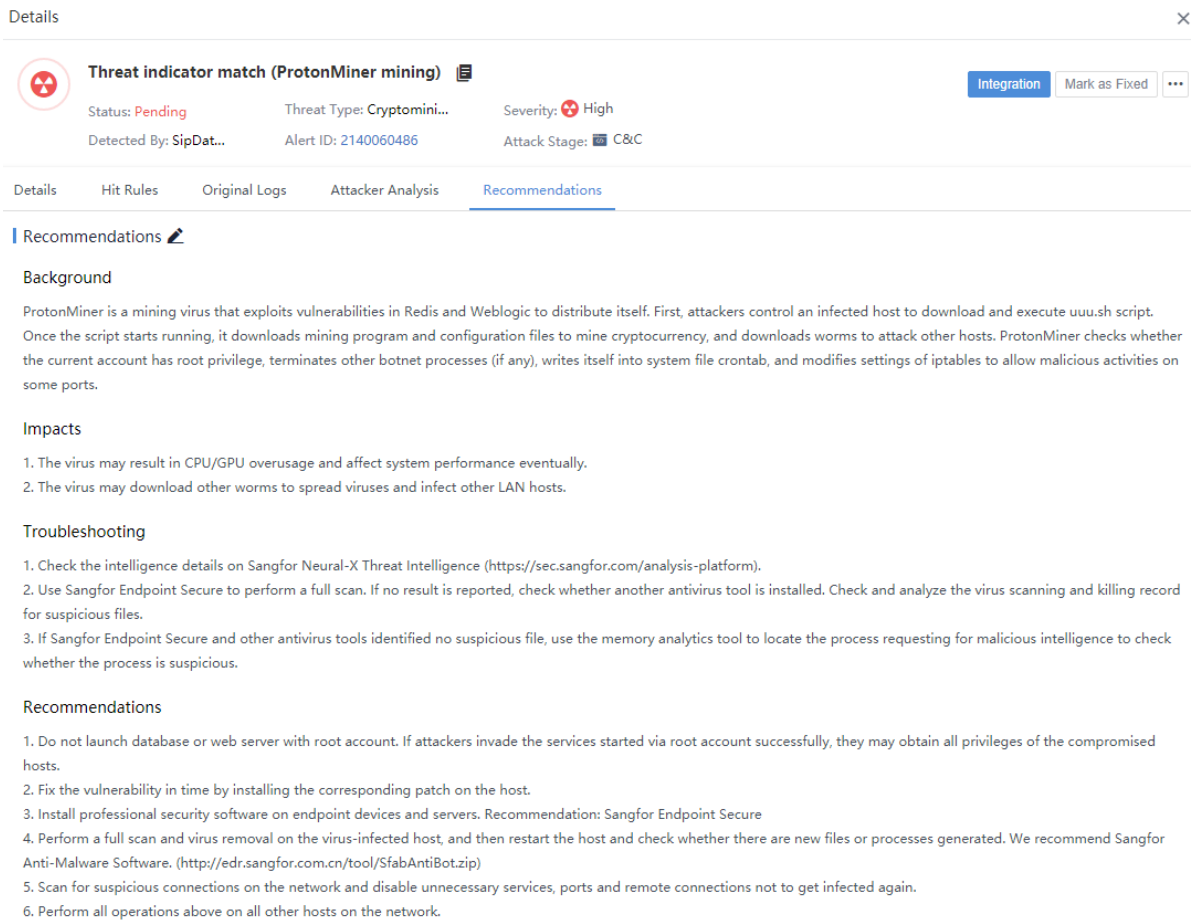




If multiple attacker IPs are associated with the alert, you can click <Export> to export the attacker IP list in the XLSX format.

Recommendations

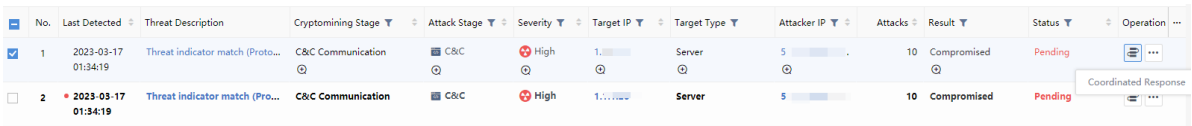
Troubleshooting and fixing suggestions are provided based on the alert background and impact, as shown in the figure below.



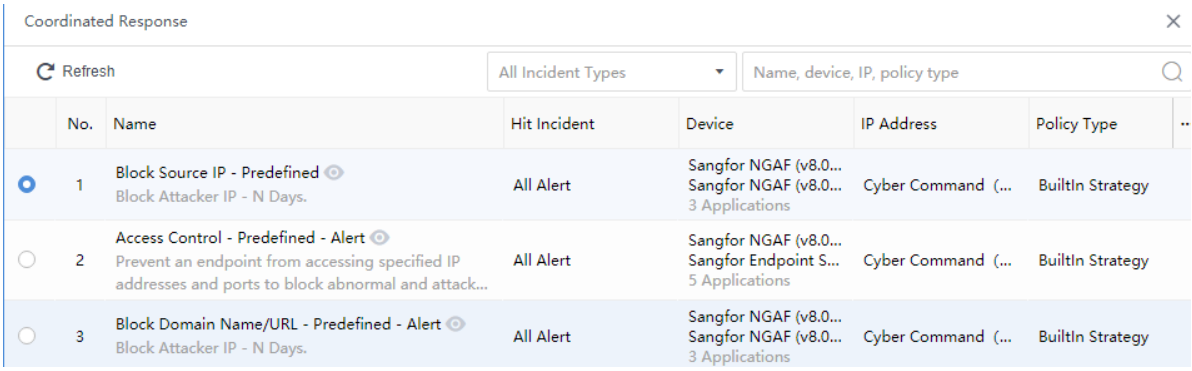
Alert Action

Coordinated response

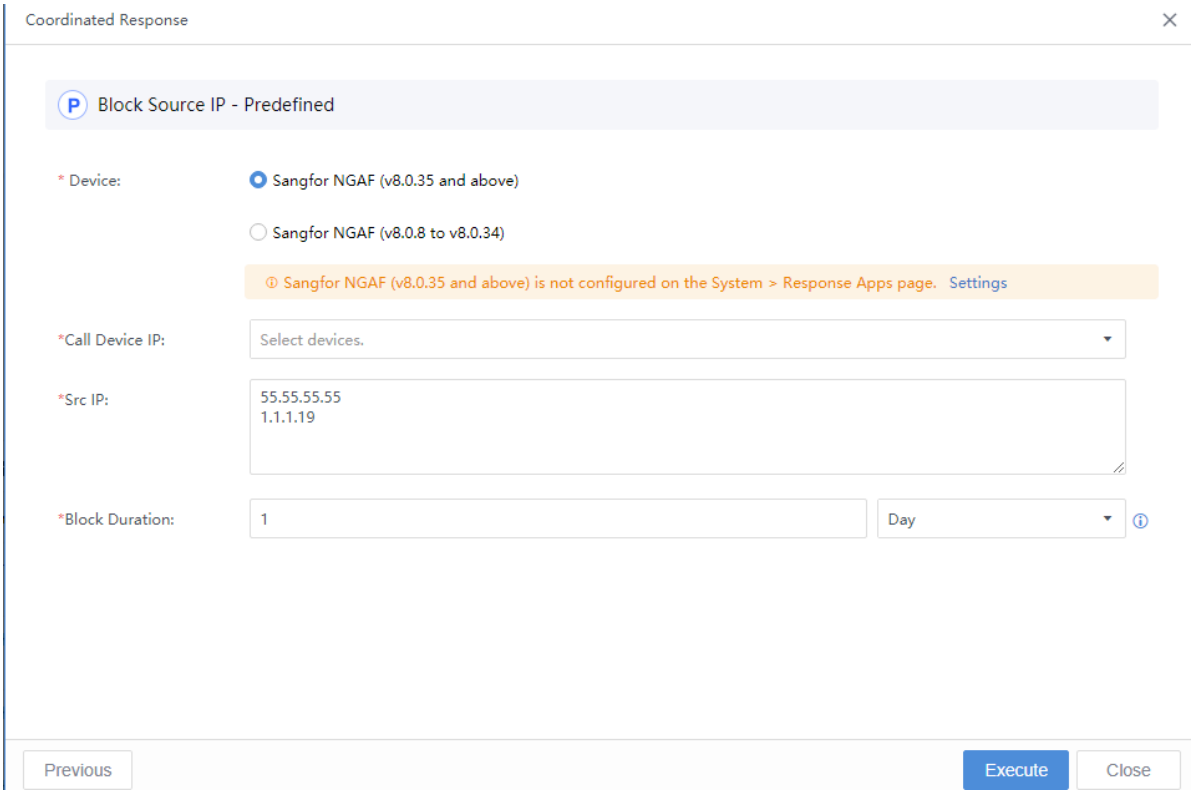
On the <Cryptomining> page, you can click the < > icon in the [Operation] column to go to the Coordinated Response dialog box. You can fix the alert based on the coordinated response policy, as shown in the figure below.



The figure below takes the policy for blocking source IP as an example.



You can click <Next> to select the correlated device, configure the block duration and other parameters, and click <Execute>, as shown in the figure below.



Fields:

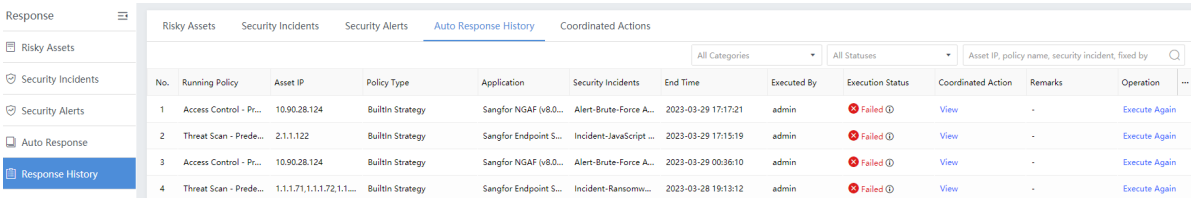
Call Device IP: The specific instance name and IP address. You can select the specific device IPs based on your requirements. All device IPs are selected by default. The instances correspond to the information on the [System/Devices/Response Apps] page.

Src IP: The source IP to be blocked. This field will be specified automatically.

Block Duration: You can set different values and select different units, such as day, hour, or minute, from the drop-down list.

The system prompts a message of <Executed> after execution.

You can go to [Response/Response History] and click the "Auto Response History" tab to view the execution history of corresponding policies, as shown in the figure below.

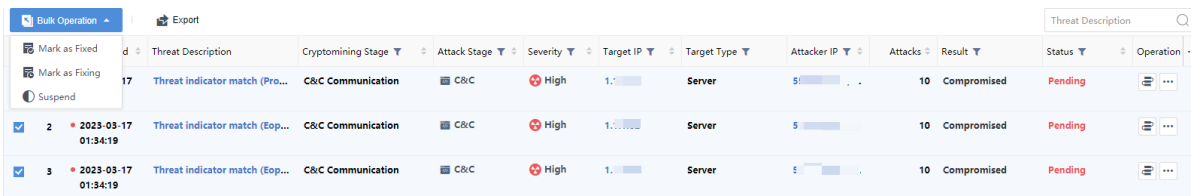


Manual operation

You can operate a single alert or multiple alerts in bulk.

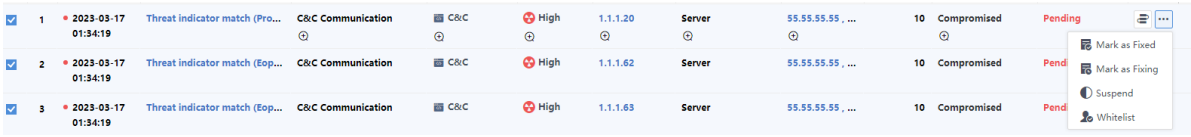
1. Bulk

You can click <Bulk Operation> for alert filtration based on the options in the drop-down list or select multiple alerts from the alert list directly to perform the bulk operation.



2. Single

You can select one alert and click the < ... > icon in the [Operation] column. Available options include Mark as Fixed, Mark as Fixing, Suspend, and Whitelist, as shown in the figure below.



File Threats

In a typical attack chain, file threats are an important part. Attackers use virus-attached files to infect LAN endpoints. Once the malicious file is executed, the attacker can control the endpoint or steal sensitive information. Nova Command can use the file threat analytics function to display the overall file threat situation and further analyze specific file threat events.

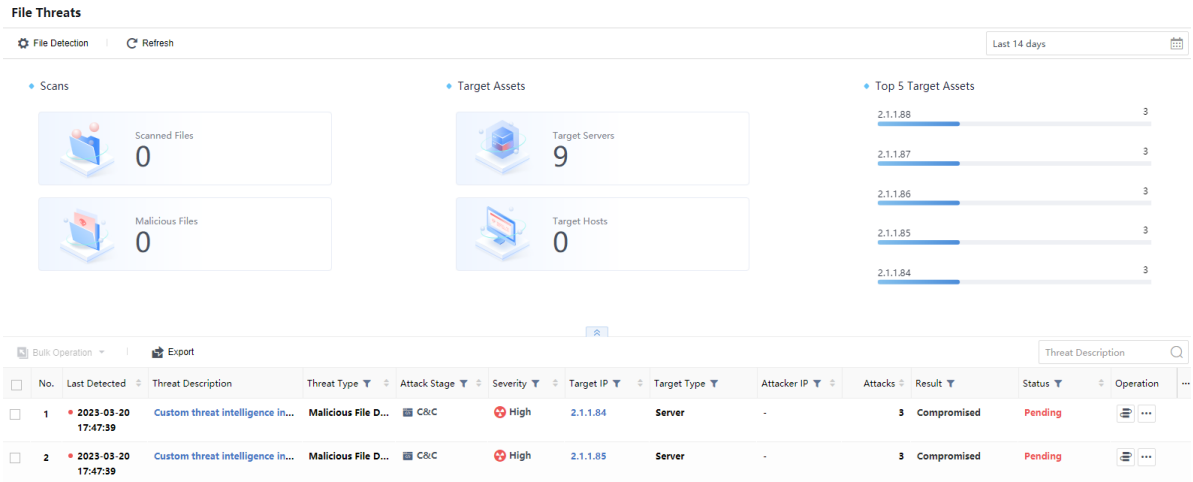
Cloud Sandbox Detection

Website allowing

To use the cloud sandbox detection function, you need to allow the following domain names for Nova Command.\
auth.sangfor.com.cn\
analysis.sangfor.com.cn\
ti.sangfor.com.cn

Function description

You can upload suspicious local files to the cloud and use the cloud sandbox detection function for detection and analysis. The results will be displayed on Nova Command. Currently, the file size for detection cannot exceed 20 MB, and the supported file formats are shown in the figure below.

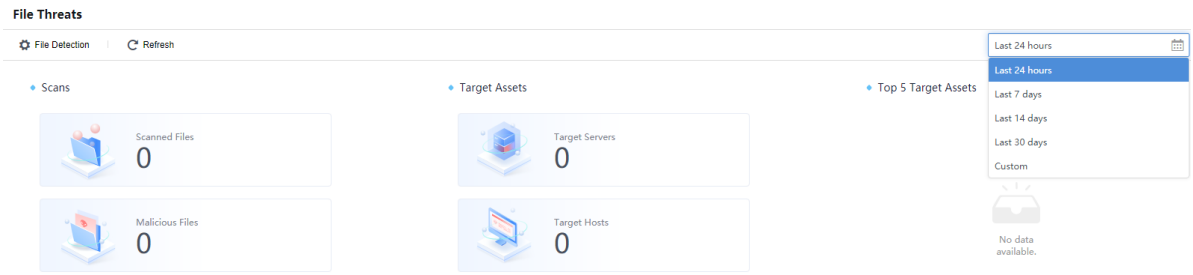


Alert Display

On the [Detection/Threats/File Threats] page, you can click <Export> to export the file threat alerts as a sheet. You can also filter file threat alerts by time period, as shown in the figure below.

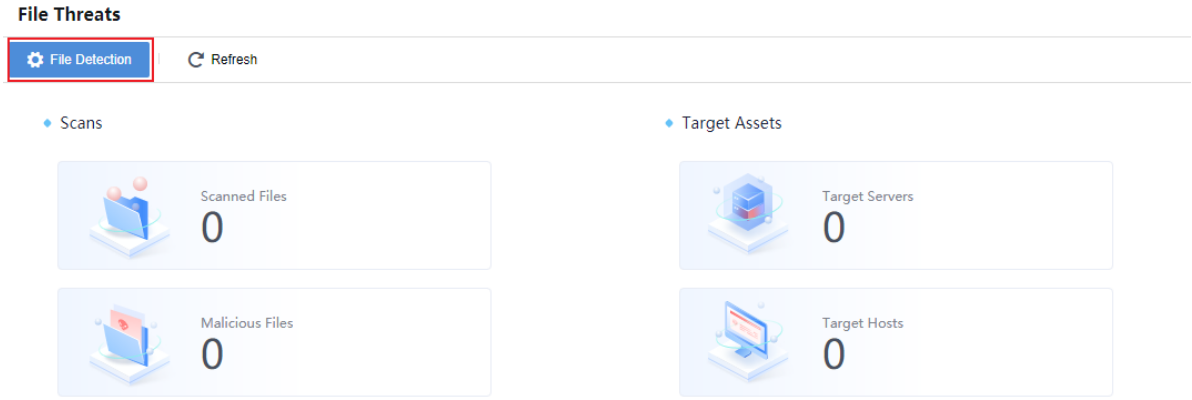
Export: A maximum of 10,000 alerts can be exported as an EXCEL file.

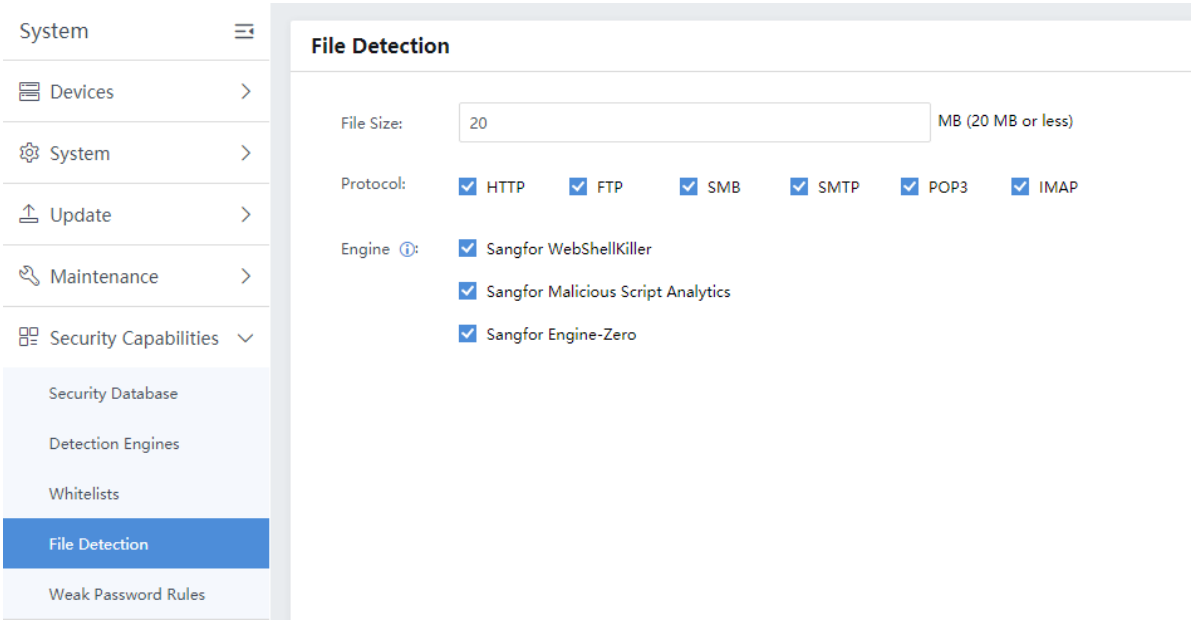
Time Period Selection: You can select Last 30 days, Last 7 days, and Today from the drop-down list.



File detection

You can click <File Detection> to go to the [System/Security Capabilities/File Detection] page, as shown in the figures below.





1. File analysis settings:

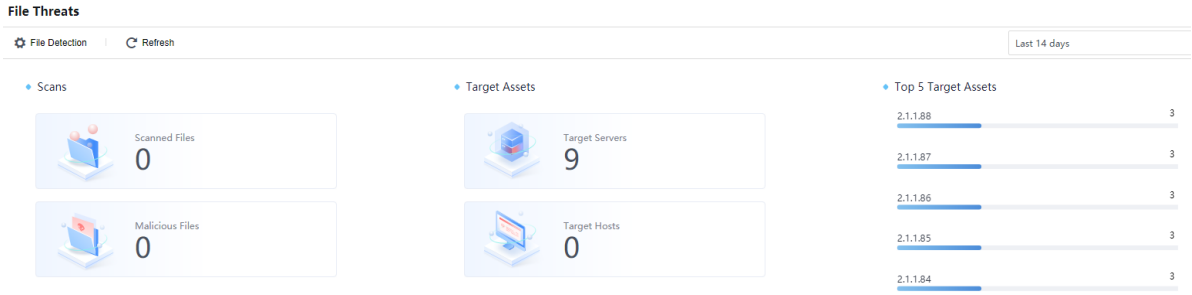
<File Size>: You can set the size of the file for detection. The file size cannot be greater than 20 MB.

<Protocol>: You can filter files by selecting the protocol used by Nova Sensor or cloud sandbox for specified audits.

2. File detection engine settings:

<Engine>: You can select a detection engine as needed. Currently, three engines, namely Sangfor WebShellKiller, Sangfor Malicious Script Analytics, and Sangfor Engine-Zero, are available.

You can know the number of scanned files and malicious files in the specified time period on the [Detection/Threats/File Threats] page, as shown in the figure below.



Alert Viewing

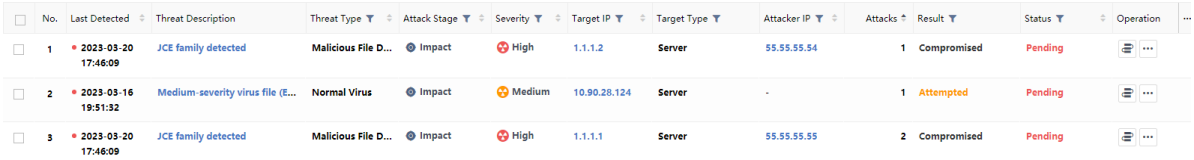
The alert list displays information such as the threat description, threat type, attack stage, severity, target IP, target type, attacker IP, attacker type, attacks, result, and status.

Threat Type: Includes Malicious File Download and LAN Transmission Virus.

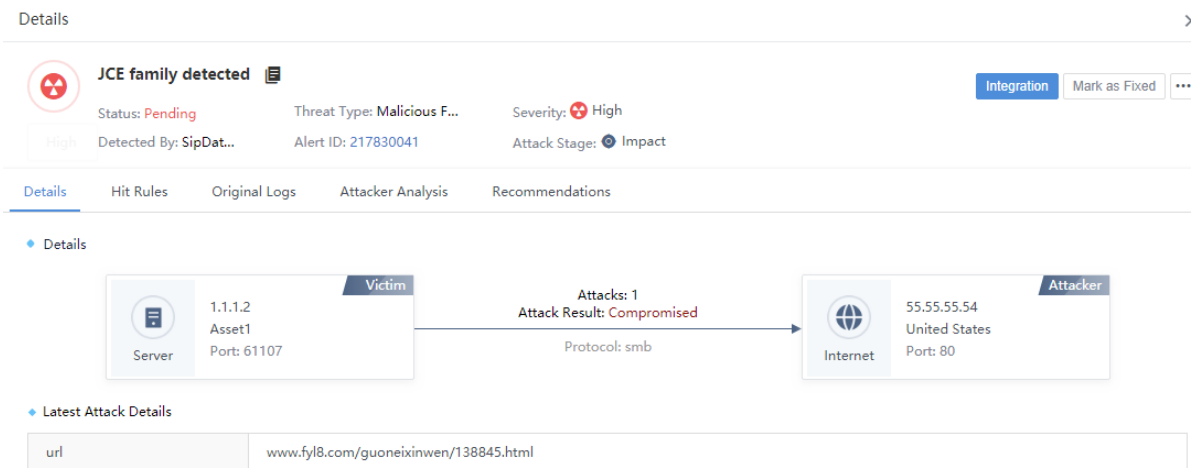
<Severity>: Includes High, Medium, and Low.

<Attack Stage>: The attack stage to which the threat belongs.

See the figure below.

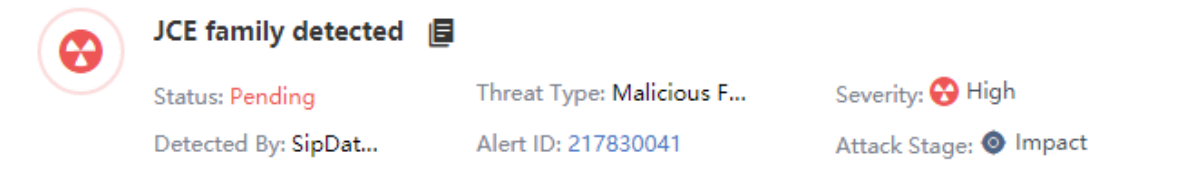


You can select a file threat alert and click the content in the <Threat Description> column to go to the <Details> page. The <Details> page has a basic information section and several tabs, including Details, Hit Rules, Original Logs, Attacker Analysis, and Recommendations, as shown in the figure below.



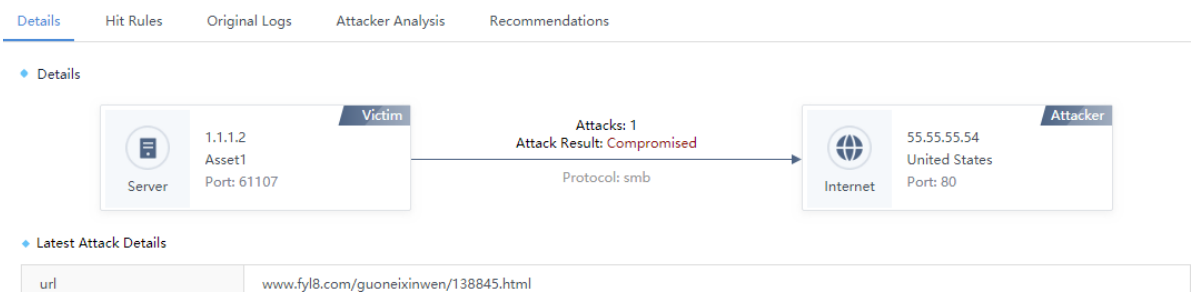
Basic information

You can view the status, threat type, severity, data source, and attack stage of the alert, as shown in the figure below.



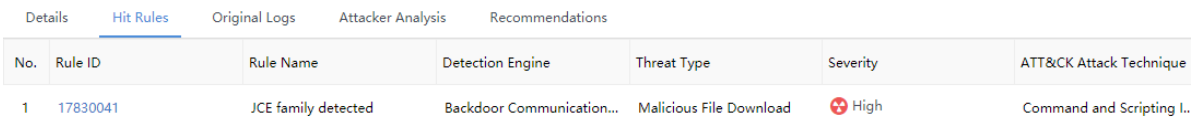
Details

You can view the attacker IP and port, target IP and port, file path, threat name, process parameter, and detection engine, as shown in the figure below.

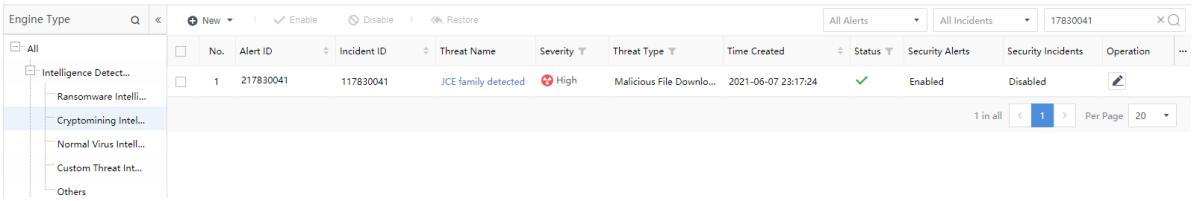


Hit rules

You can view the rule ID list related to the alert, containing information such as rule ID, rule name, detection engine, threat type, severity, and ATT&CK attack technique, as shown in the figure below.

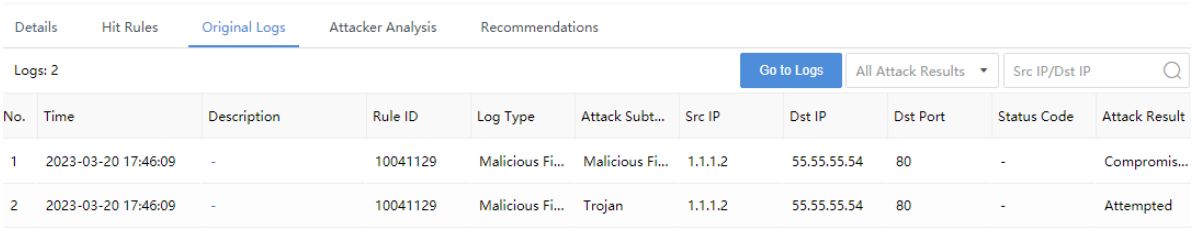


You can click a rule ID to go to [System/Security Capabilities/Detection Engines]. On the page that appears, you can view or edit the rule details, as shown in the figure below.

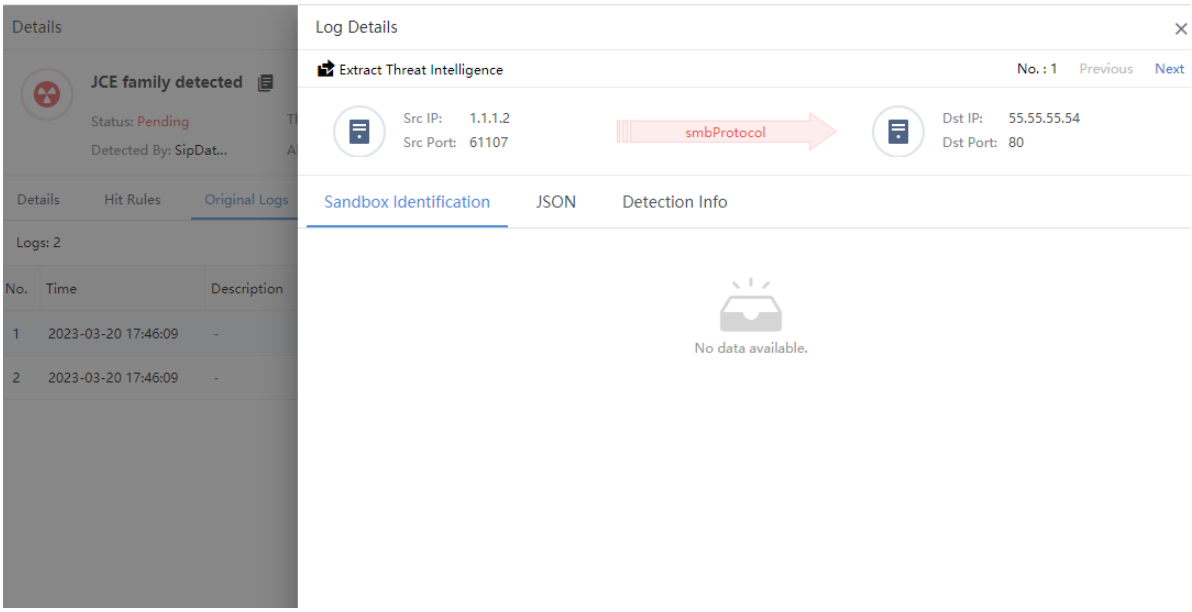


Original logs

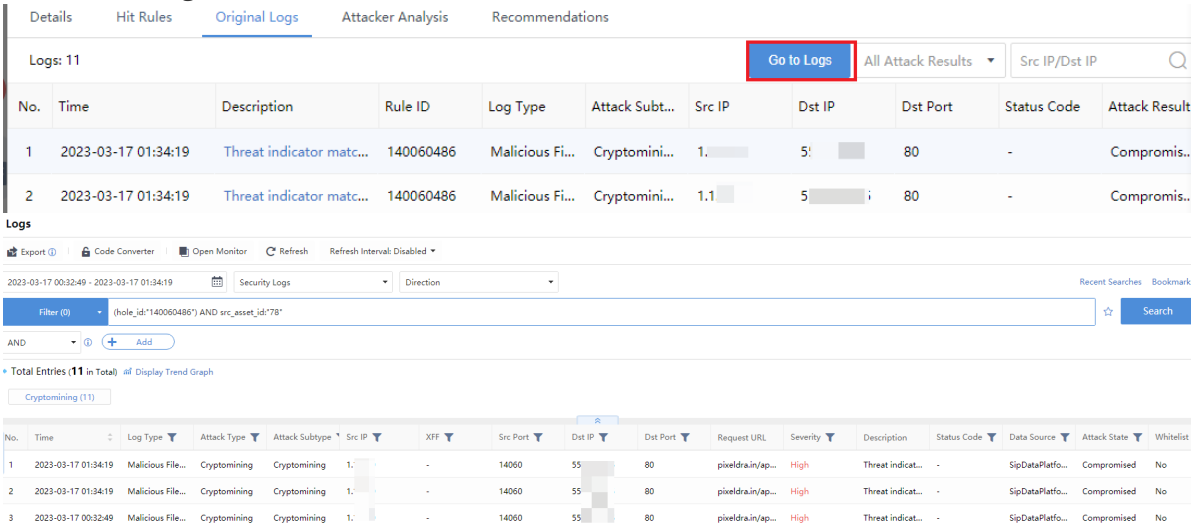
You can view the logs related to the alert, as shown in the figure below.



You can click the content in the "Description" column to view the original log information for higher judging efficiency, as shown in the figure below.

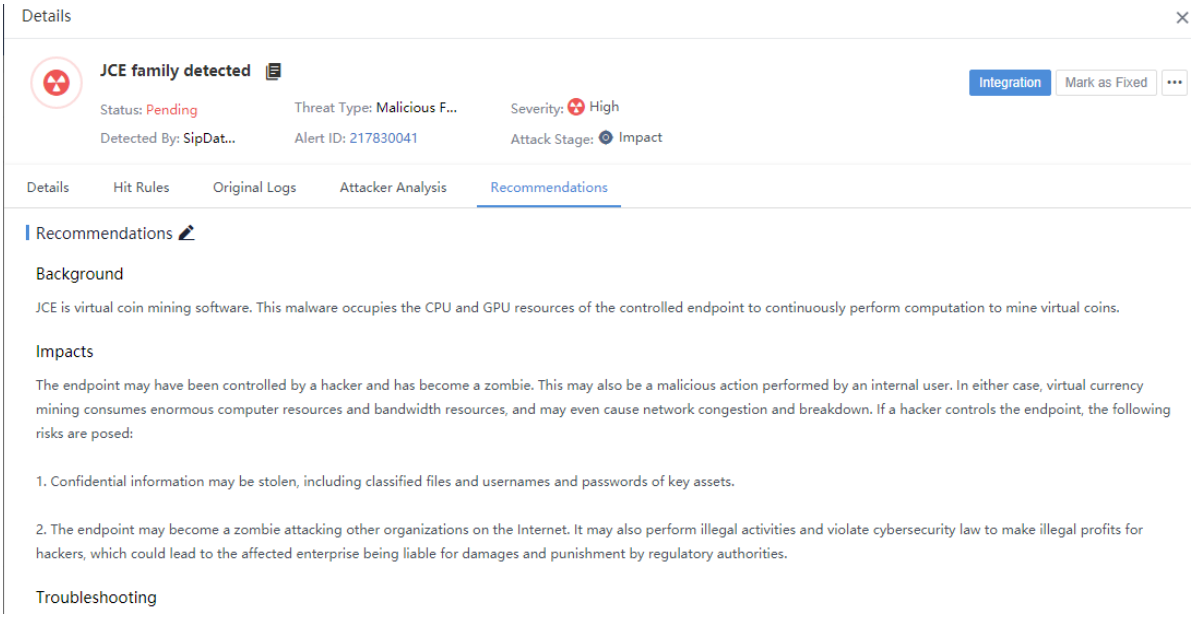


You can click <Go to Logs> to redirect to the <Logs> page and filter the logs related to this alert, as shown in the figure below.



Recommendations

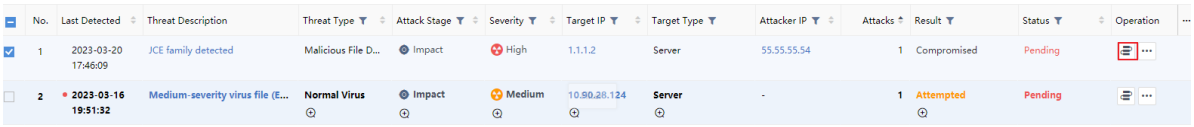
Troubleshooting and fixing suggestions are provided based on the alert background and impact, as shown in the figure below.



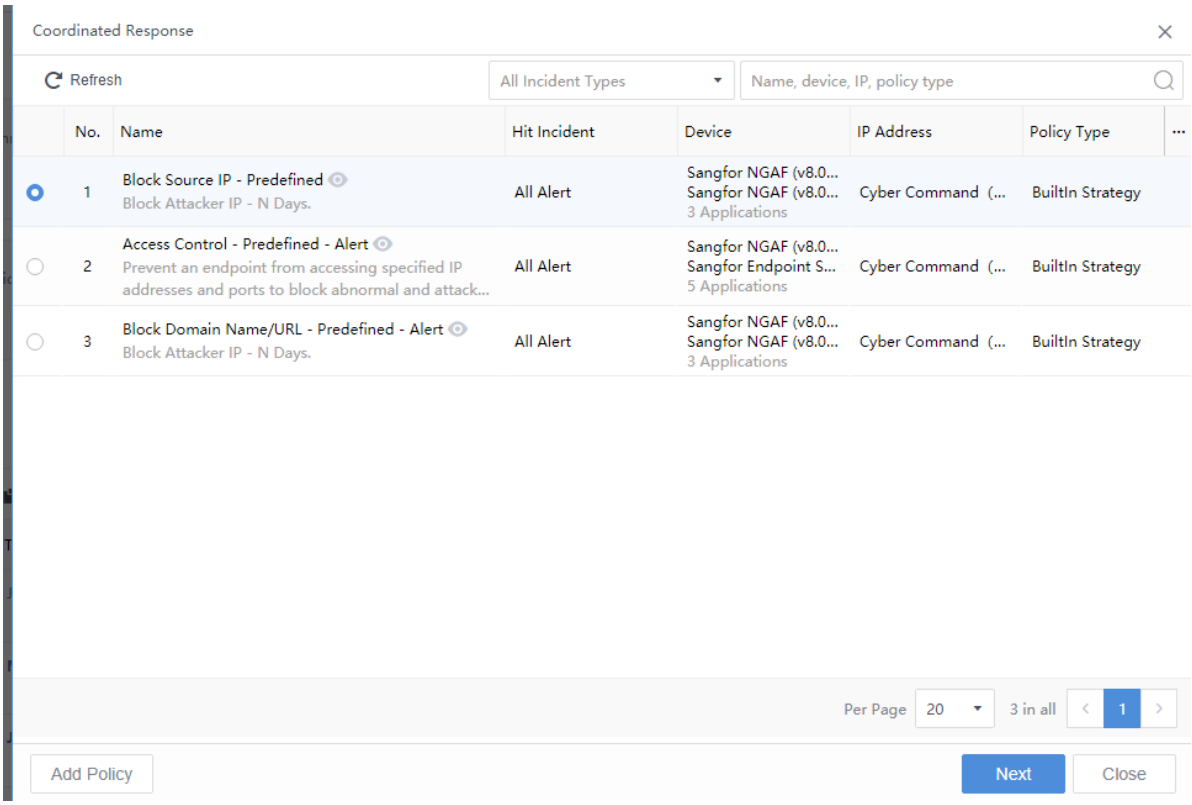
Alert Action

Coordinated response

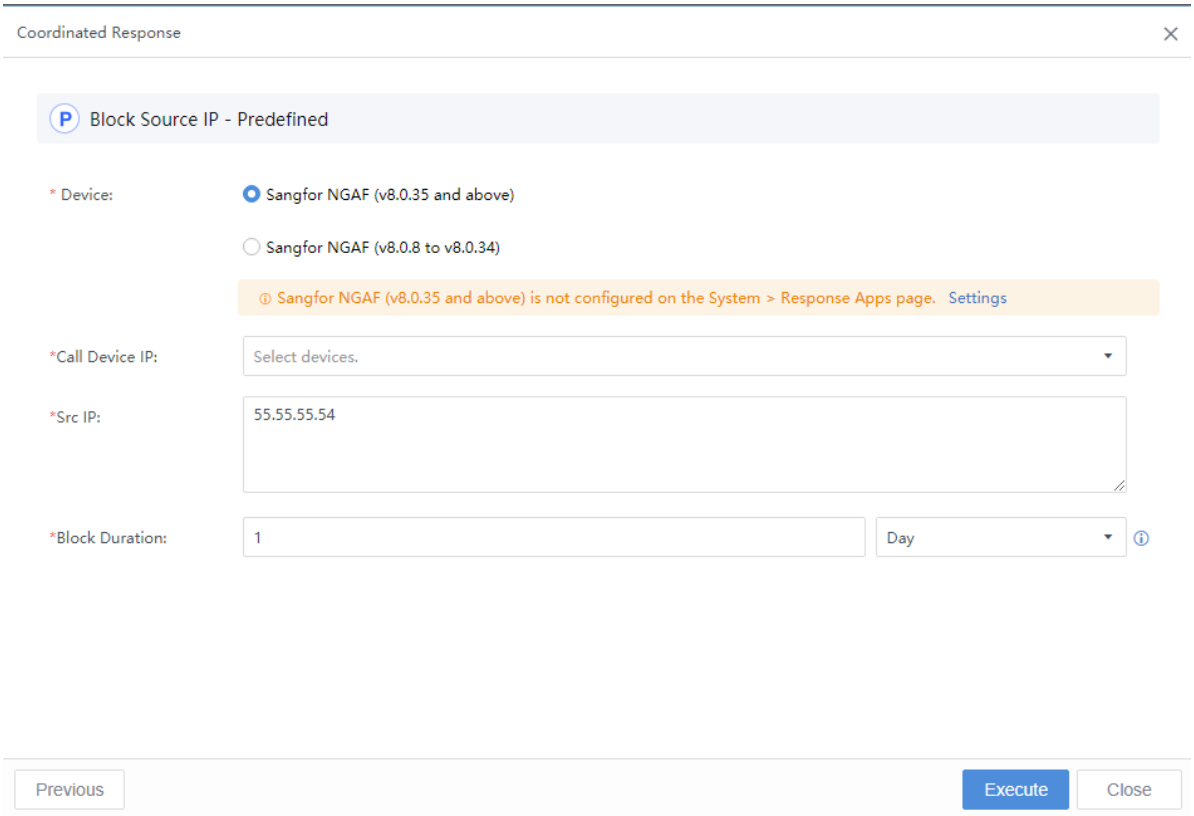
On the <File Threats> page, you can click the <> icon in the [Operation] column to go to the Coordinated Response dialog box. You can fix the alert based on the coordinated response policy, as shown in the figure below.



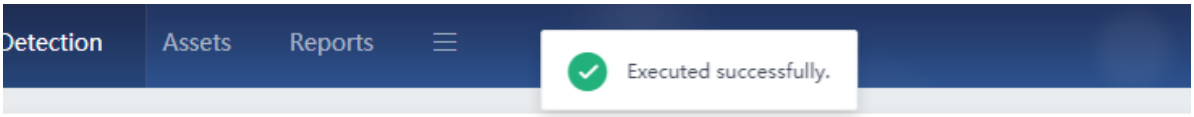
You can click <Next> to select the correlated device, configure the block duration and other parameters, and click <Execute>, as shown in the figure below.



After clicking <Next>, you will go to the parameter settings page of coordinated response based on the policy you selected., You can set the device, call device IP, source IP, and block duration. The figure below takes the policy for blocking source IP as an example.



After you click <Execute>, the response action starts to be executed. The system prompts the message of <Executed> at the top of the page after the execution is completed.



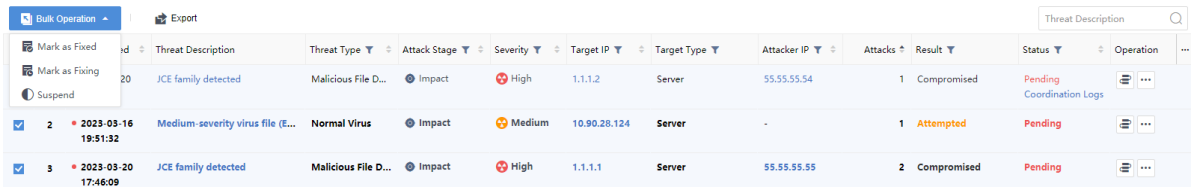
You can go to [Response/Response History] and click the "Auto Response History" tab to view the execution history of corresponding policies. Information such as execution status, result, and policy is displayed.

Manual operation

You can operate a single alert or multiple alerts in bulk.

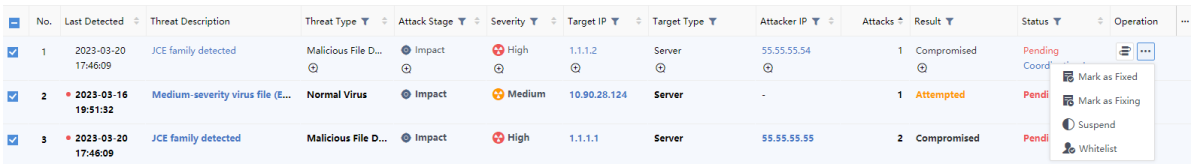
1. **Bulk**

You can click <Bulk Operation> for alert filtration based on the options in the drop-down list or select multiple alerts from the alert list directly to perform the bulk operation.



2. **Single**

You can select one alert and click the <••• > icon in the [Operation] column. Available options include Mark as Fixed, Mark as Fixing, Suspend, and Whitelist, as shown in the figure below.



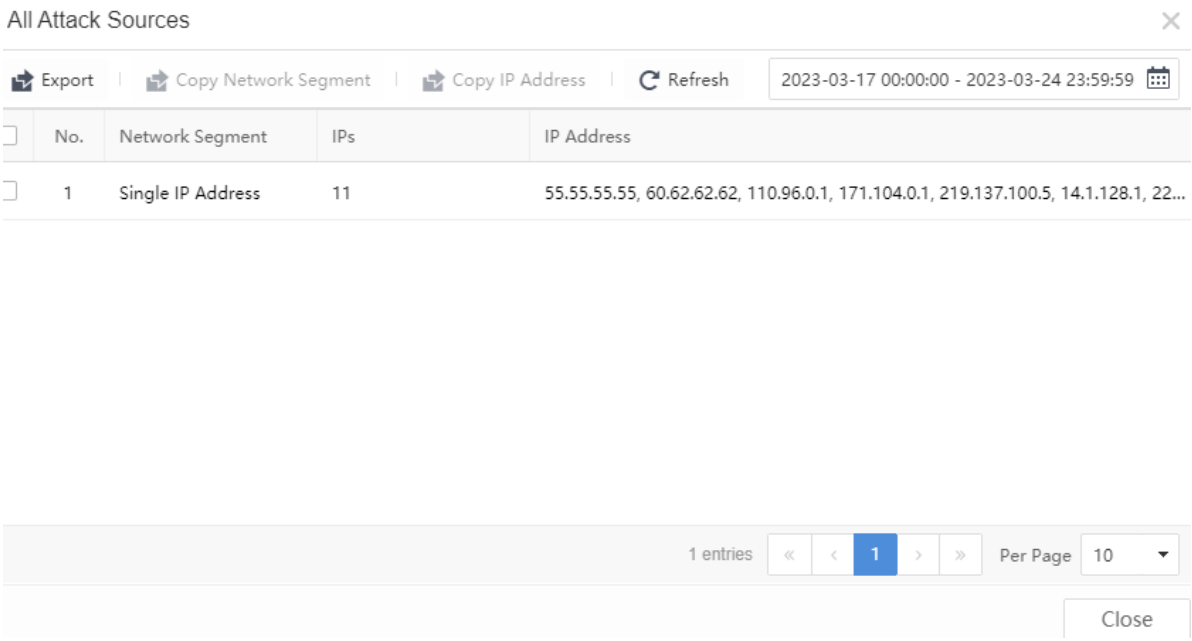
Inbound Attacks

Inbound attacks include high-severity attacks, evasive attacks, and inbound risky access.

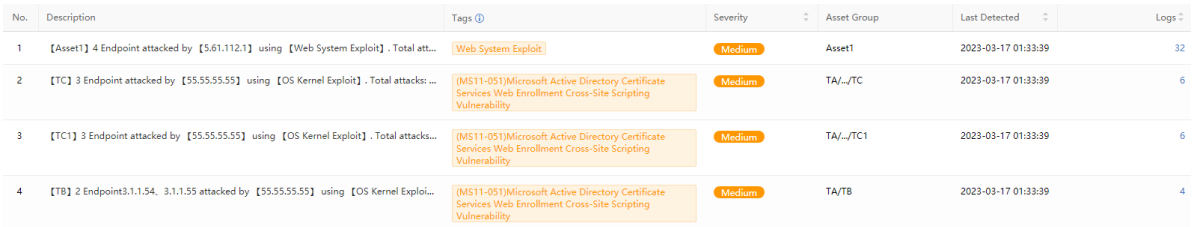
1. Nova Command can display **inbound attacks** in a period of time using the machine learning clustering algorithm, as shown in the figure below.



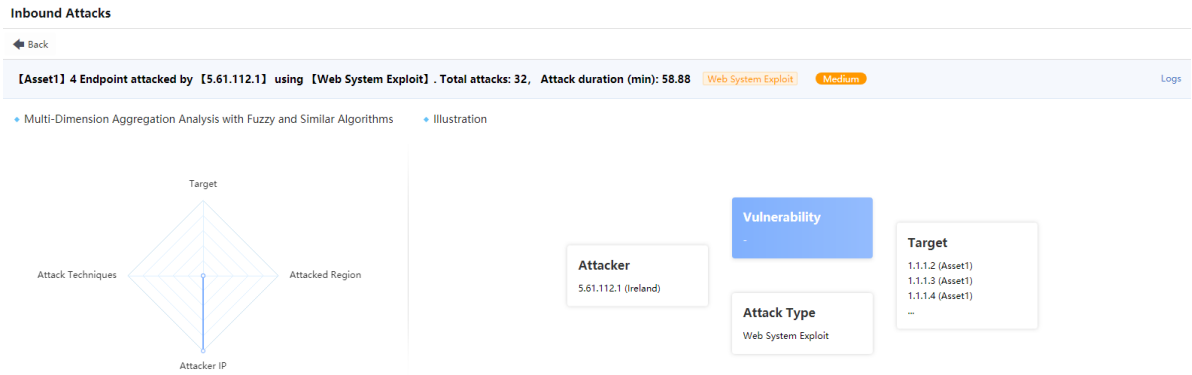
You can click <Attack Sources> to view the attack IP address. You can export the data, copy network segments, and copy IP addresses to add these IPs to the security gateway for IP block, as shown in the figure below.



2. The [Details] section shows the description, tag, severity, group, last detected time, and logs of the attack. You can filter attacks by these conditions and search for specific attacks by keywords, as shown in the figure below.



You can click the content in the <Description> column to view the description details, as shown in the figure below.



Sections:

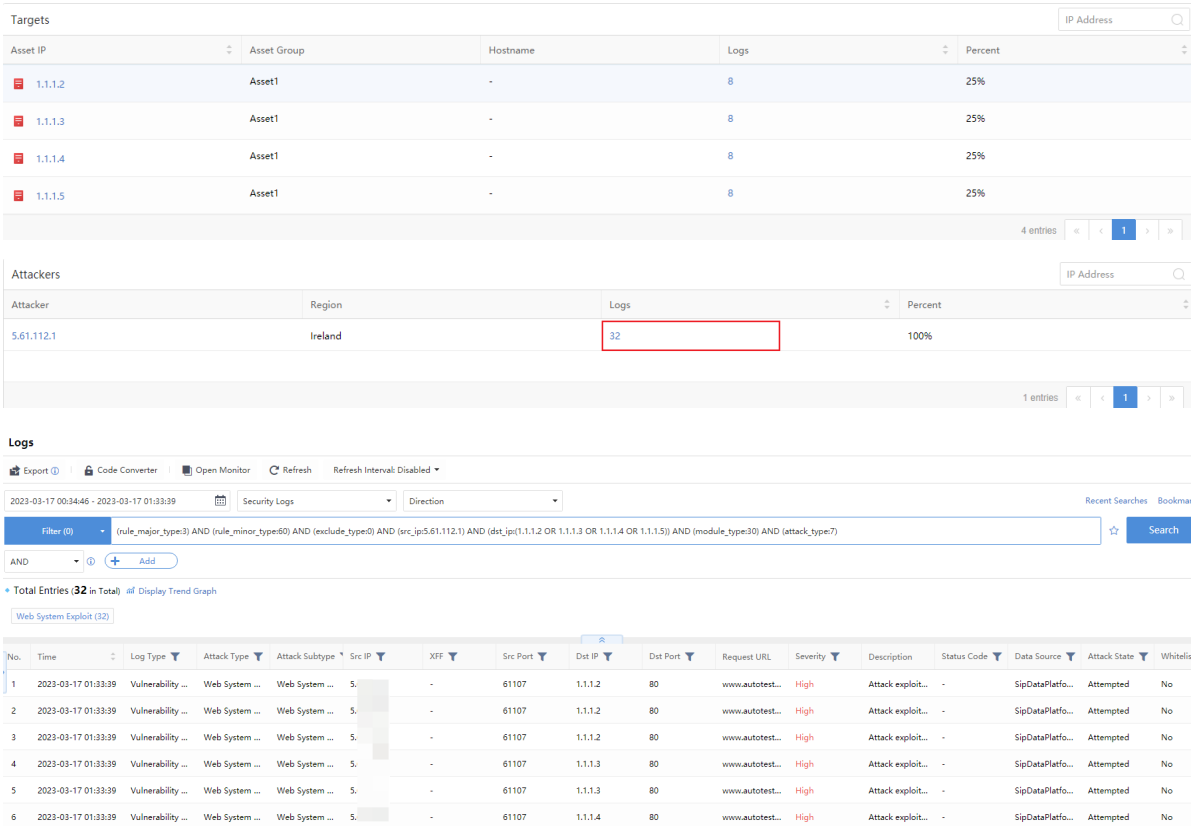
<Multi-Dimension Aggregation Analysis with Fuzzy and Similar Algorithms>: Performs aggregation analysis of attacks in a period of time based on the target, attacked region, attack technique, and attacker IP.

<Illustration>: Displays basic information about the attack types, attackers, targets, and vulnerabilities.

<Details>: Displays detailed information about the targets, attackers, vulnerabilities, attack types, and attack period.

<Recommendations>: Provides the fixing suggestions for the alert.

<Logs>: You can click the log number in the <Logs> column to go to the [Logs] page and view the detection logs, as shown in the figure below.

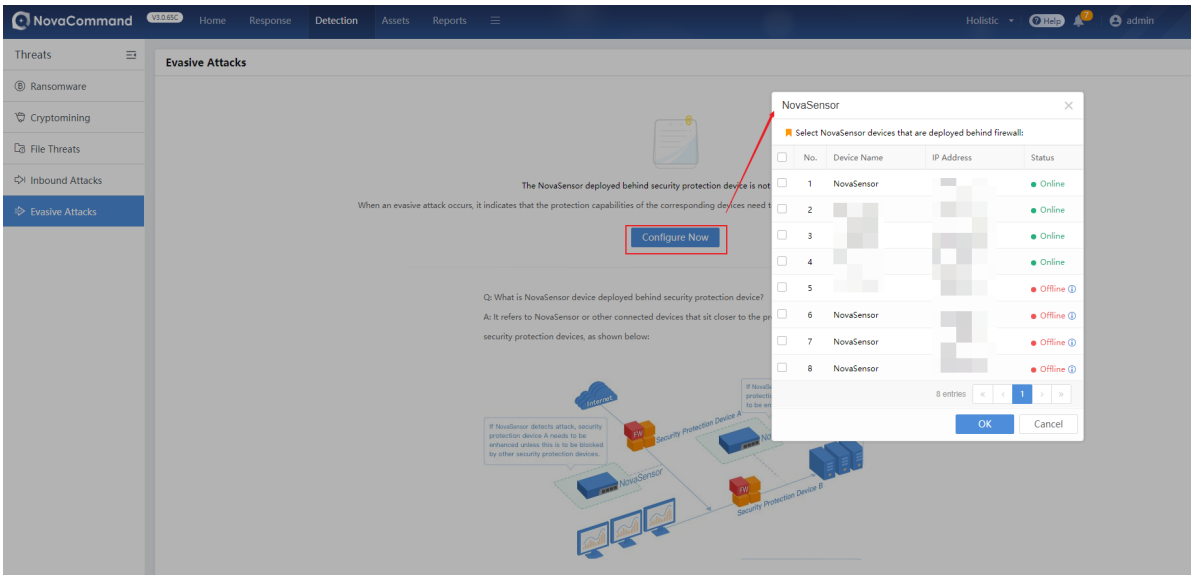


Evasive Attacks

Evasive attack refers to the attack detected by Nova Sensor deployed behind the defense system. The occurrence of this attack indicates defense capabilities and protection policies should be enhanced. Evasive attack detection and analysis can be performed by deploying Nova Sensor behind the firewall on Nova Command.

Nova Sensor deployment

To ensure the analysis accuracy of evasive attacks, you need to manually deploy Nova Sensor behind the firewall. When the Nova Sensor detects an inbound attack, the attack is identified as an evasive attack. You can go to [Detection/Threats/Evasive Attacks] and click <NS> to deploy Nova Sensor devices behind the firewall.



Overall display

Overall display

On the [Threats/Evasive Attacks] page, you can view the following data.

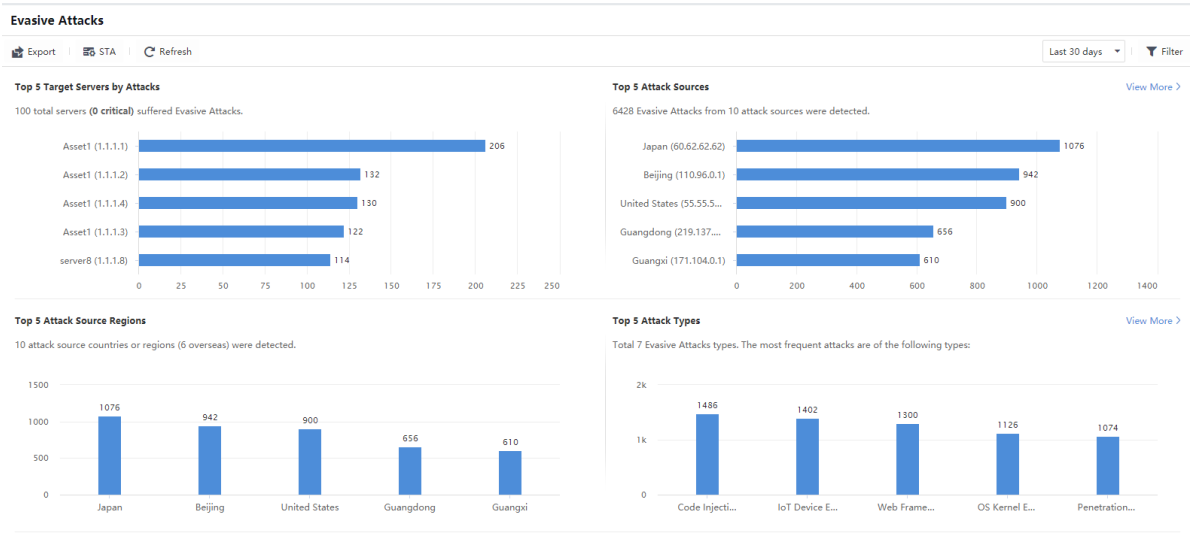
Top 5 Target Servers by Attacks: The top five servers that suffered the most evasive attacks.

Top 5 Attack Sources: You can click <View More> to view and export all attack sources.

Top 5 Attack Source Regions: The top five countries or regions that launch the most attacks.

Top 5 Attack Types: You can click <View More> to view and export detailed information, such as target IP, corresponding to the attack type.

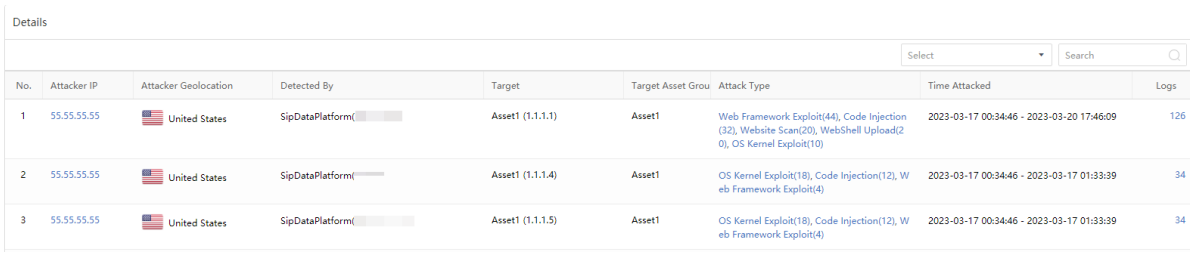
You can filter the data of last 7 days, last 30 days, today, and last 24 hours. You can also click <Filter> to filter the data by attacker geolocation and attack type, as shown in the figure below.



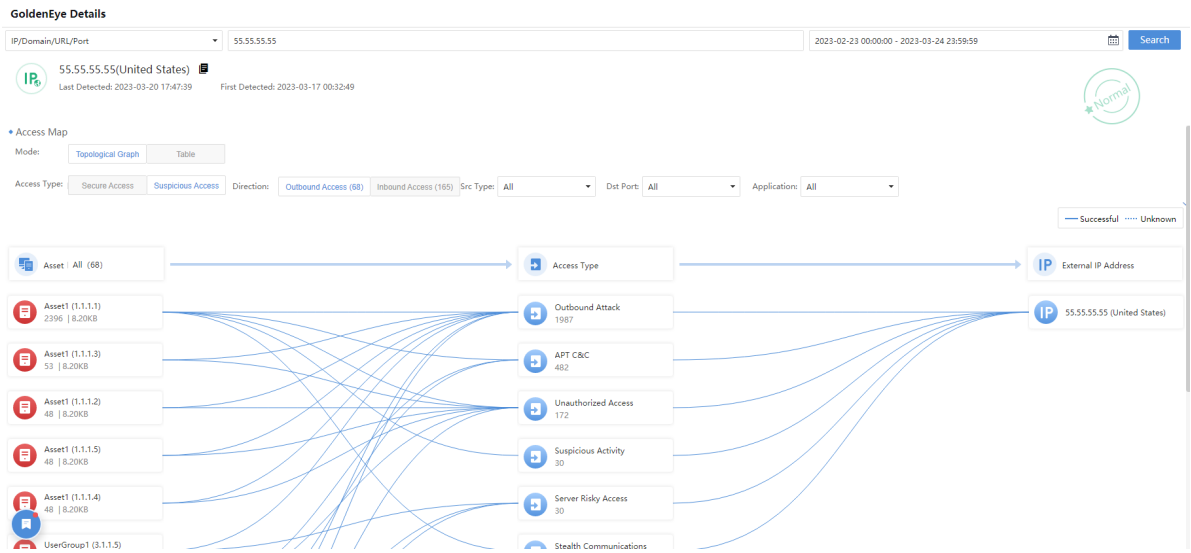
You can click <Export> in the upper left corner of the page to export all evasive attacks as an EXCEL file.

Details

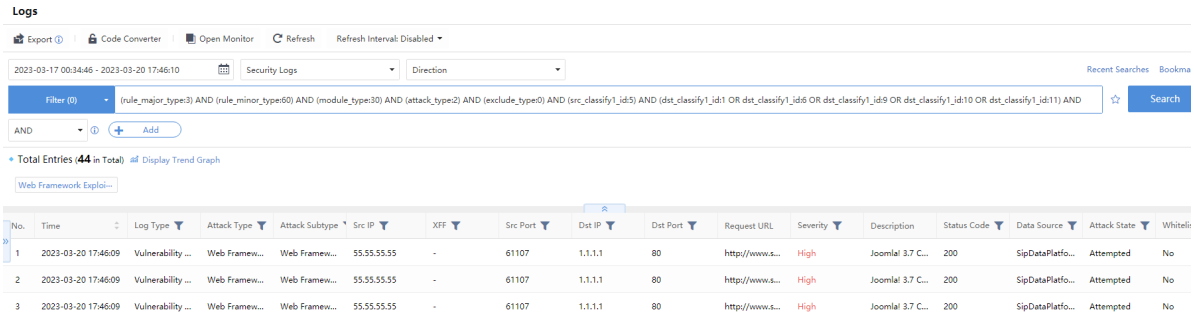
On the [Threats/Evasive Attacks] page, you can view the attack details, including attacker IP, attacker geolocation, detection device, target, target group, domain name, attack type, attack time, and logs. You can search for attacks by keywords or groups, as shown in the figure below.



You can click an attacker IP to go to the [GoldenEye Details] page to view the details of the IP address, as shown in the figure below.

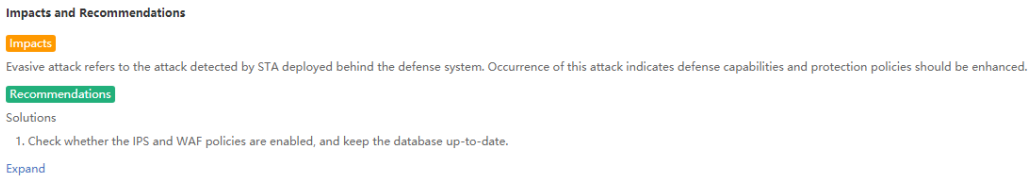


You can click an attack type or a log number to go to the [Detection/Logs] page to view the detailed logs of the attack type, as shown in the figure below.



Impacts and recommendations

On the [Threats/Evasive Attacks] page, you can view the impacts and recommendations of evasive attacks and can click <Expand> to view more details, as shown in the figure below.



Anomalies

The Anomalies menu displays results of UEBA based on the access direction, including unauthorized access, lateral access, and outbound server access.

UEBA

The UEBA module can analyze the abnormal behaviors of endpoints (servers/hosts) by using the behavior analysis engine and classify and display the behaviors based on anomaly types. On the [UEBA] page, you can view the number of days of continuous behavior learning and the number of anomaly types, abnormal endpoints, and abnormal behaviors. You can also view behavior details based on anomaly types.

1. Overview

You can filter anomalies by time period or IP address in the upper right corner of the page.

// picture

2. Anomaly type

Anomaly types include Anomalous Login, Anomalous Database, Anomalous Outbound Access, Anomalous Outbound Data, Anomalous Access, and Anomalous Traffic. You can select a specific anomaly type to view the details on the right and search for anomalies by asset groups, as shown in the figure below.

// picture

You can click a specific anomaly behavior to view the details of behavior analysis, model analysis, and access profile. If an endpoint has anomalies of multiple anomaly types, you can switch between different anomaly types.

The Behavior Analysis tab is as follows.

// picture

The Model Analysis page is as follows.

// picture

The Access Profile tab is as follows.

// picture

Note:

The UEBA function is enabled for 2U servers but not enabled for servers with low configurations by default.

Unauthorized Access

Unauthorized access refers to access that matches blacklist rules or violates whitelist rules configured on Nova Sensor, or violates any application control policies on NGAF. Frequent unauthorized accesses indicate that the endpoint is likely to be controlled by hackers, or there may be malicious actions performed by internal users. Nova Command displays the overall data, impacts, and recommendations of unauthorized accesses on the [Detection/Anomalies/Unauthorized Access] page.

Overall display

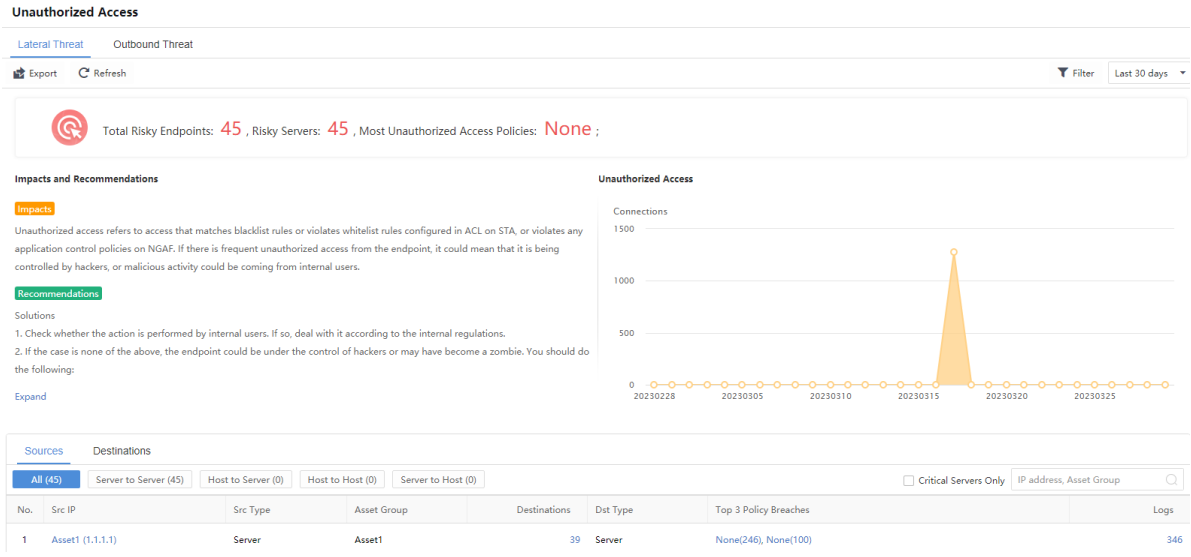
On the [Anomalies/Unauthorized Access] page, you can view the following data:

Total risky endpoints, risky servers, and violated policies.

<Unauthorized Access>: Records the daily number of unauthorized accesses in a period of time.

<Impacts and Recommendations>: Provides impact description and fixing suggestions. You can click <Expand> to view more details.

You can filter the data by time period, such as last 7 days, last 30 days, today, and last 24 hours. You can also click <Filter> to set the time period, as shown in the figure below.



You can click <Export> in the upper left corner of the page to export all unauthorized accesses as an EXCEL file.

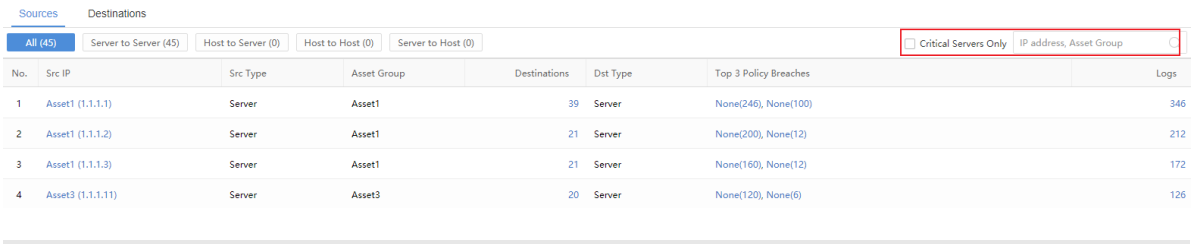
Details

On the [Anomalies/Unauthorized Access] page, you can view sources and destinations of unauthorized accesses.

1. Sources

You can click the [Sources] tab to view the source IP, source type, group, destinations, destination type, top 3 policy breaches, and logs, as shown in the figure below.

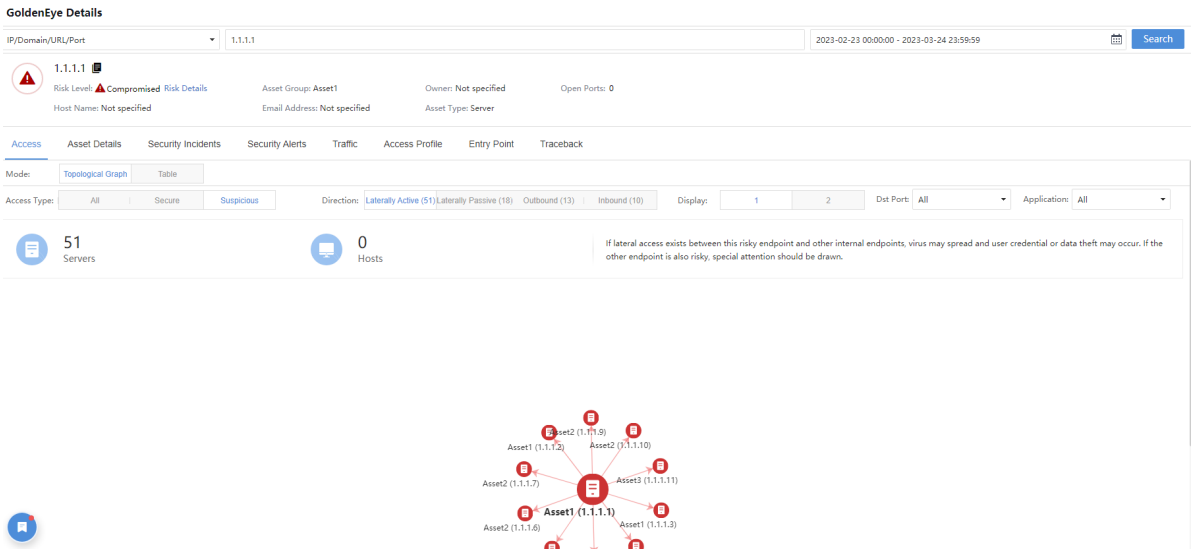
You can also filter the sources by selecting "All", "Server to Server", "Host to Server", "Host to Host", or "Server to Host" or entering the specific IP addresses and groups in the search box. If the "Critical Servers Only" check box is selected, detailed information about only critical servers is displayed.



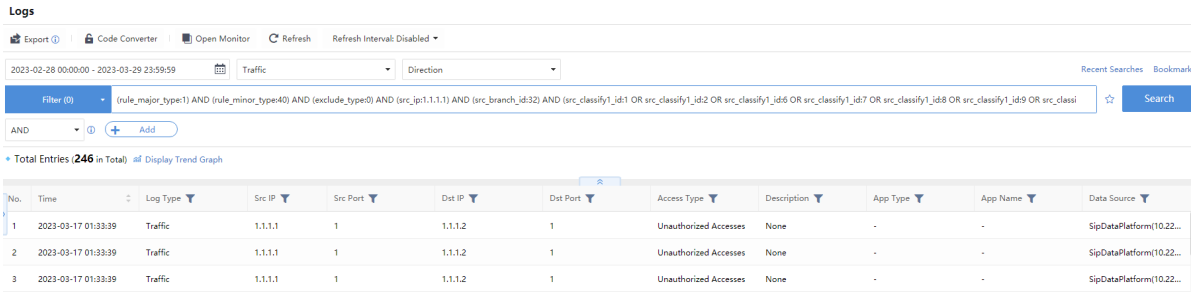
Note:

You need to configure the unauthorized access policy on the Nova Sensor first. For more information about the configuration method, see the Nova Sensor security policy configuration section.

You can click a source IP or destination number to go to the [Detection/GoldenEye Traceback] page to view the details of the IP address, as shown in the figure below.



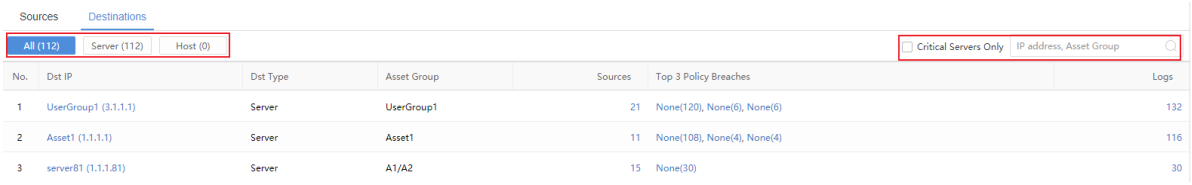
You can also click data in the [Top 3 Policy Breaches] or [Logs] column to go to the [Detection/Logs] page to filter the related logs, as shown in the figure below.



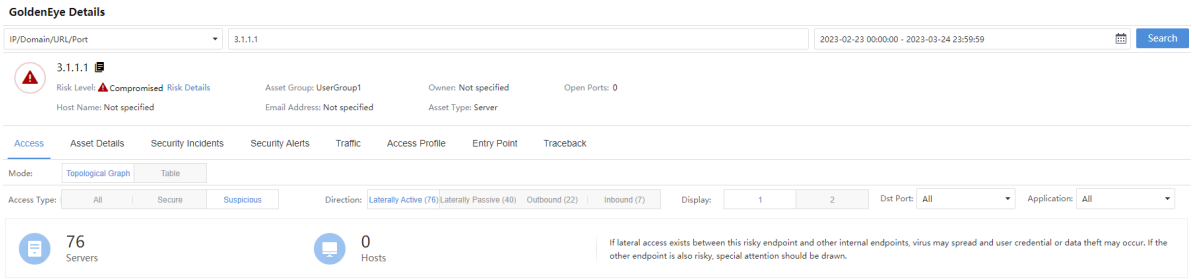
2. Destinations

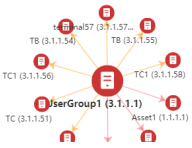
You can click the [Destinations] tab to view the destination IP, destination type, group, top 3 policy breaches, and logs, as shown in the figure below.

You can also filter the destinations by selecting "All", "Server", or "Host" or entering the specific IP addresses and groups in the search box. If the "Critical Servers Only" check box is selected, detailed information about only critical servers is displayed.

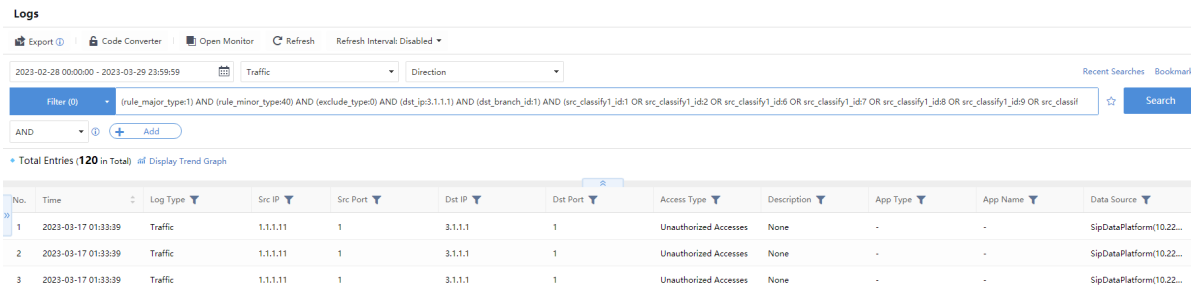


You can click a source IP or source number to go to the [Detection/GoldenEye Traceback] page to view the details of the IP address, as shown in the figure below.





You can also click data in the [Top 3 Policy Breaches] or [Logs] column to go to the [Detection/Logs] page to filter the related logs, as shown in the figure below.



Lateral Access

Lateral access refers to the attack launched by a LAN endpoint against other LAN endpoints. In this case, the endpoint is likely to be controlled by hackers and become a jump server that attempts to control other LAN endpoints, or there may be malicious actions performed by internal users. Lateral attacks can impose great impacts on LAN security. Nova Command displays the overall data, impacts, and recommendations of lateral accesses on the [Detection/Anomalies/Lateral Access] page.

Overall display

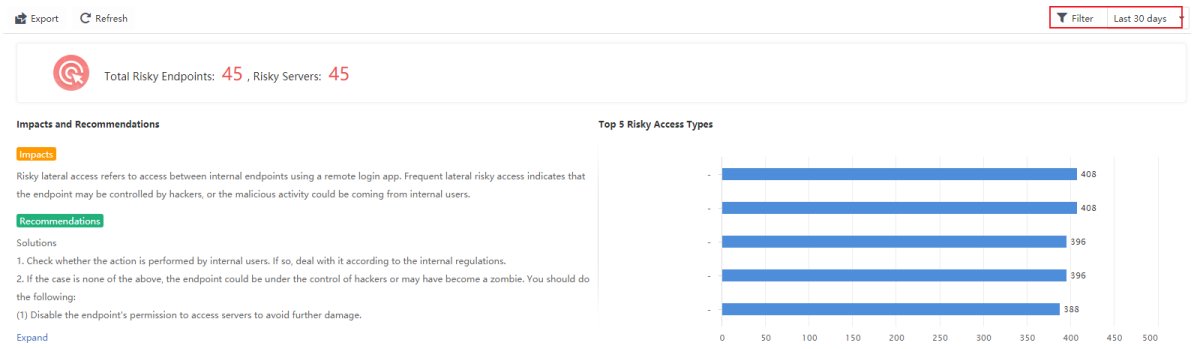
On the [Detection/Anomalies/Lateral Access] page, you can view the following data:

Total risky endpoints, risky servers, and target servers.

<Risky Access>: Records the daily number of lateral attacks in a period of time.

<Impacts and Recommendations>: Provides impact description and fixing suggestions. You can click <Expand> to view more details.

You can filter the data by time period, such as last 7 days, last 30 days, last 24 hours, and today. You can also click <Filter> to set the time period and application, as shown in the figure below.



You can click <Export> in the upper left corner of the page to export all lateral attacks as an EXCEL file.

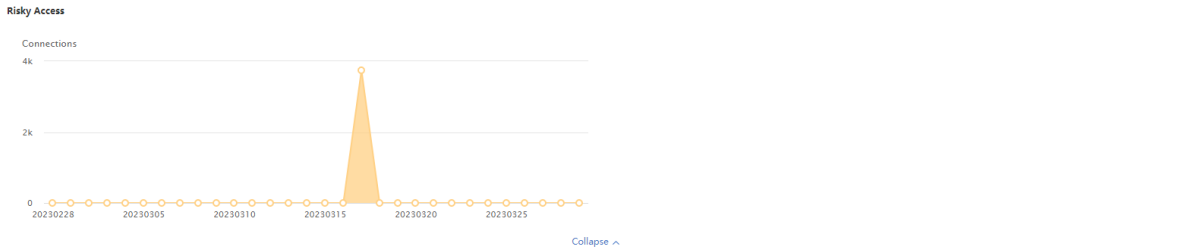
Details

On the [Anomalies/Lateral Access] page, you can view sources and destinations of lateral accesses.

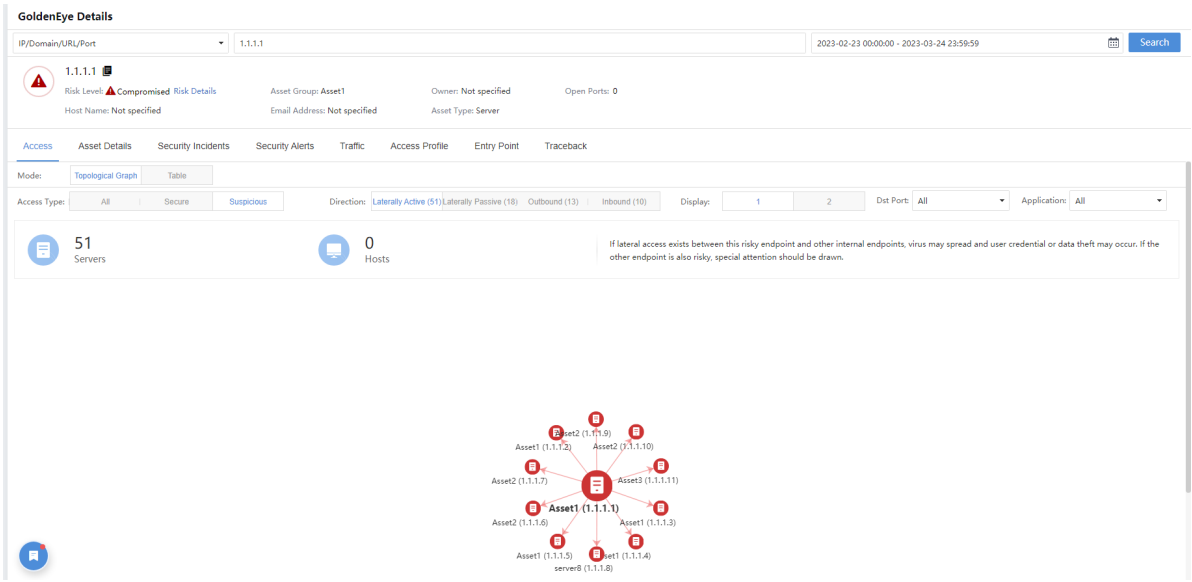
1. Sources

You can click the [Sources] tab to view the source IP, source type, group, lateral threat type, destinations, destination type, top 3 risky access types, and logs, as shown in the figure below.

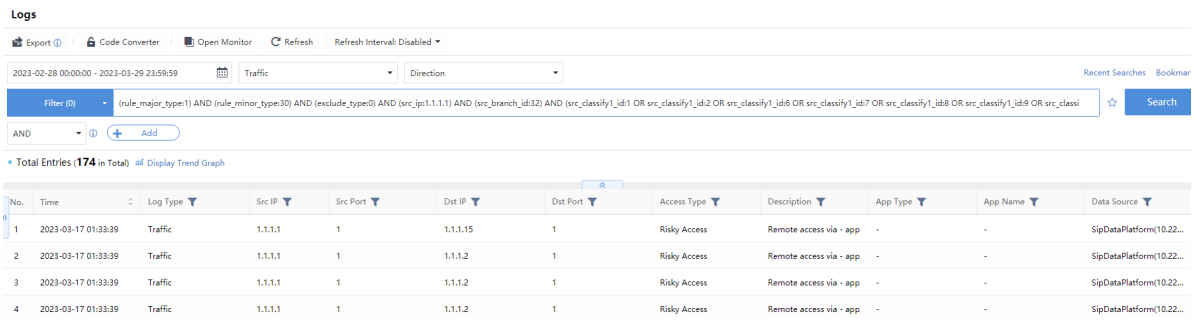
You can also filter the sources by selecting "All", "Server to Server", "Host to Server", "Host to Host", or "Server to Host" or entering the specific IP addresses and groups in the search box. If the "Critical Servers Only" check box is selected, detailed information about only critical servers is displayed.



You can click a source IP to go to the [GoldenEye Traceback] page to view the details of the IP address, as shown in the figure below.



You can also click data in the [Top 3 Risky Access Types] or [Logs] column to go to the [Detection/Logs] page to filter the related logs, as shown in the figure below.



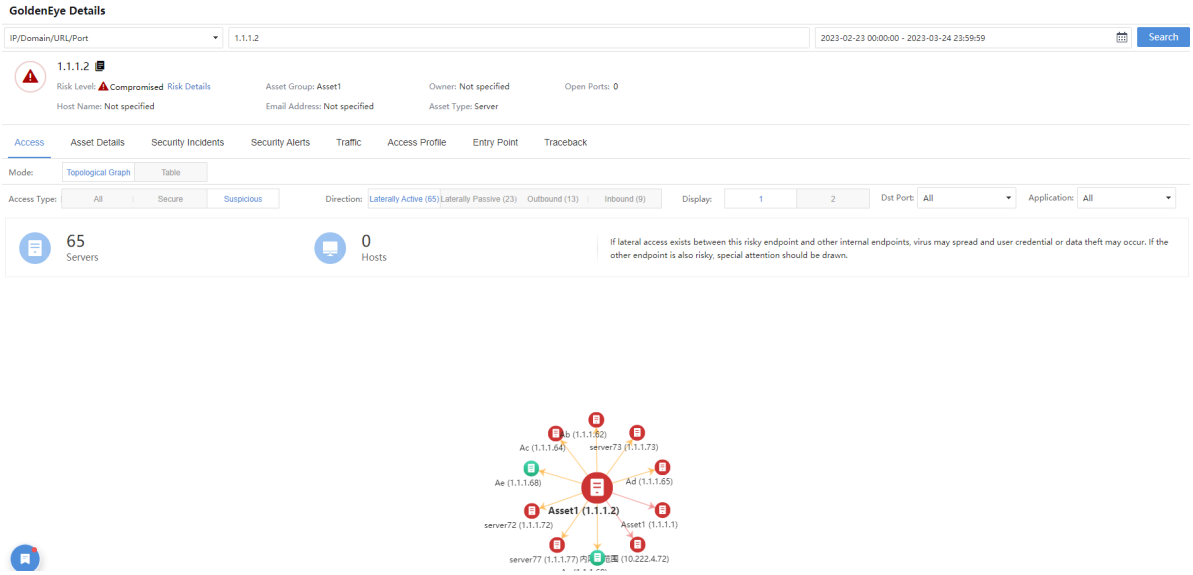
2. Destinations

You can click the [Destinations] tab to view the destination IP, destination type, group, sources, top 3 risky access types, and logs, as shown in the figure below.

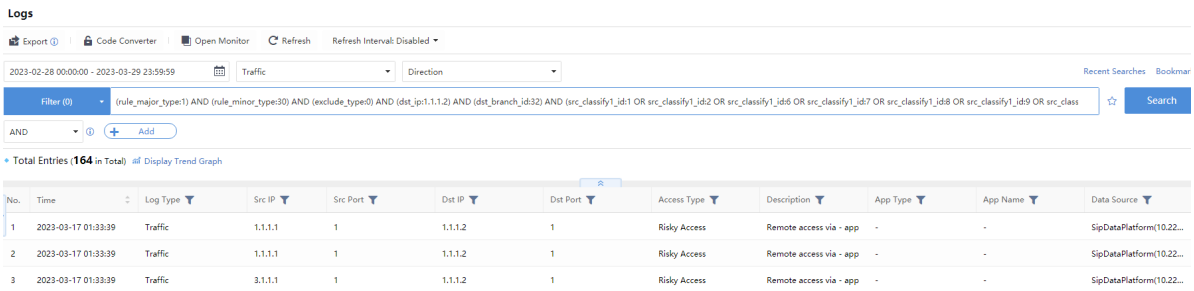
You can also filter the destinations by selecting "All", "Server", or "Host" or entering the specific IP addresses and groups in the search box. If the "Critical Servers Only" check box is selected, detailed information about only critical servers is displayed.



You can click a destination IP or source number to go to the [GoldenEye Traceback] page to view the details of the IP address, as shown in the figure below.



You can also click data in the [Top 3 Risky Access Types] or [Logs] column to go to the [Detection/Logs] page to filter the related logs, as shown in the figure below.



Outbound Server Access

Overall display

On the [Detection/Anomalies/Outbound Server Access] page, you can view the outbound server accesses in a visualized manner to prevent servers that do not have overseas business requirements from accessing outbound links. In addition, you can filter the data by server type, region, and time period. The [Outbound Server Access] page displays the following data:

<Application Traffic>: The server traffic trend of the top 5 applications is displayed by default. You can also select the Application Traffic Distribution option from the drop-down list.

<Protocol (port) Traffic>: The server traffic trend of the top 5 protocols (port) is displayed by default. You can also select the Protocol Traffic Distribution option from the drop-down list.

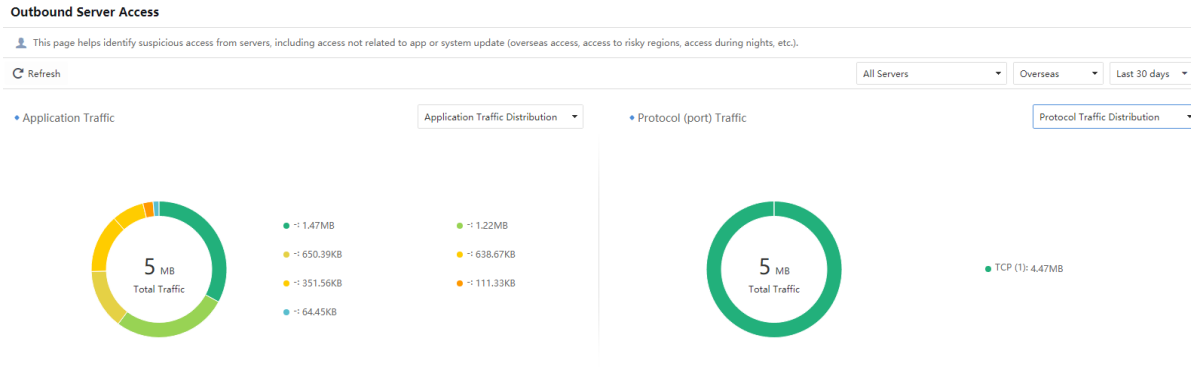
Note:

You can filter the data by server type, including options of All Servers, Critical Servers, Servers (Outbound > Inbound), and Access (00:00 to 6:00).

When Top 5 Application and Top 5 Protocol are selected, the two sections are as follows.



When Application Traffic Distribution and Protocol Traffic Distribution are selected, the two sections are as follows.

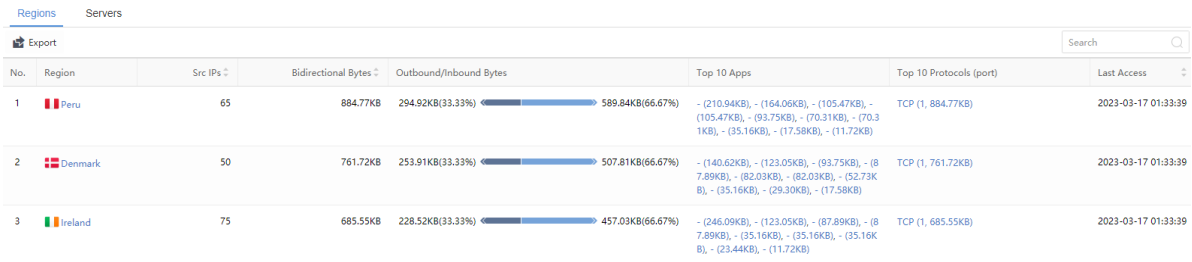


Details

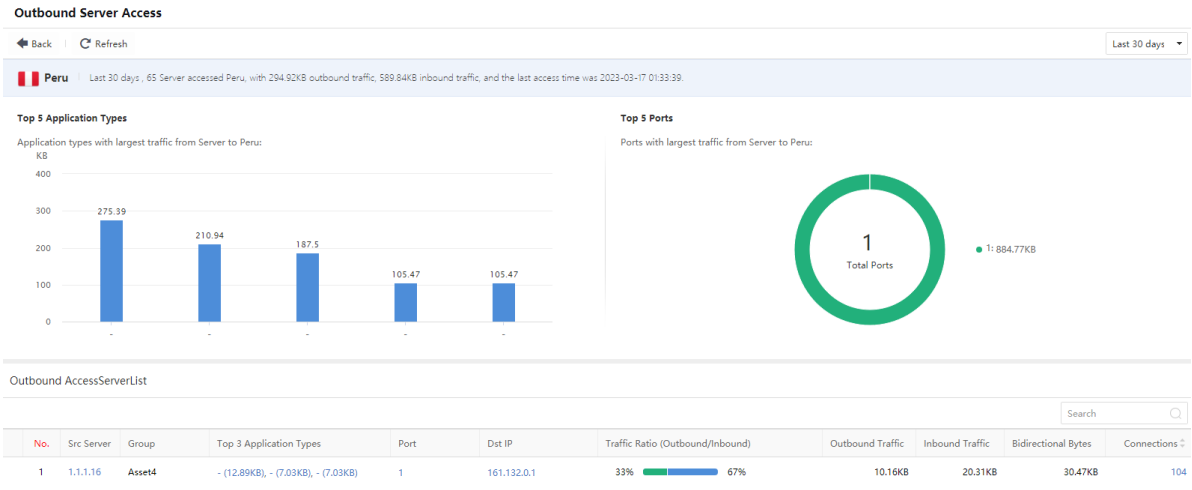
You can view outbound access details based on region or server.

Regions

On the "Regions" tab, you can view the information about the region, source IPs, bidirectional bytes, outbound/inbound bytes, top 10 apps, top 10 protocols (port), and last access. You can search for specific data by keywords and click <Export> to export the outbound access data in batches.

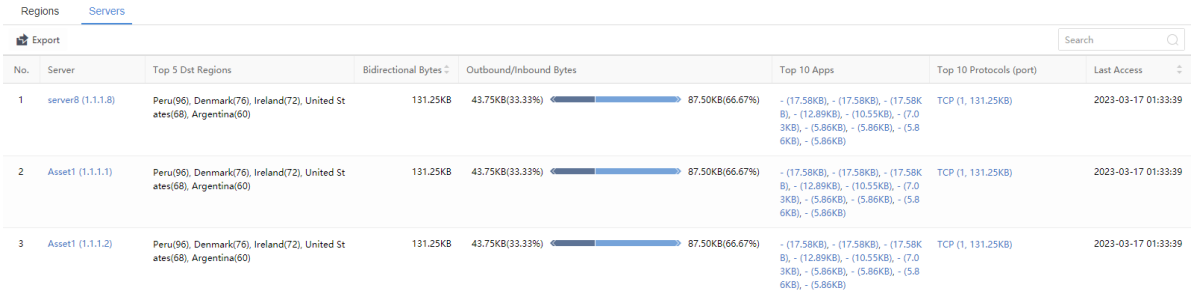


You can click the specific data in the [Region], [Top 10 Apps], or [Top 10 Protocols (port)] column to go to the corresponding pages and view the detailed information, as shown in the figure below.

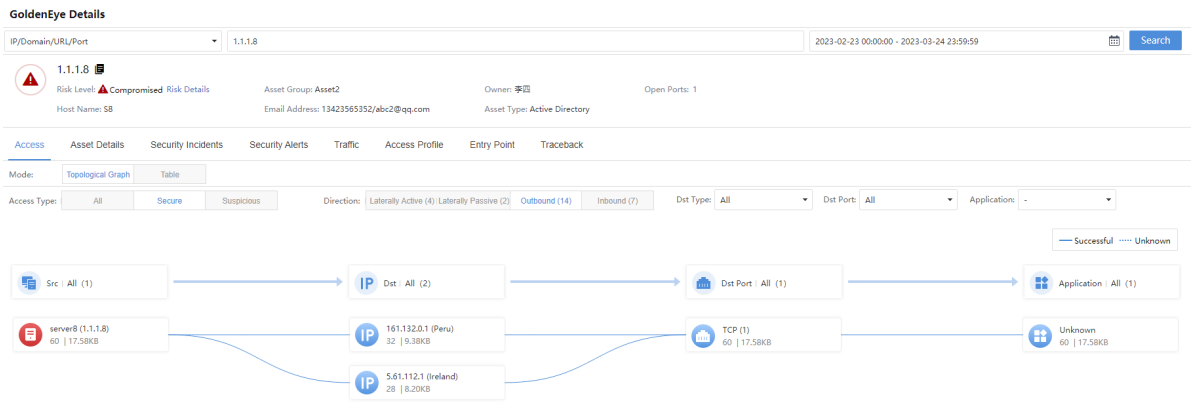


Servers

On the "Servers" tab, you can view the information about the server, top 5 destination regions, bidirectional bytes, outbound/inbound bytes, top 10 apps, top 10 protocols (port), and last access. You can search for specific data by keywords and click <Export> to export the outbound access data in batches.



You can click the specific data in the [Server], [Top 10 Apps], or [Top 10 Protocols (port)] column to go to the [GoldenEye Traceback] page and view the detailed information, as shown in the figure below.



Traffic

This module displays inbound traffic, lateral traffic, and outbound traffic in a visualized manner and provides the protocol-, application-, and traffic-based views.

Inbound Traffic

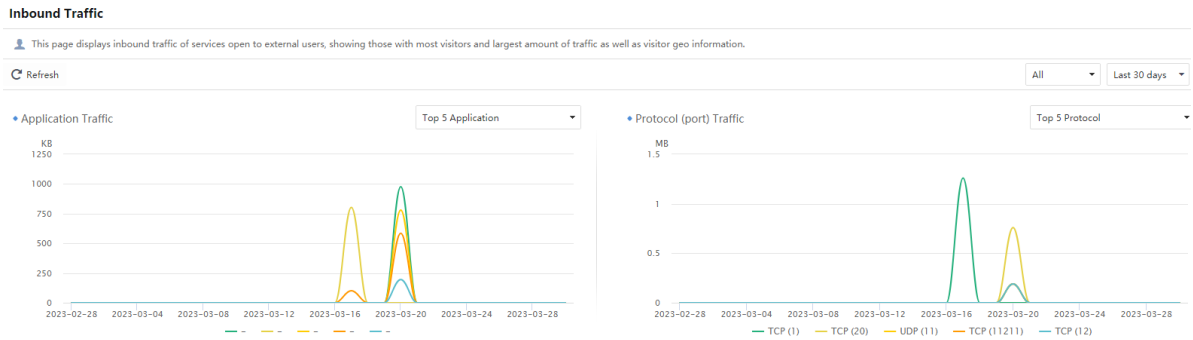
Overall display

On the [Detection/Traffic/Inbound Traffic] page, you can view the inbound traffic of services open to external users in a visualized manner. This page displays services with the most visitors and largest amount of traffic, as well as region information. You can filter the traffic data by service range (All, Overseas, or Domestic) and time period. The [Inbound Traffic] page displays the following data:

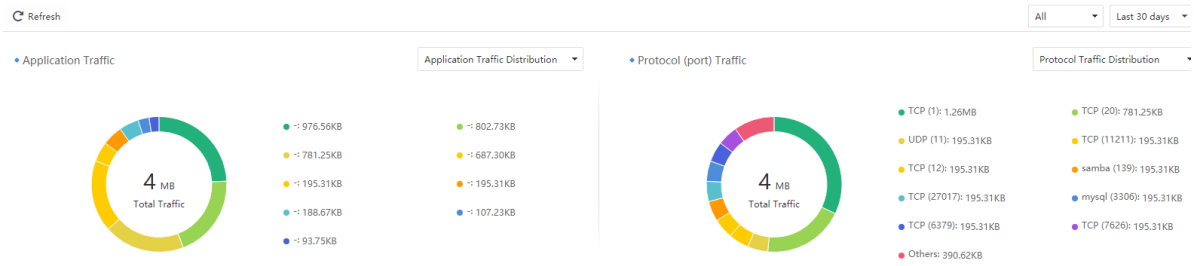
<Application Traffic>: The host traffic trend of the top 5 applications is displayed by default. You can also select the Application Traffic Distribution option from the drop-down list.

<Protocol (port) Traffic>: The host traffic trend of the top 5 protocols (port) is displayed by default. You can also select the Protocol Traffic Distribution option from the drop-down list.

When Top 5 Application and Top 5 Protocol are selected, the two sections are as follows.



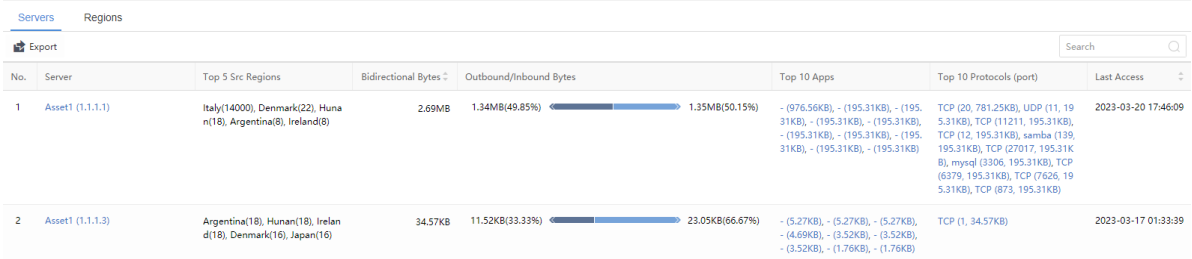
When Application Traffic Distribution and Protocol Traffic Distribution are selected, the two sections are as follows.



Details

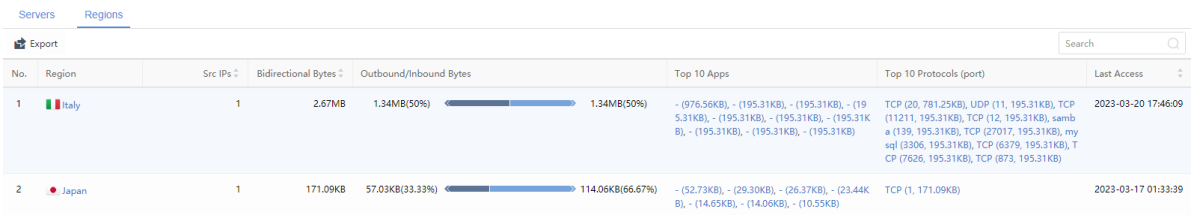
You can view inbound traffic details based on region or server.

On the "Servers" tab, you can view the information about the server, top 5 source regions, bidirectional bytes, outbound/inbound bytes, top 10 apps, top 10 protocols (port), and last access. You can search for specific data by keywords and click <Export> to export the inbound traffic data in batches.

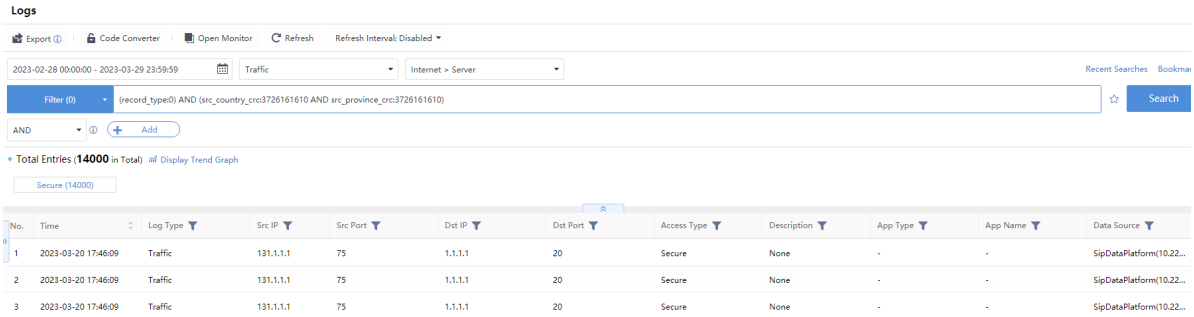


You can click the specific data in the [Server], [Top 10 Apps], or [Top 10 Protocols (port)] column to go to the [GoldenEye Traceback] page and view the detailed information.

On the "Regions" tab, you can view the information about the region, source IPs, bidirectional bytes, outbound/inbound bytes, top 10 apps, top 10 protocols (port), and last access. You can search for specific data by keywords and click <Export> to export the inbound traffic data in batches.



You can click the specific data in the [Region], [Top 10 Apps], or [Top 10 Protocols (port)] column to go to the [Logs] page and view the detailed information, as shown in the figure below.



Lateral Traffic

The Lateral Traffic page includes the Server Traffic and Most Active Sources tabs. The Server Traffic tab displays the traffic of LAN servers to show the top servers with the most traffic and visitors, as well as each asset group's access to servers. The Most Active Sources tab displays the most active source endpoints by destination IP addresses to help you discover stealthy scans rapidly.

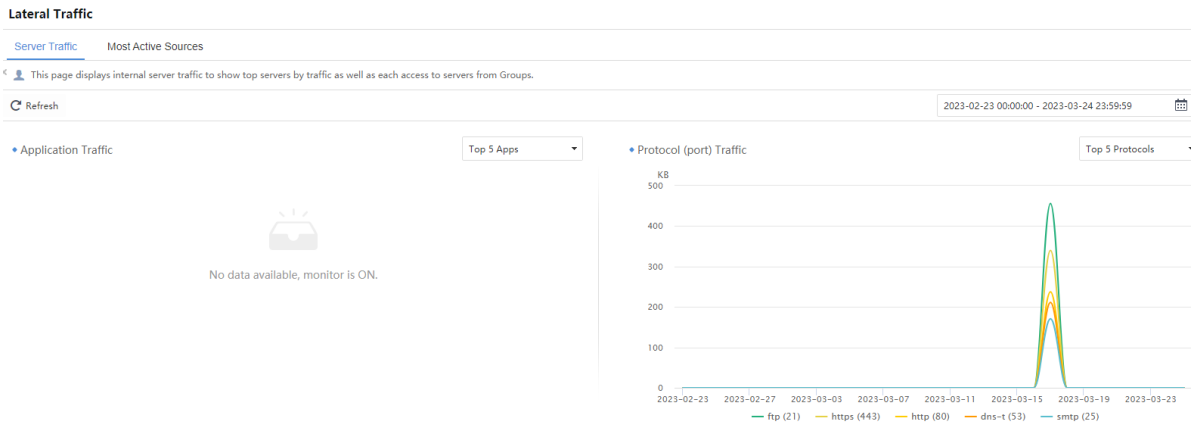
Server traffic

On the "Server Traffic" tab of the [Lateral Traffic] page, you can view the following data:

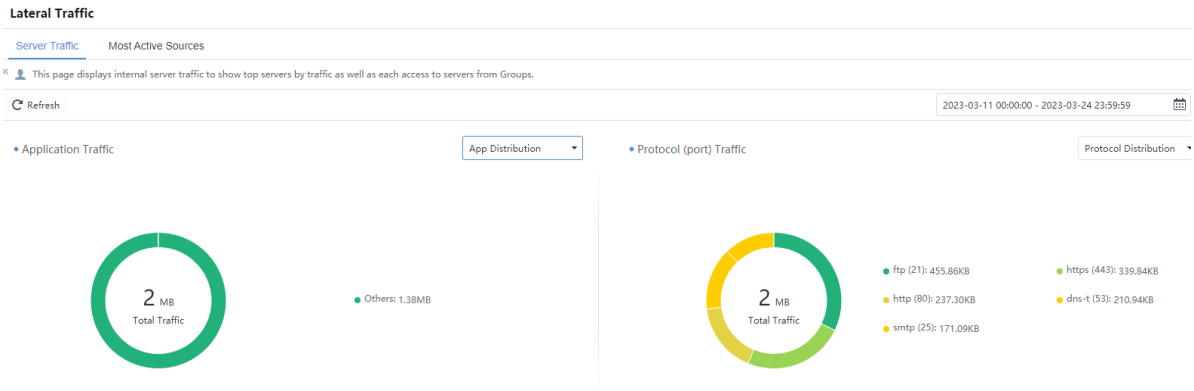
<Application Traffic>: The server traffic trend of the top 5 applications is displayed by default. You can also select the App Distribution option from the drop-down list.

<Protocol (port) Traffic>: The server traffic trend of the top 5 protocols (port) is displayed by default. You can also select the Protocol Distribution option from the drop-down list.

When Top 5 Apps and Top 5 Protocols are selected, the two sections are as follows.



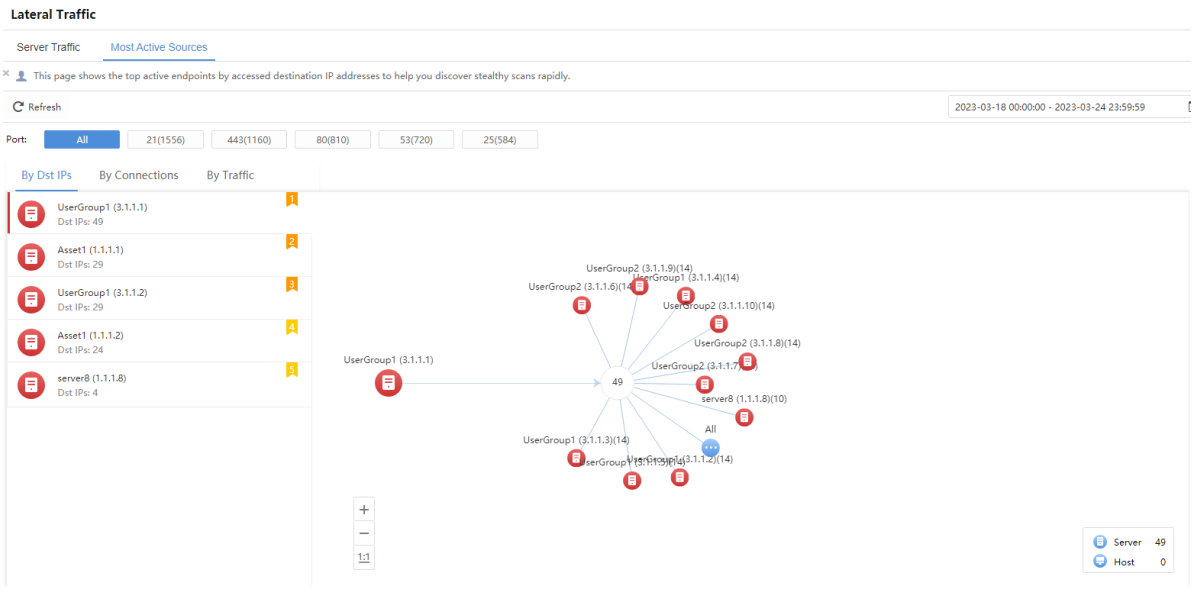
When App Distribution and Protocol Distribution are selected, the two sections are as follows.



Most active sources

This tab shows the most active endpoints by destination IP addresses to help you discover stealthy scans rapidly.

On the "Most Active Sources" tab of the [Lateral Traffic] page, you can view the access data by port connections, destination IPs, connections, and traffic. The access relationship views corresponding to each sorting type are displayed, as shown in the figure below.



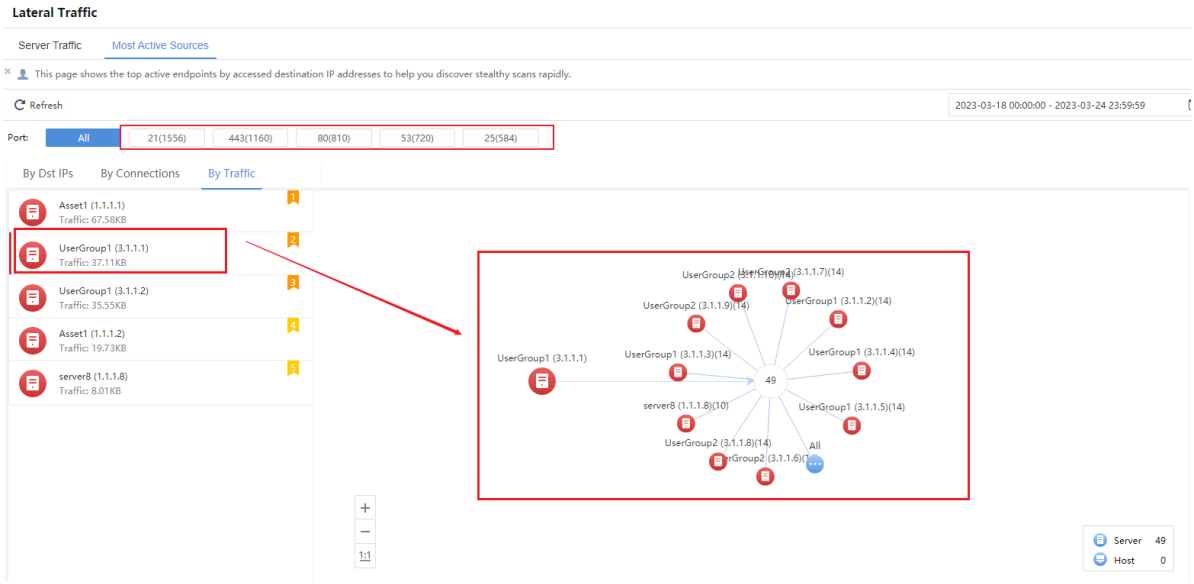
Port: The top 20 ports with the most access count and the access count of each port.

By Dst IPs: The top 5 IPs with the most access count.

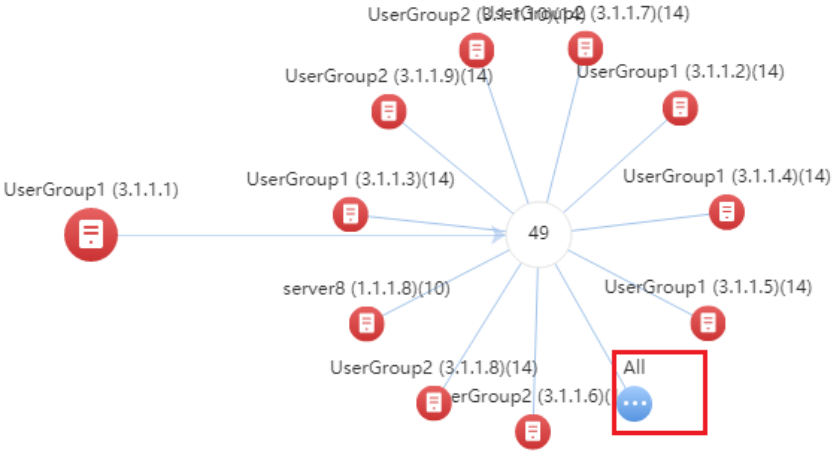
By Connections: The top 5 source endpoints with the most connections.

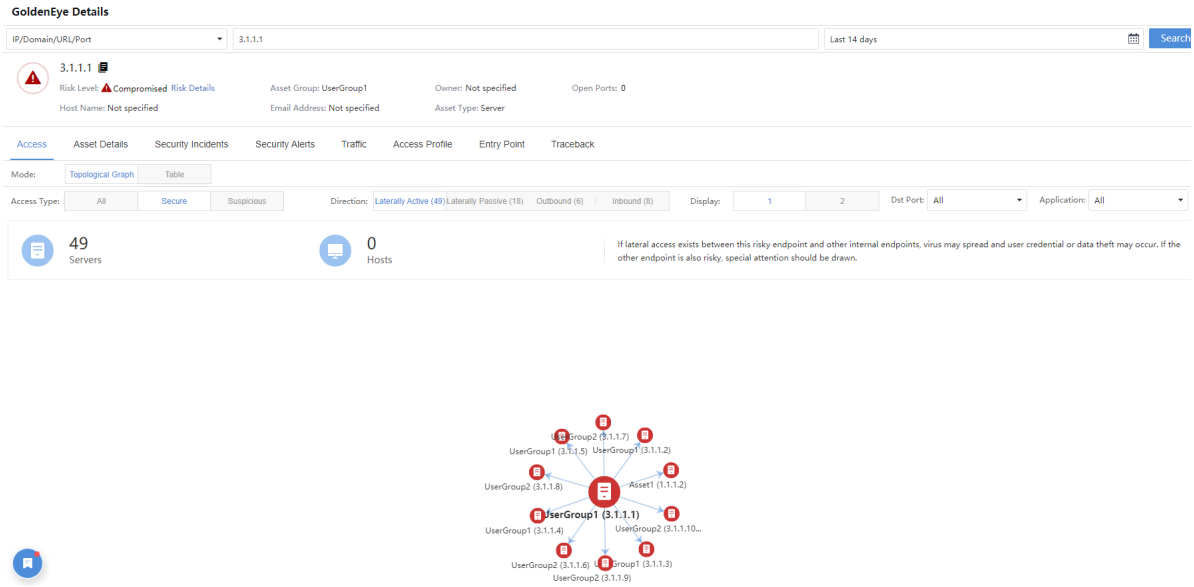
By Traffic: The top 5 source endpoints with the most traffic.

You can click a source endpoint on the left to view its access relationship view, as shown in the figure below.



You can click <All> in the view to go to the [GoldenEye Traceback] page and view more details, as shown in the figures below.

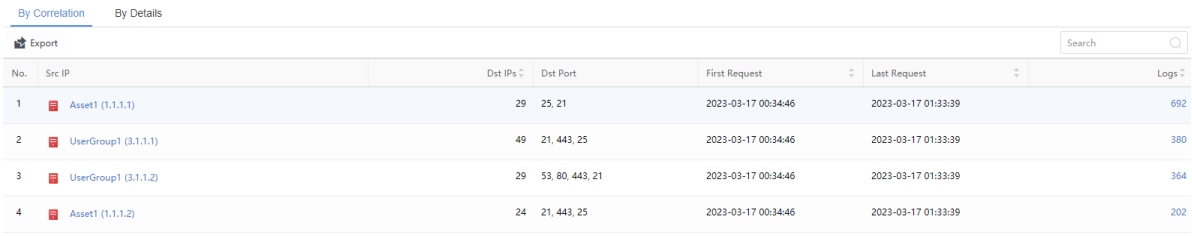




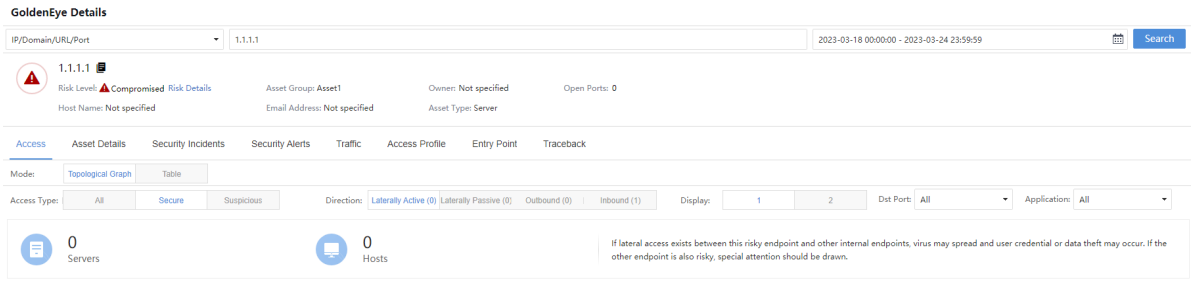
You can view source endpoint details in the correlation or details mode.

By correlation

On the [By Correlation] tab, you can view the information about the source IP, destination IPs, destination port, first request, last request, and logs. You can search for specific data by keywords and click <Export> to export the data in batches.



You can click a specific source IP to go to the [GoldenEye Traceback] page and view the detailed information. You can also click data in the [Logs] column to go to the [Detection/Logs] page to filter the related logs,
as shown in the figure below.

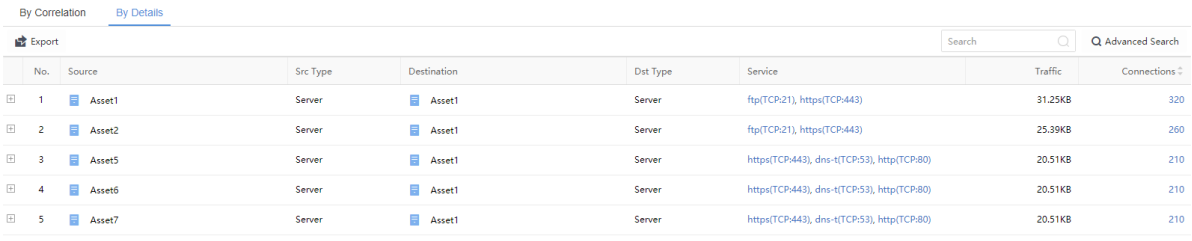


By details

On the [By Details] tab, you can view the information about the source, source type, destination, destination type, service, traffic, and connections. You can search for specific data by keywords and click <Export> to export the data in batches.

Note:

The Advanced Search function can be used to search by source group, destination group, endpoint name, endpoint IP, and keyword.

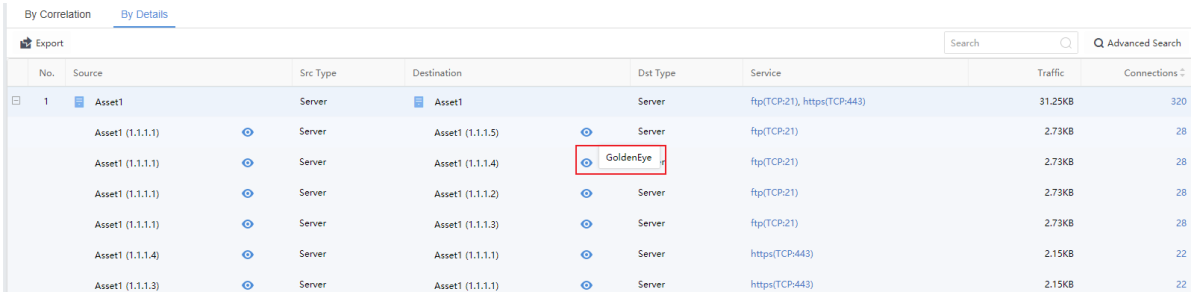


If you perform the following two operations, more detailed information will be displayed, as shown in the figure below.

Click the plus ("+") icon on the left of each row to show the details.

Click the <

> icon when you hover over a specific access source or access destination to view its destination or source for detailed information.

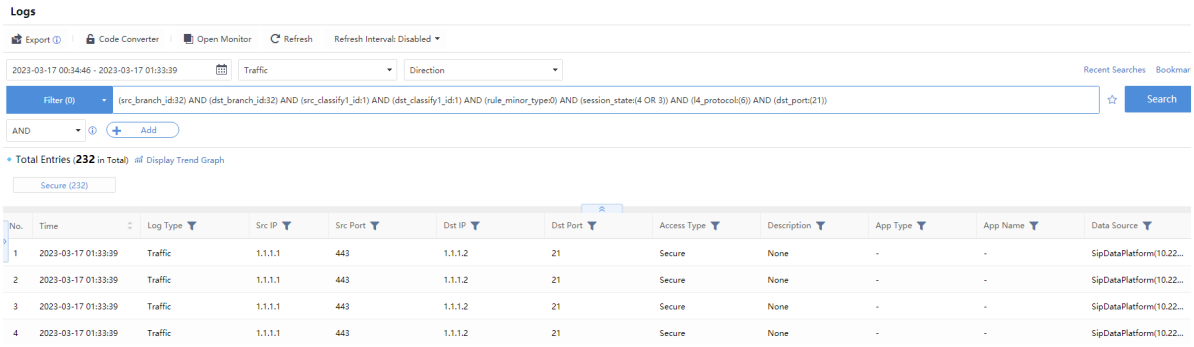


Note:

You can click the <

> icon to go to the [GoldenEye Traceback] page to view the related information.

You can also click data in the [Service] or [Connections] column to go to the [Detection/Logs] page to filter the related logs, as shown in the figure below.

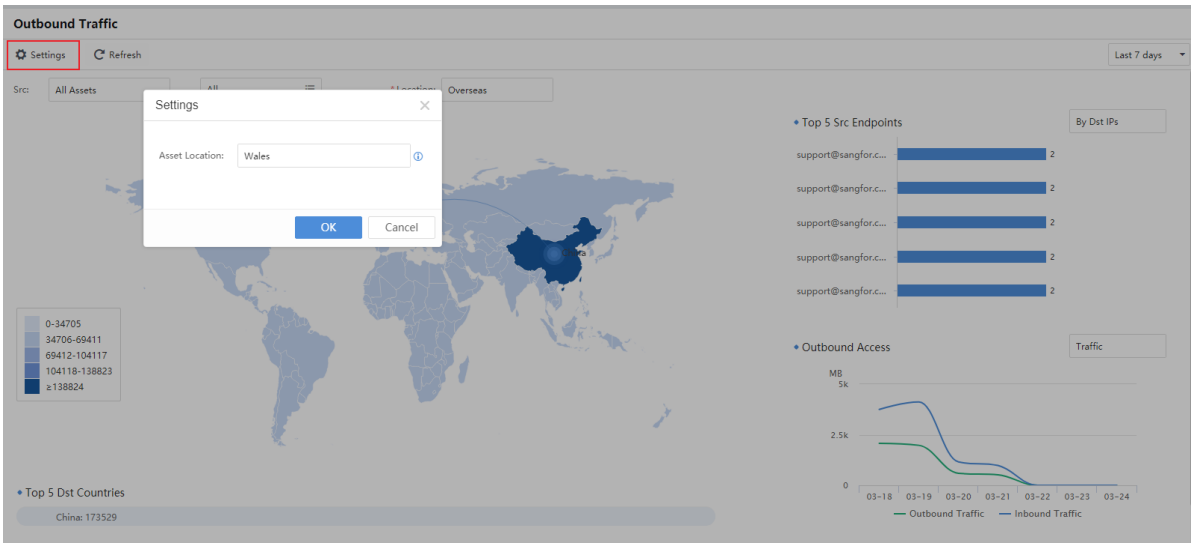


Outbound Traffic

The [Outbound Traffic] page displays the top 5 source endpoints, outbound access, top 5 destination countries, and detailed information in the form of a map by using lines connected from the LAN IP address to the destination country or region.

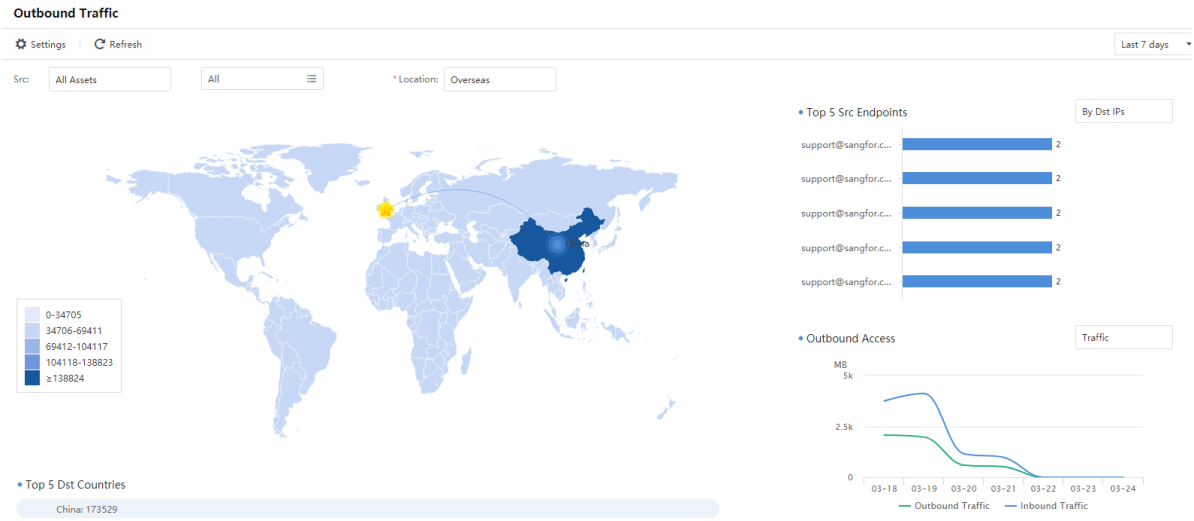
Asset location

To ensure the authenticity of the map, you need to click the <Settings> button to select a location on the map first to represent a LAN endpoint for displaying its outbound access, as shown in the figure below.



Overall display

On the [Outbound Traffic] page, you can view the outbound traffic between the endpoints or servers and the Internet in a general manner. The data, such as the top 5 destination countries, map, top 5 source endpoints, and outbound access, is displayed. You can filter the data by time period (last 24 hours and last 7 days), source, and location, as shown in the figure below.



Sections:

<Map>: Displays the domestic or overseas outbound traffic. You can hover over a country or region to view the corresponding outbound connection count.

Top 5 Dst Countries: Displays the top 5 countries or regions with the most outbound connections and the connection count of each country or region.

Top 5 Src Endpoints: Displays the top 5 source endpoints by destination IP count, connection count, or outbound traffic.

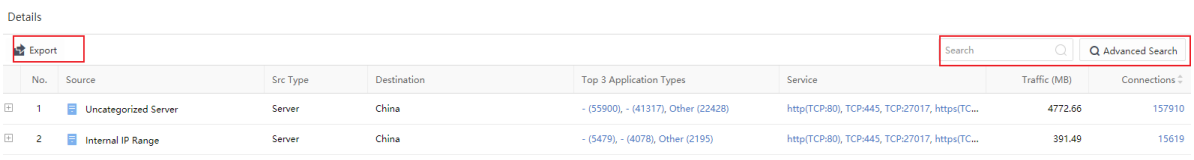
<Outbound Access>: Displays the outbound access by traffic or connection count.

Details

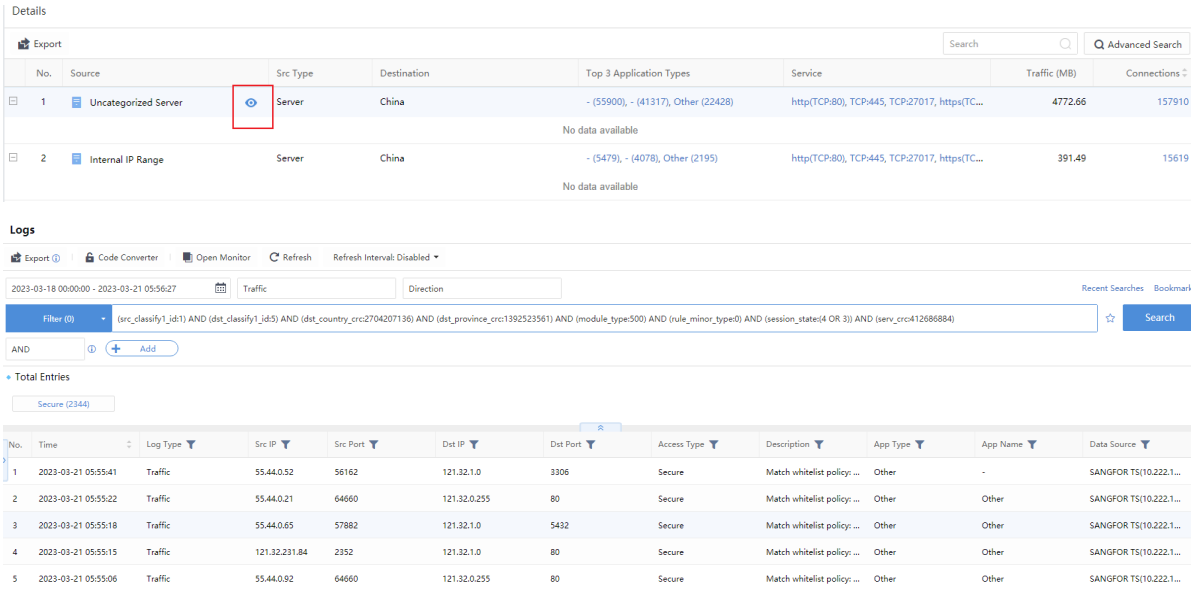
On the [Traffic/Outbound Traffic] page, you can view the detailed information about source endpoints in the [Details] section, including source, source type, destination, top 3 application types, service, traffic, and connections. You can search for specific data by keywords and click <Export> to export the source endpoint data in batches.

Note:

The Advanced Search function can be used to search by source group, destination group, endpoint name, endpoint IP, and keyword.



You can click the plus (+) icon on the left of each row to show the details, or click the <  > icon to go to the [GoldenEye Traceback] page to view the related information. You can also click data in the [Top 3 Application Types], [Service], or [Connections] column to go to the [Detection/Logs] page to filter the related logs, as shown in the figures below.



Assets

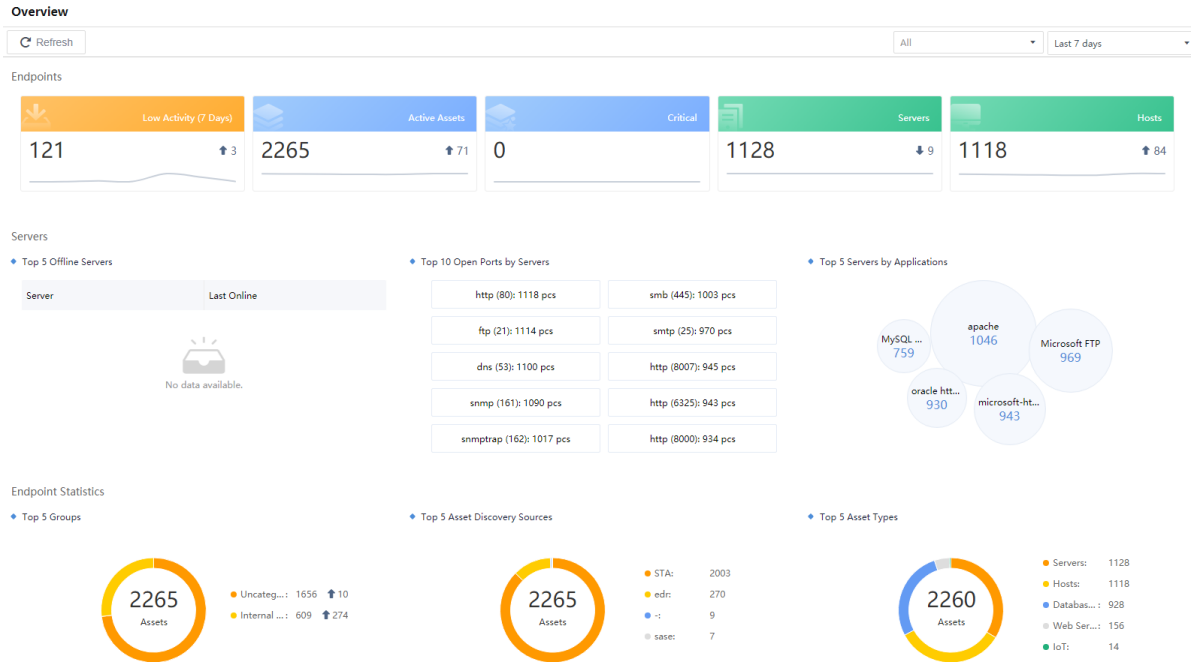
The [Assets] module supports the asset integration of Sangfor and third-party manufacturers, such as VRV Software and Yuanwang Technology.
The products of Sangfor include IAG, NovaGuard, SSL VPN, and WAC.

Life Cycle Management

The [Assets] module allows you to manage asset approval, risk identification, and offline assets by asset life cycle. It displays active assets preferentially to help you operate the active assets first.

Overview

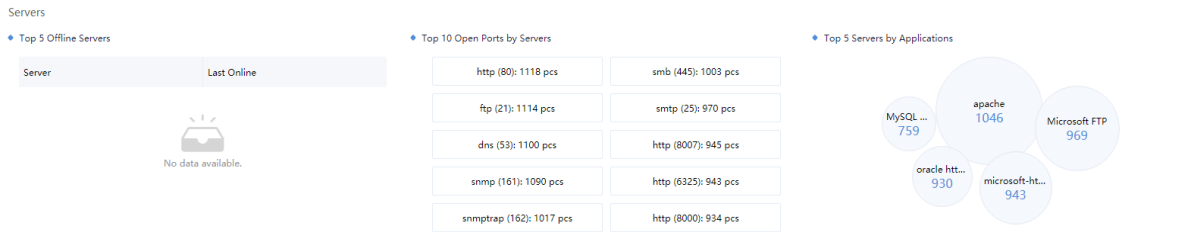
The [Overview] page of the [Assets] module displays the assets and trends in multiple dimensions to help you control and manage the assets. You can filter assets by asset group and time period, as shown in the figure below.



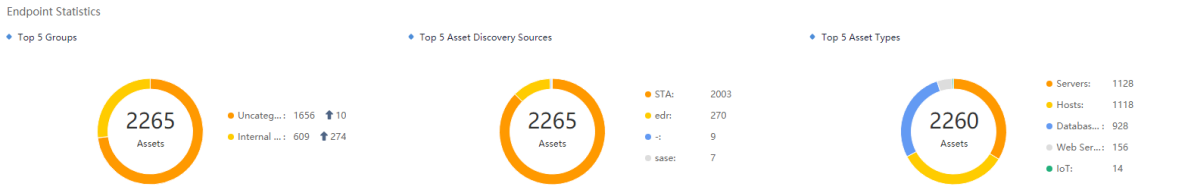
Sections:

<Endpoints>: Displays low activity assets (7 days), active assets, critical assets, servers, hosts, and the asset change trend.

<Servers>: Displays the top 5 offline servers (by last online time), top 10 open ports by servers (by device quantity corresponding to the open port), and top 5 servers by applications (by device quantity corresponding to the application).

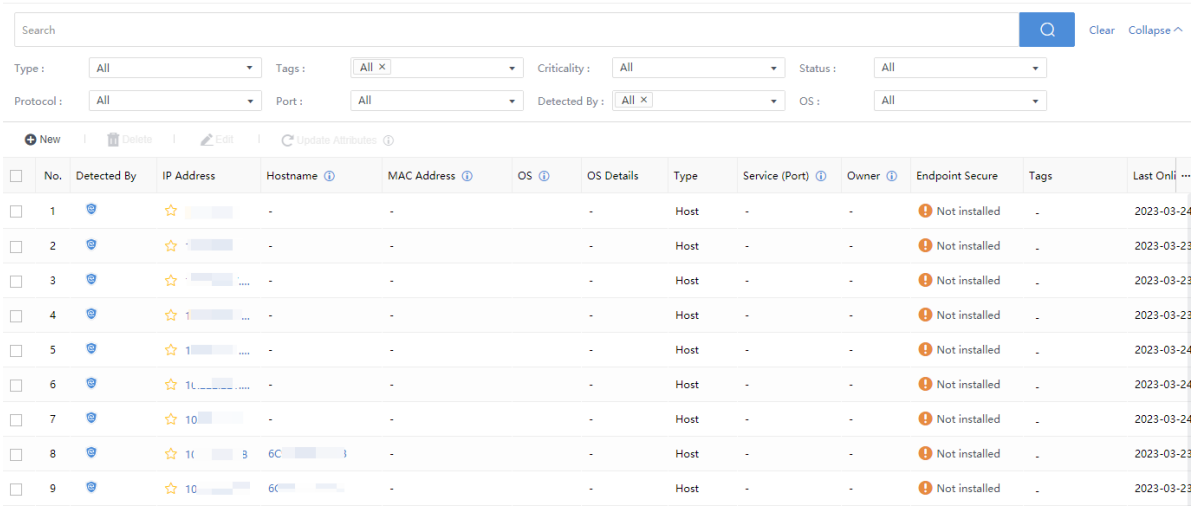


<Endpoint Statistics>: Displays top 5 groups (by asset quantity), top 5 asset discovery sources, top 5 asset types, asset distribution by OS, top 10 server tags, and low activity assets (7 days) with information about the name, tags, and time to be inactive.



Global Search

The [Assets] page supports the global search to help you filter assets. You can enter keywords, such as the endpoint name, MAC address, IP address, and owner, in the search box to search for assets. You can filter by the operating system, service, port, and other conditions, as shown in the figure below.

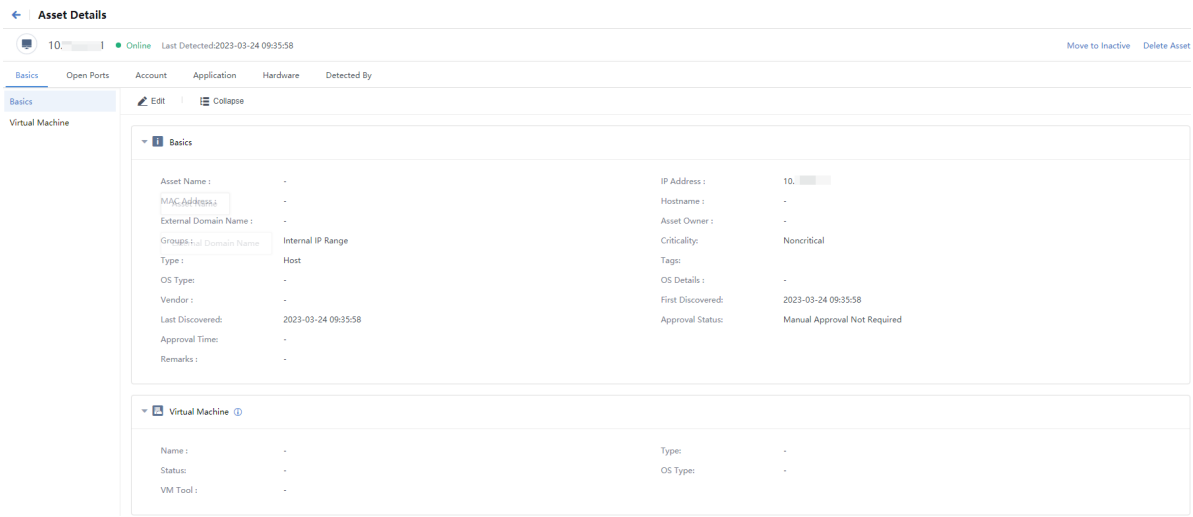


Asset Details

This page allows you to update existing assets and manage assets.

Assets

On the [Assets/Assets/Assets] page, you can click <Details> in the [Operation] column to go to the [Asset Details] page and update or edit the asset information, as shown in the figure below. You can also compare assets, move an asset to inactive, or delete the asset.



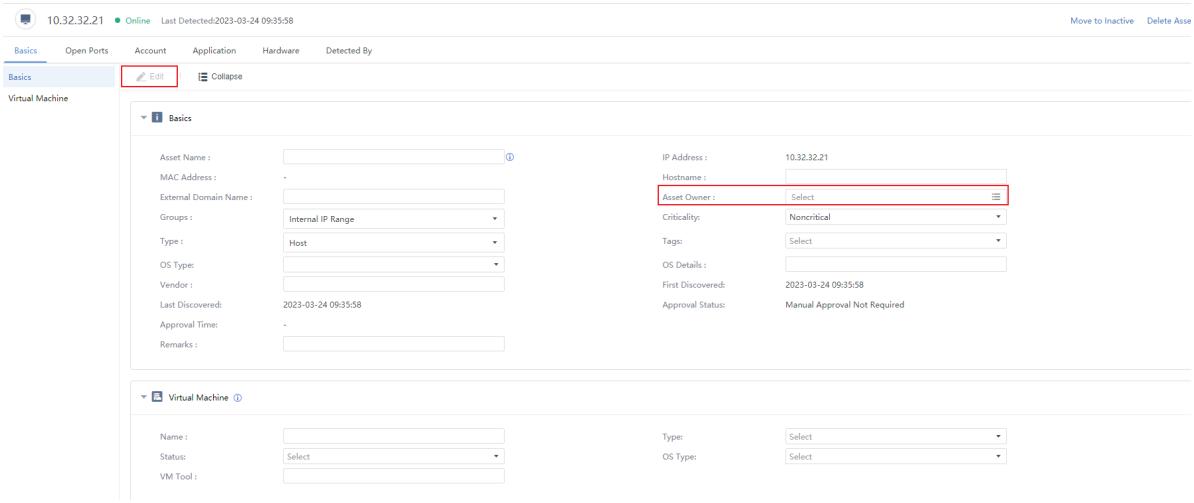
Note:

After the asset is deleted, the corresponding security events and weakness data are also deleted. You can update the asset attributes first, and the platform will update the historical data of the asset synchronously.

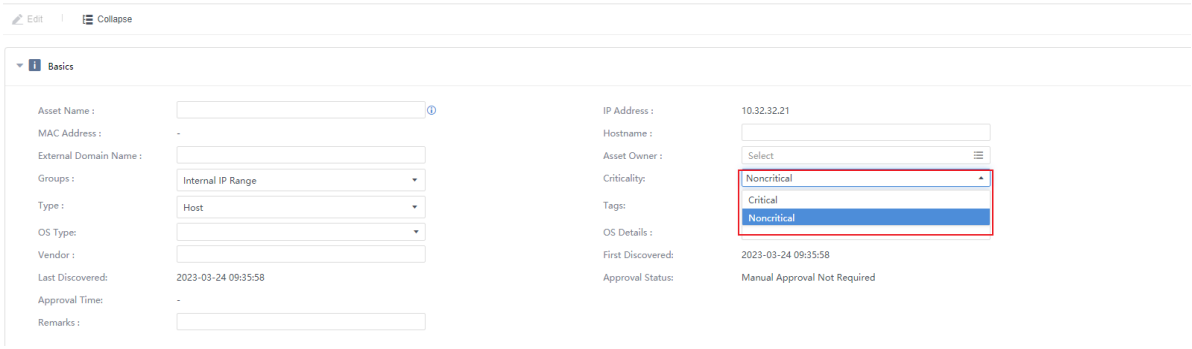
The asset information that can be edited is as follows.

<Basics>: Includes asset name, group, asset owner, location, OS type & details. The virtual machine information on the bottom can also be edited.

<Asset Owner>: You can click the button on the right to select one or multiple asset owners, as shown in the figure below.



<Criticality>: You can select Critical or Noncritical from the drop-down list, as shown in the figure below.



<OS Type> and <OS Details>: You can specify the OS type, vendor, version, and version No.

Virtual Machine: You can fill in VM parameters assigned to the guest OS and VM status obtained from VMP.

<Open Ports>: This tab displays information such as the port, protocol, port accessibility, service, and status. You can filter assets by port accessibility and protocol. You can also search for specific ports by keywords and click <Export> to export the port data.

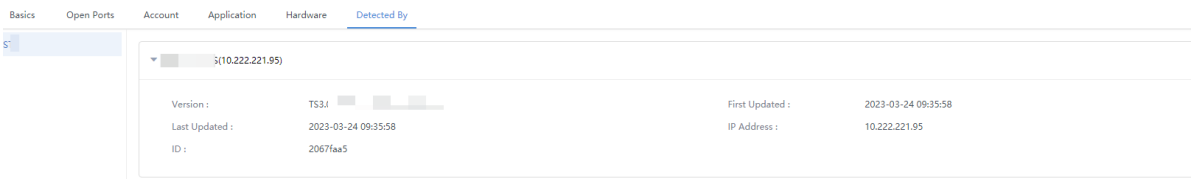
<Account>: This tab displays the account type, account source and last login time. You can search for specific accounts by keywords and click <Export> to export the account data.

<Application>: This tab displays the software, version, category, vendor, installation time, and other information.

<Asset Anomalies>: After the security baseline is configured, this tab can display the asset anomalies.

<Hardware>: This tab displays the information about the motherboard, CPU, MEM module, disk, partition, sound card, GPU, and monitor.

<Detected By>: This tab displays the information about the asset data source, such as Sangfor Visioner, Nova Sensor, and NovaGuard, as shown in the figure below.

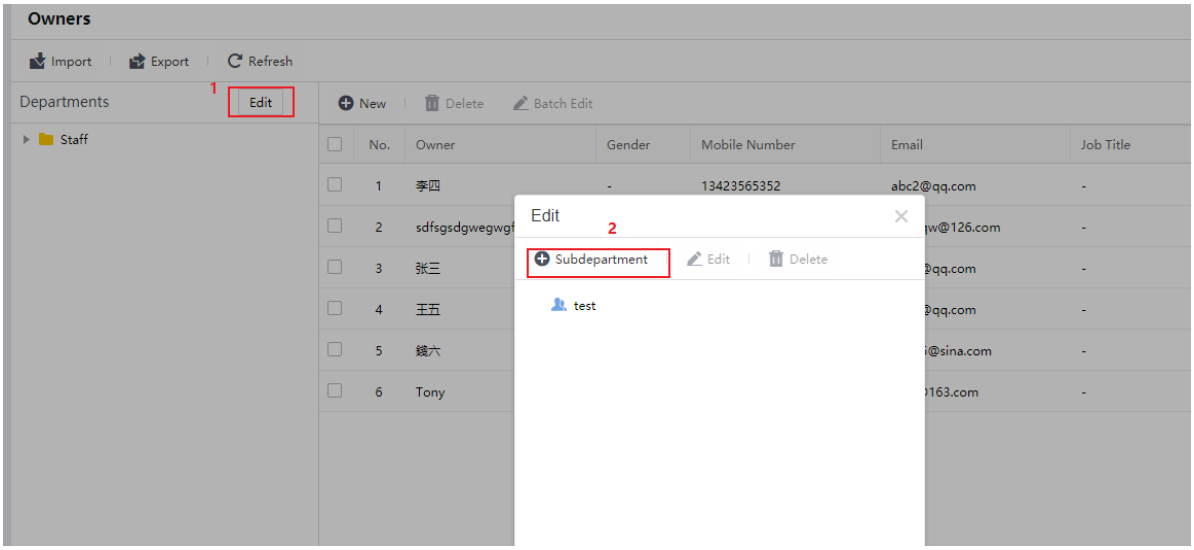


Owners

On the [Assets/Assets/Settings/Owners] page, you can view the information about the owner, including the name, mobile number, email, and assets. You can add new owners or edit or delete existing owners.

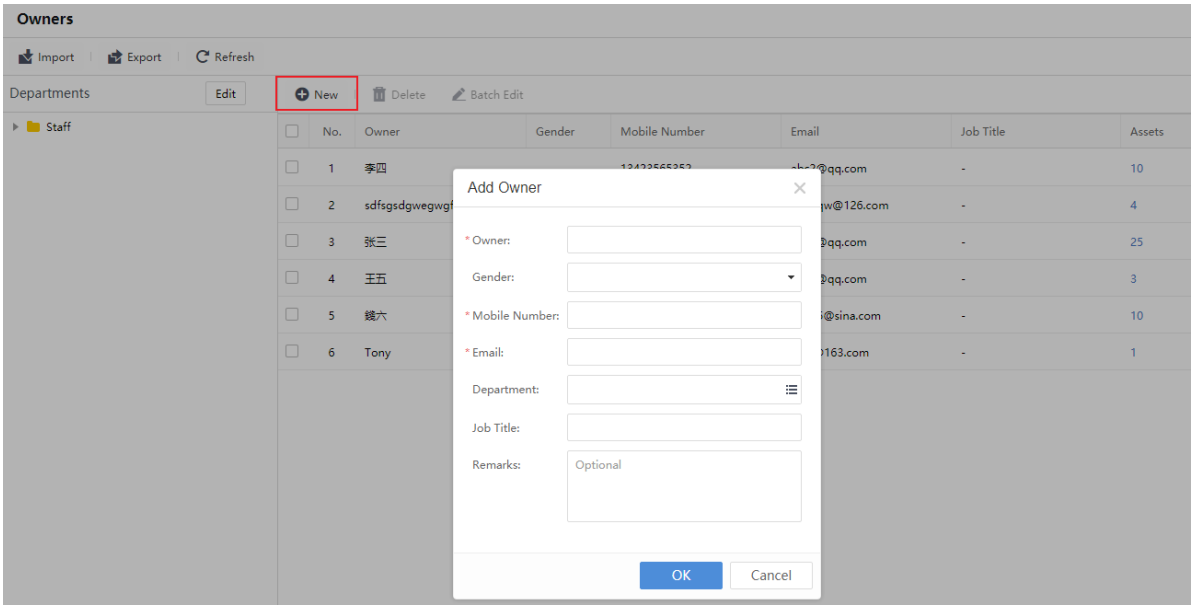
Department management

You can click the <Edit> button on the right side of <Departments> to add new sub-departments or edit or delete existing sub-departments, as shown in the figure below.

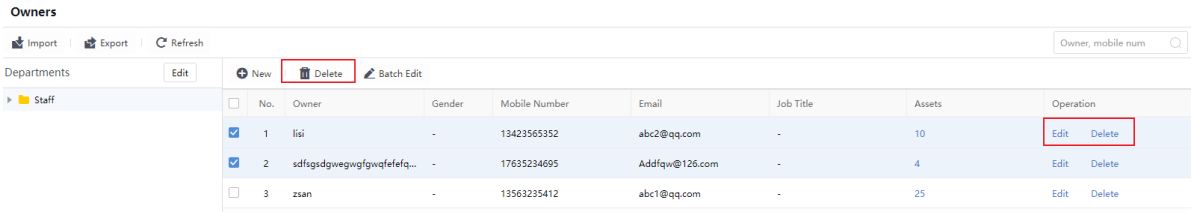


Owner addition

1. To add a new owner, click <New> to pop up the <Add Owner> dialog box. Then, specify the name, mobile number, email, and department information and click <OK>.



2. To import owners in a batch, click<Import> to pop up the <Browse> dialog box. Then, click <Sample File> to download the sample CSV file, specify the owner information in the file, and click <Select> to select and import the file.
3. You can select an owner and click <Edit> in the [Operation] column to edit the owner's information.
4. You can select one or multiple owners and click <Delete> in the [Operation] column to delete them.
5. You can also click <Export> to export the owner's information.

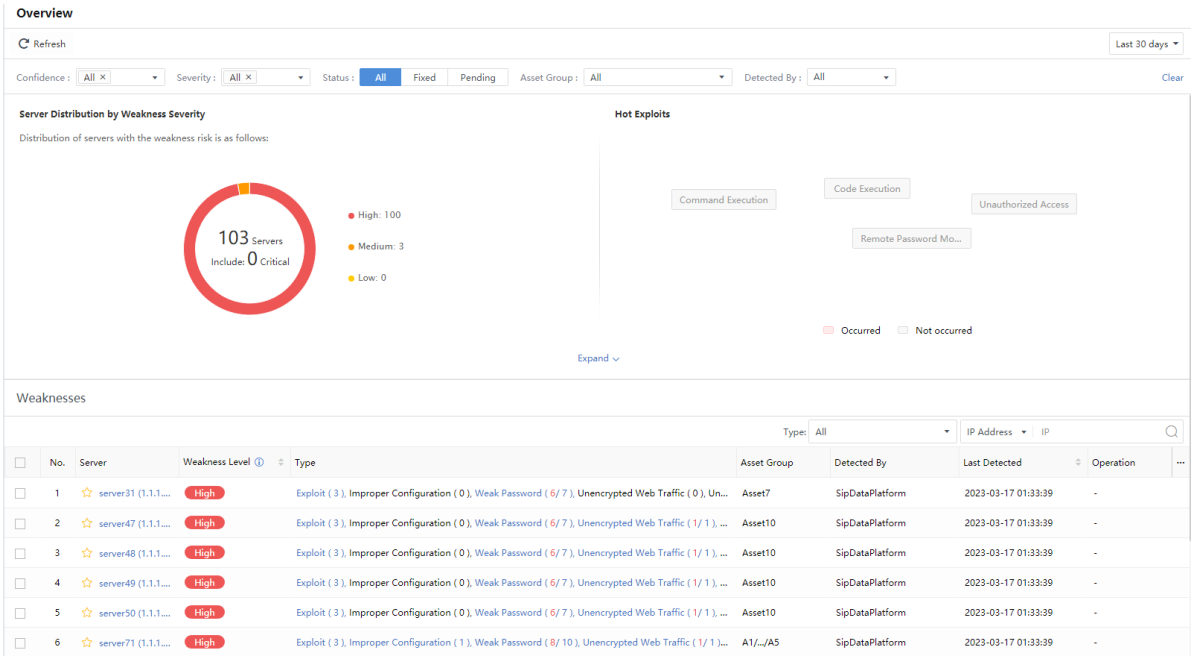


Weaknesses

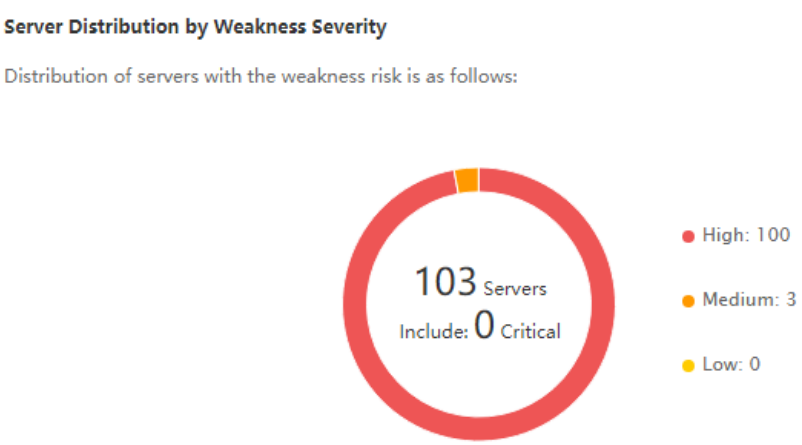
Weaknesses in this module belong to the server itself. Since all threats can only cause damage by exploiting certain server weaknesses, server weaknesses identification and fixing are vital for preventing threats. The [Weaknesses] module can implement weakness analysis of LAN assets, covering vulnerability, weak password, unencrypted web traffic, and improper configuration.

Overview

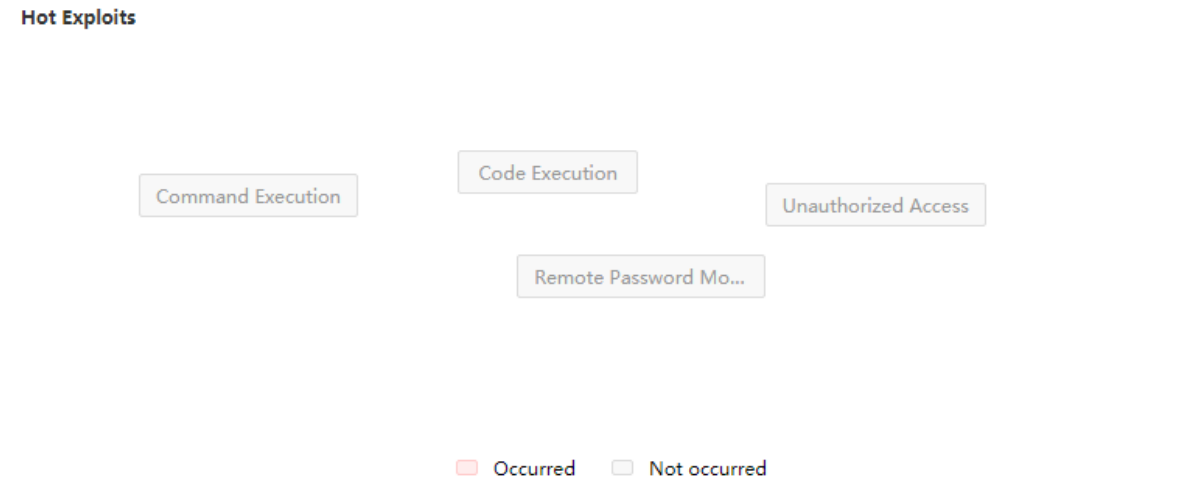
On the [Assets/Weaknesses/Overview] page, you can view the server distribution by weakness severity, hot exploits, and weaknesses information.



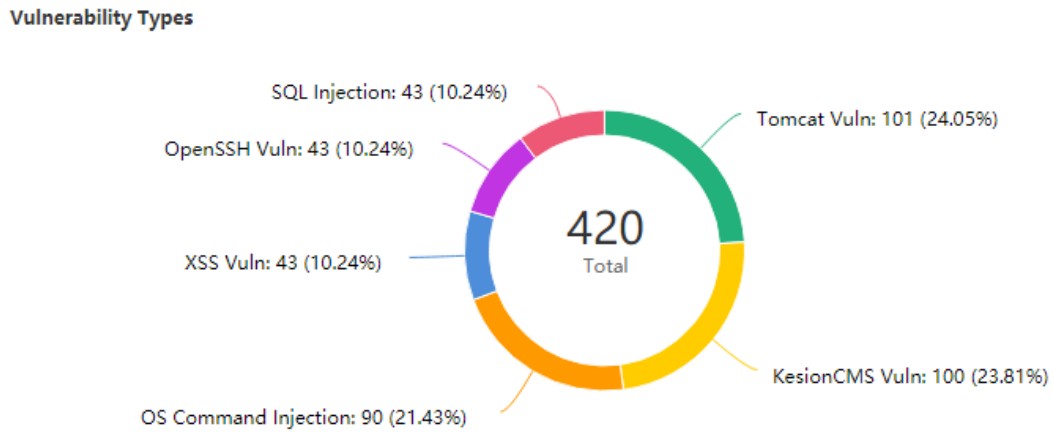
<Server Distribution by Weakness Severity>: This section displays the servers with high, medium, and low-risk weaknesses.



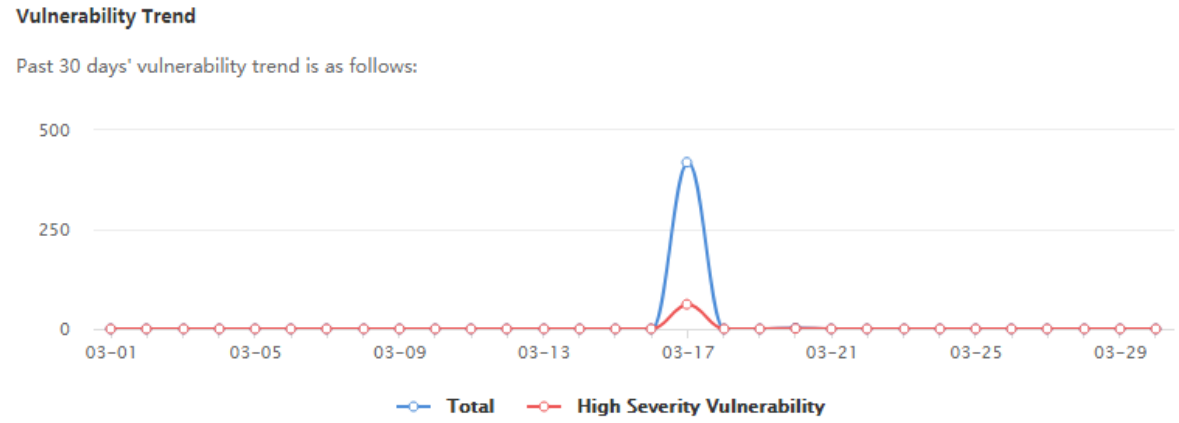
<Hot Exploits>: This section displays common vulnerabilities. The vulnerabilities in red are existing ones.



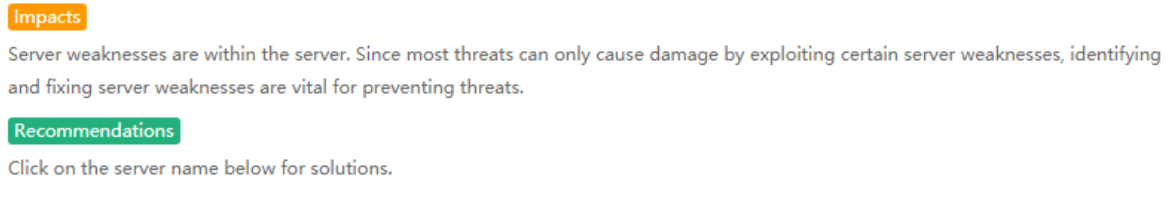
<Vulnerability Types>: This section displays the detected vulnerabilities and the number corresponding to each vulnerability.



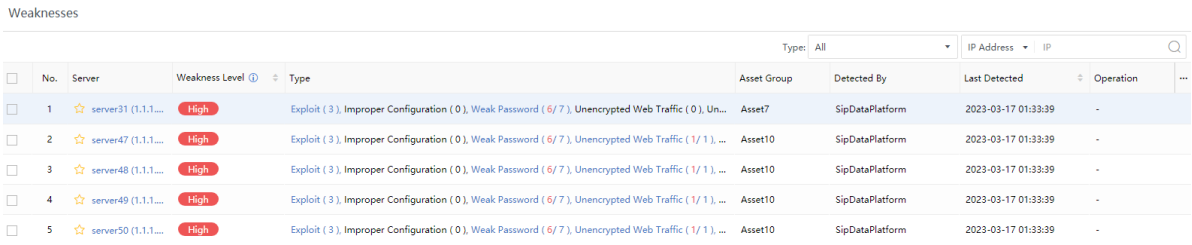
<Vulnerability Trend>: This section displays the trend of total vulnerabilities and high severity vulnerabilities by timeline.



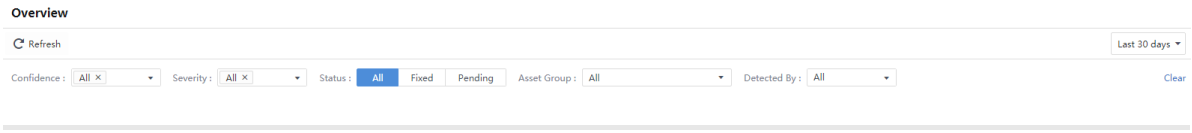
<Impacts and Recommendations>: This section displays descriptions of and fixing solutions to the vulnerabilities.



<Weaknesses>: You can filter weaknesses by type, IP address, vulnerability name, and CVE ID. You can click the data in the [Server] or [Type] column to go to the detailed page of the weakness risk, as shown in the figure below.

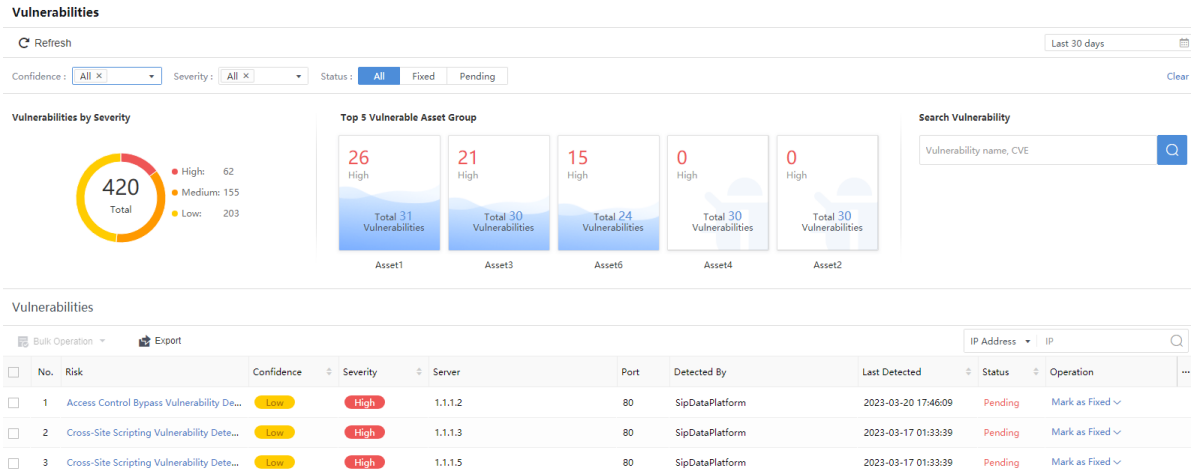


You can filter weaknesses by time period, such as last 24 hours, last 7 days, and last 30 days. After specifying the time period, you can further filter weaknesses by confidence, severity, status, asset group, and data source. The filtered data is saved by default. If you want to filter again, click <Clear>, as shown in the figure below.



Vulnerabilities

On the [Vulnerabilities] page, you can view information about vulnerability severity and top 5 vulnerable groups. You can search for vulnerabilities by vulnerability name and CVE ID. You can also filter vulnerabilities by time period, such as last 24 hours, last 7 days, last 30 days, and custom. After specifying the time period, you can further filter vulnerabilities by confidence, severity, and status, as shown in the figure below.



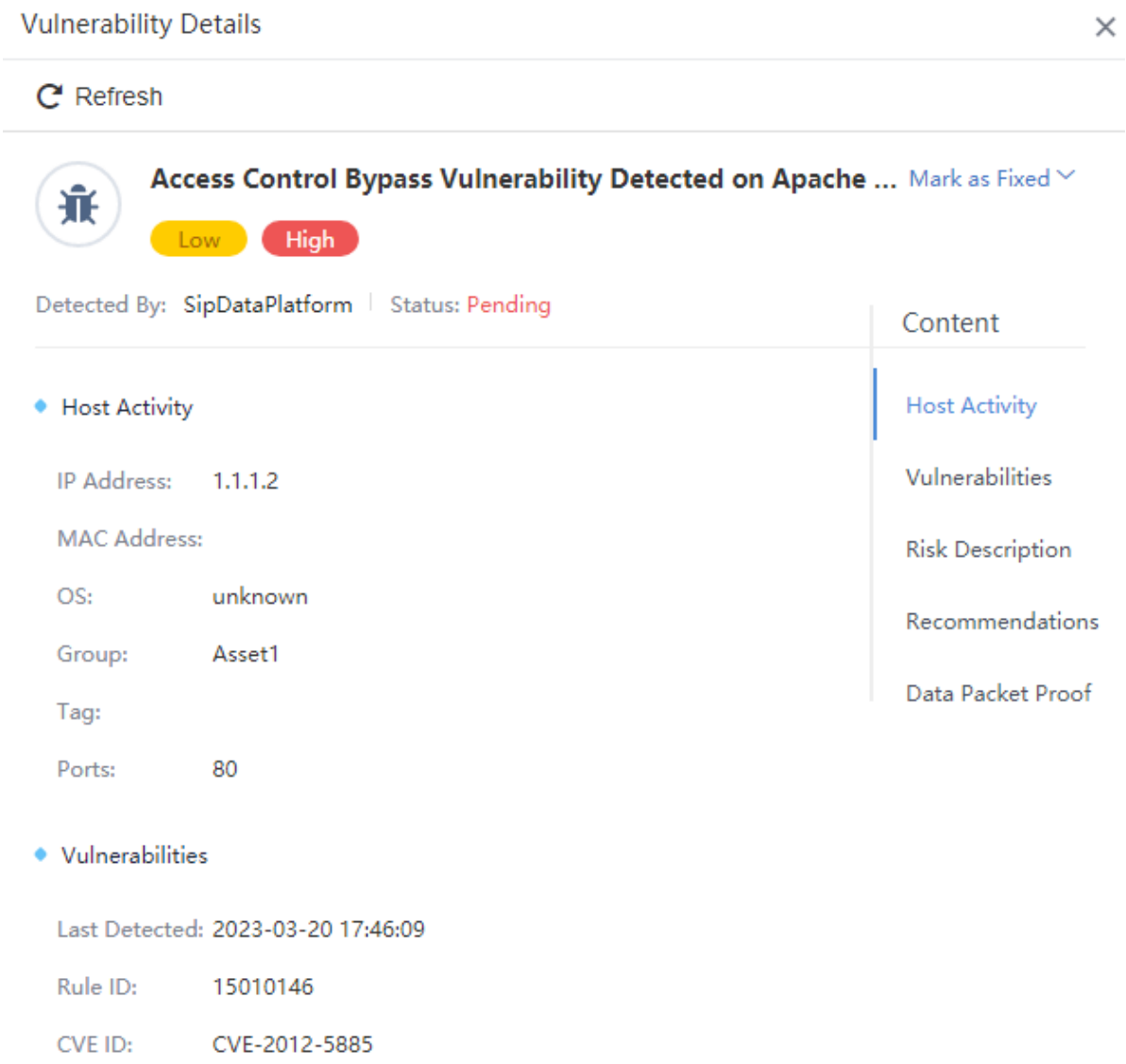
Sections:

<Vulnerabilities by Severity>: This section displays the distribution of high, medium, and low-risk vulnerabilities.

Top 5 Vulnerable Groups: This section displays the top 5 asset groups with the most vulnerabilities and highlights the number of high-risk vulnerabilities.

<Search Vulnerability>: This section allows you to search for vulnerabilities by vulnerability name and CVE ID.

<Vulnerabilities>: This section allows you to filter vulnerabilities by IP address, vulnerability name, and CVE ID. You can click the specific vulnerability to view the detailed information and select "Mark as Fixed" in the [Operation] column, as shown in the figure below.

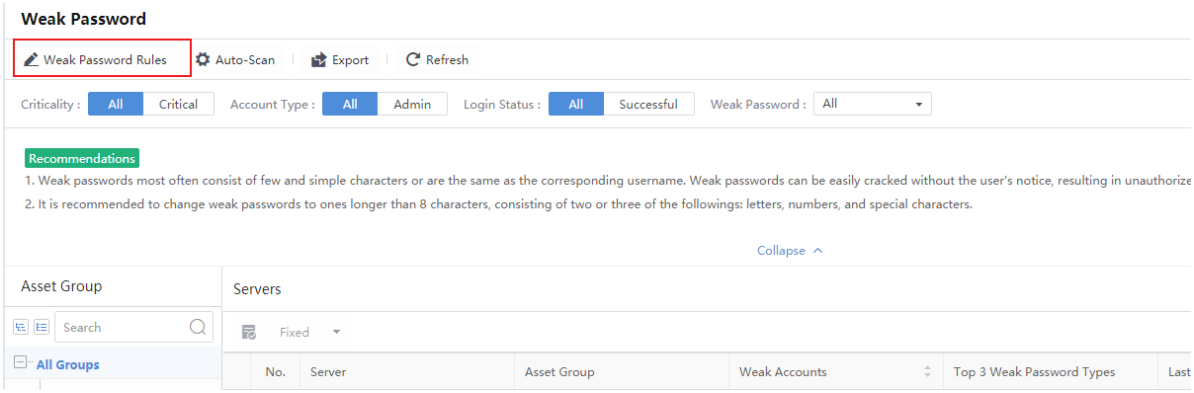


Weak Password

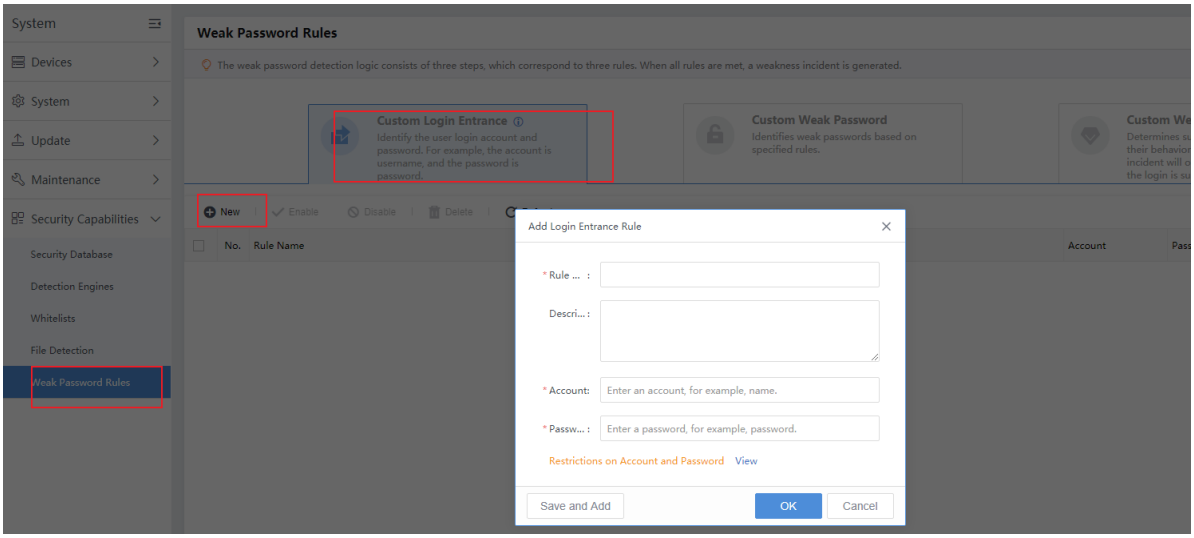
A weak password is of low complexity. For example, the password is a simple combination of digits, the same as the username, or too short. Weak passwords can easily be cracked and exploited by hackers, allowing them to log in and perform control operations by using legitimate accounts and passwords. Such hacking operations are difficult to be detected. On the [Weak Password] page, you can view and operate weak passwords.

Custom login entrance

The [Custom Login Entrance] module allows you to customize web weak passwords and send the weak passwords to Nova Sensor for weak password addition when the built-in login identifier fields cannot meet the requirements for all service scenarios. You can log in to Nova Command and go to the [Assets/Weaknesses/Weak Password] page and click <Weak Password Rules>, as shown in the figure below.



The [System/Security Capabilities/Weak Password Rules] page then appears. You can click <New> on the <Custom Login Entrance> tab.



Fields:

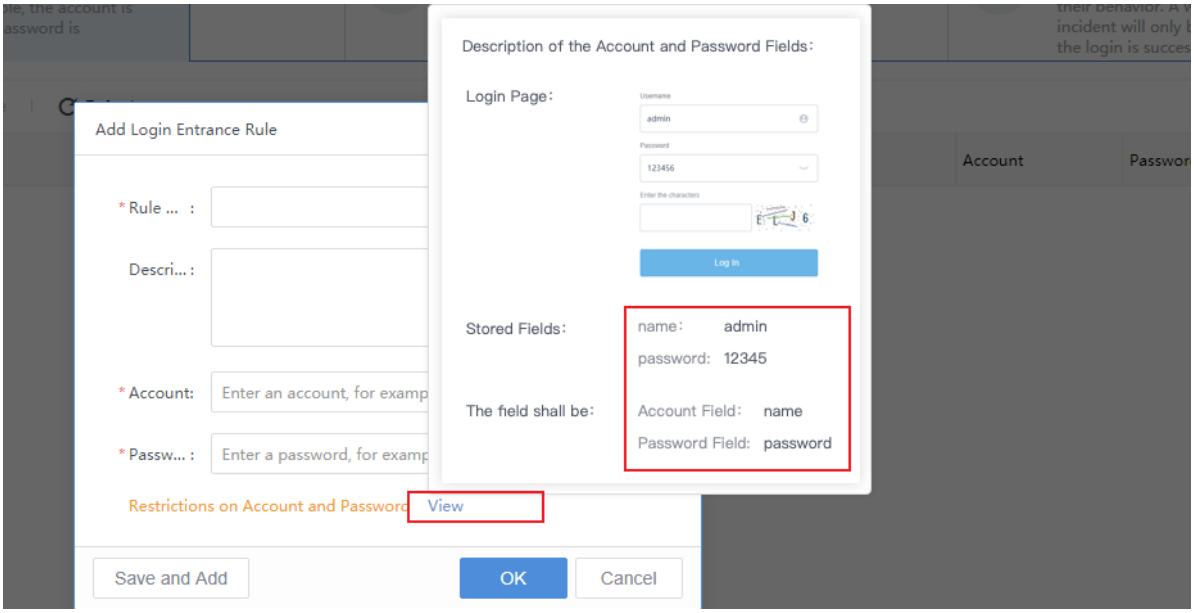
Rule Name: The custom rule name. Digits and letters are supported.

Description: The custom rule description.

Account: The account in the request header or body. Confirm it with the web application O&M personnel of the customer.

Password: The password in the request header or body. Confirm it with the web application O&M personnel of the customer.

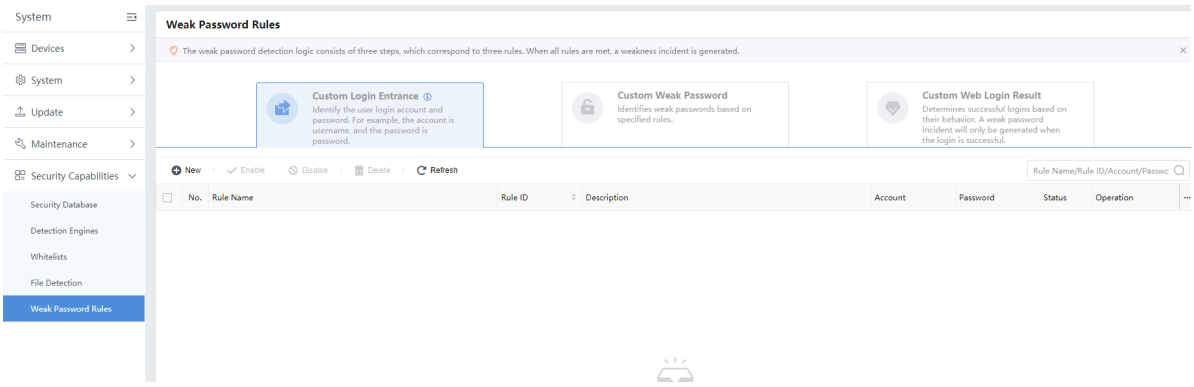
You can click <View> to view the sample of account and password fields.



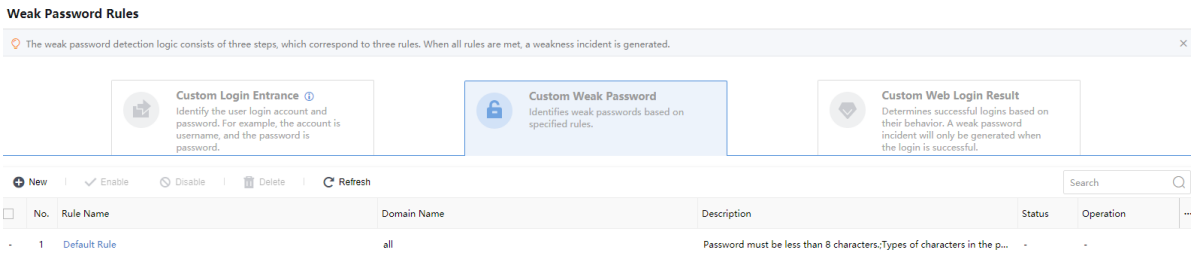
The weak password list with login entrance customized will be pulled by Nova Sensor regularly and synchronized to the [Add Custom Application Ident Rules] page on the Nova Sensor platform.

Custom weak password

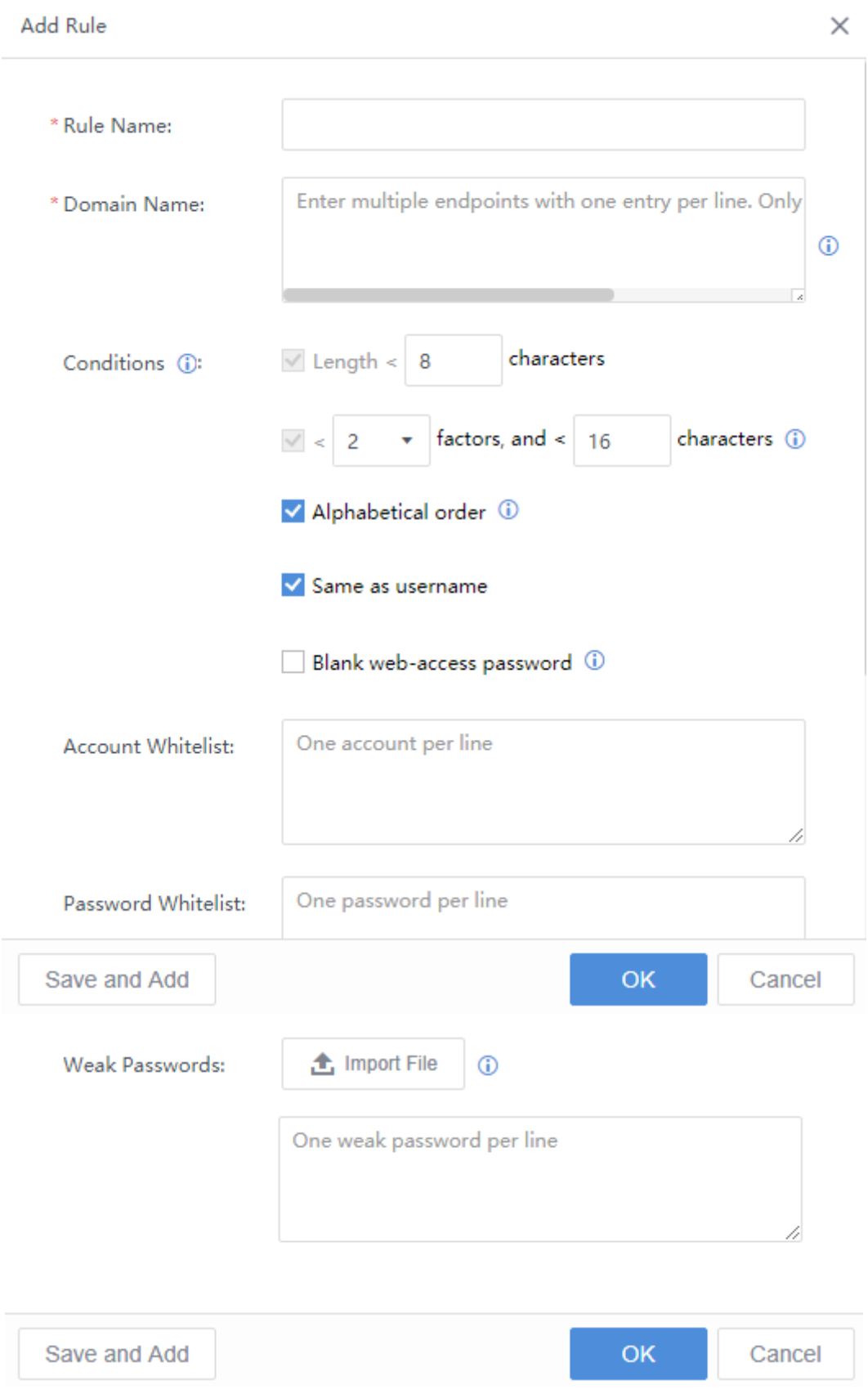
The [Custom Weak Password] module is used for detecting custom weak passwords used by web systems. The rule can be flexibly adjusted based on the customer's actual needs, industry standards, and laws and regulations. You can click <Weak Password Rules> to go to the [System/Security Capabilities/Weak Password Rules] page, as shown in the figure below.



A default rule is provided. You can also customize rules. The built-in default rule applies to both web and non-web applications. The custom rules apply only to web applications. You cannot edit or delete the default rules, as shown in the figure below.



You can click <New> to pop up the [Add Rule] dialog box and then specify the domain name, conditions, account whitelist, password whitelist, and other information, as shown in the figure below.



Fields:

Rule Name: The custom rule name for the weak password rule.

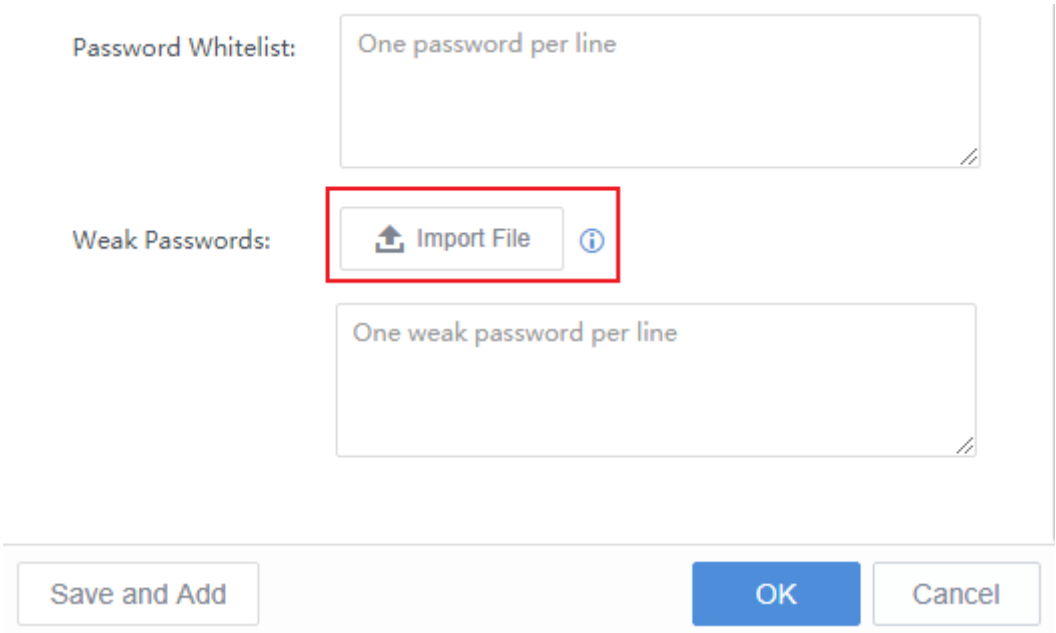
Domain Name: The applicable domain name or URL. Example: http://xxx:80/a/b/c?1=1{.url target="_blank"}. In this URL, http:// indicates the request protocol of the traffic. xxx indicates the endpoint address, which can be the domain name, endpoint name, or endpoint IP address. 80 next to the colon (:) indicates the port number. /a/b/c indicates the resource path.

1=1 next to the question mark (?) indicates the domain name content.
You can refer to the value of Host in the request traffic.

Conditions: The minimum password length, character factors and number, and options of alphabetical order, same as username, and blank web-access password need to be specified.

Account Whitelist: If the weak passwords obtained through the product-side analysis do not meet the customer's service scenario or actual situation requirements, you can customize the whitelist to prevent vulnerability events.

Weak Passwords: If only several weak passwords exist, you can enter them in the text box directly. If there are too many weak passwords, you can import them using a TXT file by clicking <Import File>, as shown in the figure below.

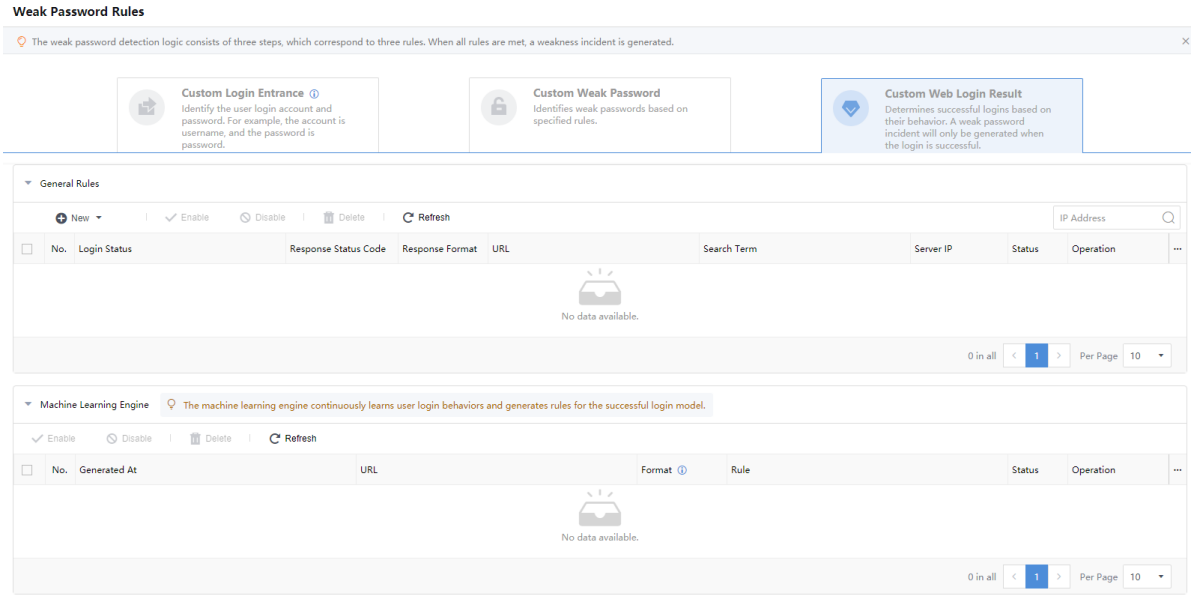


Note:

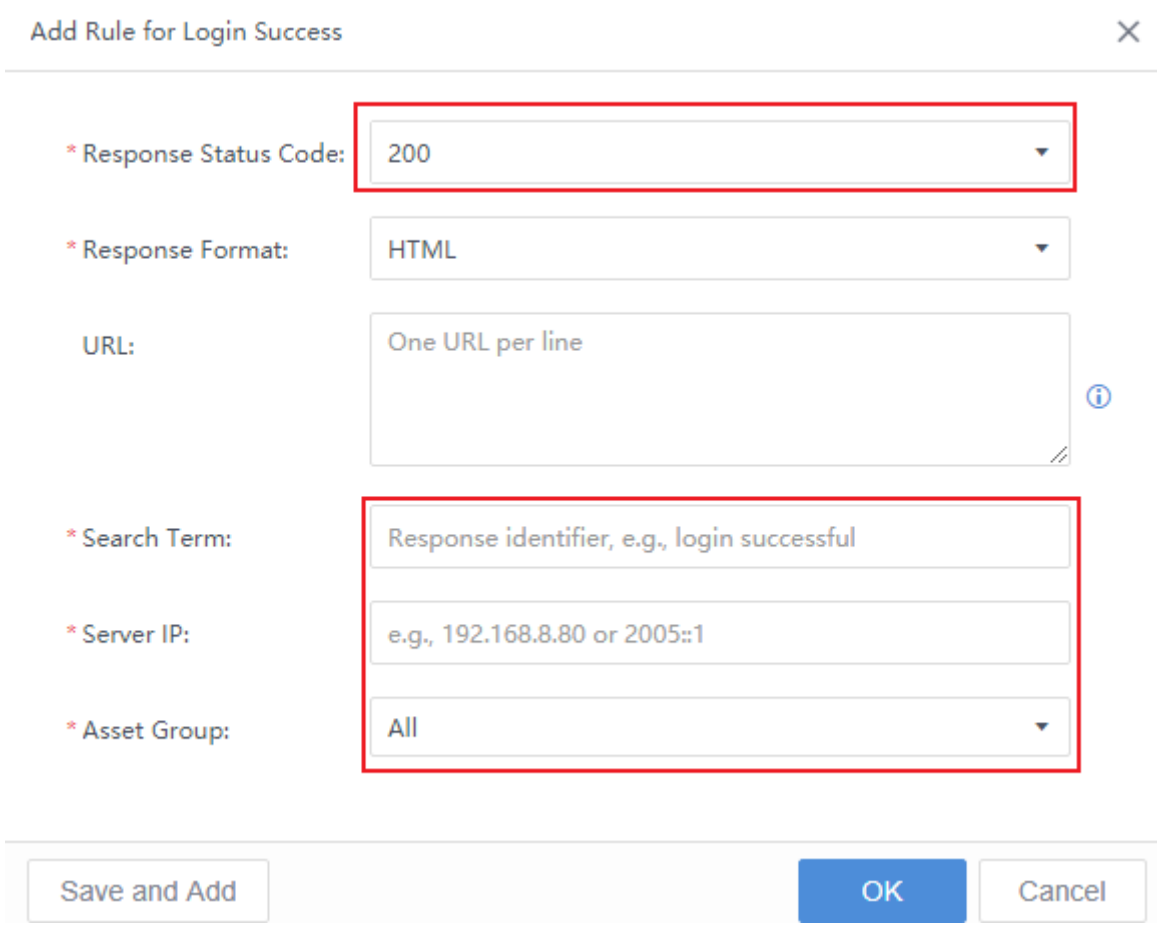
1. A maximum of 50 web domain names or URLs related to the custom weak password rule are allowed.
2. Priority: The custom weak password rule has a higher priority than the default rule. Weak passwords are identified based on the custom rule first and then the default rule.

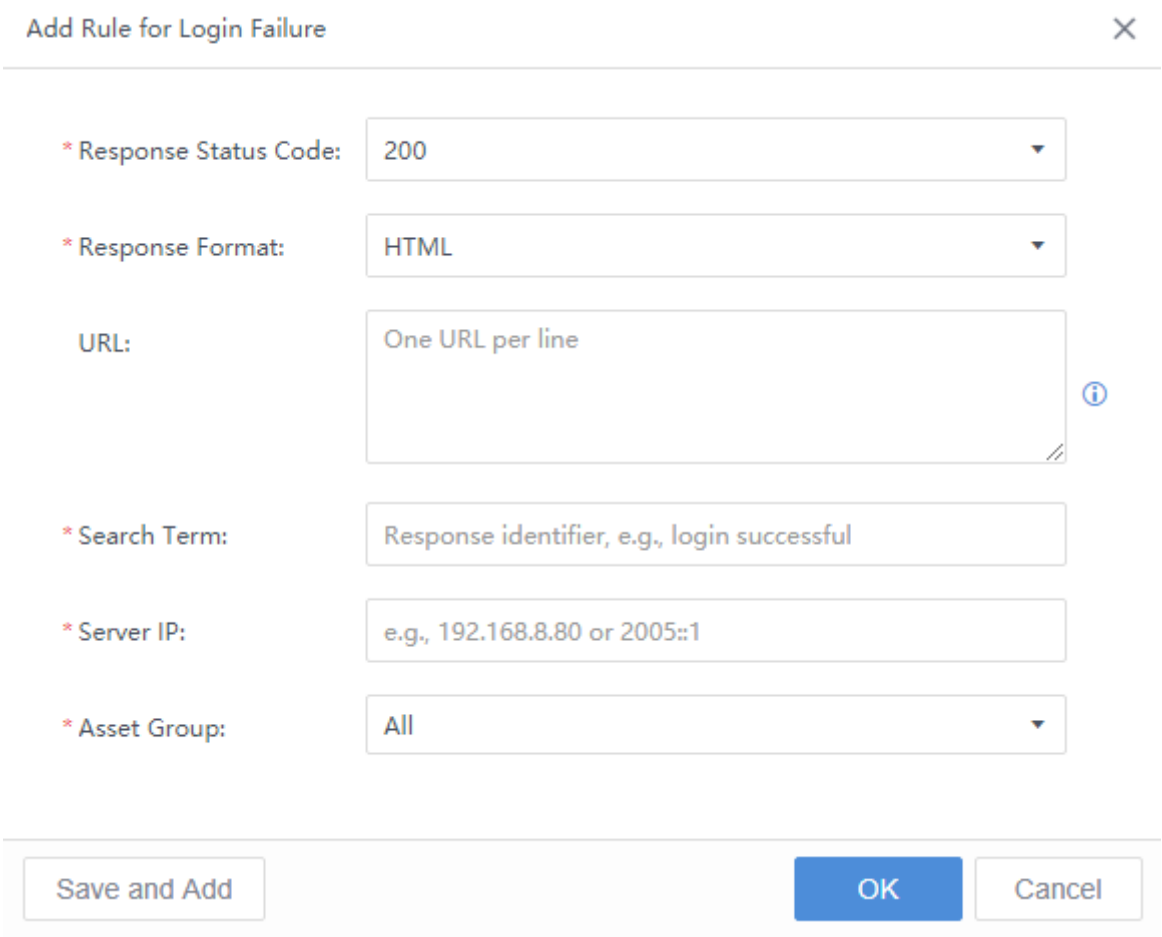
Custom web login result

On the [Assets/Weaknesses/Weak Password] page, click <Weak Password Rules> to go to the [Weak Password Rules] page. Then, click the [Custom Web Login Result] tab, as shown in the figure below.



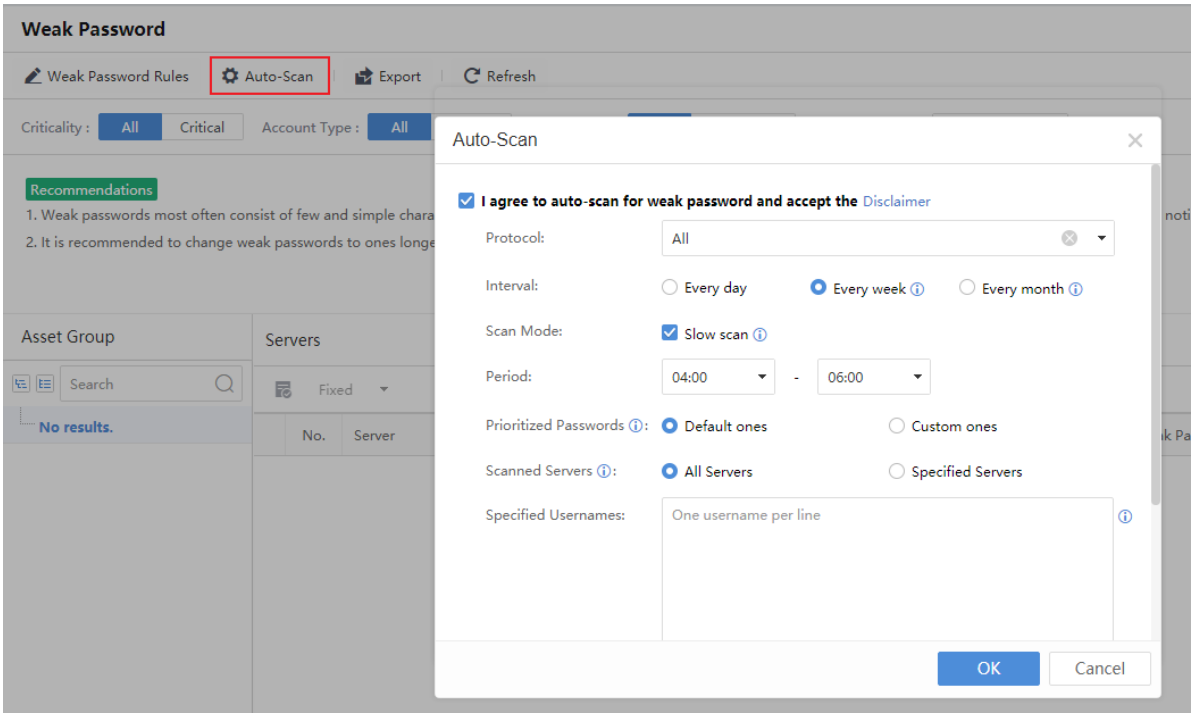
Successful login and failed login are two results of web login. The web login rules are used on Nova Command to correct the identification result of the login result if the login result is different from the customer's actual situation. The rules use the status codes of success and redirection in the HTTP protocol to match the content of the successful login and server IP address, as shown in the figure below.





Auto-Scan

You can click <Auto-Scan> to modify the scanning policy, including parameters such as the protocol, interval, and scan mode, as shown in the figure below.



Fields:

<Protocol>: All protocols are selected by default. SMB, MySQL, Oracle, and more protocols are supported.

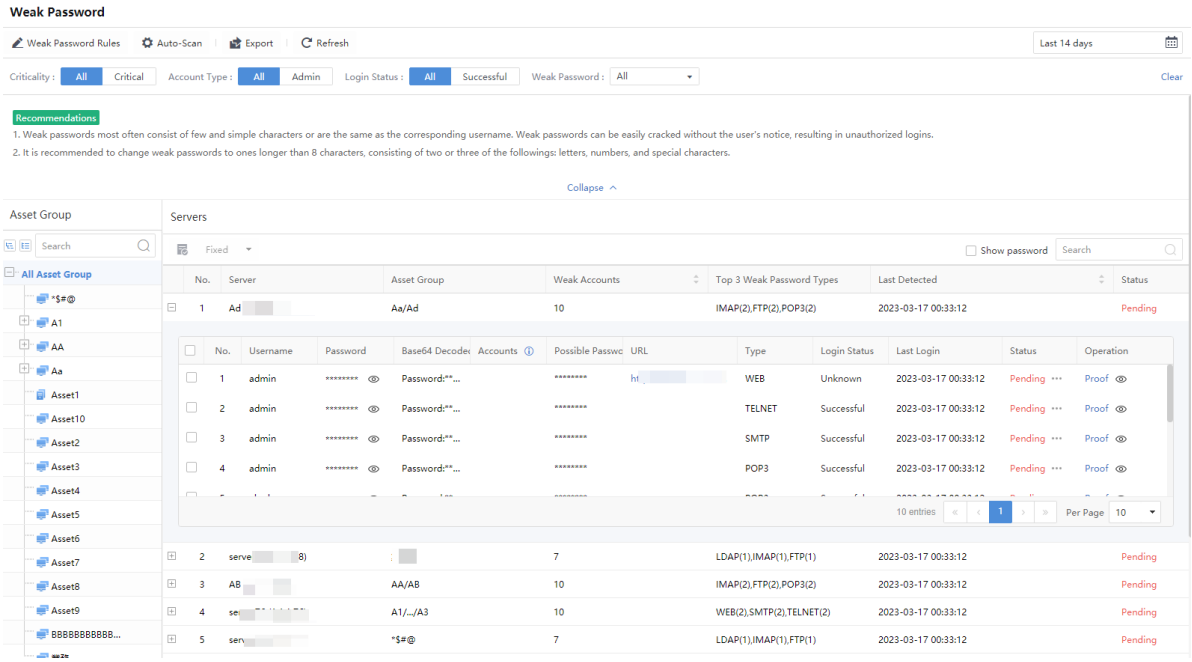
<Scan Mode>: We recommend that you select slow scan to reduce the server load and avoid blocks by security devices.

<Prioritized Passwords>: The possibility exists in logins to some applications, such as MySQL and Oracle, with multi-factor credentials that login with secondary credentials may be rejected since those applications most often apply multi-factor authentication, supporting configuration of maximum login attempts of 10. You can specify this parameter as required.

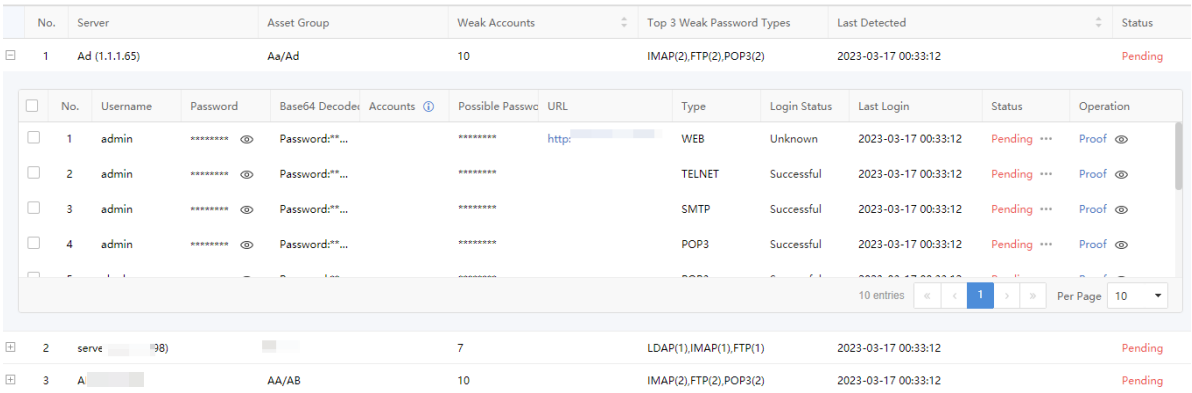
<Scanned Servers>: All servers indicate the servers detected on Assets. Specified servers indicate the specified ones that have been detected.

Weak password search

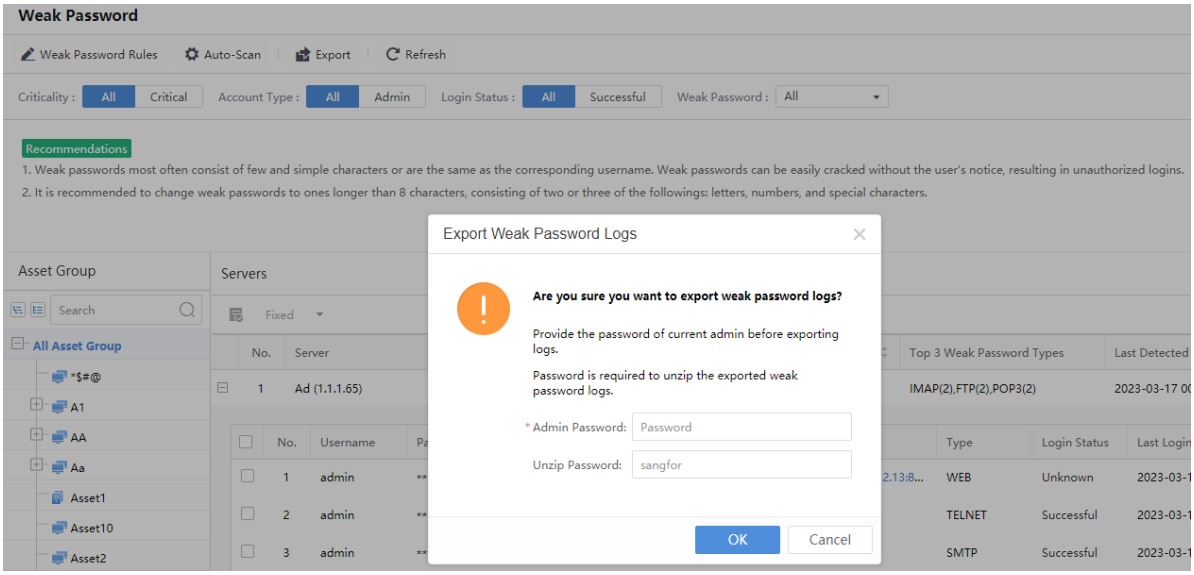
You can filter weak passwords by time period, criticality (All or Critical), account type, login status, weak password type, and group, as shown in the figure below.



You can click the plus (<+>) icon on the left of a server to view details and click <Proof> in the [Operation] column to view the hidden account password, as shown in the figure below. You can select fixed weak password events in batches and mark them as <Fixed> on the top of the table.



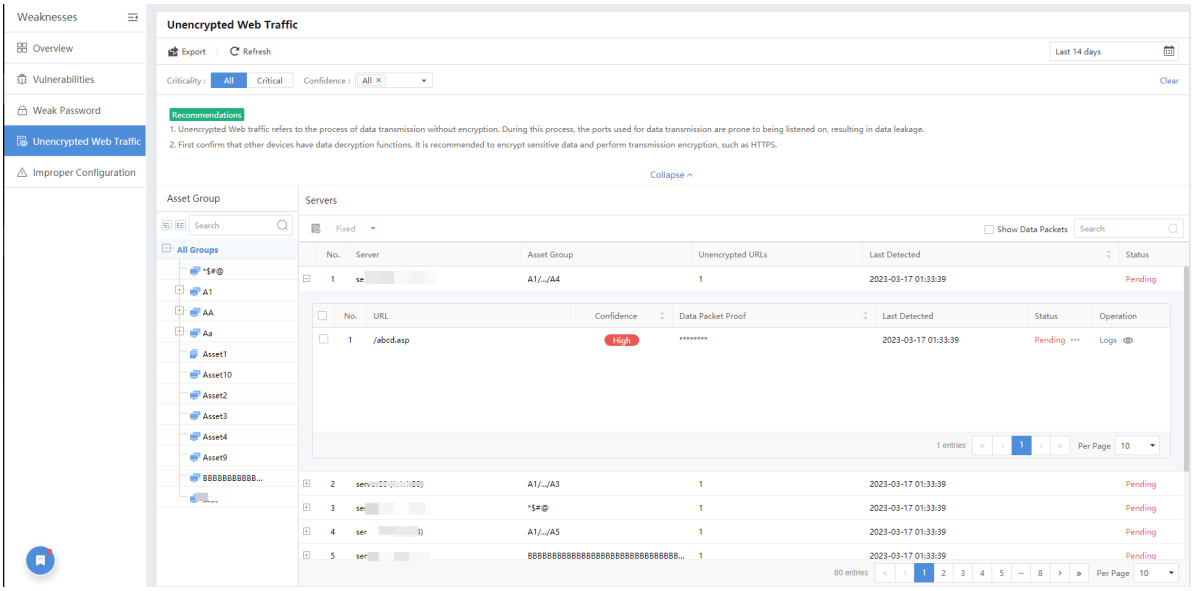
You can click <Export> to export the weak password detection results. This operation requires the admin password, which is <sangfor> by default. You can also customize the file decompression password to ensure data security.



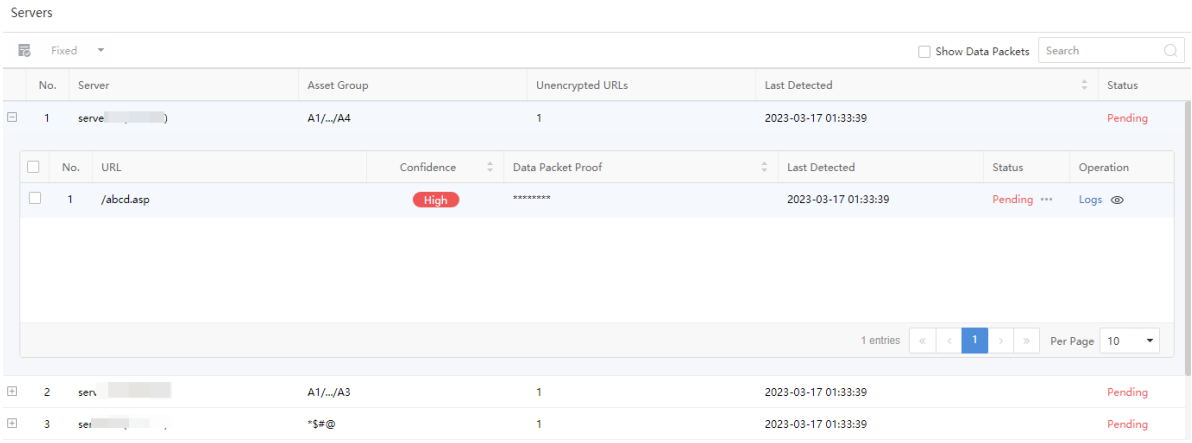
Unencrypted Web Traffic

Unencrypted Web traffic refers to the process of data transmission without encryption. During this process, the ports used for data transmission are prone to be listened to, resulting in data leakage. On the [Unencrypted Web Traffic] page, you can view and operate detection results of the unencrypted web traffic.

You can filter the detection results by time period, criticality (All or Critical), confidence, and group. You can also view data packets and search for specific results by keywords, as shown in the figure below.



You can click the plus ("+") icon on the left of a server to view details and click <Logs> in the [Operation] column to view the hidden data packet proof. You can select fixed unencrypted web traffic events in batches and mark them as <Fixed>, as shown in the figure below.



Fields:

<Server>: The IP address of servers that have unencrypted web traffic.

<Unencrypted URLs>: The number of detected unencrypted URLs.

<Last Detected>: The latest occurrence time of unencrypted web traffic.

<URL>: The domain name or URL that involves unencrypted web traffic.

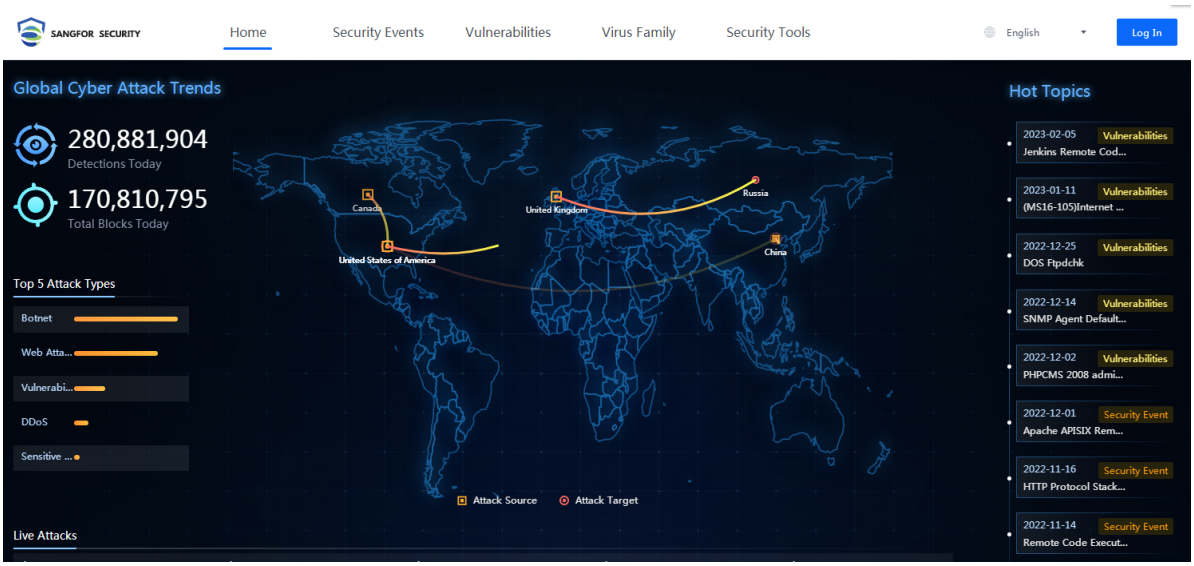
<Data Packet Proof>: The password is obtained by checking the data of packet.

You can click <Export> to export the unencrypted web traffic detection results.

Toolkit

Security Incident Database

A database offered by the Sangfor Security team. Security Incident Database provides professional and detailed introductions to common vulnerabilities and attack techniques, as well as specialized and practical security solutions. You can click <Details> to go to the security incident database website (https://wiki.sec.sangfor.com/index/abroad{.urltarget="_blank"}) to view and search for security events, as shown in the figure below.

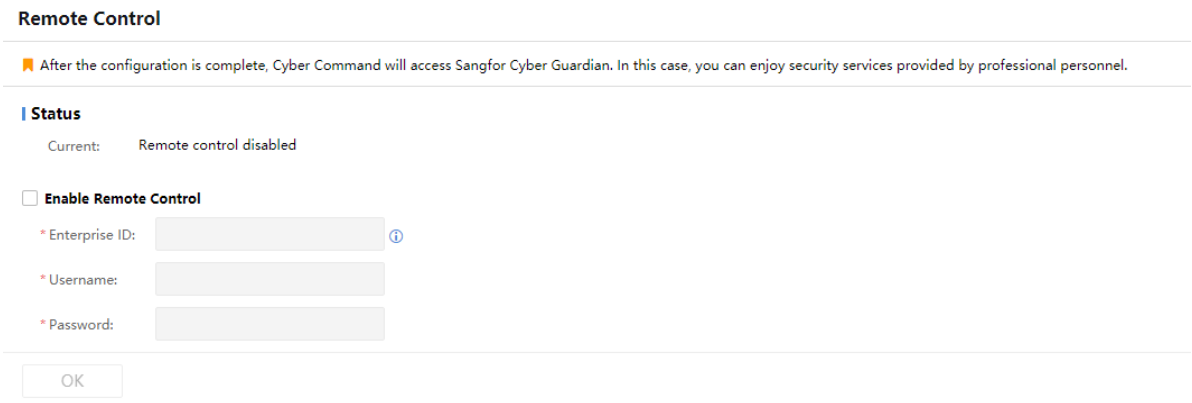


NovaMDR

A security service management platform that integrates cloud monitoring, endpoint monitoring, traffic detection, big data analysis, threat intelligence, and experts. NovaMDR helps you quickly identify and resolve security problems 24/7 hours. NovaMDR provides remote control and data upload modules. The Remote Control module allows remote access from the expert team, and the Data Upload module aims to report the detection data to the cloud for analysis by the expert team.

Remote control

On the [NovaMDR/Remote Control] page, you can select <Enable Remote Control> and specify the enterprise ID, username, and password, and synchronize the data to local storage. After the configuration is completed, Nova Command will be connected to NovaMDR. In this case, you can enjoy security services provided by professional personnel, as shown in the figure below.



Note:

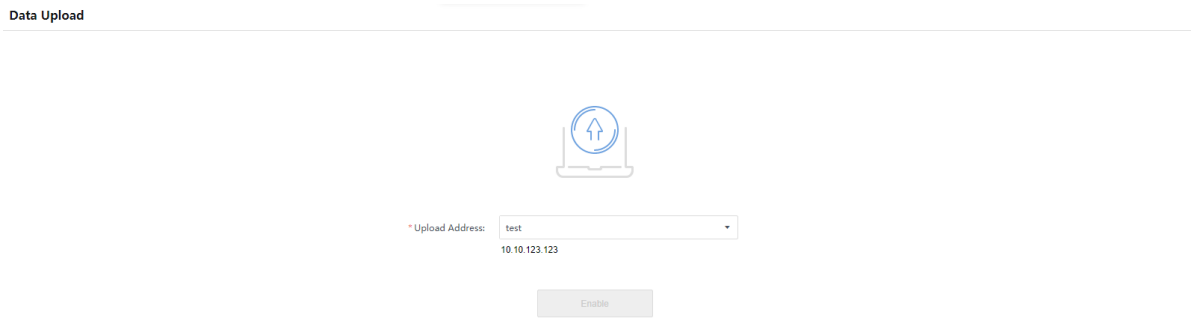
1. You can click <Help> in the upper right corner for more details about NovaMDR.
2. The enterprise ID is the unique ID of the enterprise that purchased the NovaMDR service. The supported formats include:

a. Eight digits. Example: 18654723.

b. Combination of a single IP address and port. Example: 200.200.222.111:8080.

Data upload

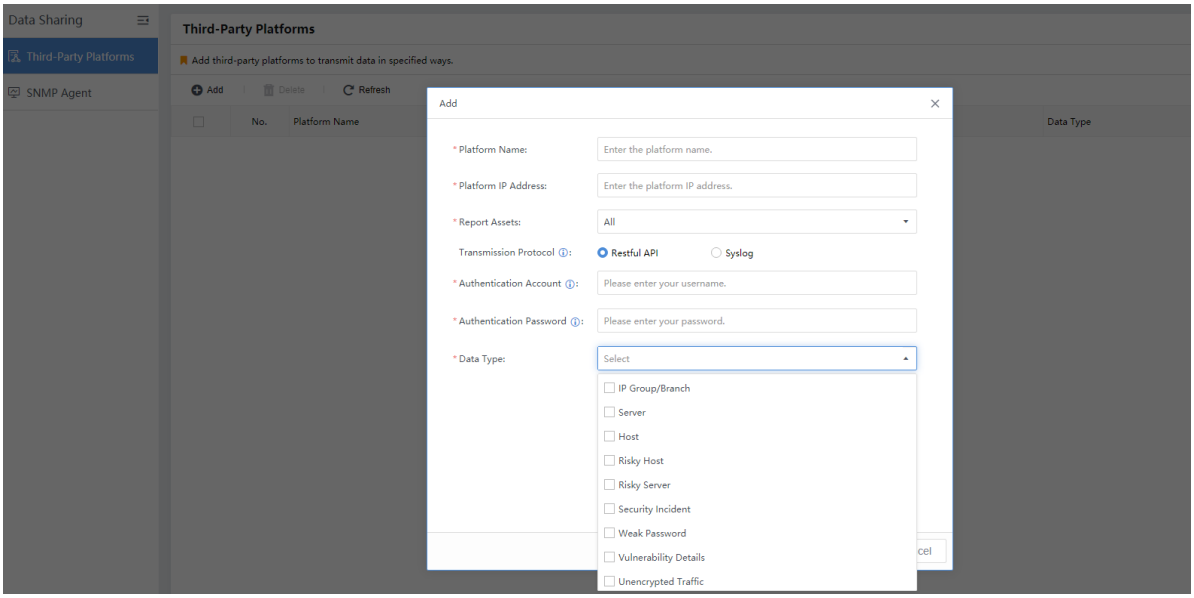
On the [NovaMDR/Data Upload] page, you can click <Enable> to enable data upload for analysis by the expert team. You can also synchronize the data to local storage, as shown in the figure below.



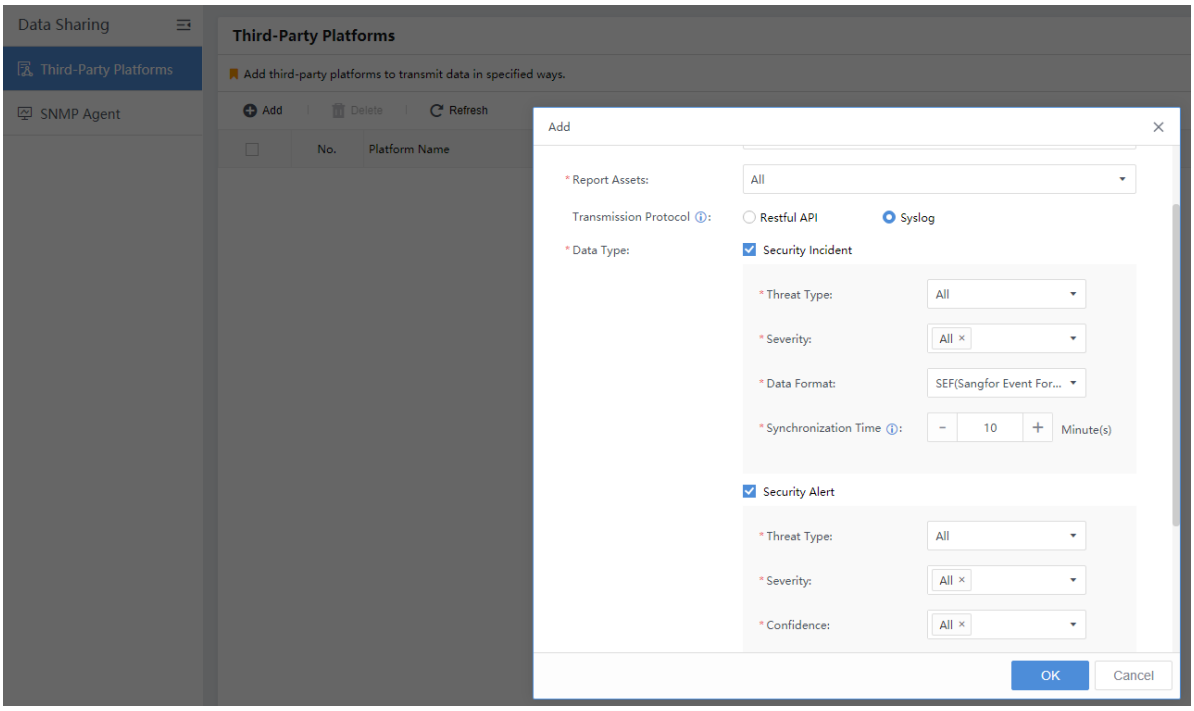
Compliance and Sharing

Data Sharing

The Data Sharing function can make data more valuable
by opening and sharing them through the RESTful API/Syslog protocol. You can click <Details> to go to the [Data Sharing/Third-Party Platforms] page. On the page that appears, click <Add> to add a third-party platform that uses the RESTful API/Syslog protocol for connection, as shown in the figure below.



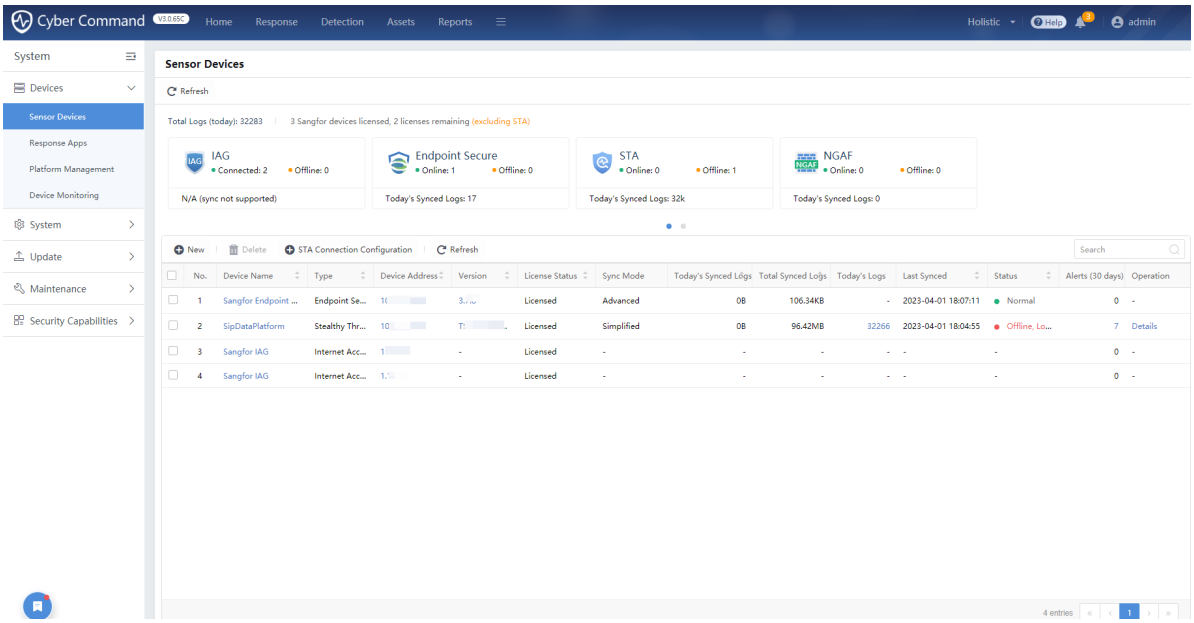
When you use Syslog to synchronize security events and security alerts, you can filter them by "Threat Type" and "Severity". The default synchronization period is 10 minutes. You can also manually change the period to a value from 3 minutes to 30 minutes, as shown in the figure below.



System Settings

System

You can make detailed settings for Nova Command here, including settings of devices, system, update, maintenance, and security capabilities.



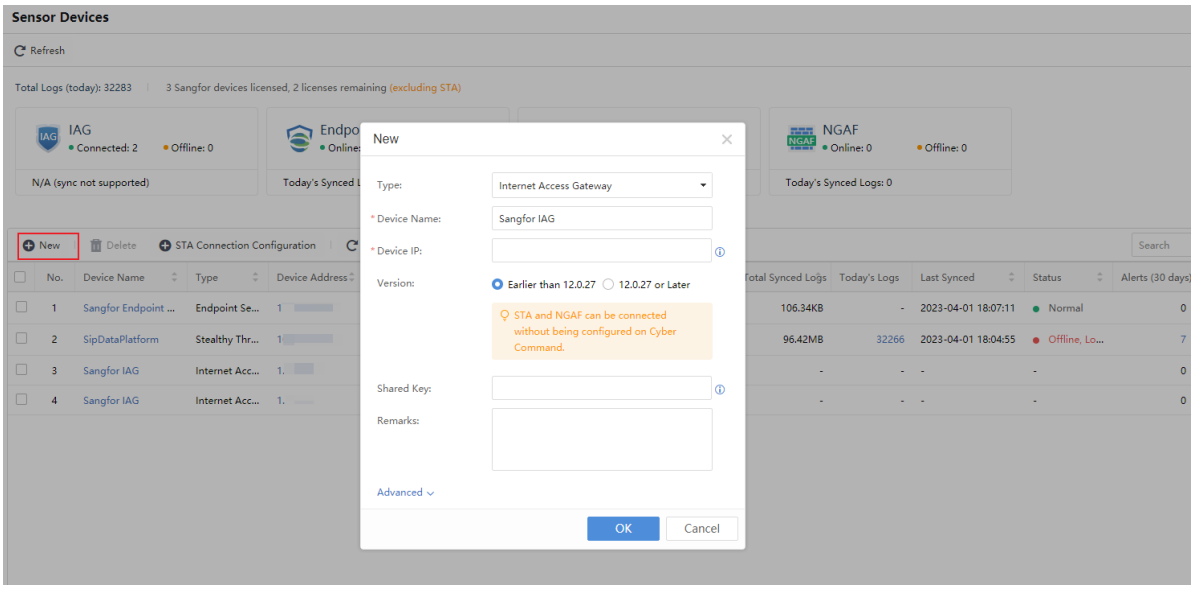
Devices

This module mainly contains the management of connected devices and application scenarios and monitoring of Nova Command. Devices such as Nova Sensor, IAG, NGAF, and NovaGuard can be connected to Nova Command. You can add, delete, and view devices on the Sensor Devices page. Application scenarios include connected platforms and clusters.

Management of Connected Devices

Configuration of new connected devices

1. On the [admin/System/Devices/Sensor Devices] page, click <New> to add a new device to be connected to Nova Command, as shown in the following figure. You can refer to [Sangfor Device Connection] for the configuration of the connected device.



2. Enter the IP address and name of the connected device and select the device type. Then, click <OK>.

Fields:

Sync Mode: The synchronization mode for uploaded logs, including simplified mode, standard mode, and advanced mode.

Today's Synced Logs: The size of logs uploaded by the device on the current day, in unit of B, KB, or MB.

Total Synced Logs: The total size of logs uploaded by the device, in unit of B, KB, or MB.

Today's Logs: Quantity of logs uploaded by the device on the current day.

<Last Synched>: The time of last log uploading by the device.

Status: Status of the device, which can be Online or Offline. The status of IAG and SSL VPN is displayed as a short dash (-).

Alerts (30 days): An alert will be generated when the connected device reports an error.

Operation: You can view the traffic details of the connected device.

Note

1. To connect IAG to Nova Command, the same shared key is required.
2. To connect NGAF to Nova Command, complete the configuration on NGAF. When the configuration is completed, NGAF info will be displayed on the [Sensor Devices] page. If NGAF uses two-way authentication, the same account and password should be configured on Nova Command.
3. To connect NovaGuard to Nova Command, complete the configuration on NovaGuard or Nova Command.
4. To connect SSL VPN to Nova Command, specify the IP address of SSL VPN.
5. To connect Nova Sensor to Nova Command, complete the configuration on Nova Sensor.

Platform Management

In this module, the data of a branch platform is synced to the primary platform. You can view all security incidents on the primary platform.

Application scenarios

This module is mainly used by the supervision organization and the regulatory organization.

1. When a severe security incident occurs in the branch platform, a notification will be sent, requiring the branch platform to make rectifications to avoid the risk of wider spread.
2. Regarding hot and emergency incidents, alerts will be generated and sent to the branch platform in a timely manner for taking corresponding measures.
3. A primary platform can be connected to multiple branch platforms, and a branch platform can be connected to multiple primary platforms.

Steps

1. Complete the platform settings.
2. After the settings are completed, you can view the name, IP address, status, type, owner, synched content, device time difference, last synchronization time, and operation of the connected platform on the page.
3. You can select a single or multiple connected devices and click <Delete> to delete or batch delete the connected devices. The deleted devices are not displayed in the list after you click

<Refresh>.

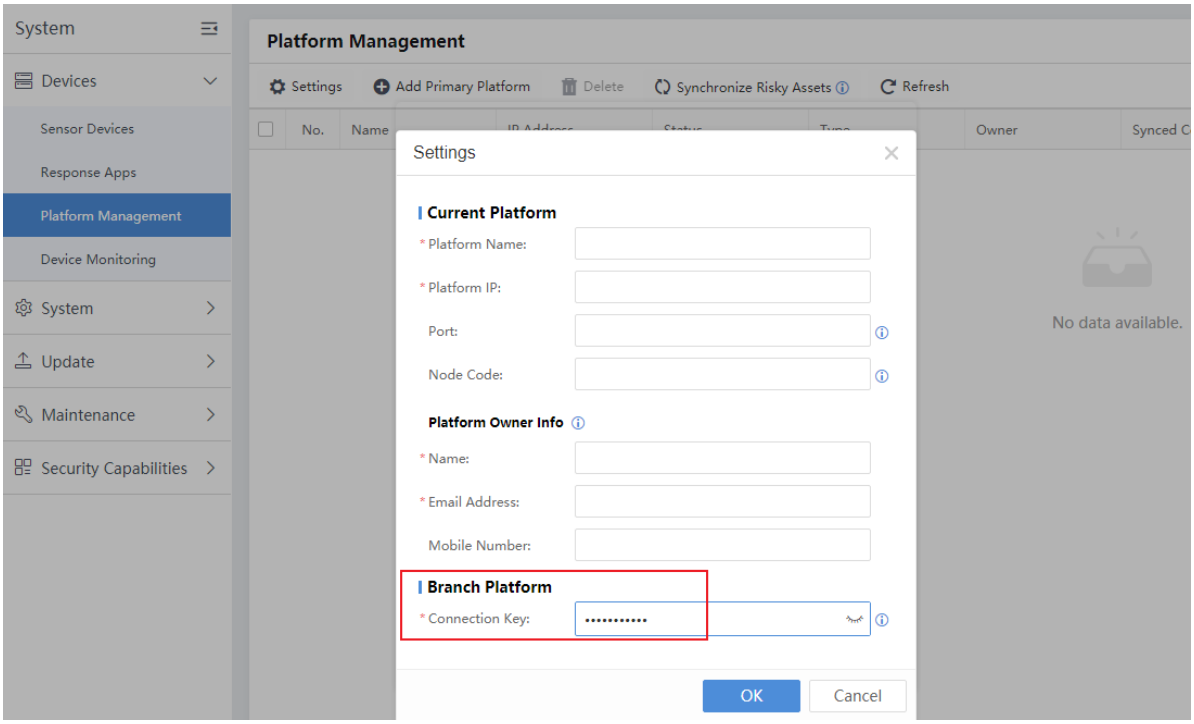
Note

The connection key for the primary platform should be the same as that for the branch platform.

Steps

Step 1. Complete settings of the current platform.

On the [admin/System/Devices/Platform Management] page, click <Settings> and configure the IP address, port (such as 7443), and connection key of the connected platform. Then, click <OK>, as shown in the following figure.



Fields:

<Node Code>: Optional. Node ID, which can be customized.

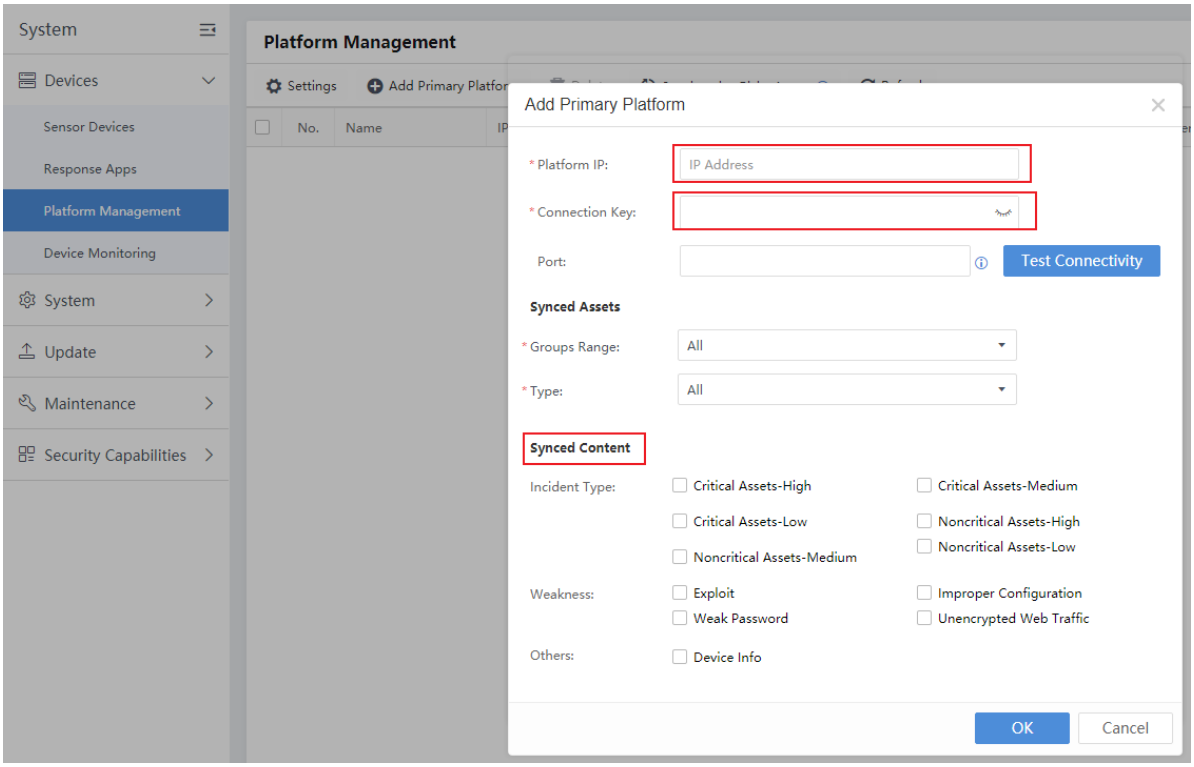
<Connection Key>: This key is used for the authentication of a branch platform when connected to the primary platform.

Step 2. Connect the branch platform to the primary platform.

When connecting a branch platform to the primary platform, click <Add Primary Platform> on the [admin/System/Devices/Platform Management] page. Then, complete the configuration on the pop-up window. After the configuration is completed, click <OK>, as shown in the figure below.

Note:

After entering the IP address, port, and connection key of the primary platform, click <Test Connectivity> to check the connectivity. If the connectivity is normal, configure the remaining fields.



Fields:

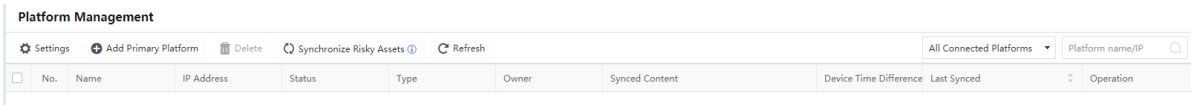
Synced Assets: You can specify assets to be synced by asset group range and type as required by the primary platform.

Synced Content: You can specify the content to be synced by incident type, weakness type, and device info as required by the primary platform.

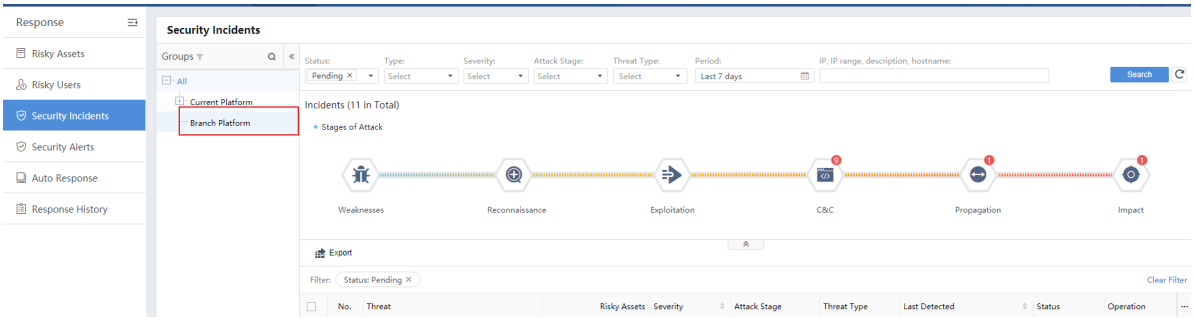
Step 3. Manage platforms.

1. View connected platforms

On the [admin/System/Devices/Platform Management] page, you can view the information about connected platforms, including the name, IP address, status, type, and synced content.



After completing the configuration of connected platforms, you can view the information about branch platforms on the [Response/Risky Servers] page, as shown in the figure below.

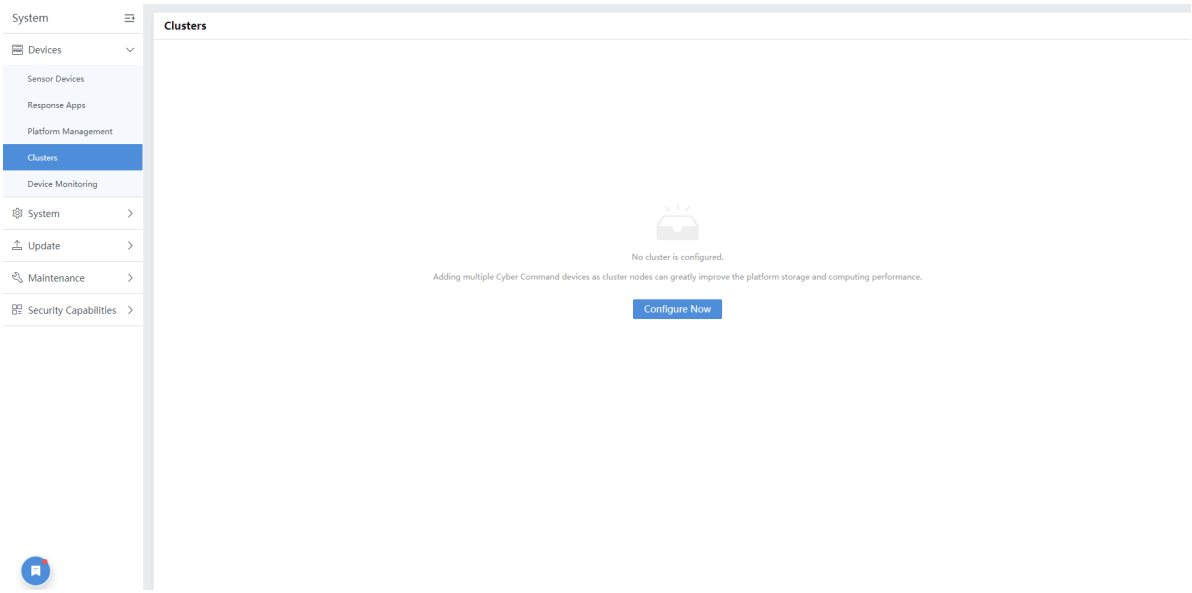


Deletion of connected platforms

You can select a single or multiple connected platforms and click <Delete> to delete or batch delete the connected platforms.

Clusters

You can create a cluster using multiple Nova Command devices as nodes to greatly improve the storage and computing performance of Nova Command. A computing cluster can properly allocate idle resources of multiple devices to improve the computing and query performance of multiple components, as shown in the figure below.



Note

IP addresses of Nova Command devices that are added to a cluster should be on the same network segment and can be accessed by each other.

Nova Command devices that are added to a cluster should have the same hardware model and platform version.

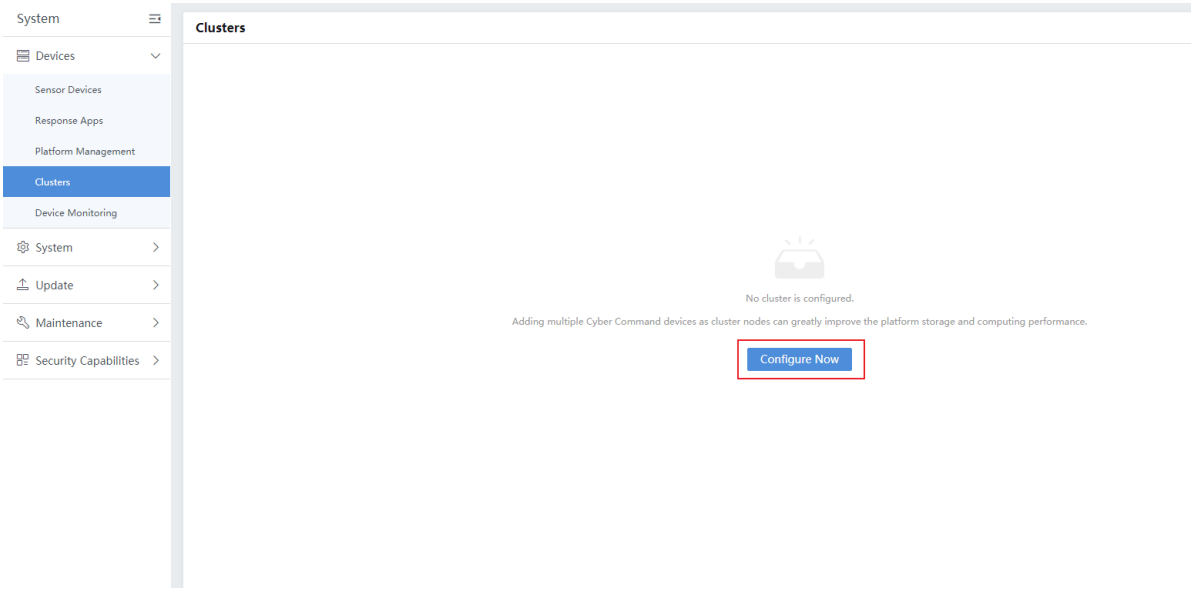
When a cluster is deleted, part of the data will be lost. Please operate with caution.

An active node should be configured for Nova Command devices that are added to a cluster. When it is configured, other devices are served as standby nodes. When Maintenance Mode is enabled for the active node, you can log in to the platform of standby nodes.

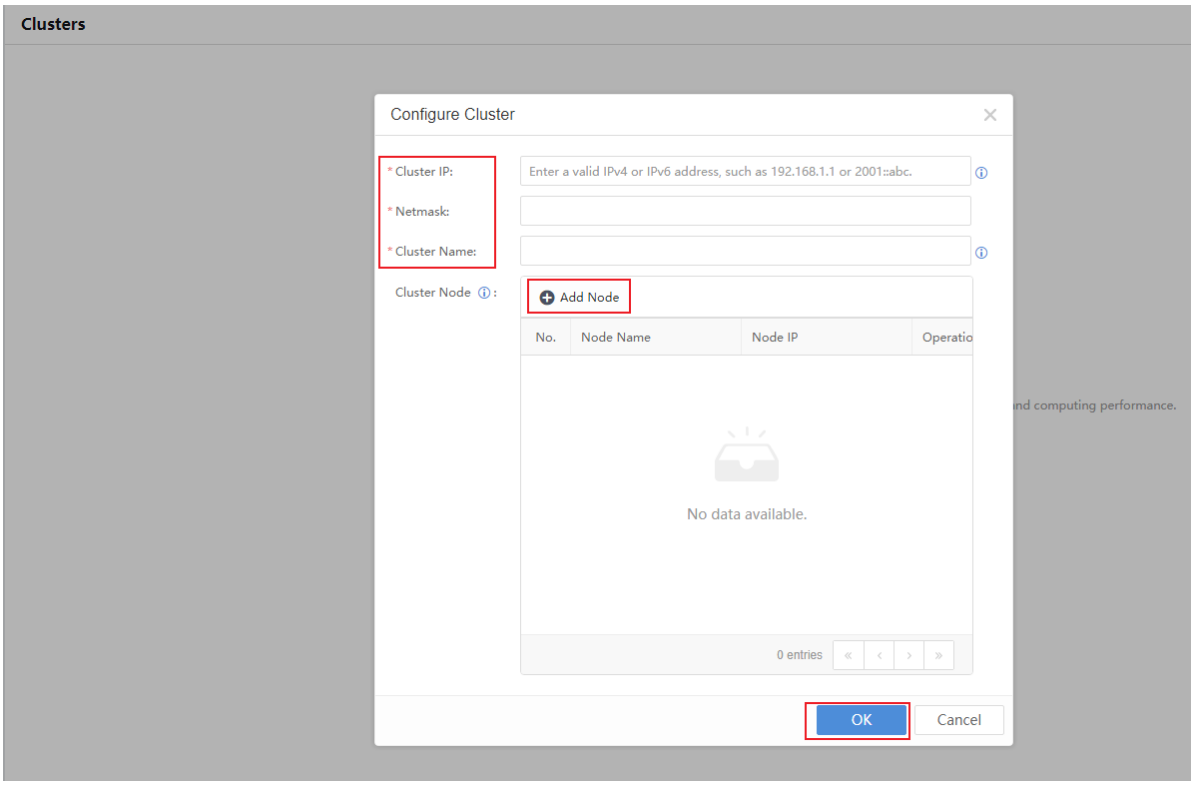
When a cluster is created, standby nodes will be restored to defaults with all data deleted. The configuration and data of the active node will be applied.

Steps of cluster creation

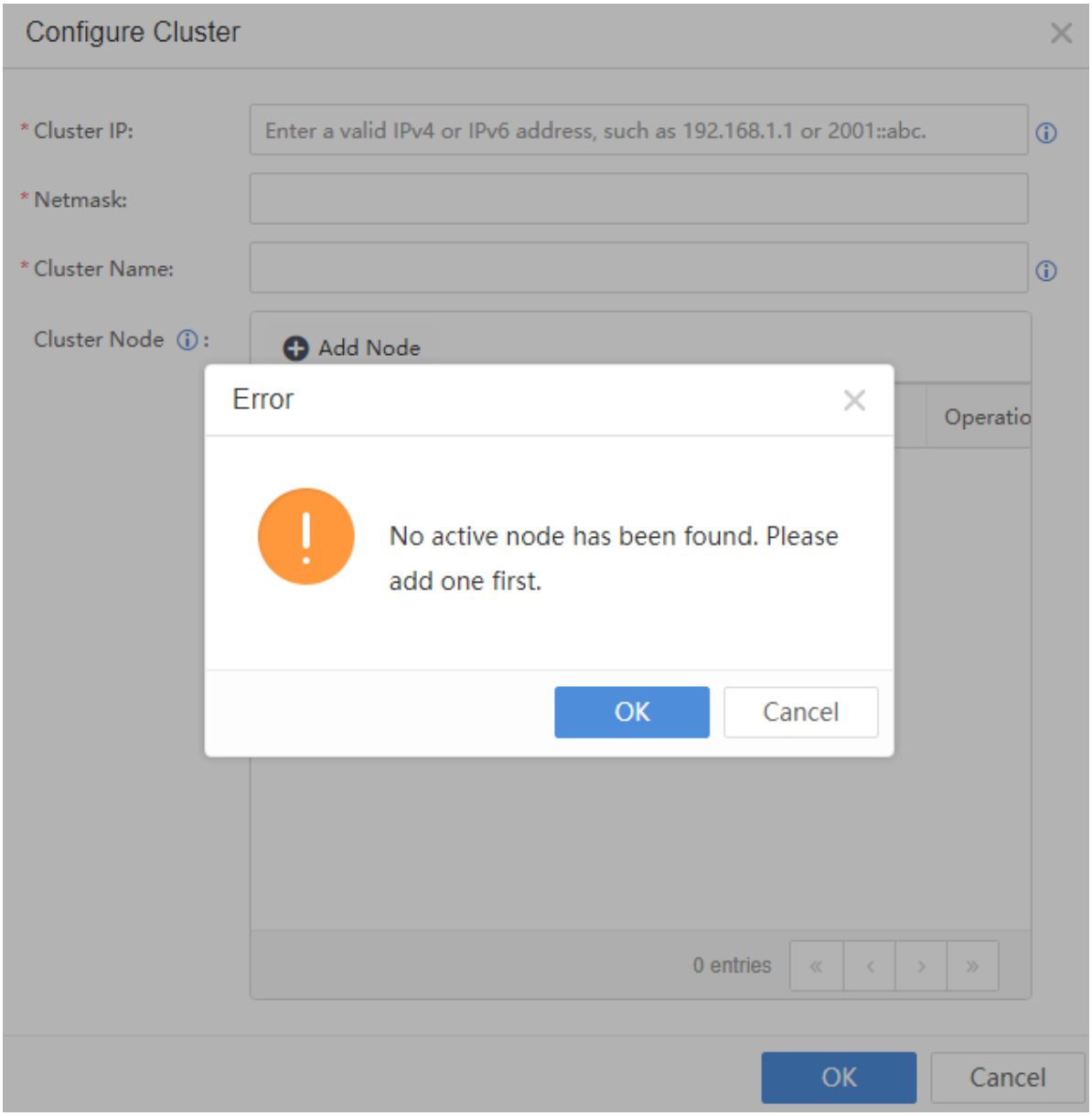
1. On the [System\Devices\Clusters] page, click <Configure Now>.



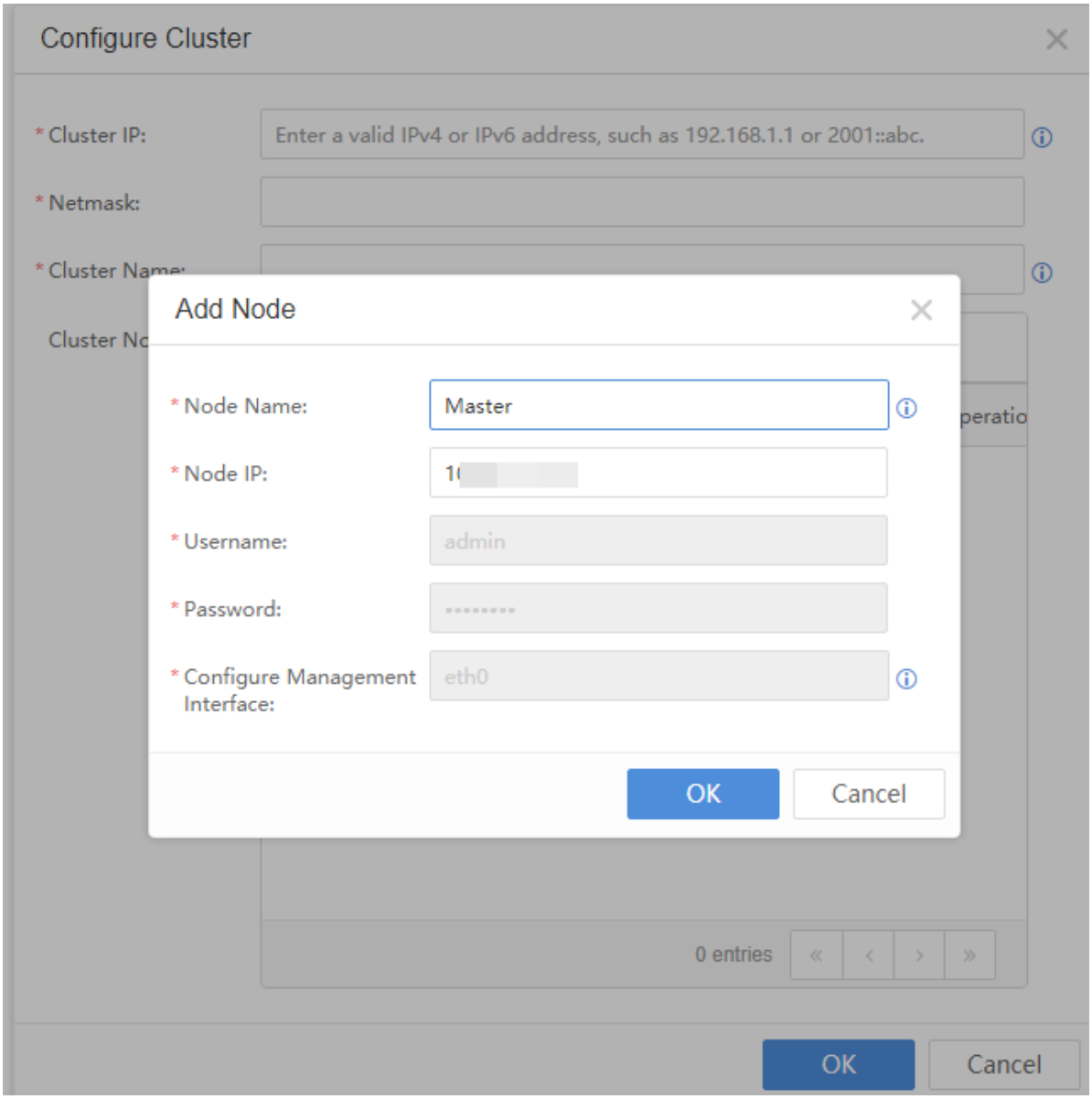
2. Enter the cluster IP, netmask, and cluster name, and click <Add Node>.



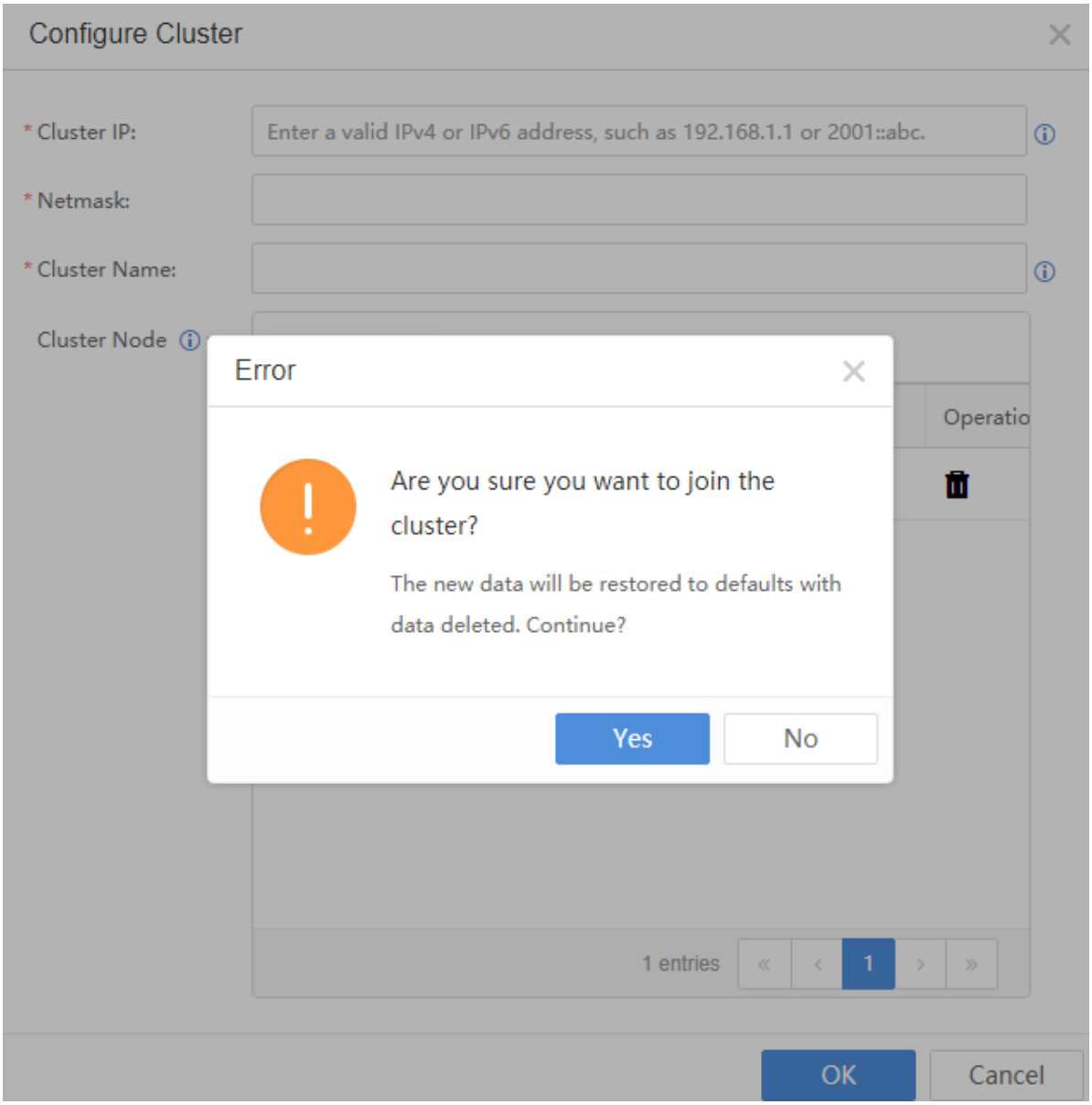
3. The current Nova Command device is added as the active node automatically. Then, click <OK>.



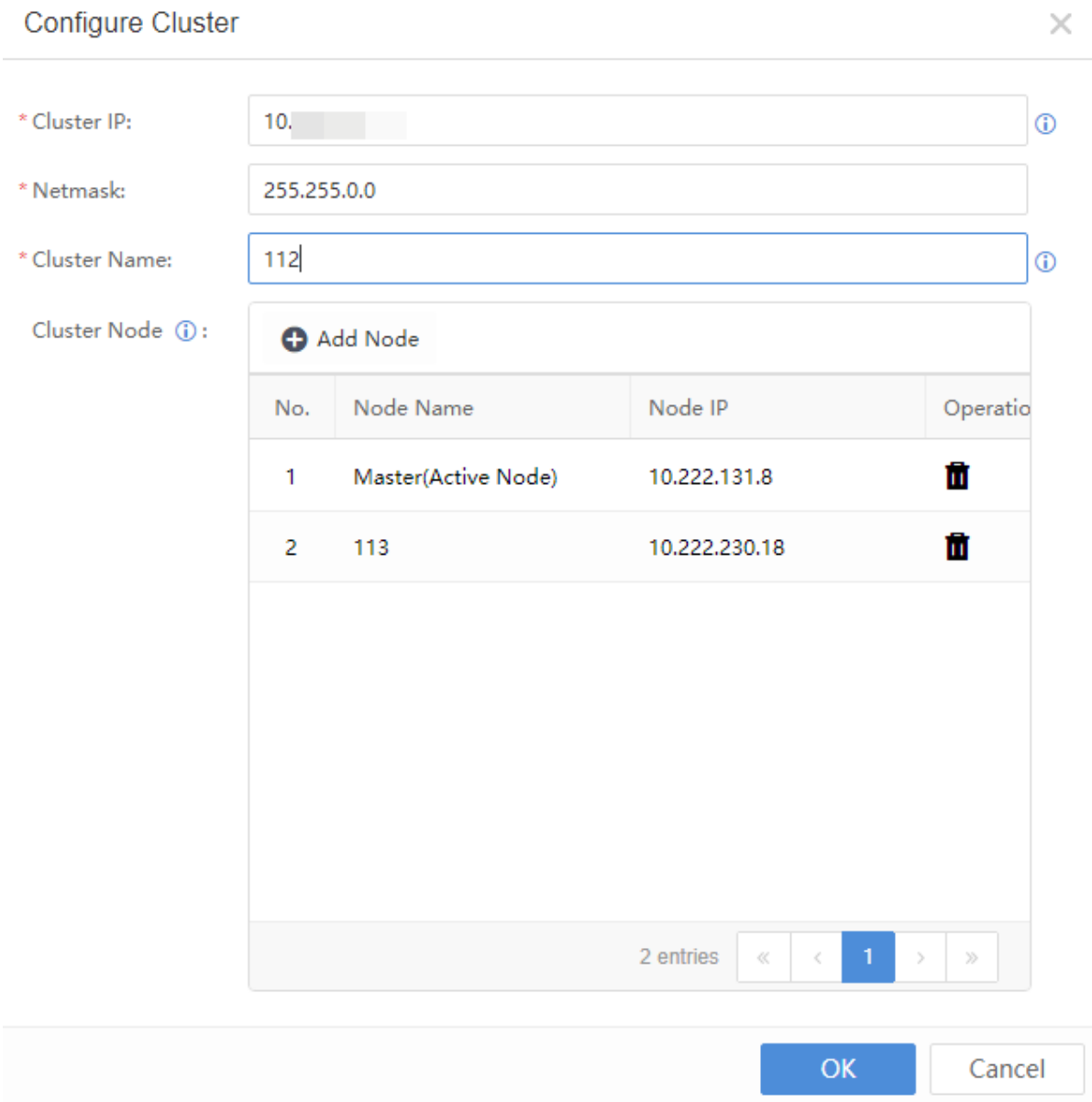
4. Specify the name and IP of the active node. Use the default values in other fields. Then, click <OK>.



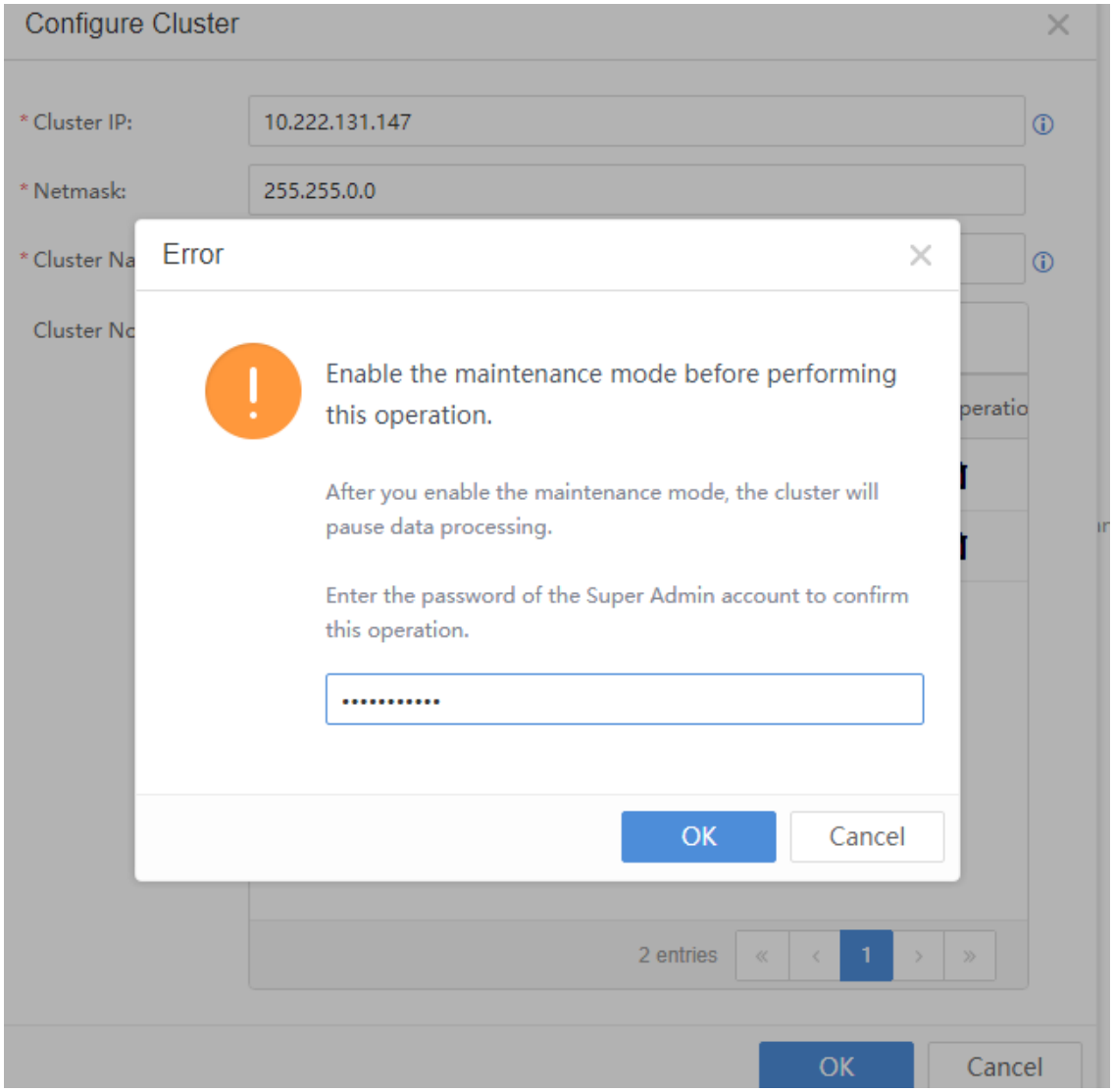
5. Click Add Node again and click <Yes> on the pop-up window.

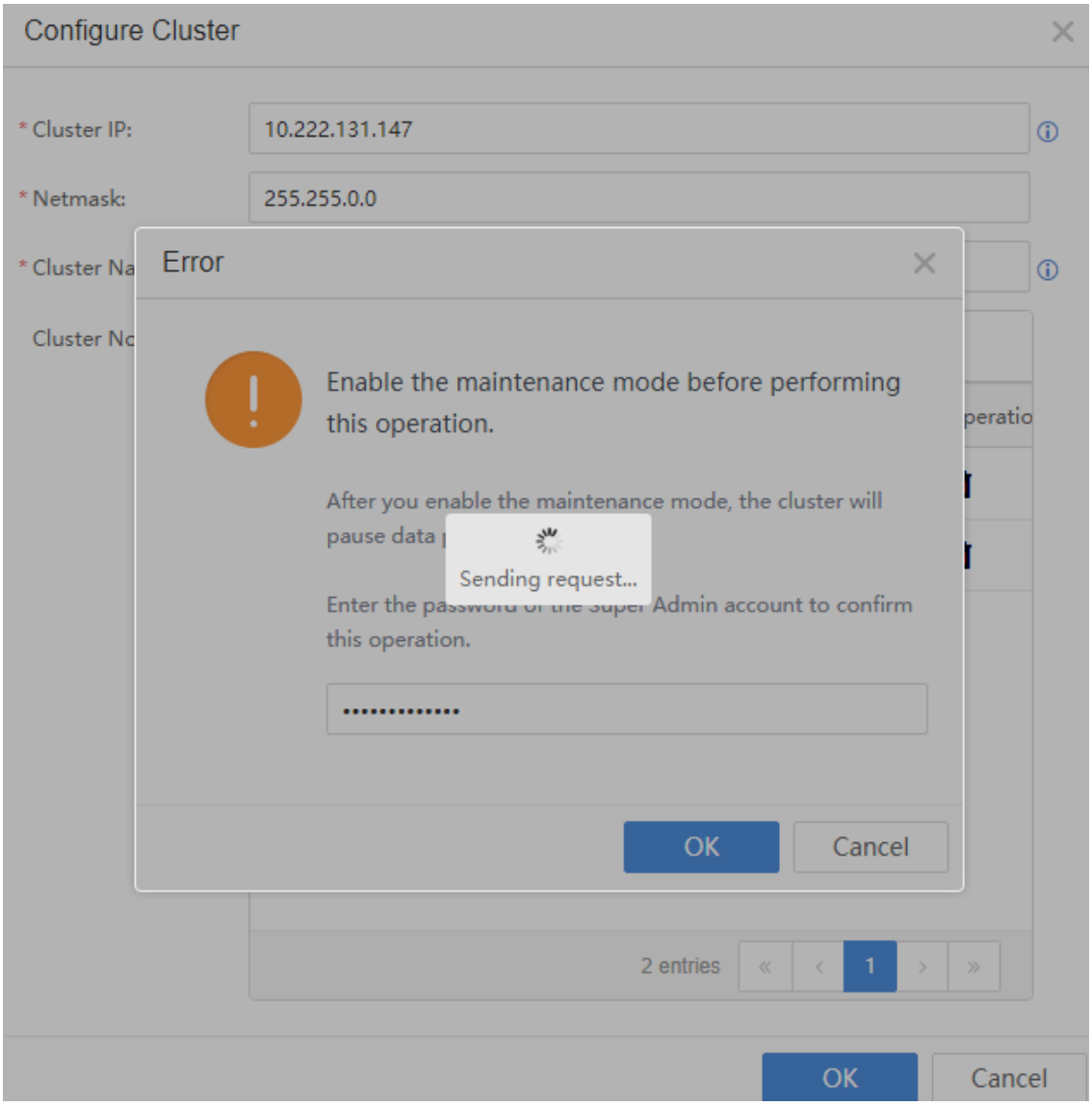


6. Standby node: Enter the node name, node IP, and admin username and password. Then, click <OK>.
7. To add more standby nodes, repeat steps 5 and 6, as shown in the following figure.



8. Enter the password of the admin account to enable Maintenance Mode. Click <OK> and wait for process to complete.


Configure Cluster
* Cluster IP:
10.222.131.147
* Netmask:
255.255.0.0
* Cluster Na
Cluster Nc
Error
Enable the maintenance mode before performing this operation.
After you enable the maintenance mode, the cluster will pause data processing.
Enter the password of the Super Admin account to confirm this operation.
OK
Cancel
2 entries
1
OK
Cancel



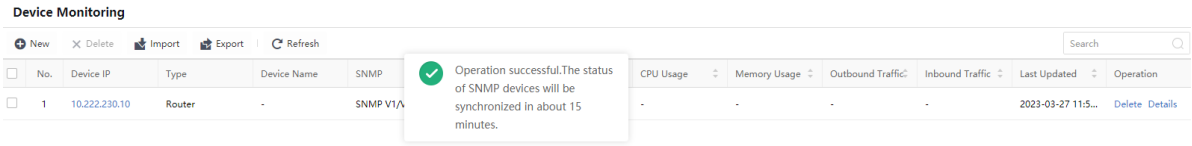
9. A progress bar appears. Wait for the cluster configuration to complete.
10. Click <Disable Maintenance Mode>. Wait for the cluster to change from synchronizing to normal. The cluster is then created successfully.

Steps of cluster deletion

1. Enable Maintenance Mode. Enter the password of the admin account and click <OK>.
2. Click <Delete> on top of the list to delete the whole cluster. (Data will be lost when a cluster is deleted.) Enter the password and click <OK>. Wait for process to complete.
3. To delete a single node (enable Maintenance Mode first), select the node to be deleted, click Delete, and enter the password. Then, click <OK>.
4. After the node is deleted, disable Maintenance Mode.

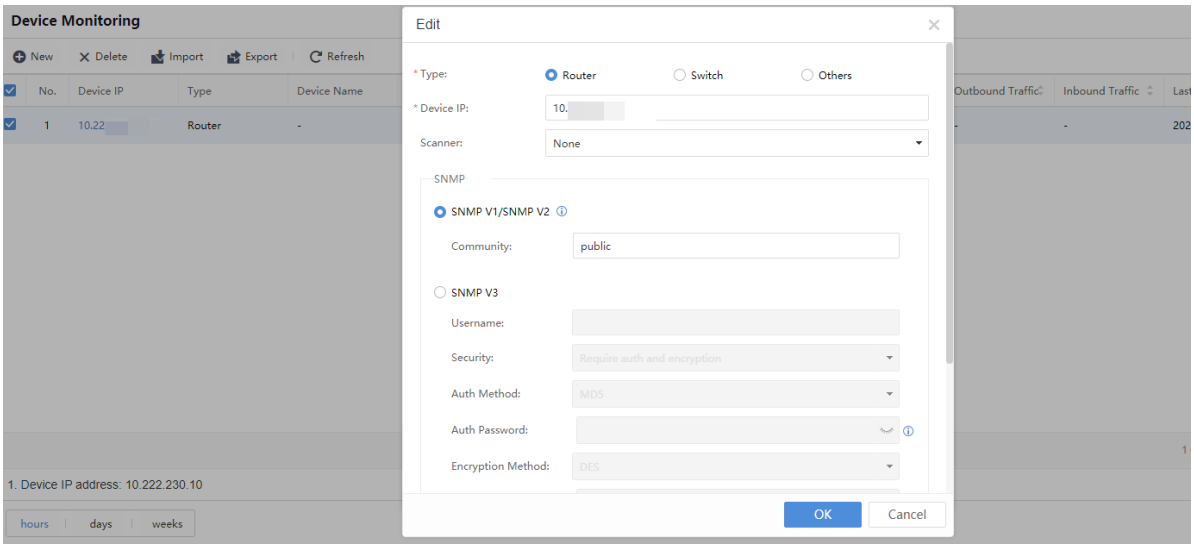
Device Monitoring

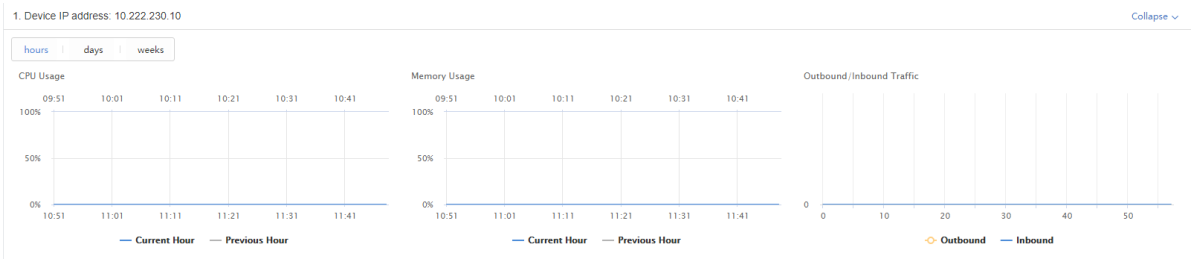
Monitor the operation of connected devices through SNMP. Devices that have enabled SNMP V1, V2, or V3 can be monitored.



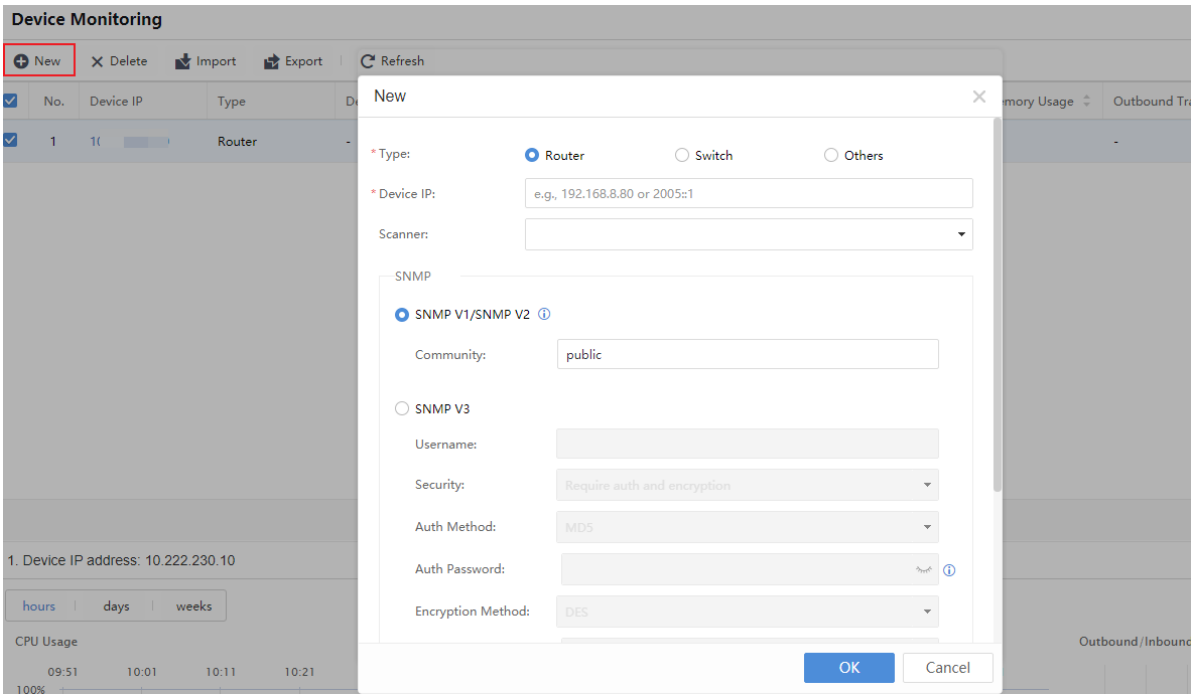
1. On the [Devices/Device Monitoring] page, you can click <Details> in the Operation column to view the operation information of the current device. You can also view the operation

information of any device by entering keywords in the search box. You can click the IP address of a device to edit the device information.





2. You can click <New> and configure the information of a new device, as shown in the following figure.



Fields:

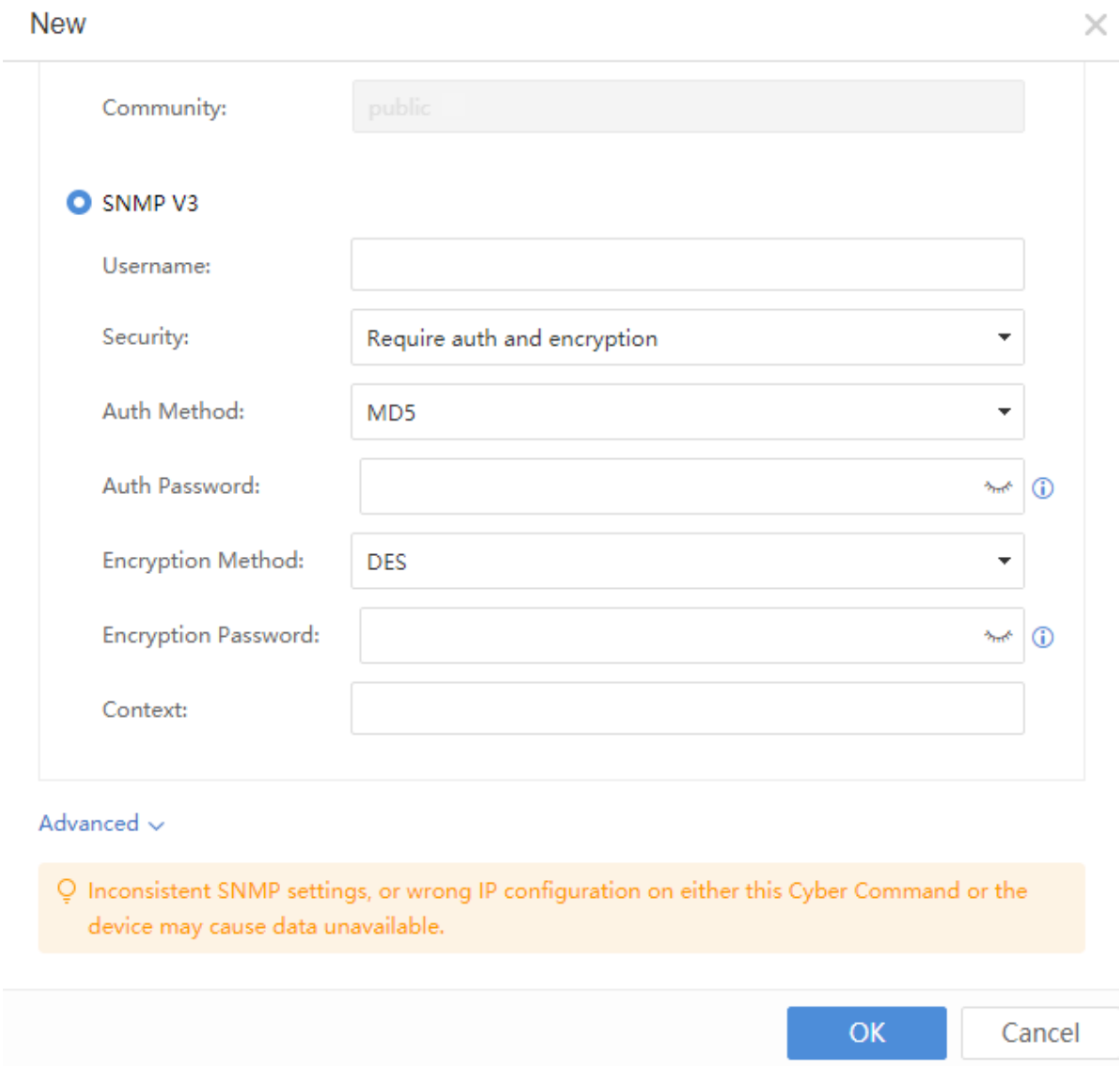
Device IP: IP address of the device to be connected.

SNMP V1/SNMP V2: Name of the community, which is configured on the connected device.

SNMP

V3: Two-way authentication. You need to configure the username, security level, authentication method, authentication password, encryption method, and encryption password, which should match the settings on the connected device.

3. You can click [Advanced] to obtain information about free CPU, total memory, free memory, outbound traffic, and inbound traffic through OID. OID should match the connected device.



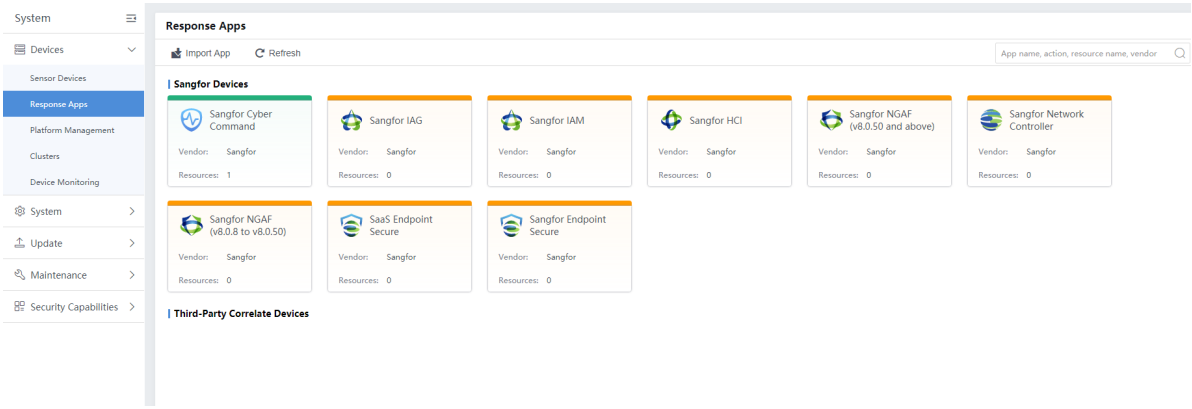
4. You can select a device and click <Delete> to delete the device. The deleted device is not displayed in the list after you click <Refresh>.

Note:

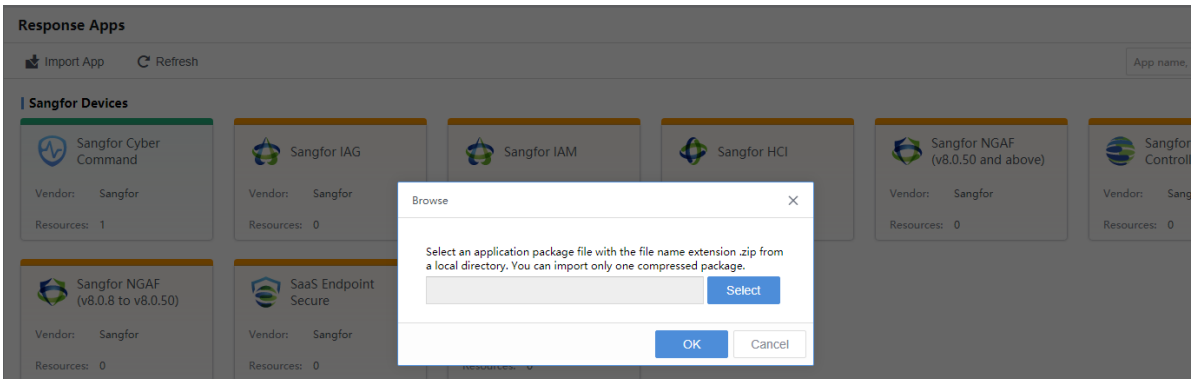
SNMP V1/SNMP V2
does not support obtaining traffic information, so no traffic information is displayed. To obtain traffic information, please select SNMP V3.

Response Apps

The [System/Devices/Response Apps] page allows you to configure the apps and devices to be connected to Nova Command and maintain correlated devices. Some apps have been added on Nova Command. You can use the import function to import more apps. For apps that have been connected, connection requirements and corresponding interface documents can be submitted to the supplier for developing an app package. You can import the package to Nova Command, as shown in the following figure.



Click <Import App> to pop up the [Browse] box. Then, select and import the app package in ZIP format. You can import multiple apps at a time because one package can contain multiple apps. In addition, apps that will be updated by the supplier can also be imported using a package, as shown in the following figure.



You can click the app to view the app details in the window that appears on the right, including the app version and supported actions. You can also add corresponding resources in this window. To enable the app, you need to add the corresponding resources. The parameters of resources added vary by app.

System

This module allows you to set the admin account, licensing, network, general items, and logging options.

Admin account

On the Admin Account page, you can view the information about the admin account and role.

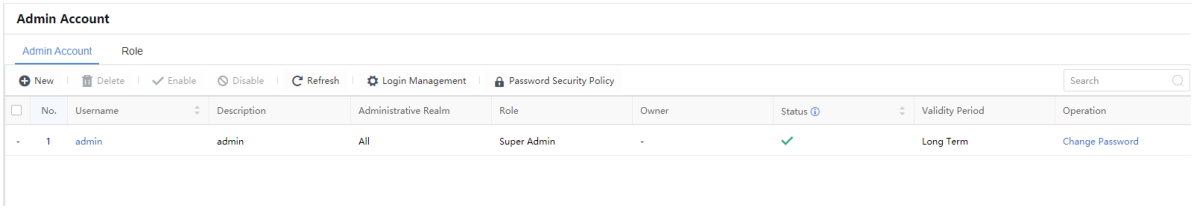
Role

Nova Command provides four roles by default, including Super Admin, System Admin, Security Admin, and Audit Admin.

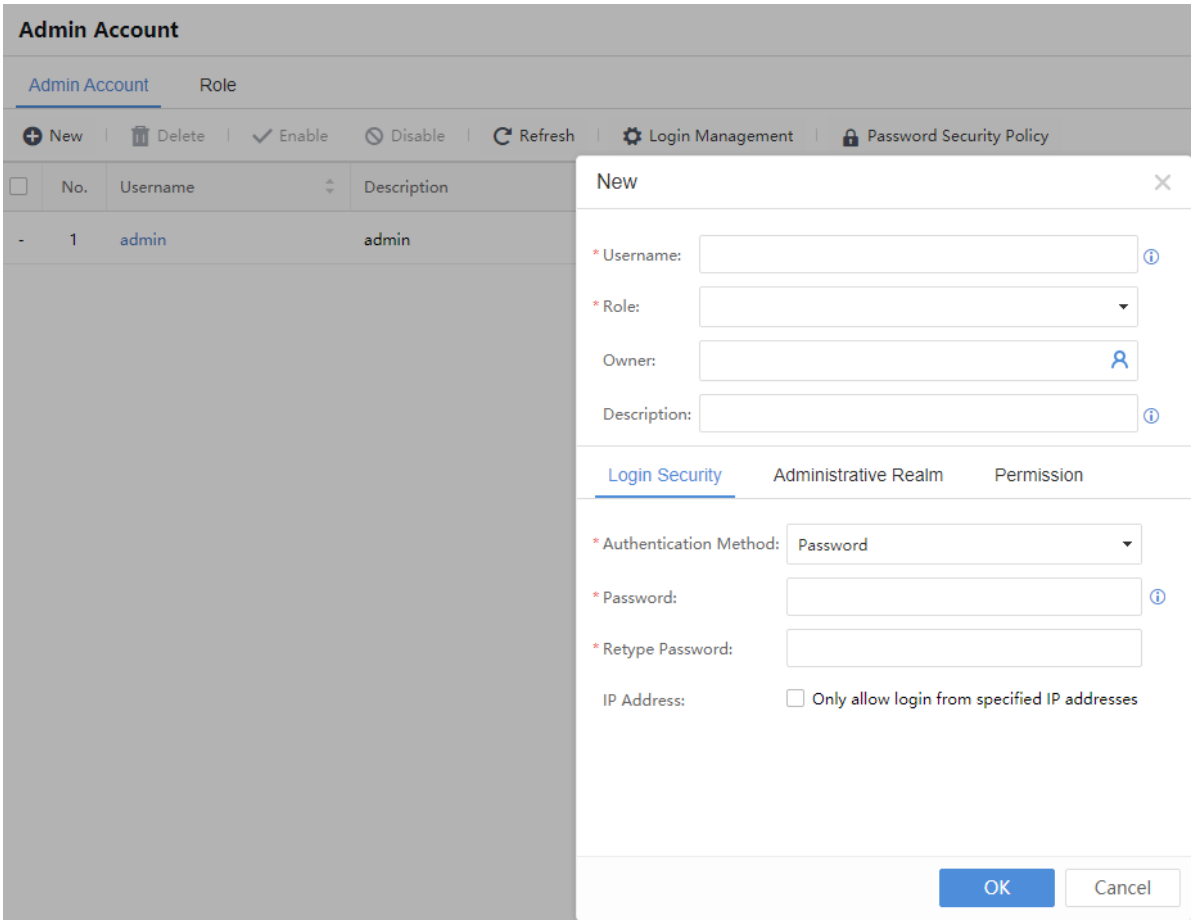
Admin account

As an admin, you can add an account, modify the password, and control the access permission of an account. An admin account has the highest permission.

1. On the [Admin Account] tab, you can view the username, description, administrative realm, role, owner, status, and operations of an account, as shown in the following figure.



2. You can click <New> to add an admin account or an ordinary account, as shown in the figure below.



Fields:

Role: Includes Ordinary Admin, System Admin, Security Admin, and Audit Admin.

<Type>: Includes Admin and Ordinary Account. The admin can add, edit, and delete an account, but an ordinary user can only view an account.

Owner: Owner of the account.

Description: Describes the usage of the account with 0 to 127 characters.

Login Security: Defines the login method.

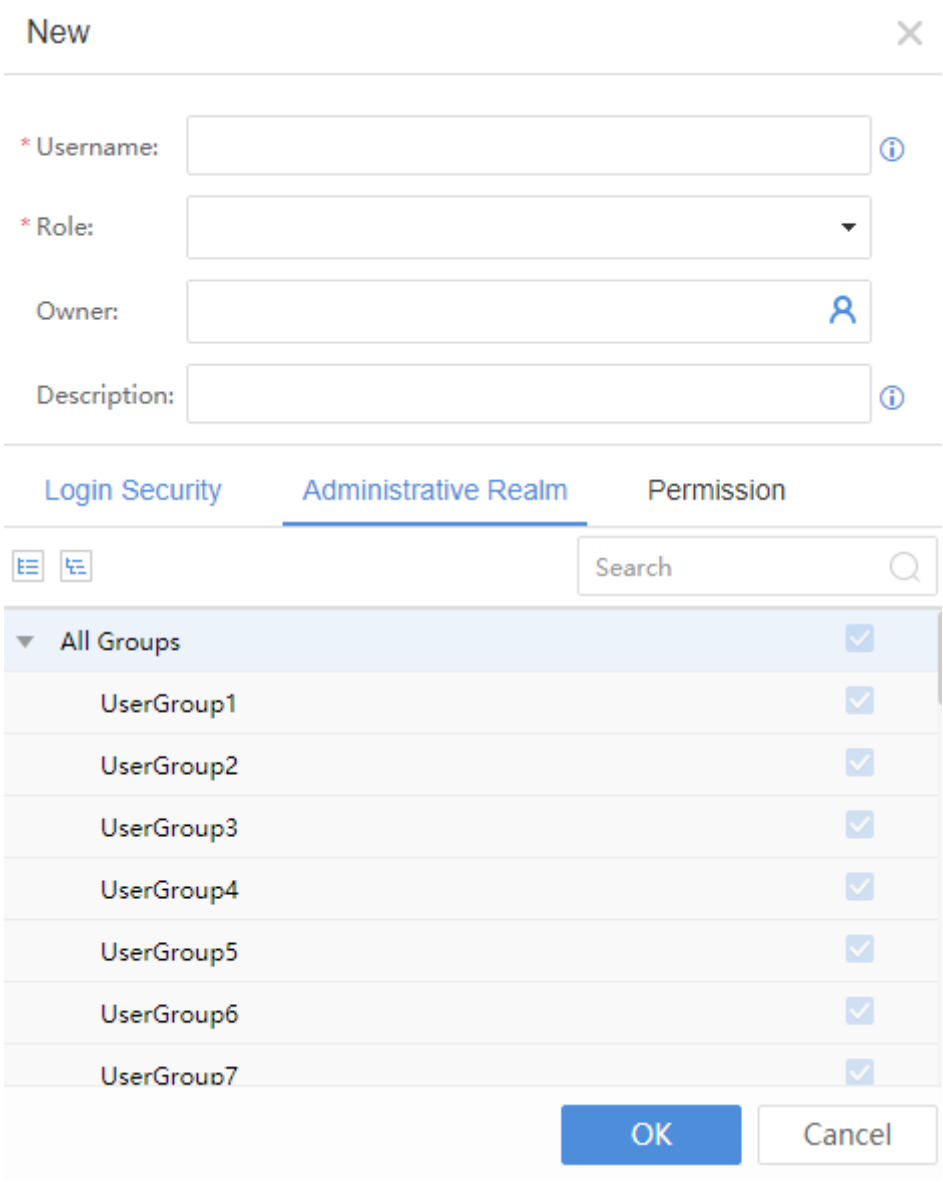
Authentication Method: Includes "Password" or "Password + USB Key".

Password: Password of the account for login.

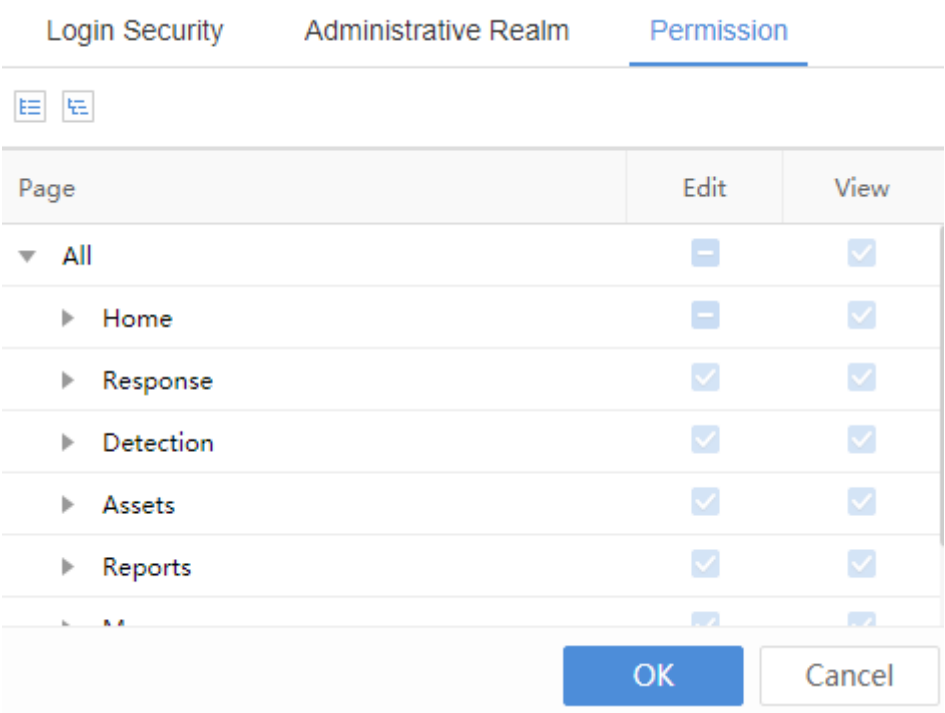
Retype Password: The password is filled in again for confirmation.

IP Address: IP address to be bound with the current account. Login is allowed from bound IP addresses only.

Administrative Realm: Branches to be managed by the account. Only an ordinary admin account can select branches as needed. For other accounts, all branches are selected.

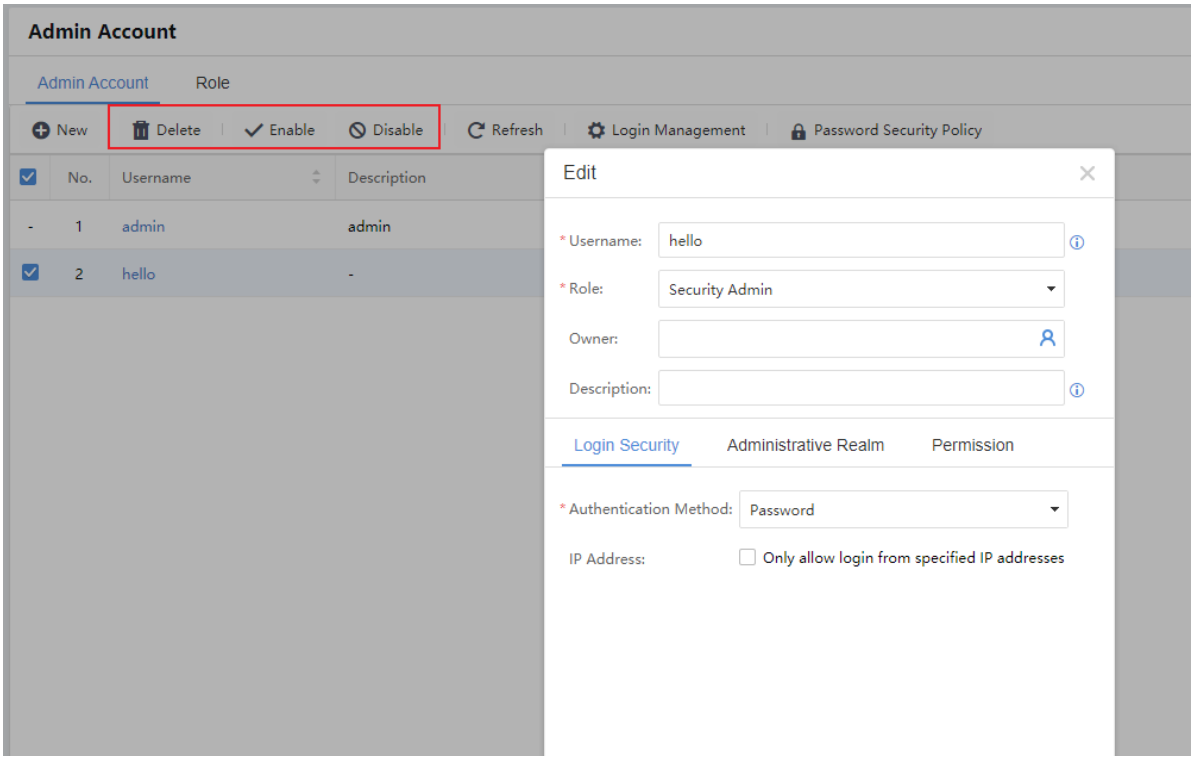


Permission: Ordinary admin account has the permission to edit and view the modules of Nova Command.

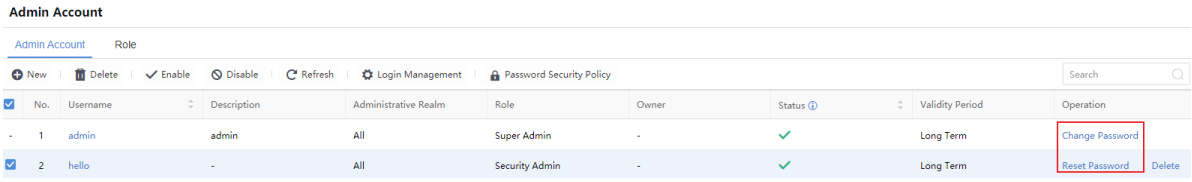


3. Click <OK>.

4. For created accounts, you can click the name in the <Username> column to change the permissions of the account. You can also select an account and delete, enable, or disable it to facilitate O&M.



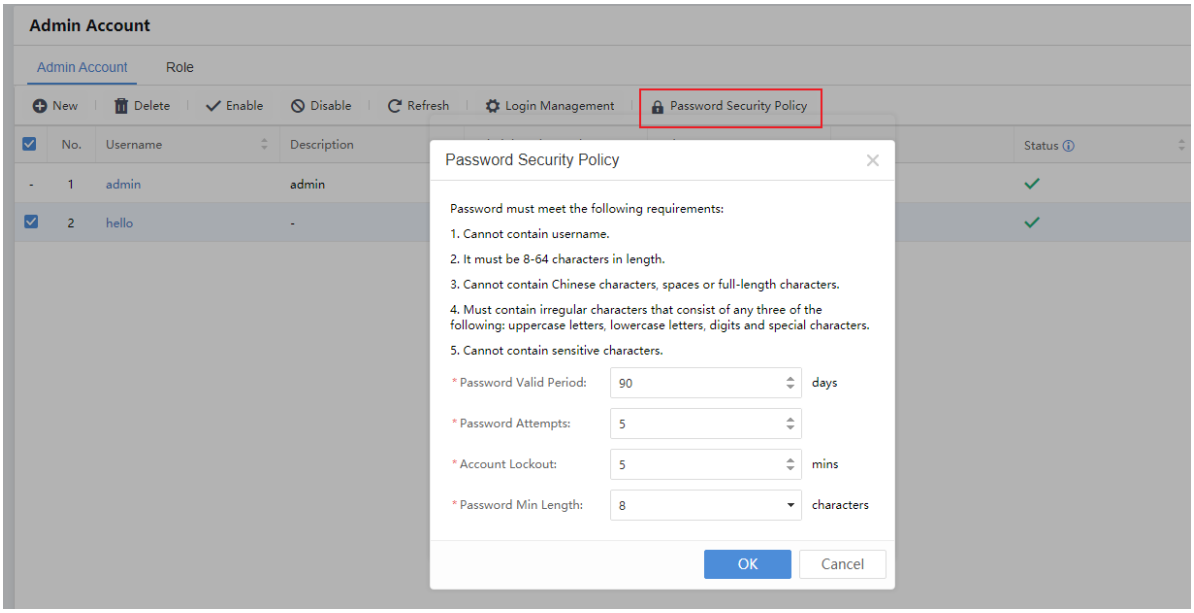
5. You can click <Change Password> or <Reset Password> to change the password of the account.



Note:

To change the password of the currently logged-in account, you need to enter the old password. To modify the password of a new account, you can directly change the password.

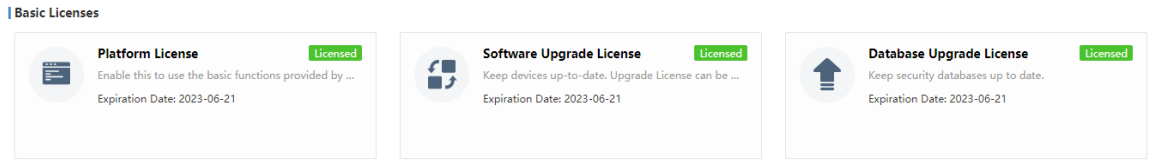
1. Password security policy is added to meet the standards for e-government networks. You can specify the complexity and validity period of the password, the number of password attempts, the account lockout duration, and the minimum password length as needed. Corresponding settings are shown in the following figure.



Licensing

You can check whether the license key and its expiration date are correct. Basic licenses and function module licenses are provided on this page.

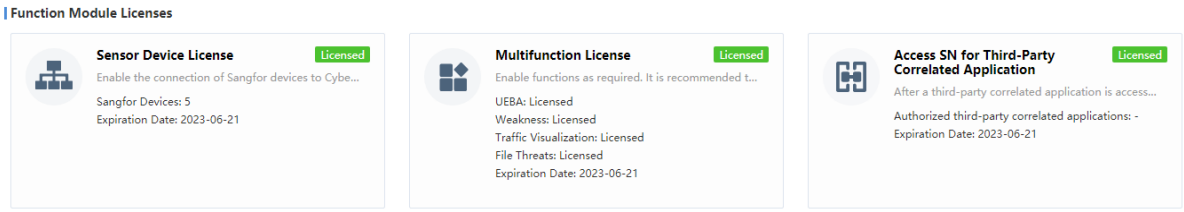
1. Basic licenses include the platform license and upgrade licenses, as shown in the following figure.



2. Function module licenses include the device integration license, multifunction license, and access SN for third-party correlated application, as shown in the following figure.

Device Integration License: Licenses Sangfor devices and third-party devices connected to Nova Command.

Multifunction License: Licenses modules such as UEBA, Weaknesses, Traffic, and File Threats.



Network

This module contains interfaces, static routes, and DNS servers. You can configure the interface IP addresses and routes of Nova Command.

Interfaces

You should enable the interface first before configuring the IP address. To enable the interface, you need to plug in the network cable. The interface light must be on.

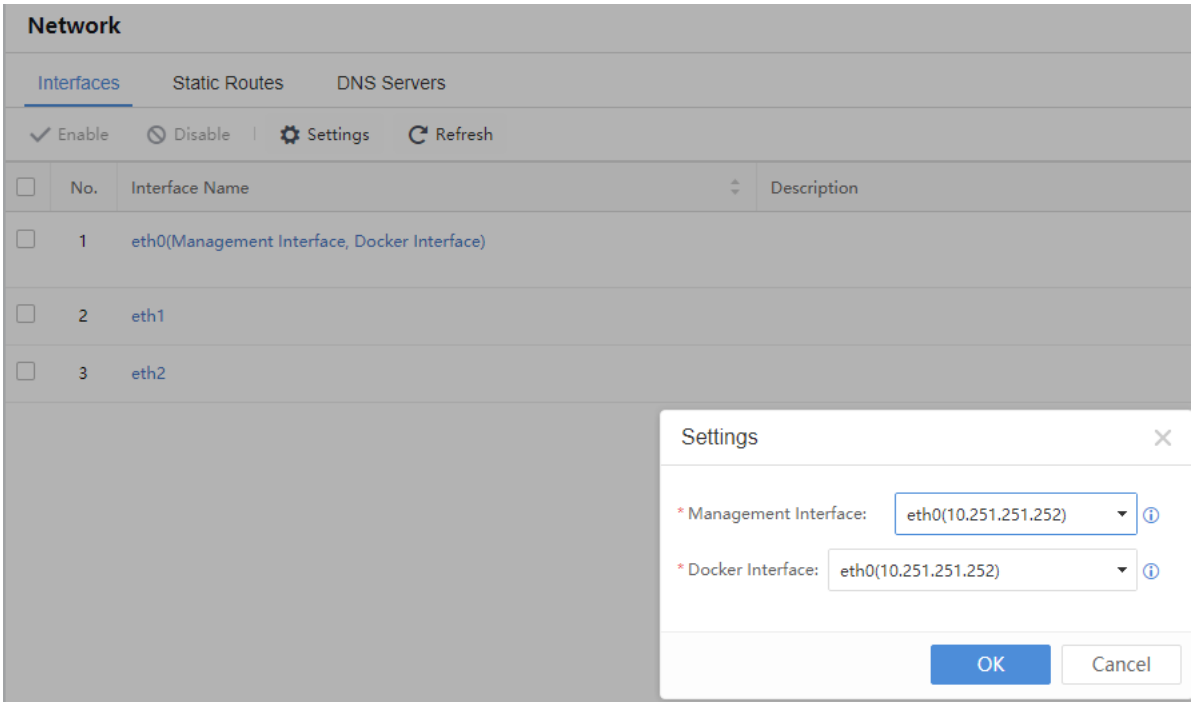


Operations:

Enable: Select an interface to enable it.

Disable: Select an interface to disable it.

Settings: Set the management interface for a cluster to sync data between clusters.



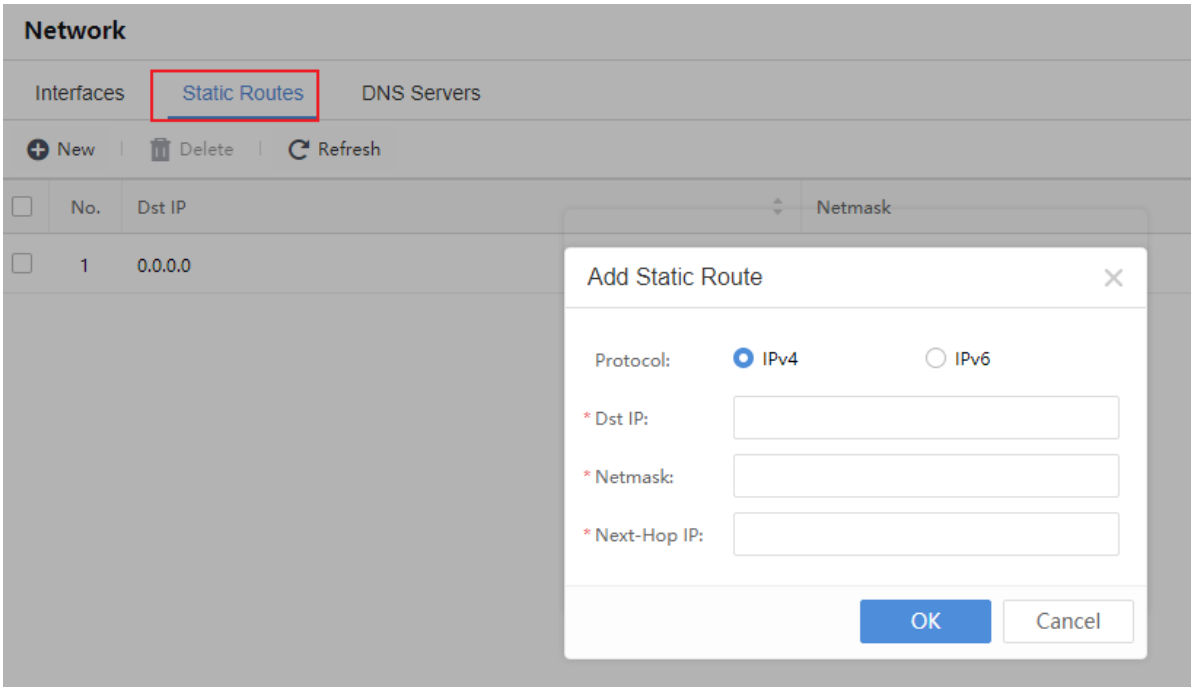
Note:

The default management interface is eth0. You can add IP addresses (IPv6) used by the customer.

Do not disable all interfaces.

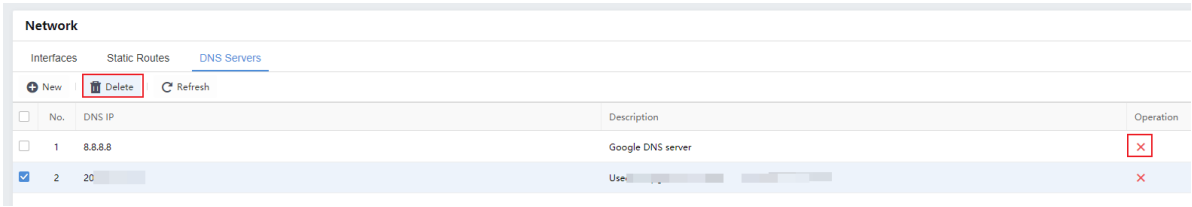
Static routes

By default, one route for the gateway of the interface is enough. IPv6 addresses are supported.



DNS servers

You can click <New> to configure DNS servers according to the actual situation. You can select one or multiple DNS servers to delete or batch delete them, as shown in the figure below.

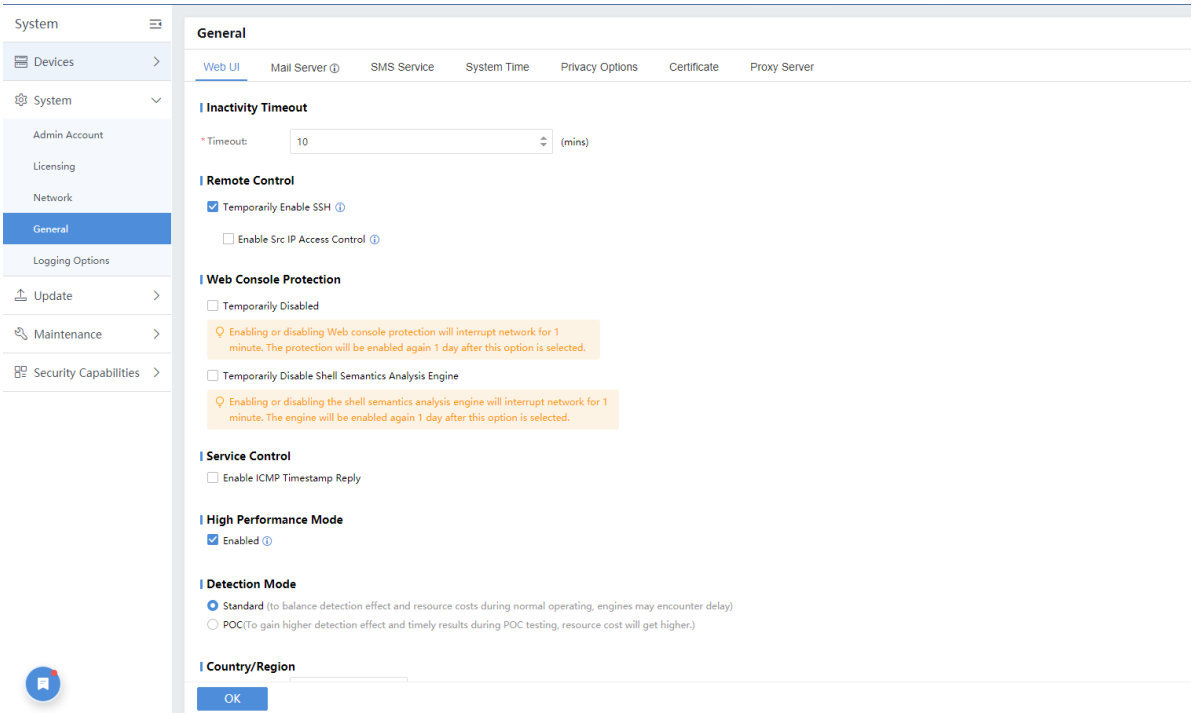


General

General settings include settings for web UI, mail server, SMS service, system time, and privacy options.

Web UI

You can configure the console, as shown in the figure below.



Fields:

Inactivity Timeout: For a logged-in admin account, the account will be logged out after the specified timeout period.

Remote Control: This feature is available for R&D personnel who log in to Nova Command for troubleshooting. If temporarily enabled, remote control will be automatically disabled eight hours later.

<Web Console Protection>: If you enable or disable web console protection, the network connection will be interrupted for one minute. The protection will be enabled again one day after it is temporarily disabled.

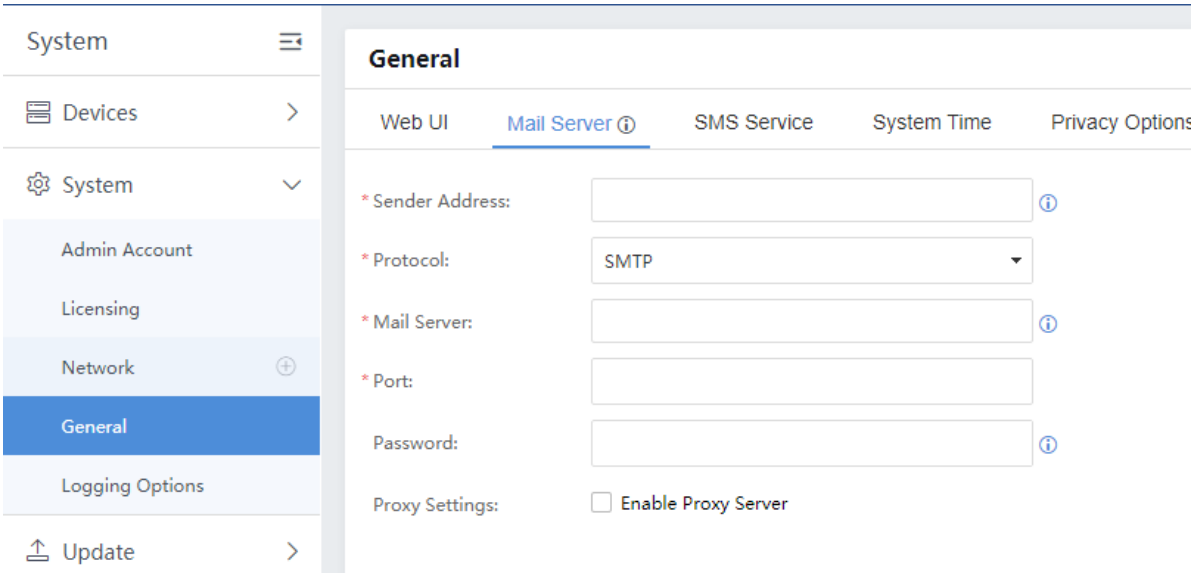
Service Control: You can select the Enable ICMP Timestamp Reply check box.

High Performance Mode: If enabled, Nova Command will offer a smoother experience.

Detection Mode: Standard mode is enabled during normal operation, and POC mode is enabled during POC testing.

Mail server

You can configure items related to the email address used in Nova Command to send emails, including the sender's address and port.



Fields:

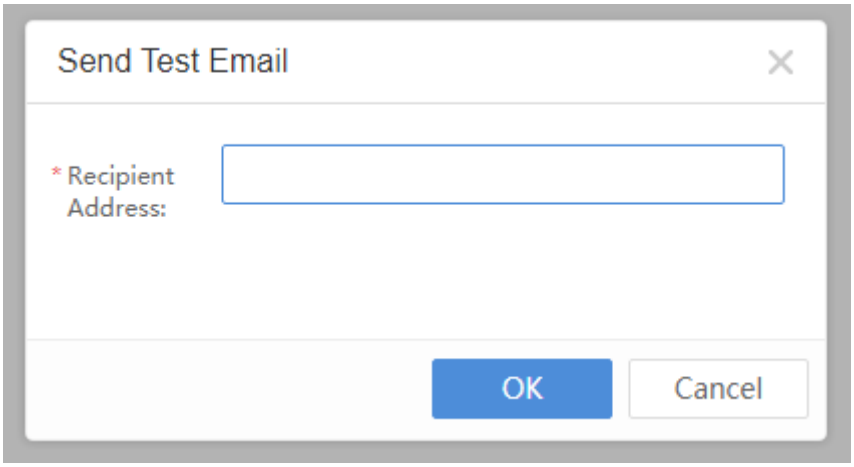
Sender Address: Email address used to send alerts or reports.

Mail Server: IP address of the mail server used to send emails.

Port: Port of the mail server.

Password: Password used to log in to the mail server.

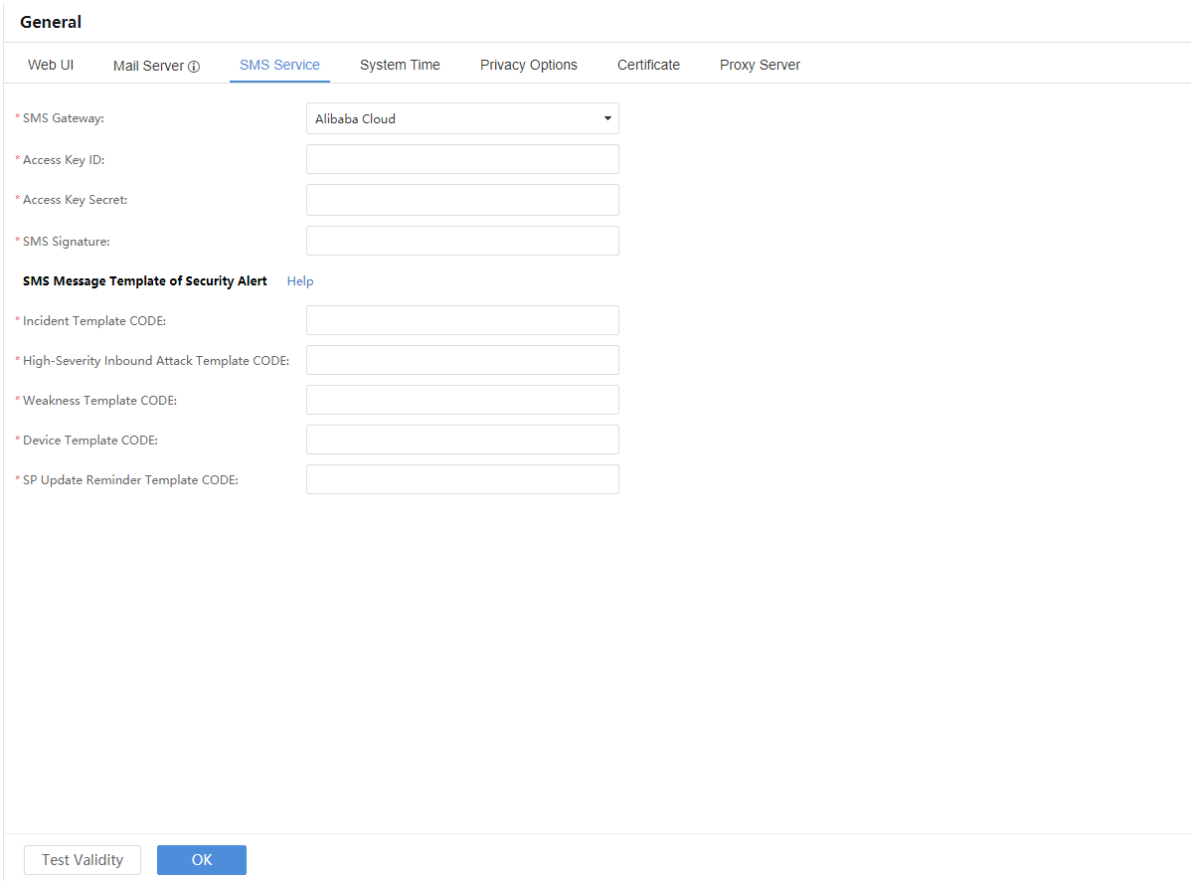
You can click <Send Test Email> to check whether the configured information is correct, as shown in the figure below.



You need to enter the recipient address and then click <OK> to conduct the test.

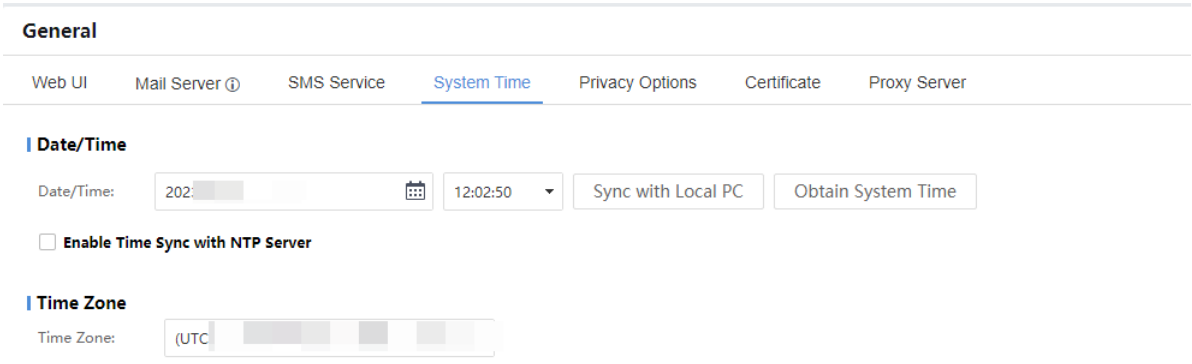
SMS service

You can configure the information related to the SMS service used in Nova Command to send messages. You can use the SMS gateway of Alibaba Cloud or Tencent Cloud, or GSM Modem to send messages, as shown in the figure below.



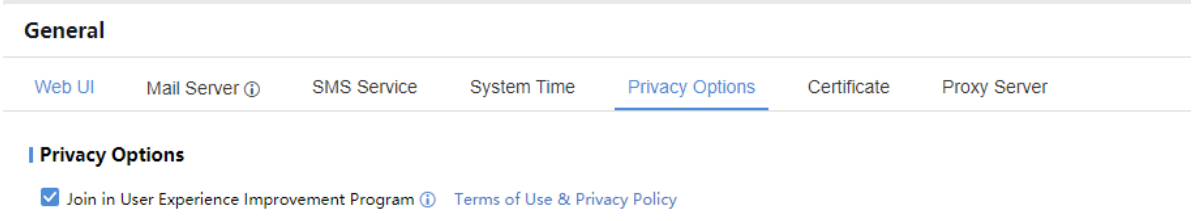
System time

You need to set the current time. A wrong time will have a negative impact on the display of security incidents on Nova Command. If Nova Command is connected to the Internet, you can enable time sync with NTP server, as shown in the figure below.



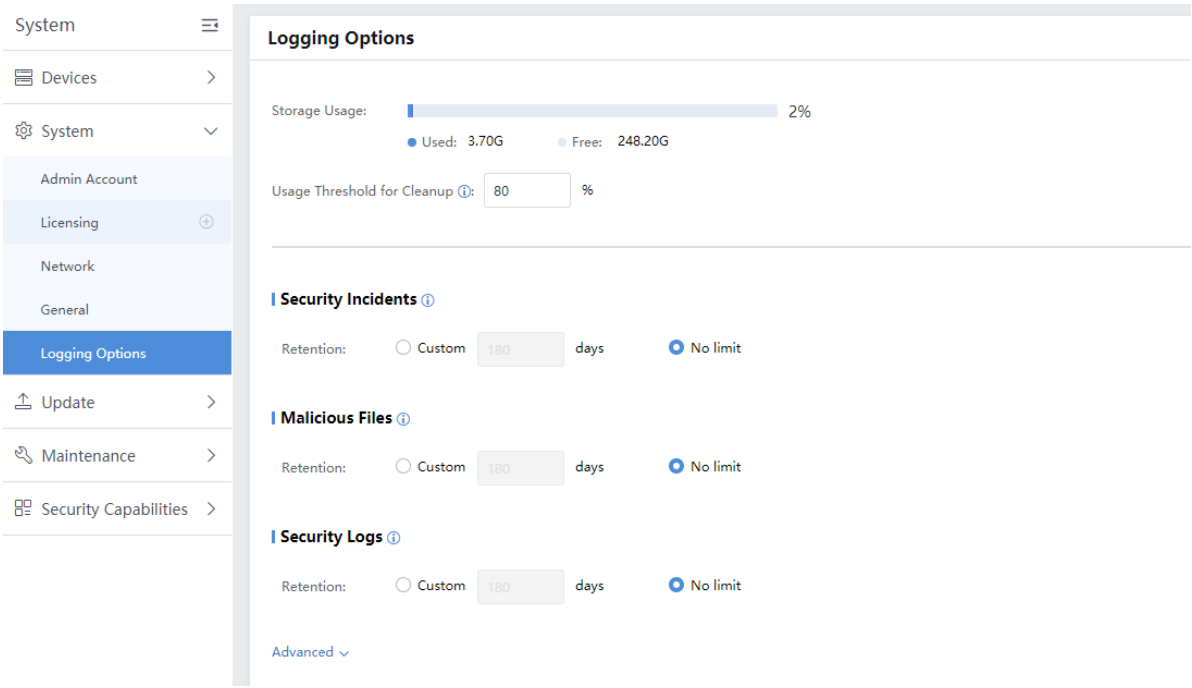
Privacy options

You are advised to select Join in User Experience Improvement Program to optimize user experience.



Logging Options

You can view the storage usage and the retention duration and content of different logs. To store logs, you need to evaluate the disc capacity and the size of logs stored.

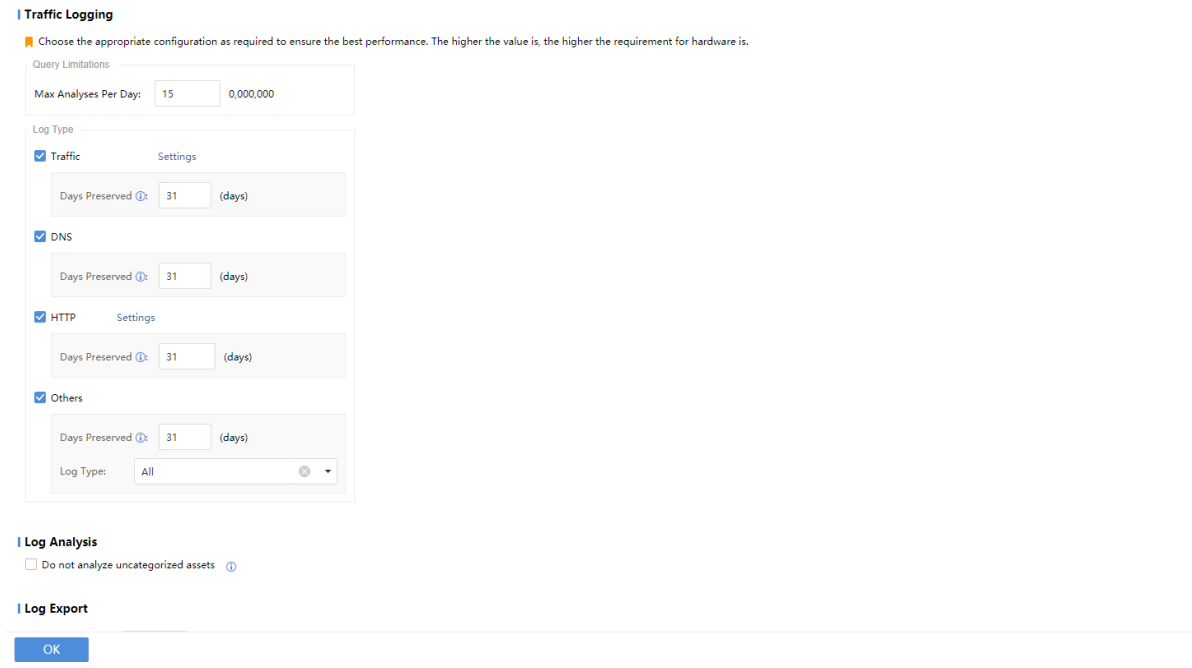


Note:

Security Logs - Retention: Number of days that security logs can be stored.

Security Incidents - Retention: Number of days that security incidents can be stored.

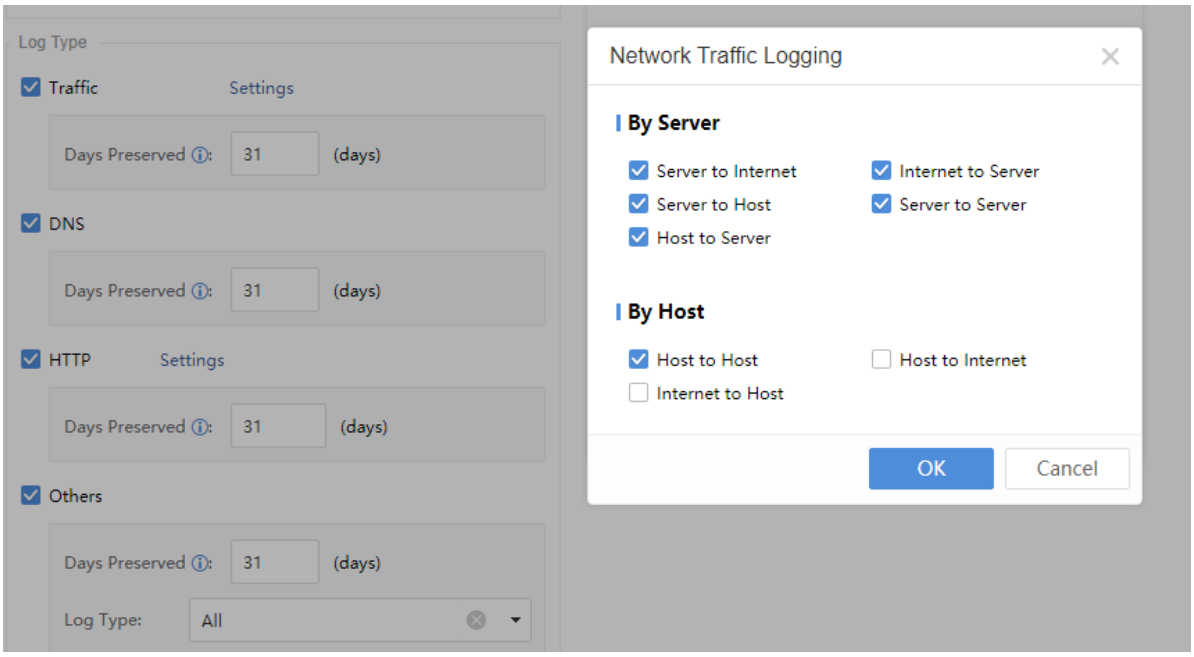
Click <Advanced> for more settings, as shown in the figure below.



Fields:

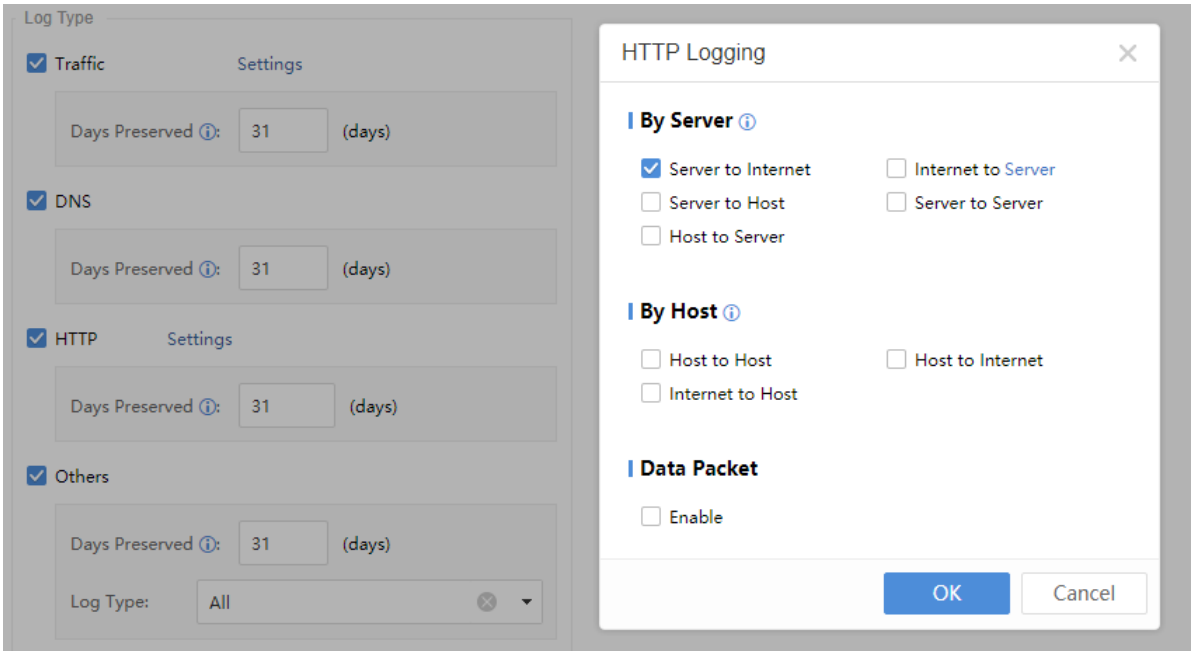
Max Analyses Per Day: You can set the number of log entries to be analyzed each day. Default configuration is recommended.

Traffic: You can review the network traffic and record the 5-tuple information. By clicking <Settings>, you can configure the data direction for logging.

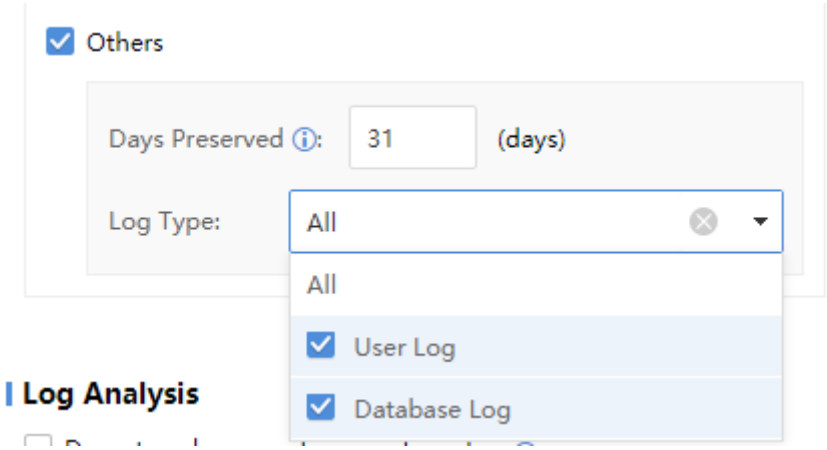


DNS: If selected, the DNS request logs of servers or hosts will be recorded. You can set the retention duration.

HTTP: If selected, the HTTP logs of endpoints will be recorded. You can click <Settings> to configure the direction and data packet of HTTP logs.



Others: Logs of protocols, including Telnet and SMTP, can be recorded. You can set the retention duration.



Log Analysis: If <Do not analyze uncategorized assets> is selected, only uncategorized assets will be filtered, thus reducing performance consumption.

Log Export: Default configuration is recommended.

Update

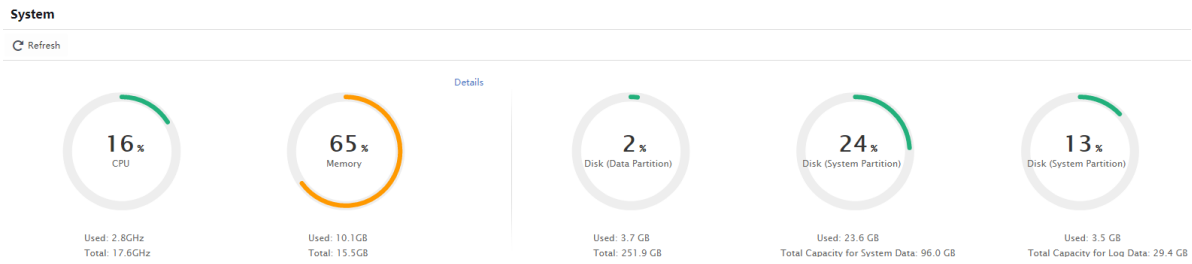
You can update Nova Command, Nova Sensor, service packs, security databases, and security engines and configure update options. For details, see "[Product and Component Update]".

Maintenance

Engineers can conduct troubleshooting for Nova Command in this module. This module contains pages of System, Data Backup, Restore/Restart, and System Check.

System

You can view the usage of CPU, memory, disk (data partition), and disk (system partition), as well as core processes.

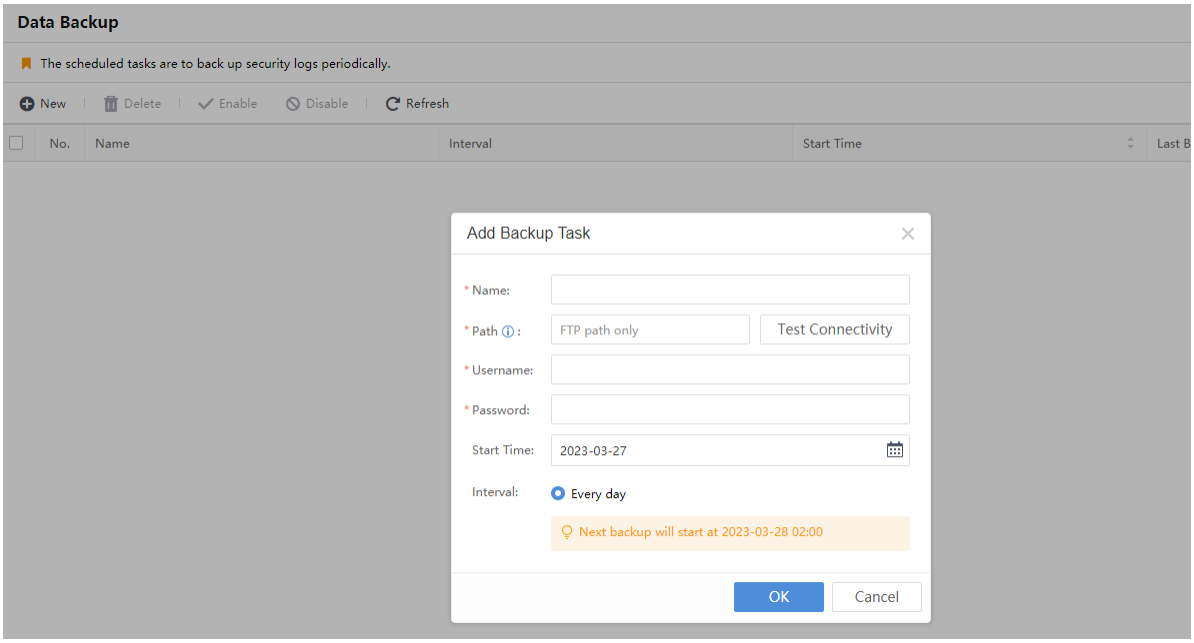


Data Backup

Only security logs of Nova Command can be backed up currently and will be uploaded to the FTP server. Data recovery will be available in later versions.

Backup policy settings

1. Click <New> to set the policy for data backup.



2. Set the policy name and storage path. Click <Test Connectivity> to test the connectivity.
3. Enter the FTP username and password, select the start time, and click <OK>. The settings are completed.

Fields:

Name: Name of the backup policy.

Path: Path to store the backup files on the FTP server.

Username: Account of the FTP server.

Password: Password of the above account.

Start Time: Time when backup starts.

Interval: Backup will be conducted every day if you select Every day.

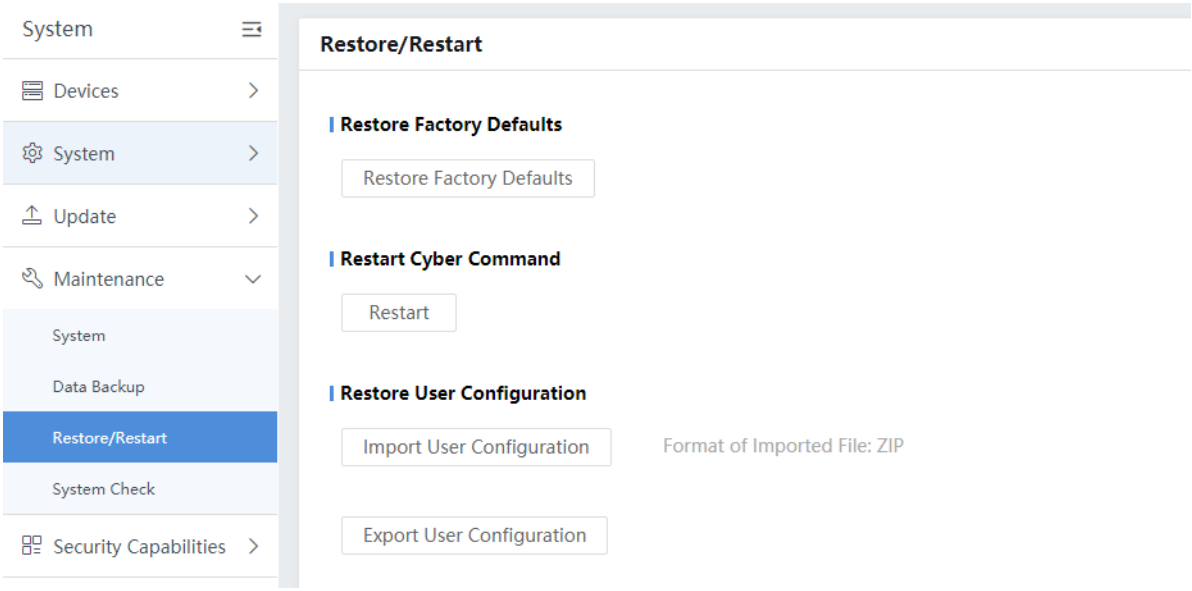
Backup policy management

You can select a single or multiple data backup policies to delete/batch delete, enable, and disable these policies to facilitate management by O&M personnel. You can select an operation according to the actual condition.

Restore/Restart

You can restore Nova Command to factory defaults and restart Nova Command here.

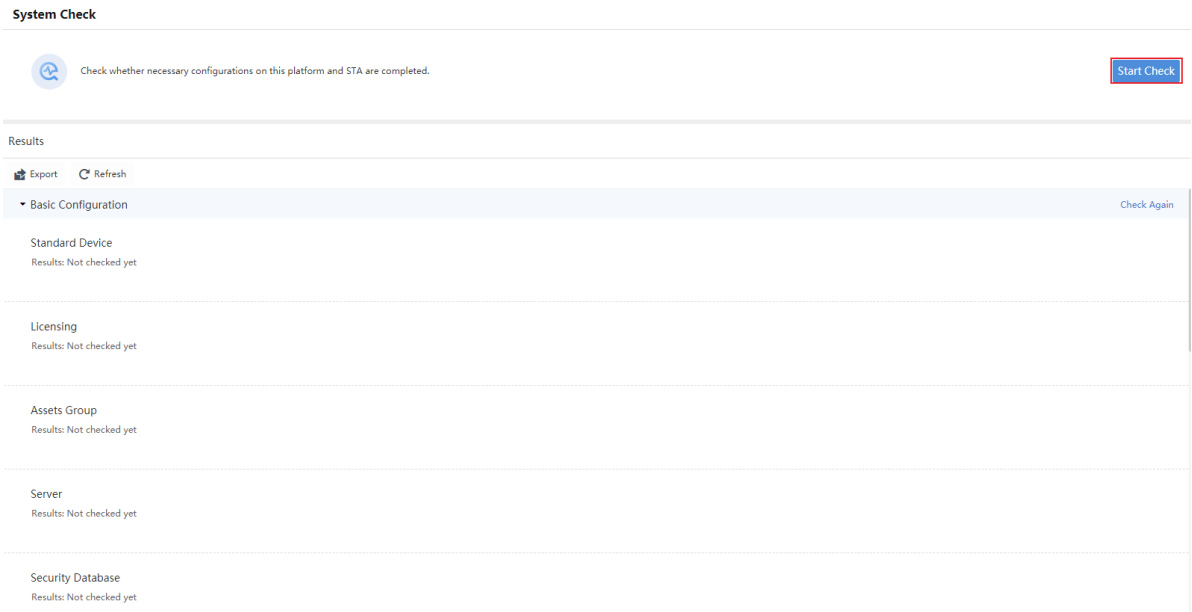
1. On the [System/Maintenance/Restore/Restart] page, you can click <Restore Factory Defaults> to delete all data and configurations of Nova Command. Please operate with caution.
2. You can click <Restart> to restart Nova Command. As Nova Command is deployed in one arm mode in the network, restart will not affect the network.
3. You can click <Export User Configuration> to export and back up the configurations of Nova Command or <Import User Configuration> to import the configurations for restoration.



System Check

You can check whether necessary configurations of Nova Command and Nova Sensor are complete with one click when Nova Command has just been installed or during system health check. Pay attention to alerts.

1. On the [System/Maintenance/System Check] page, you can click <\Start Check>, as shown in the figure below.



Configuration items:

Basic Configuration: You can check basic configuration items, including standard device, licensing, asset group, server, security database, and security engine.

System: You can check CPU, memory, disk status, and core processes.

Connected Devices: You can check the connectivity of ports and the status of connected devices.

Traffic Detection: You can check whether the traffic is mirrored correctly. The asset group should be configured first.

Proxy Detection: You can check the proxy server.

Nova Sensor Security Check: You can check the open ports, login with default admin password, and weak passwords.

Nova Command Security Check: You can check the open ports, login with default admin password, password-free login, and weak passwords.

2. You can click <Export> to export current results to facilitate system maintenance by O&M personnel.
3. You can click <Refresh> to refresh the page.

Security Capabilities

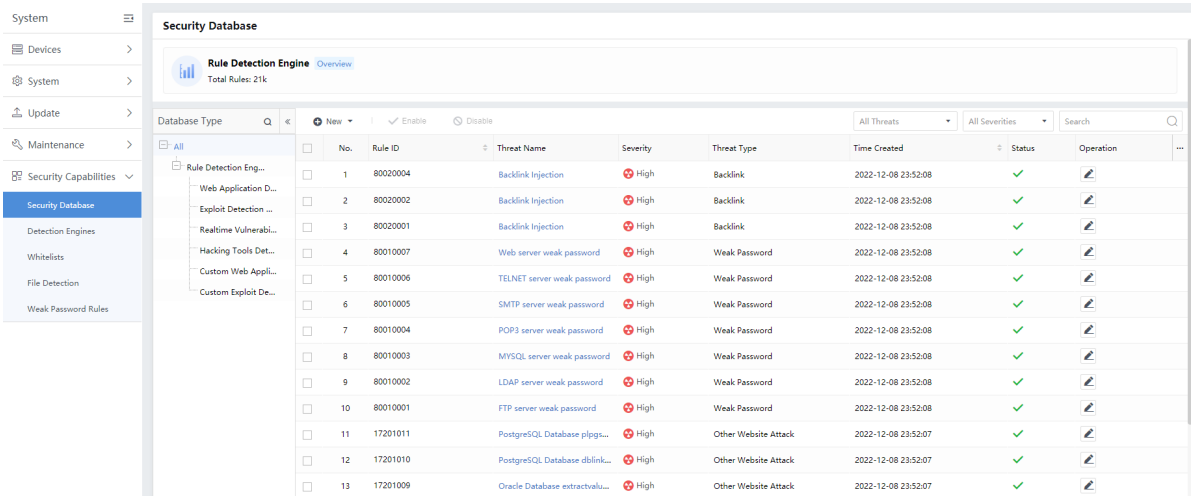
This part contains pages of Security Database, Detection Engines, Whitelists, File Detection, and Weak Password Rules.

Security Database

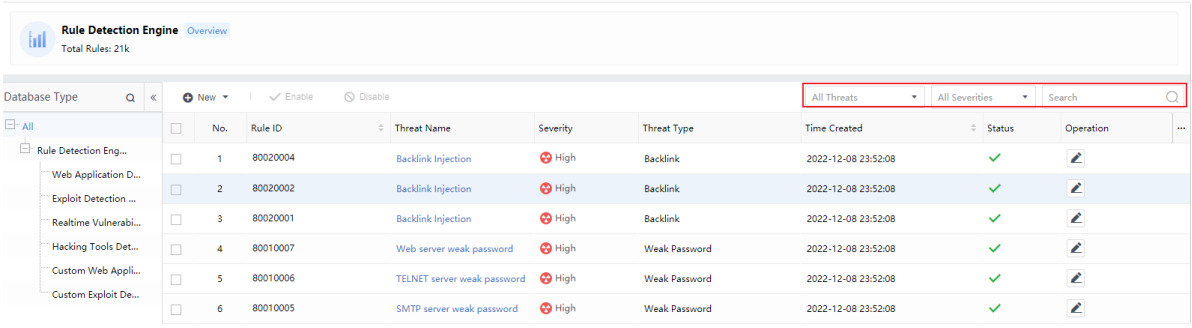
You can manage web application detection database, exploit detection database, realtime vulnerability analytics and detection database, hacking tool detection database, and custom detection databases on the Security Database page.

Filter and search

On the [System/Security Capabilities/Security Database] page, you can select a database type to view the information about corresponding rules, including rule ID, threat name, severity, threat type, time created, status, and operation, as shown in the figure below.

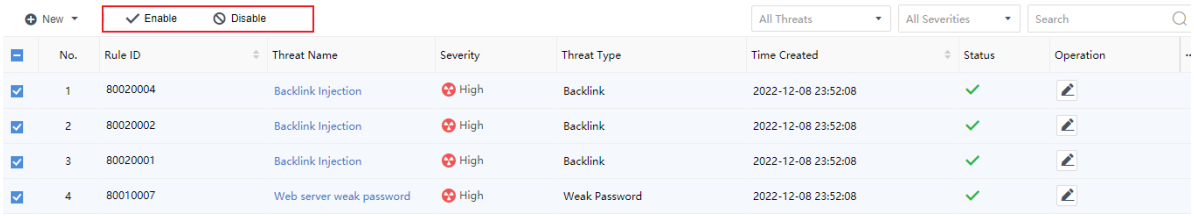


During actual operation, you can filter rules by threat type, severity, and rule ID or search for rules through fuzzy search using keywords, as shown in the figure below.

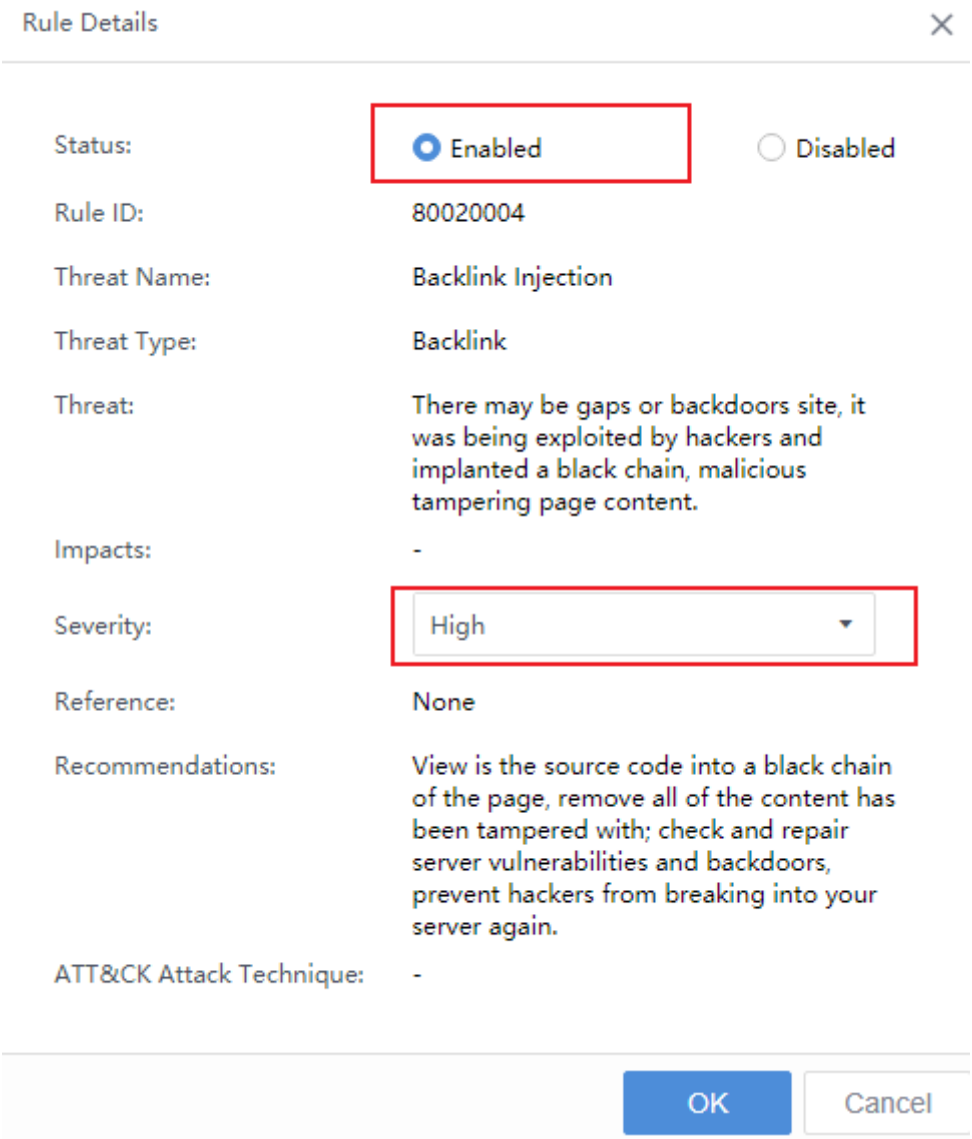


Editing

You can batch change the status of multiple rules, as shown in the figure below.

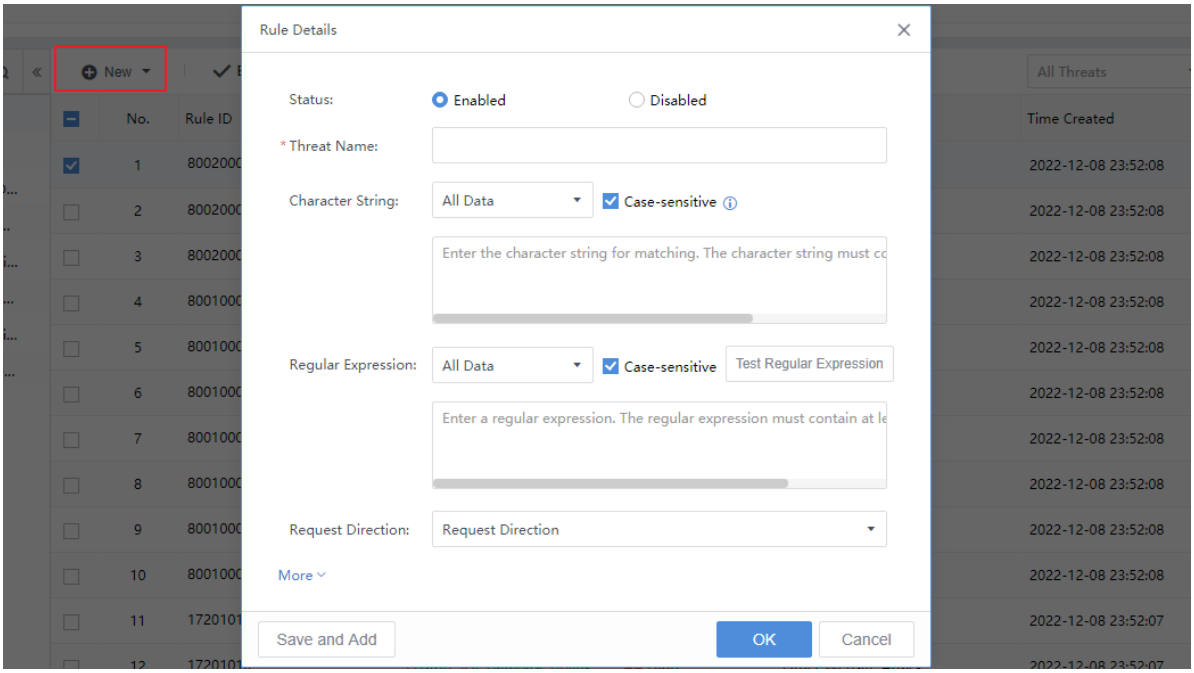


For a single rule, you can switch the status. You can also click < > to go to the details page and change the severity of the rule, as shown in the figure below.



Custom web application detection rules

On the [System/Security Capabilities/Security Database] page, you can click <New> and select [Custom Web Application Detection Rules] from the drop-down list, as shown in the figure below.



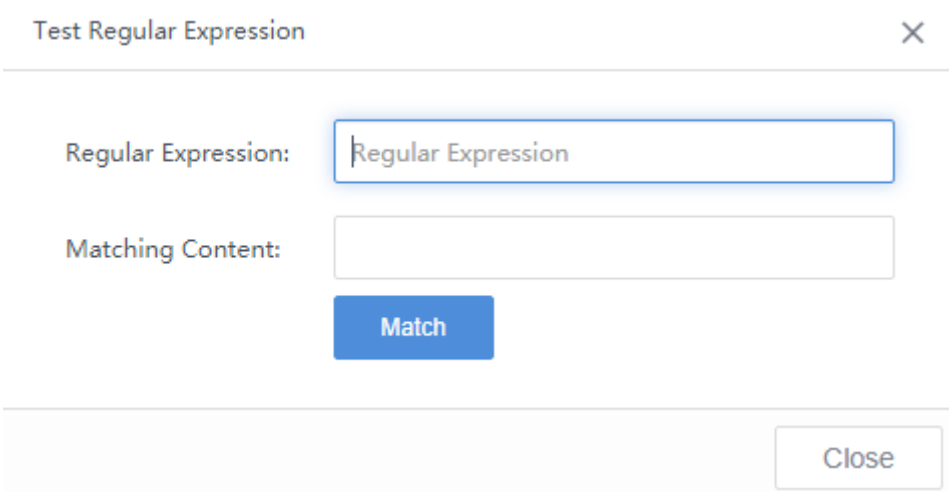
Fields:

Status: Default status is "Enabled".

Threat Name: You can specify the name.

Character String: The character string for matching. Available options include All Data and Match URL/Cookie/Table Data. You need to enter the character string for matching. Text and binary characters are supported.

Regular Expression: The character string is translated to a regular expression. You can click <Test Regular Expression> to test the format of the regular expression and character string in the pop-up box, as shown in the figure below.



Request Direction: Includes Request Direction, Response Direction, and Bidirectional Matching.

Severity: Includes High, Medium, and Low.

Description: Custom rule description.

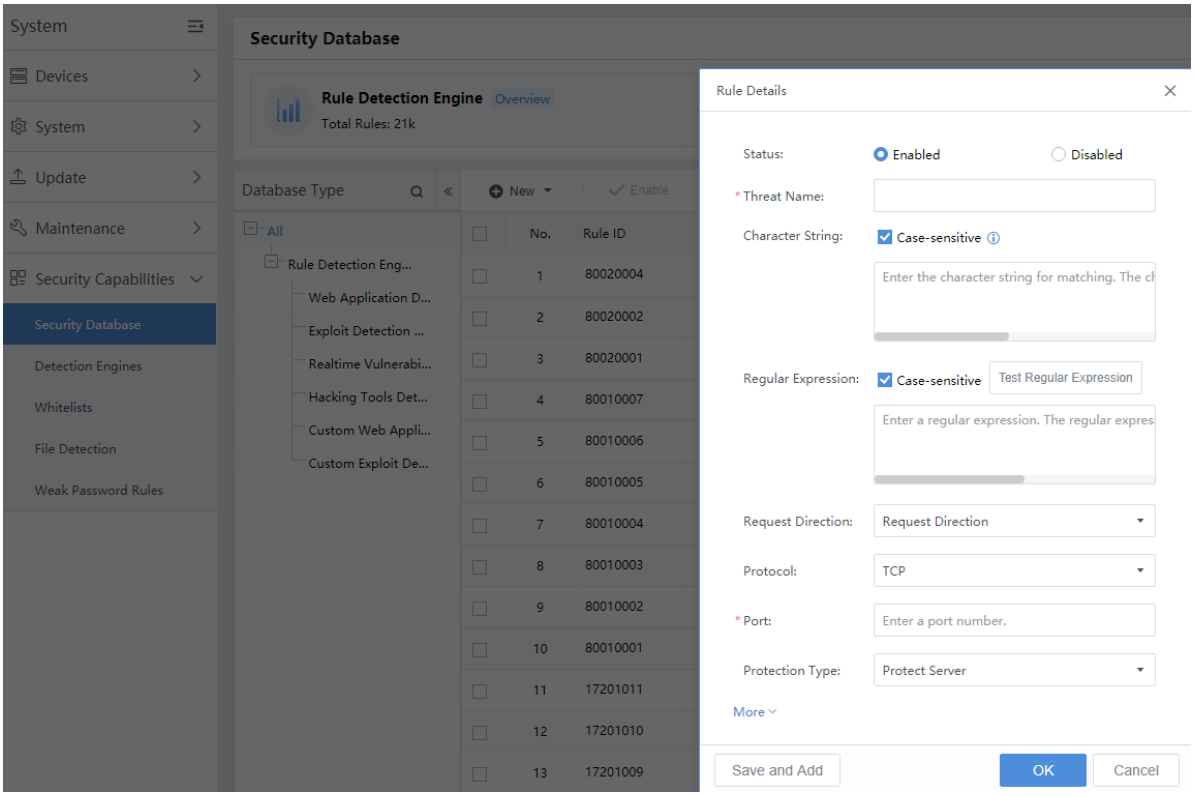
Impacts: Impact of the rule on attacks.

Note

Either the character string or regular expression is required.

Custom exploit detection rules

On the [System/Security Capabilities/Security Database] page, you can click <New> and select [Custom Exploit Detection Rules] from the drop-down list, as shown in the figure below.



Fields:

Status: Includes Enabled and Disabled. The default status is "Enabled".

Threat Name: You can specify the name.

Character String: The character string for matching. Available options include All Data and Match URL/Cookie/Table Data. You need to enter the character string for matching. Text and binary characters are supported.

Regular Expression: The character string is translated to a regular expression. You can click <Test Regular Expression> to test the format of the regular expression and character string in the pop-up box, as shown in the figure below.

Request Direction: Includes Request Direction and Response Direction.

<Protocol>: Protocol corresponding to the rule. Available options include TCP and UDP.

<Port>: Port associated with the rule. A single port is supported.

Severity: Includes High, Medium, and Low.

Description: Custom rule description.

Impacts: Impact of the rule on attacks.

Note

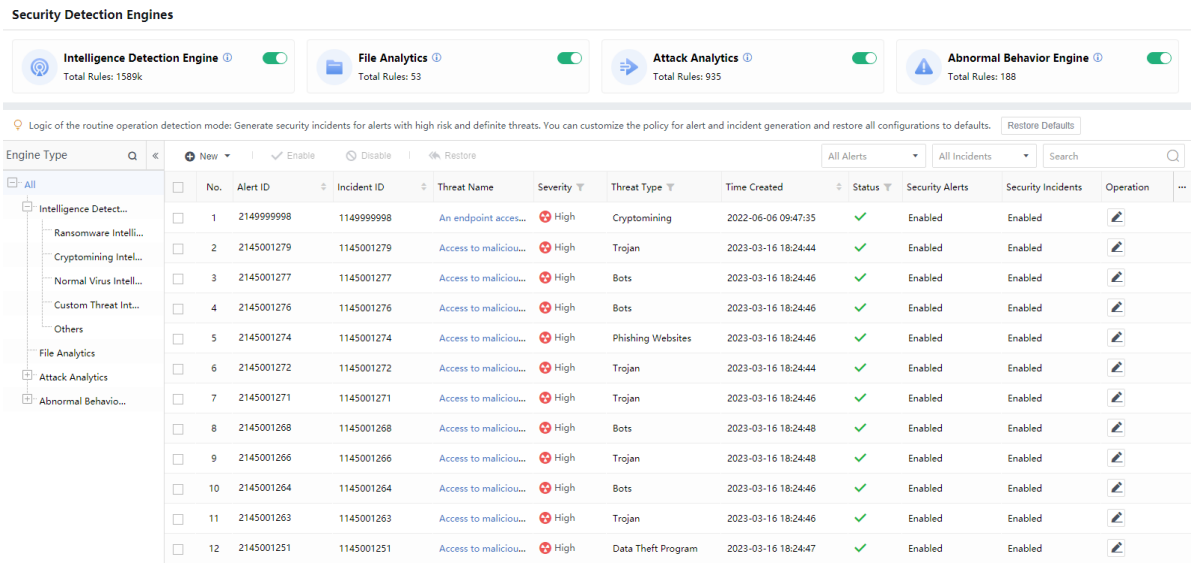
Either the character string or regular expression is required.

Detection Engines

Types of detection engines for security incidents/security alerts include Threat Intelligence Engine, File Analytics, Attack Analytics, and Abnormal Behavior Engine. You can edit, filter, search for, and add rules.

Filter and search

On the [System/Security Capabilities/Detection Engines] page, you can hover the mouse over the icon for <introduction> next to the engine name to view the brief introduction of each detection engine. The attributes of each rule displayed in the table include alert ID, incident ID, threat name, severity, threat type, time created, status, generation settings of security alert/incident, and operation, as shown in the figure below.



Fields:

Alert ID

Displayed on the security alert details page. It usually starts with the digit "2".

Incident ID

Displayed on the security incident details page. It usually starts with the digit "1".

Severity

Includes High, Medium, and Low.

Threat Type

The same as the threat type on the Security Alerts and Security Incidents pages of the Response module.

Security Alerts

Indicates whether a security alert is generated based on this rule, which can be "Enabled" or "Disabled". As a security incident is the result of a security alert, when the Security Alerts field is set to "Disabled", the Security Incidents field will be set to "Disabled".

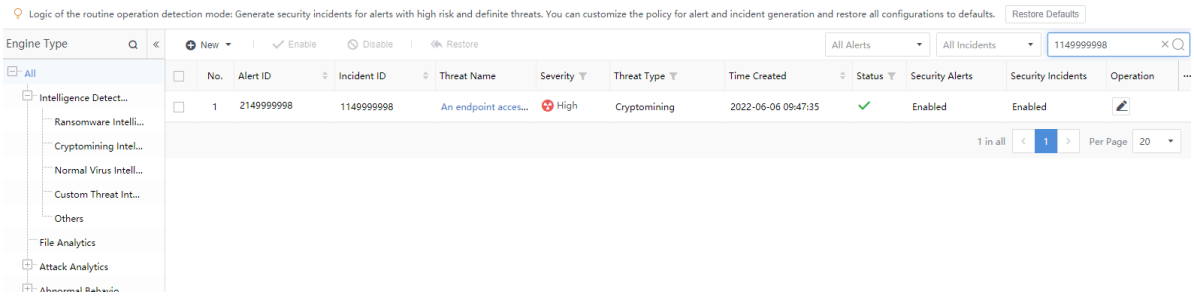
Security Incidents

Indicates whether a security incident is generated based on this rule, which can be "Enabled" or "Disabled".

Status

You can change the status of each rule. " ✓ " means "Enabled", and " ⊘ " means "Disabled".

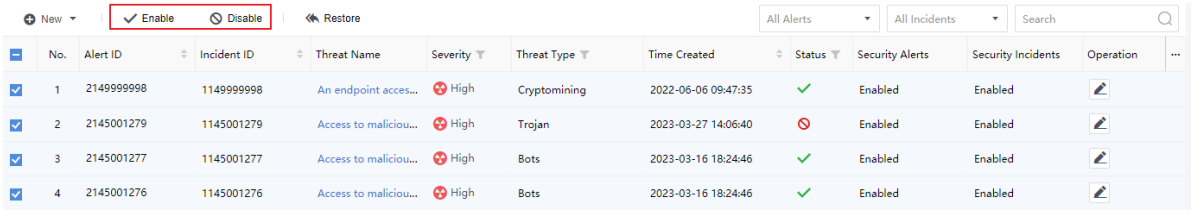
Rules in the rule table can be displayed by threat type and severity. You can also enter keywords or a rule ID to perform a fuzzy search, as shown in the figure below.



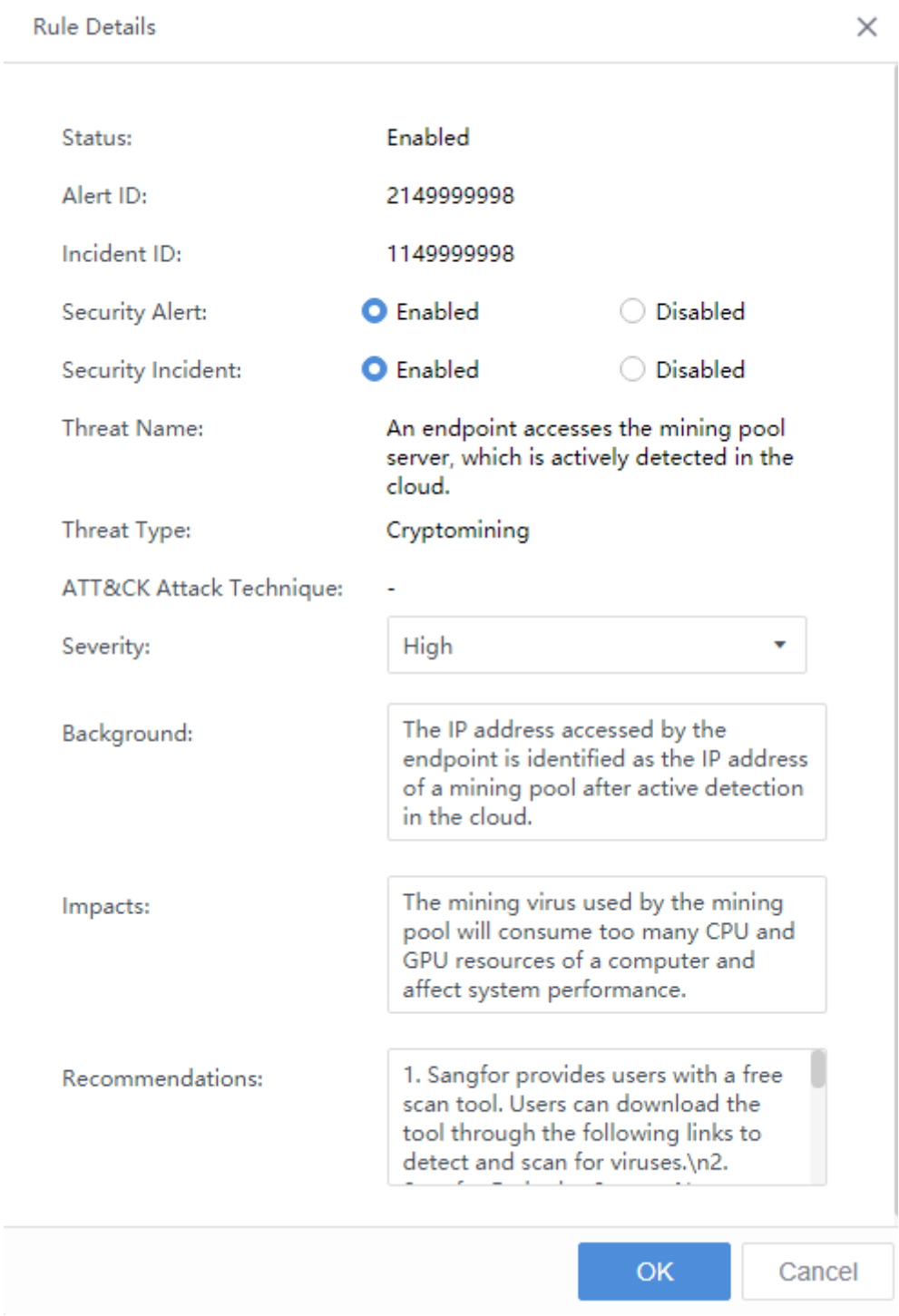
In the rule table, you can click the " ✎ " icon of a rule in the Operation Column to edit it.

Editing and managing

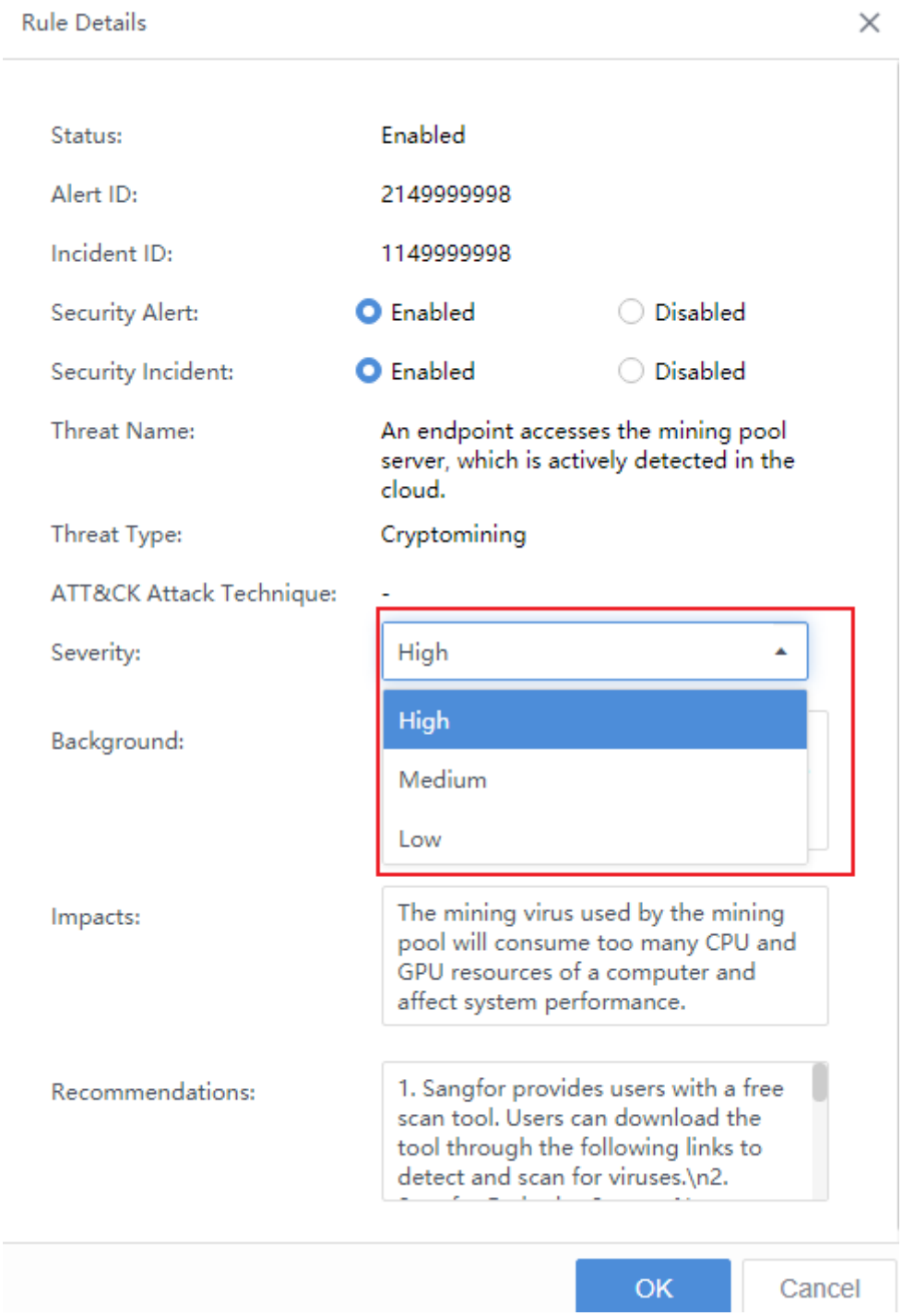
On the [System/Security Capabilities/Detection Engines] page, you can select a single or multiple rules and click <Enable>, <Disable>, or <Restore> to batch enable or disable the rules or restore them to defaults, as shown in the figure below.



You can click the content in the Threat Name column of a rule to enter the details page, which displays information such as current status, alert ID, incident ID, security alert, security incident, threat name, threat type, background, impacts, and severity. You can specify whether a security incident or alert is generated based on the rule, as shown in the figure below.

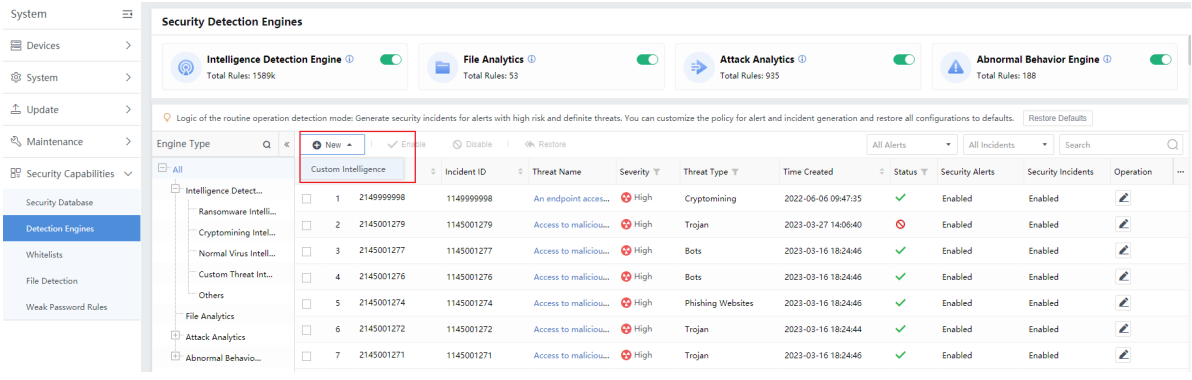


You can select a severity from the drop-down list, as shown in the figure below.



Custom threat intelligence

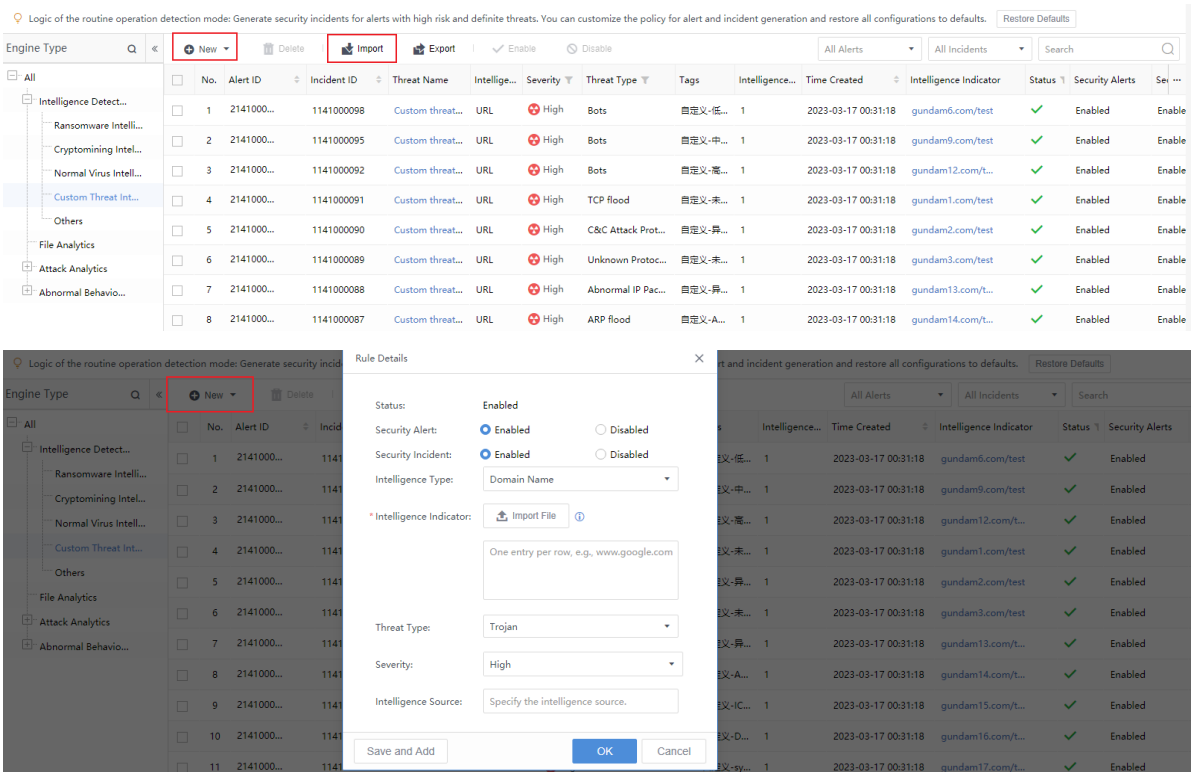
On the [System/Security Capabilities/Detection Engines] page, you can customize the threat intelligence, as shown in the figure below.



Creating threat intelligence

On the [System/Security Capabilities/Detection Engines] page, you can select the Custom Threat Intelligence type on the left and then click <New> or <Import> to create threat intelligence and specify fields, such as Security Alert, Security Incident, Intelligence Type, Threat Type, Severity, and Intelligence Source.

You can also update threat intelligence information by editing the intelligence type, threat type, severity, and intelligence source. The page for addition is shown in the following figure.



Fields:

Security Alert: Indicates whether a security alert is generated.

Security Incident: Indicates whether a security incident is generated.

Intelligence Type: Includes Domain Name, IP, URL, and File MD5.

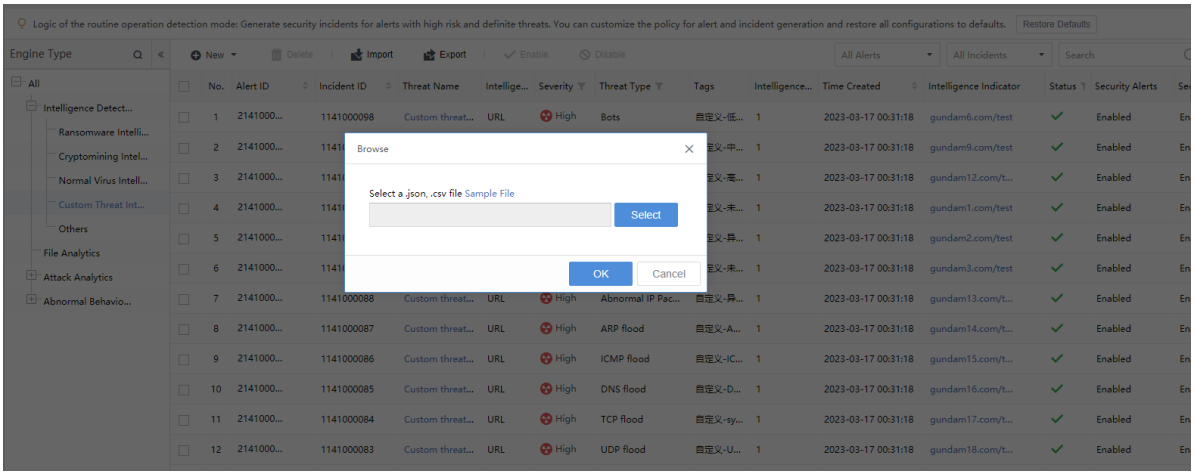
Threat Type: Threat type of the threat intelligence.

Severity: Includes High, Medium, and Low.

Intelligence Source: Source of the intelligence.

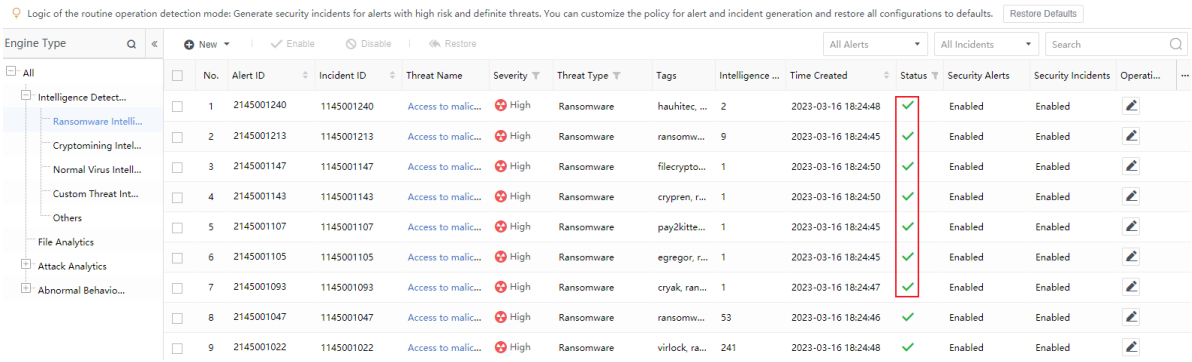
Importing threat intelligence

You can click <Import> and <Sample File> to download the sample file and then edit and import the .csv/.stix2 sample file to import threat intelligence in batches, as shown in the figure below.



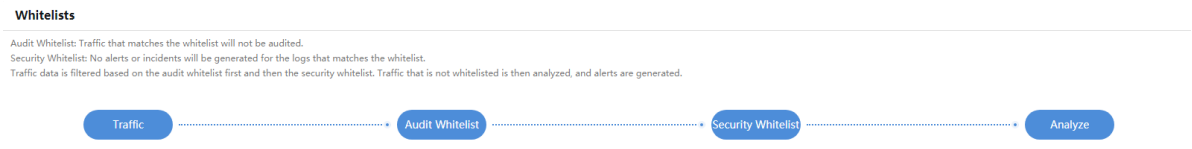
Managing threat intelligence

After selecting a single or multiple threat intelligence entries, you can enable, disable, or delete them one by one or in batches by clicking the corresponding button. You can also search for specific threat intelligence by entering keywords in the search box in the top right corner. You can view the status in the Status column and click " ✔ " to disable or enable the rule. You can also export threat intelligence, as shown in the figure below.



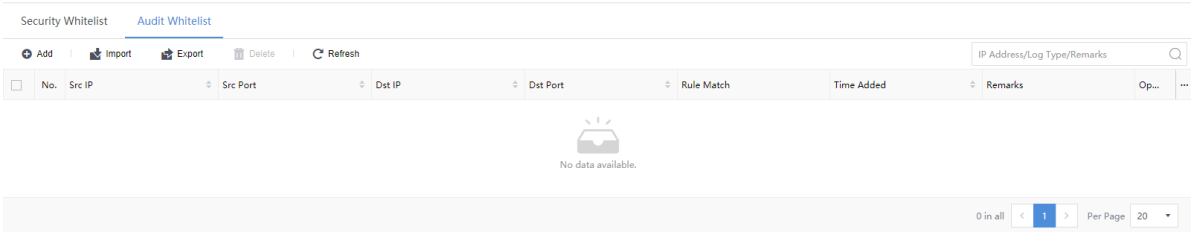
Whitelists

This feature is a basic feature of Nova Command and is frequently used. During actual operation, DNS servers, vulnerability scan tools, and other special devices in the network should be added to the whitelists to avoid being reported as compromised devices. Whitelists include security whitelist and audit whitelist. Traffic data is filtered based on the audit whitelist first and then the security whitelist. Traffic that does not match the whitelists is then analyzed, based on which threat data is generated for each business system.



Audit Whitelist: It is used as the filter for generating logs. Logs will not be generated for traffic that matches the whitelist.

Security Whitelist: It is used as the filter for generating alerts. No alerts or incidents will be generated for the logs that match the whitelist, as shown in the figure below.



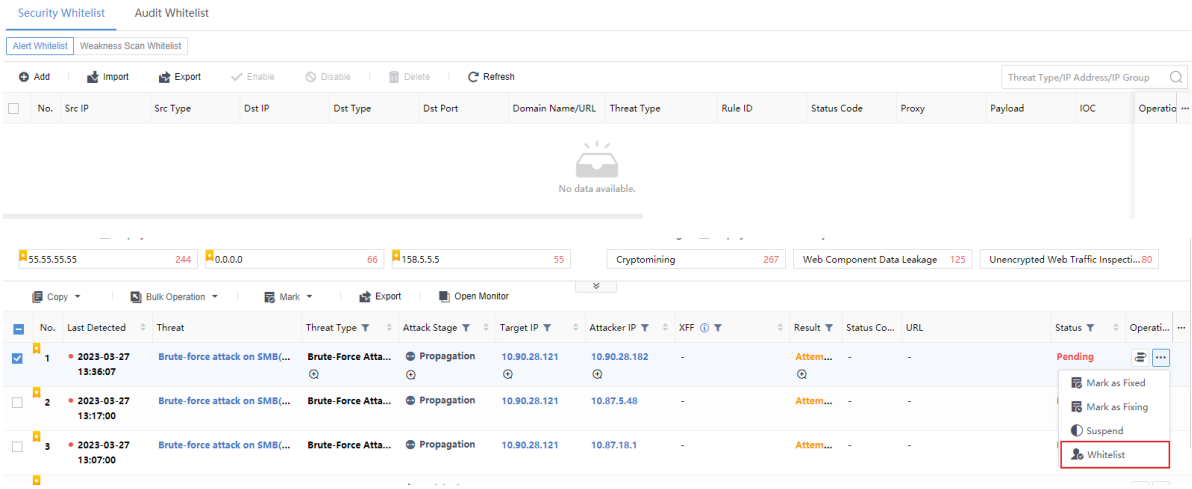
Analyze: Data, such as security alerts and security incidents, is generated.

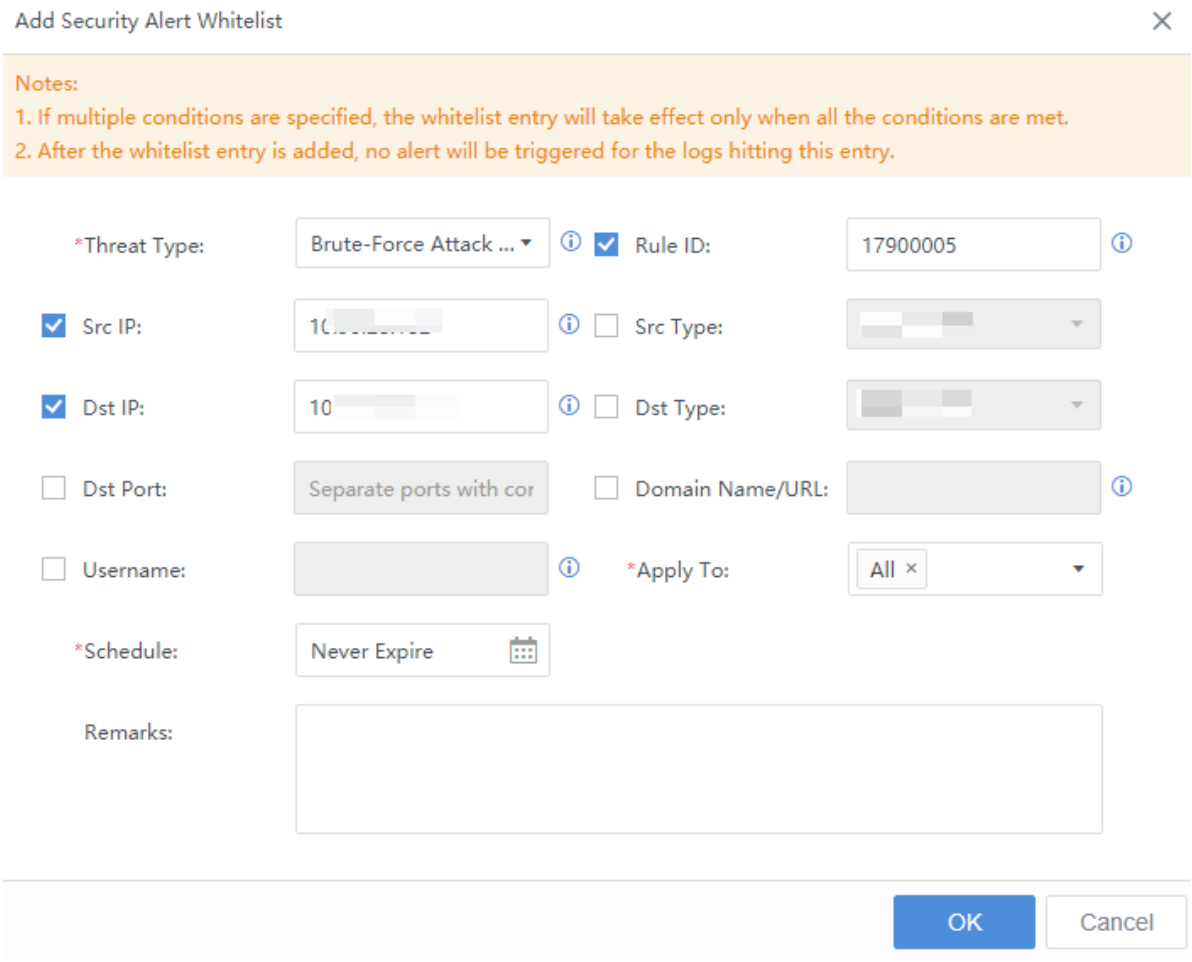
Creating security whitelist

A security whitelist is used to whitelist a security alert or a weakness alert at the log level. Once whitelisted, alerts will not be generated for corresponding logs and will not be displayed in modules including Home, Response, and Detection.

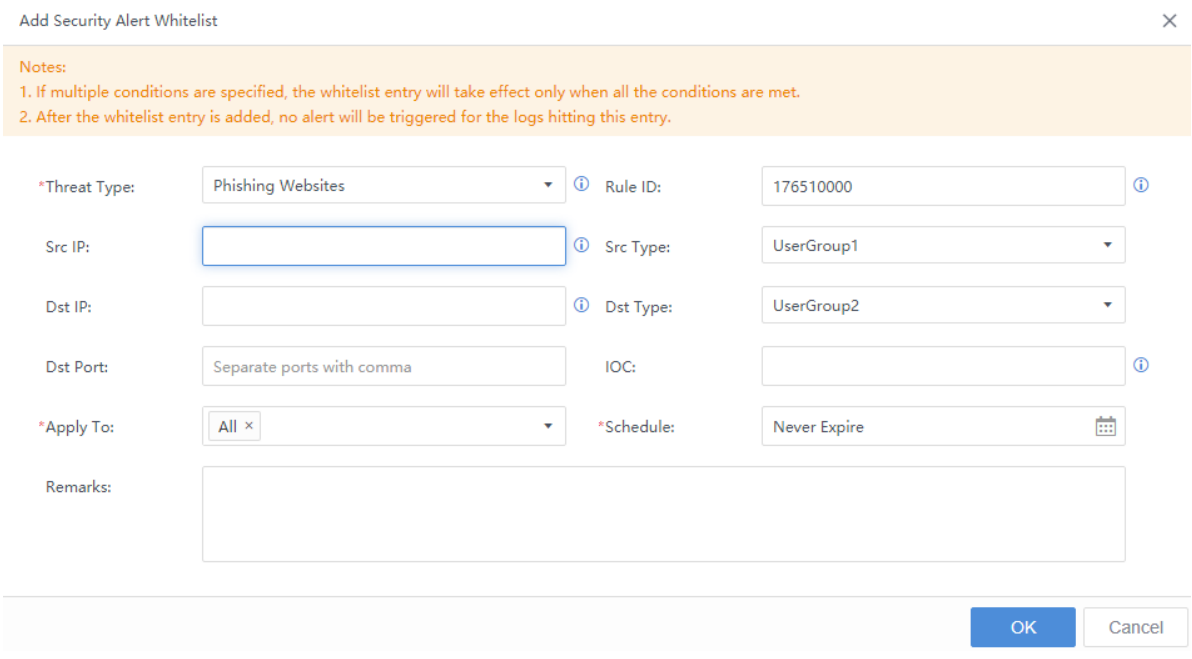
1. Alert whitelist

During daily operation, in modules including Response and Detection, you can select an alert and click <Whitelist> in the Operation column to go to the whitelist configuration page, as shown in the figures below.





You can also add a whitelist on the [System/Security Capabilities/Whitelists] page following these steps: 1. Click <Security Whitelist>, select [Alert Whitelist] tab, and then click <Add>. 2. The Add Security Alert Whitelist page appears. You can specify the threat type, rule ID, source and destination IP addresses, source and destination types, applicable device, and schedule. Those conditions are in an "AND" relationship, which means the whitelist will take effect only when all the conditions are met, as shown in the figure below.



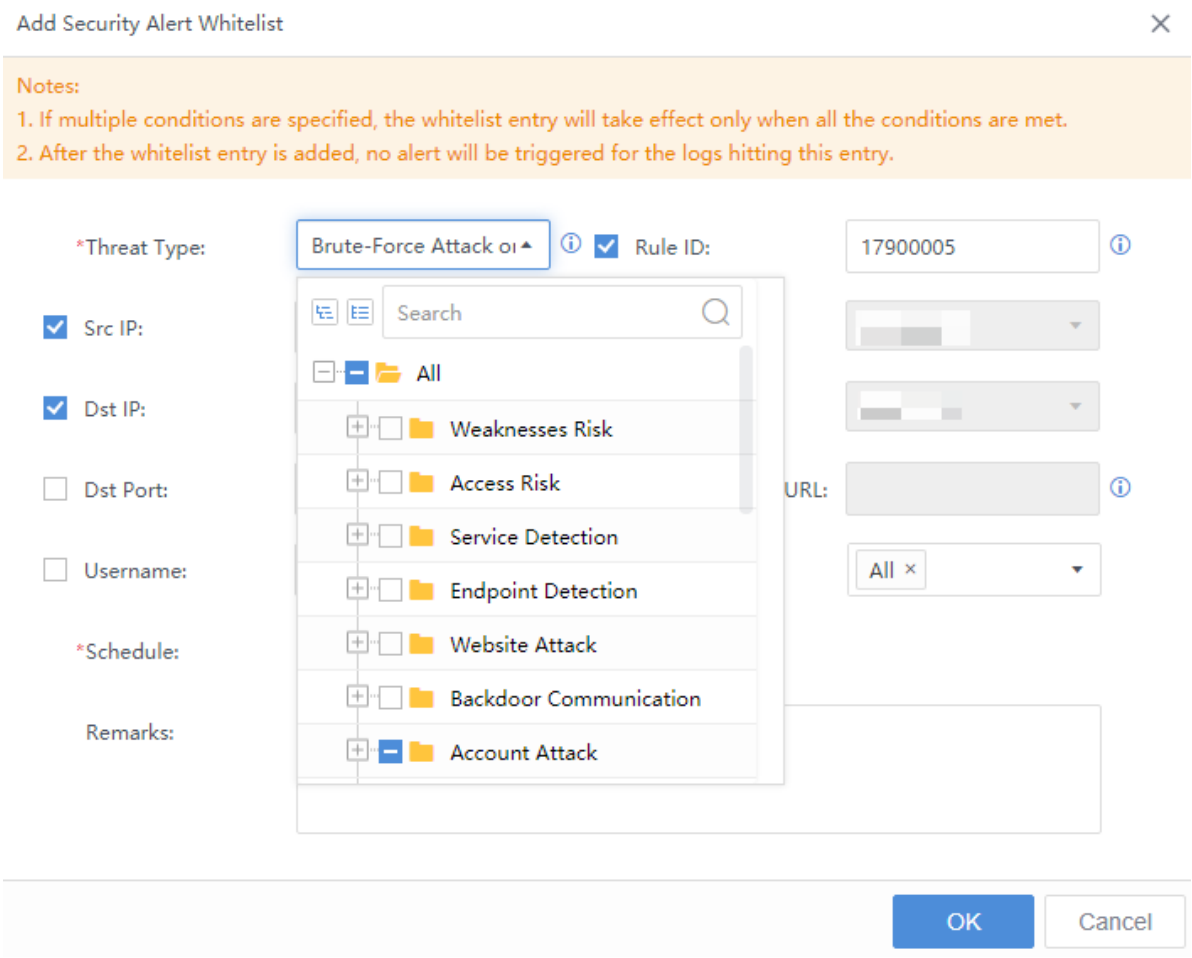
Fields:

Src IP: When the IP address is specified, no alerts will be generated for data from this IP address.

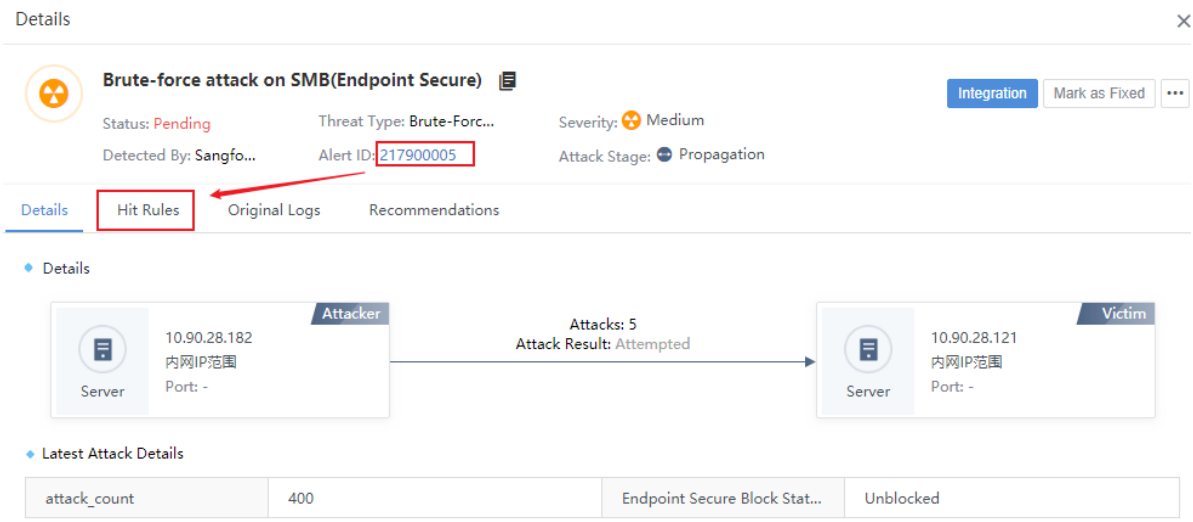
Dst IP: When the IP address is specified, no alerts will be generated for data to this IP address.

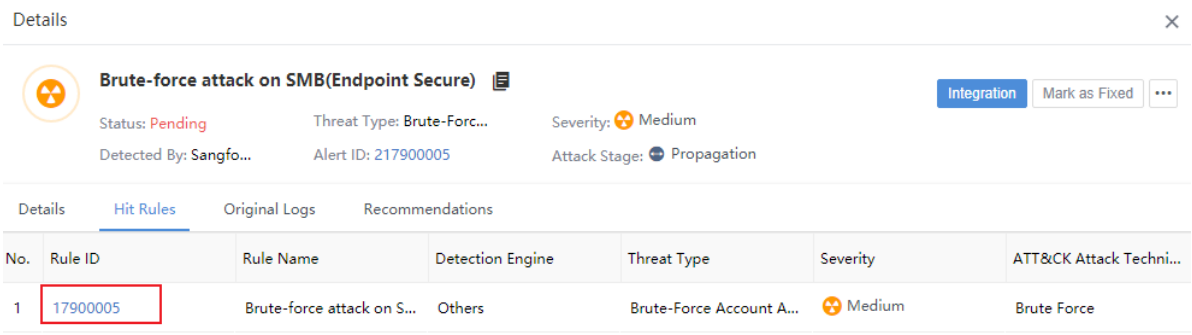
Domain Name/URL: When the domain name/URL is specified, no alerts will be generated for data from this domain name/URL.

Threat Type: The matched threat type. You can select all or a specific type from the drop-down list according to the actual situation.

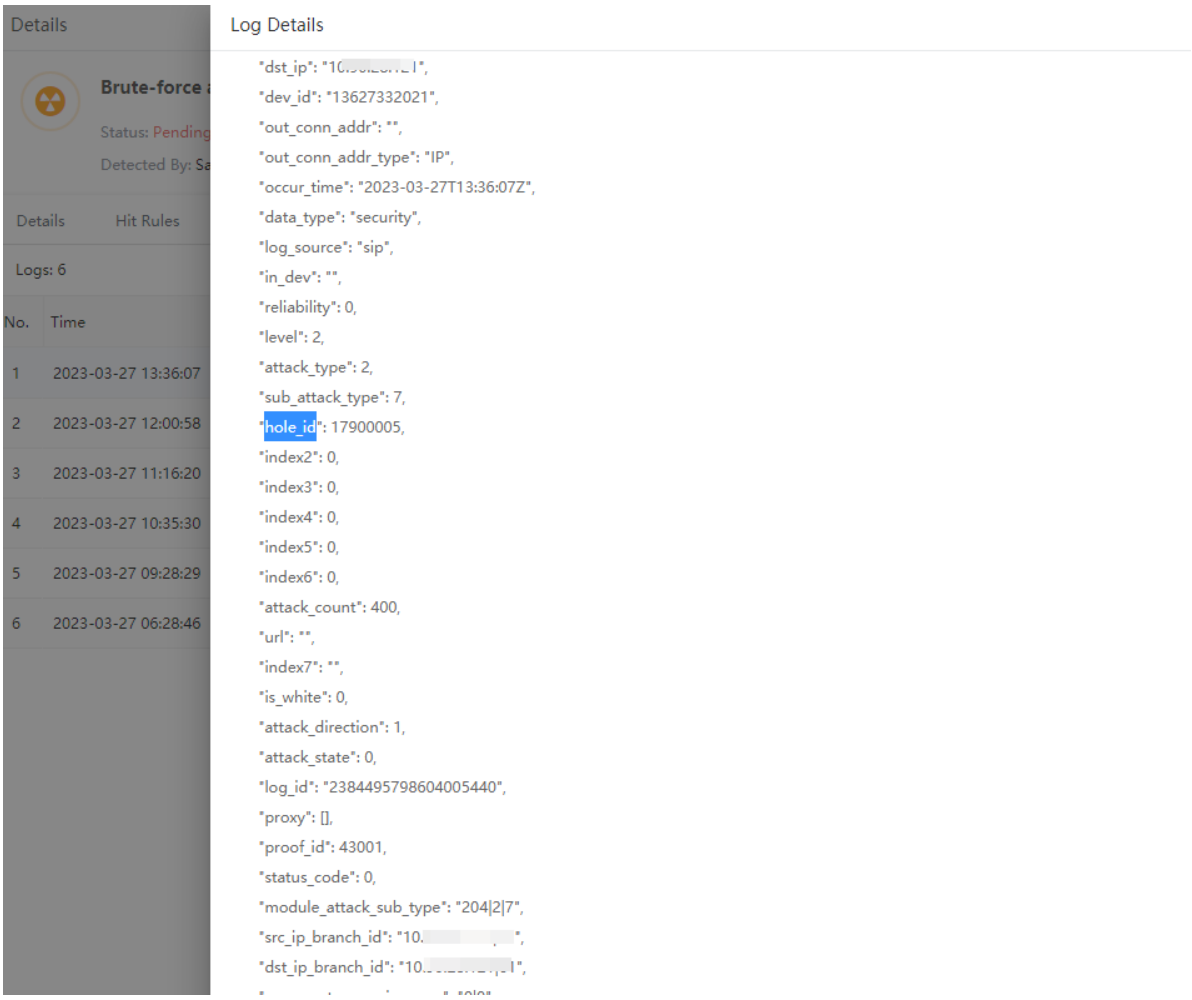


Rule ID: No alerts will be generated for the corresponding rule ID. It is used to whitelist some IDs in some threat types. For example, SQL injections involve many rule IDs, so it is required to whitelist some IDs according to the actual situation. The rule ID here is neither alert ID nor incident ID. See the following figure.





Corresponding **hole_id** in the logs:

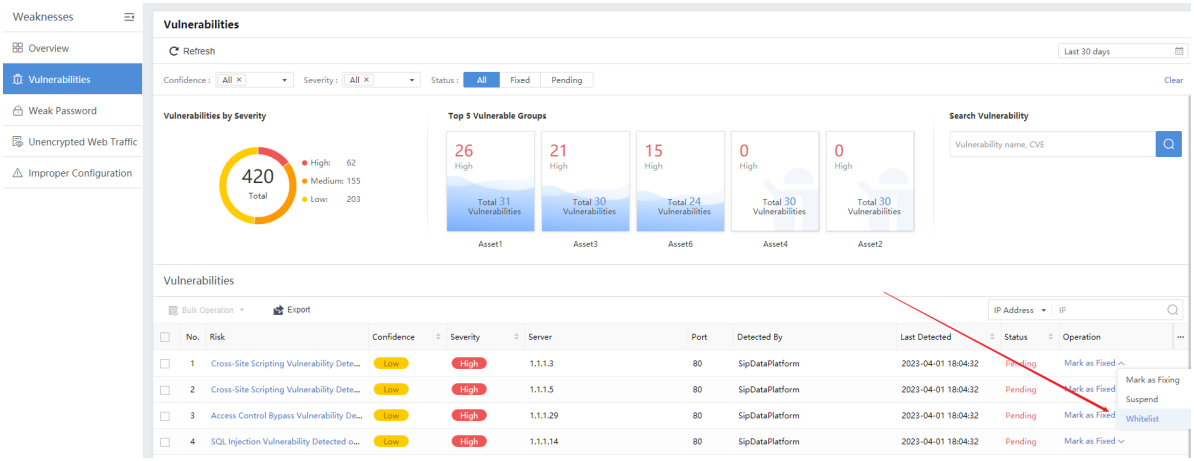


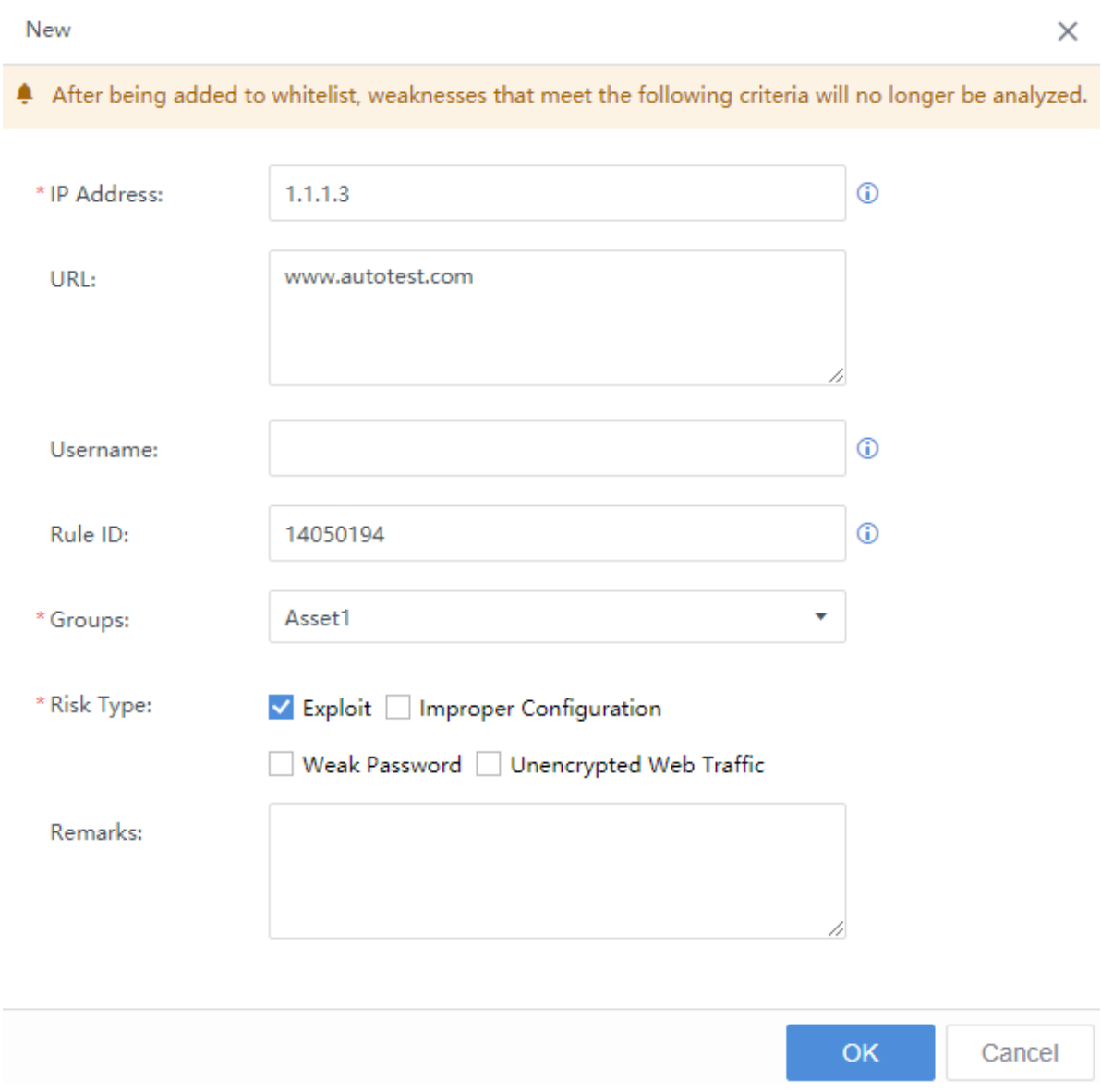
Apply To: "All" is selected by default. You can also select the applicable device from the drop-down list based on the device which generates security alerts.

Schedule: The default value is "Never Expire". You can also change it to a specific time range. During daily operation, in modules including Response and Detection, you can select an alert and click <Whitelist> in the Operation column to go to the whitelist configuration page.

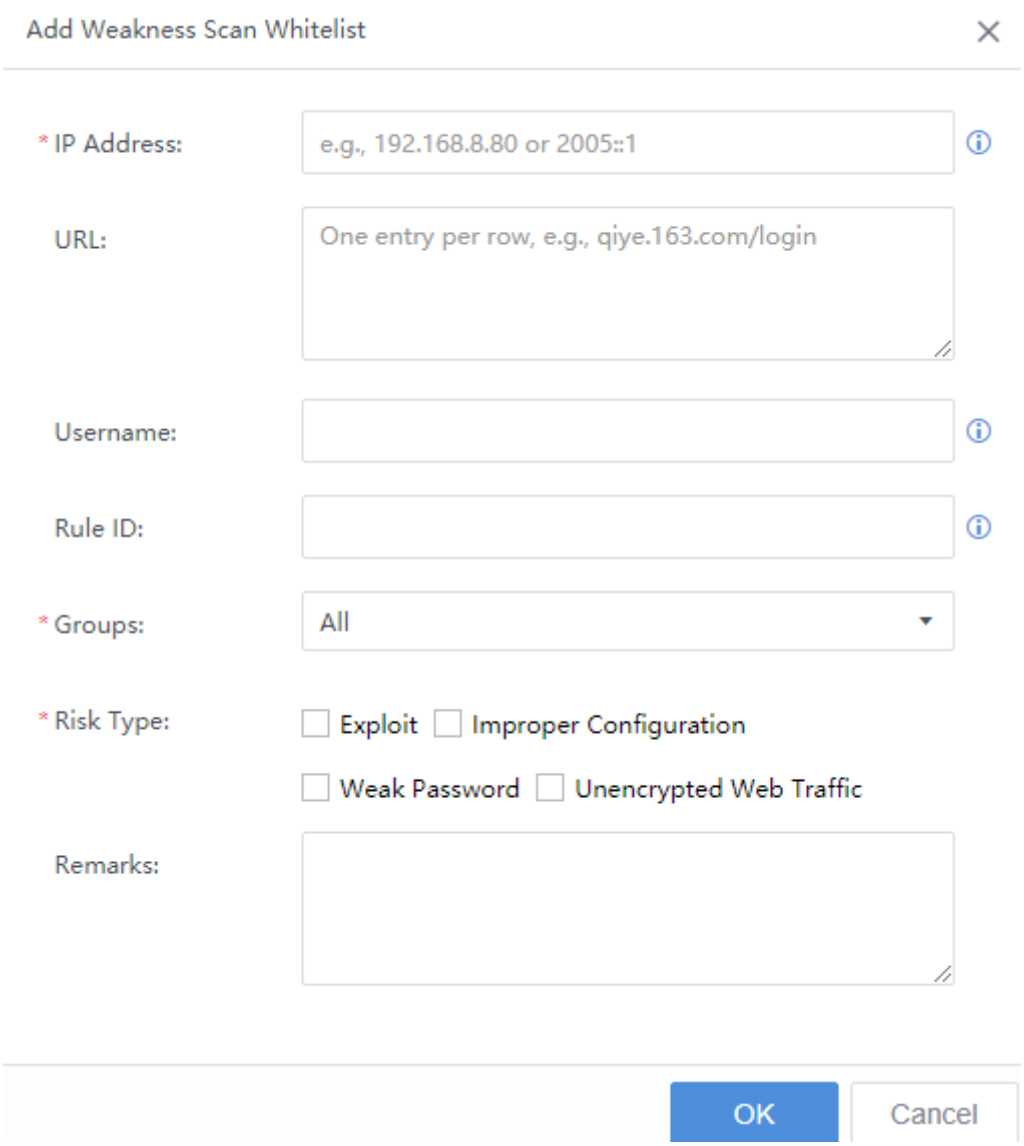
2. Weakness scan whitelist

The Weakness Scan Whitelist mainly applies to Vulnerabilities, Weak Password, Unencrypted Web Traffic, and Improper Configuration in the [Assets/Weaknesses] module. During normal operation, to whitelist a weakness on these pages, you can click <\Whitelist> in the Operation column to go to the whitelist configuration page and complete required information, as shown in the figures below.





On the [Security Capabilities/Whitelists] page, you can select Weakness Scan Whitelist and then click <Add> to manually configure a weakness scan whitelist. On the Add Weakness Scan Whitelist page that appears, you can enter the IP address, URL, username, rule ID, asset group, and risk type. After you complete the information, click <OK>, as shown in the following figure.



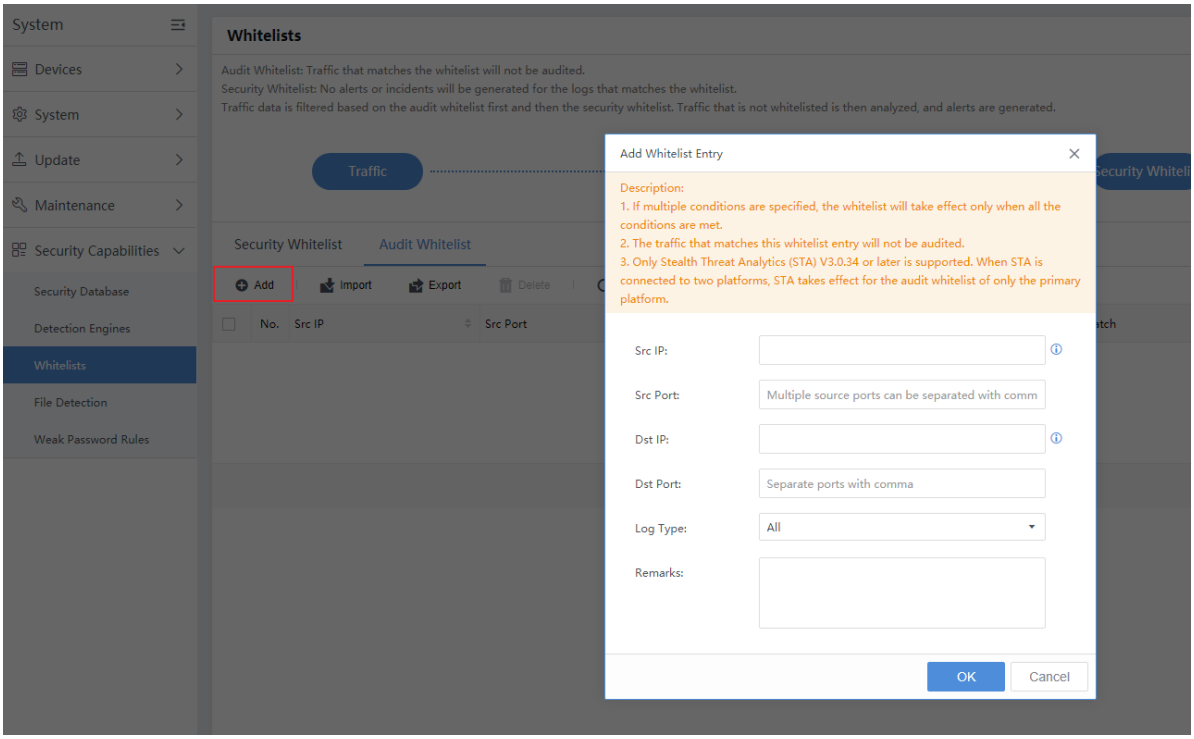
Audit whitelist

说明

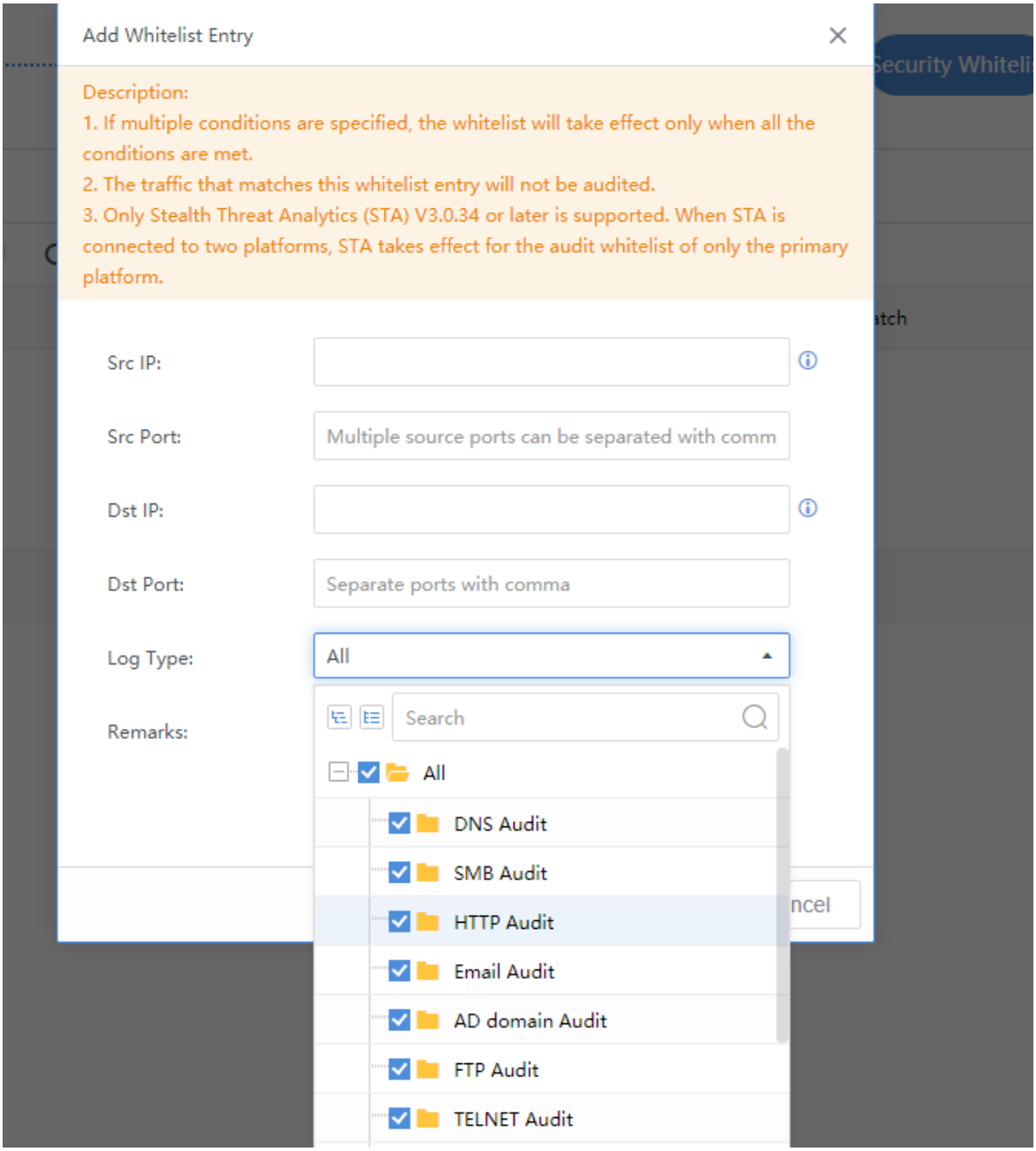
1. Only Nova Sensor V3.0.34 or later is supported. When Nova Sensor is connected to two platforms, the audit whitelist of the main platform applies.
2. If multiple conditions are specified, the whitelist will take effect only when all the conditions are met.

The Audit Whitelist is mainly implemented at the Nova Sensor side and applicable to logs at the traffic level. Logs will not be generated for traffic that matches the whitelist. Unlike the Security Whitelist, which can be configured through automatic redirection in modules such as Response, Detection, and Assets, the Audit Whitelist can only be added manually on the Audit Whitelist tab.

On the [Audit Whitelist] tab of the [Security Capabilities/Whitelists] page, you can click <Add> to pop up the Add Whitelist Entry dialogue box. You can then enter the source IP, destination IP, source port, destination port, and log type, as shown in the figure below.



In the drop-down list of Log Type, you can perform a fuzzy search with keywords, as shown in the figure below.



Src IP: When the IP address is specified, no logs will be generated for data from this IP address.

Src Port: When the source port is specified, no logs will be generated for data from this port.

Dst IP: When the IP address is specified, no logs will be generated for data to this IP address.

Dst Port: When the destination port is specified, no logs will be generated for data to this port.

Log Type: The matched log type.

Besides adding whitelist entries one by one, you can also import and export whitelist entries in batches. For example, when devices are connected to Nova Command, the overall whitelist may be a merged whitelist based on whitelists of all devices. To add or move entries in a great number, you can use the import and export features, as shown in the figure below.

Export

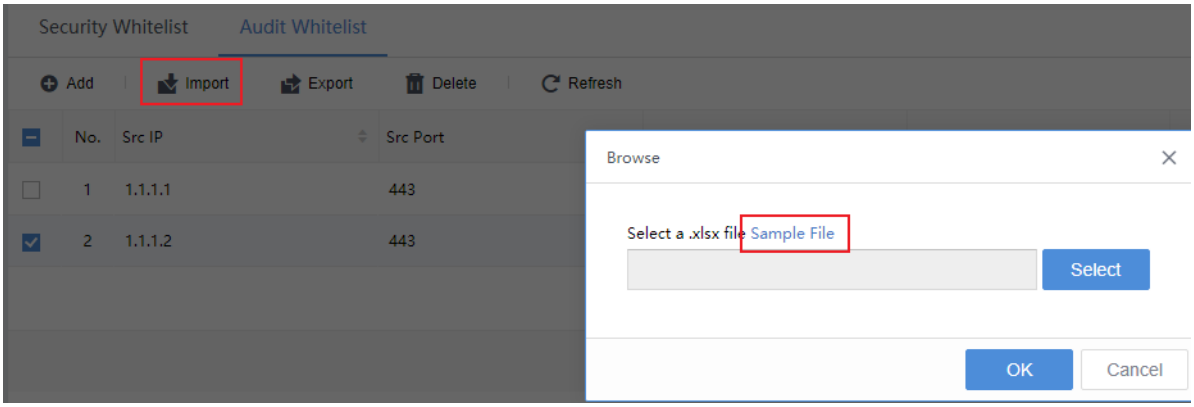


You can export all entries in XLSX format.

No.	Src IP	Src Port	Dst IP	Dst Port	Rule Match	Remarks
1	'1.1	'443	'2.	'448	'All	
2	'1.1.1.2	'443	'1.1.1.1	'225	'All	

Import

You need to download the sample file first.



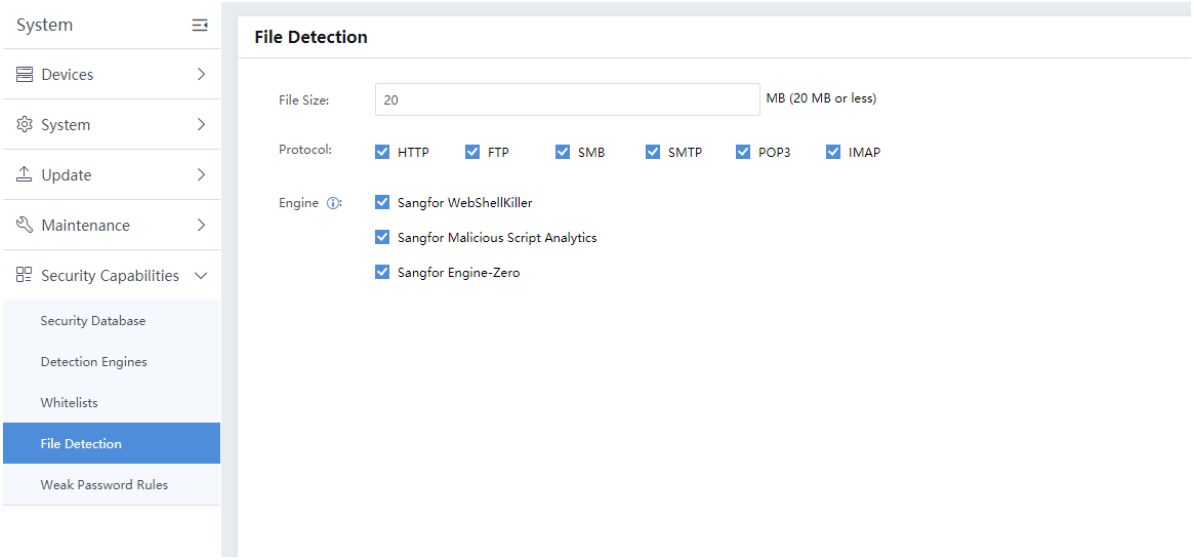
Then, you need to fill in the sample file with required information and then import it.

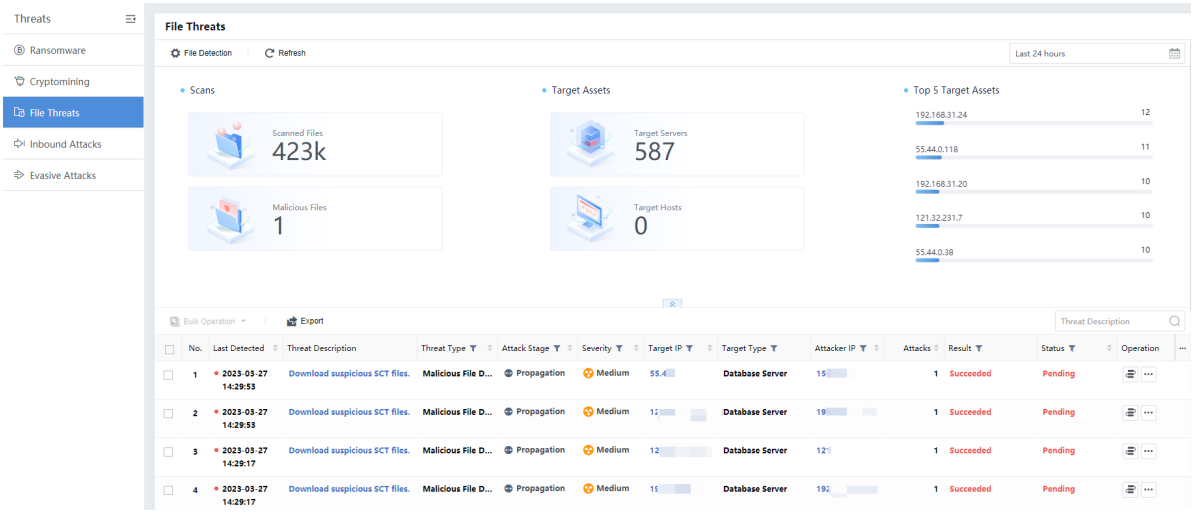
⚠ 注意

The validity of the whitelist is related to assets. To import a whitelist, check whether the assets in the whitelist are configured in the target platform. If they are not configured or do not exactly match, change them manually.

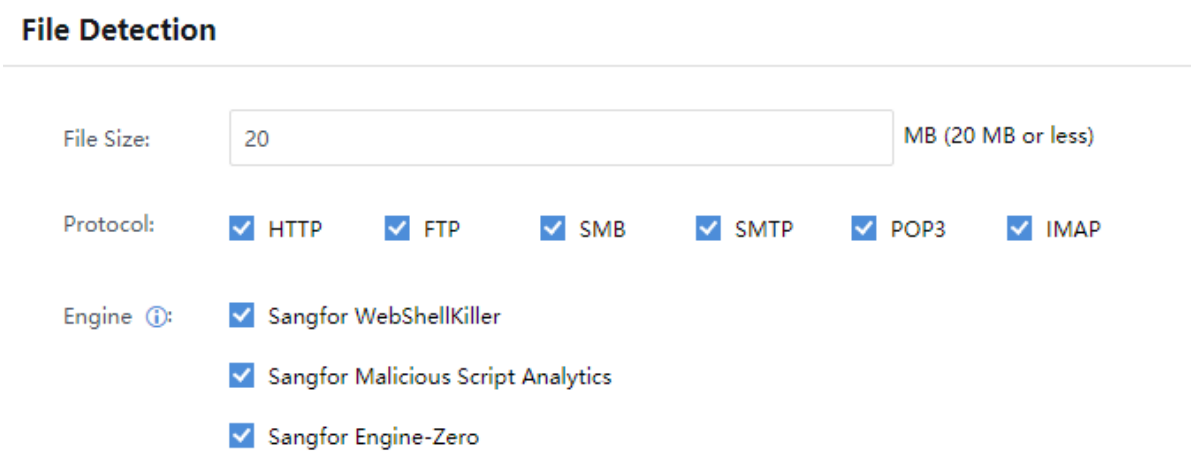
File Detection

The [Security Capabilities/File Detection] page corresponds to the [Detection/Threats/File Threats] module, as shown in the figures below.





You can change the file detection settings, including file size (20 MB or less), protocol, and selected engine, as shown in the figure below.



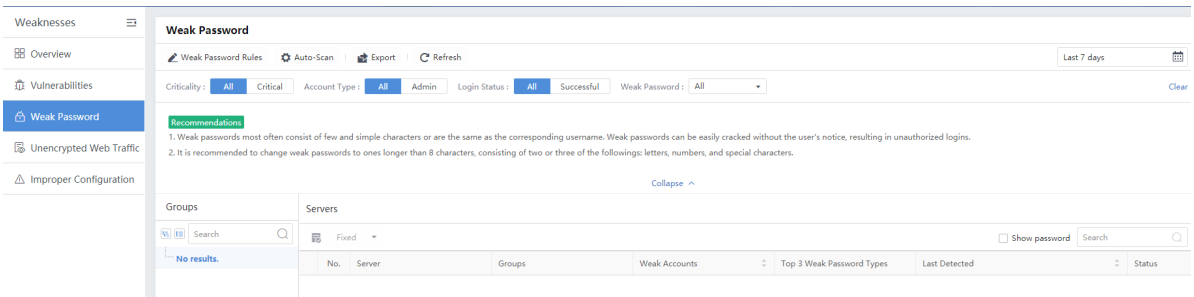
Fields:

Protocol: Includes HTTP, FTP, SMB, SMTP, POP3, and IMAP. Select the protocol as needed.

Engine: Includes
Sangfor WebShellKiller, Sangfor Malicious Script Analytics, and Sangfor Engine-Zero.

Weak Password Rules

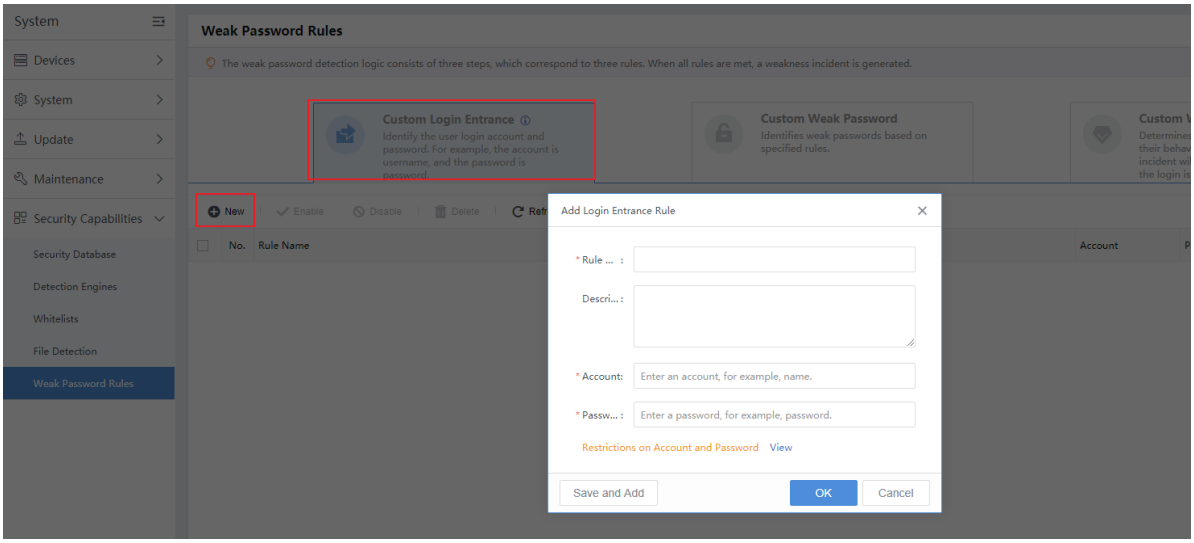
The [Security Capabilities/Weak Password Rules] page corresponds to the [Assets/Weaknesses/Weak Password] module, as shown in the figure below.



The Weak Password Rules page contains three rules: "Custom Login Entrance", "Custom Weak Password", and "Custom Web Login Result". When all rules are met, a weakness incident is generated.

Custom login entrance

On the [Weak Password Rules\Custom Login Entrance] page, click <New>, as shown in the figure below.



Fields:

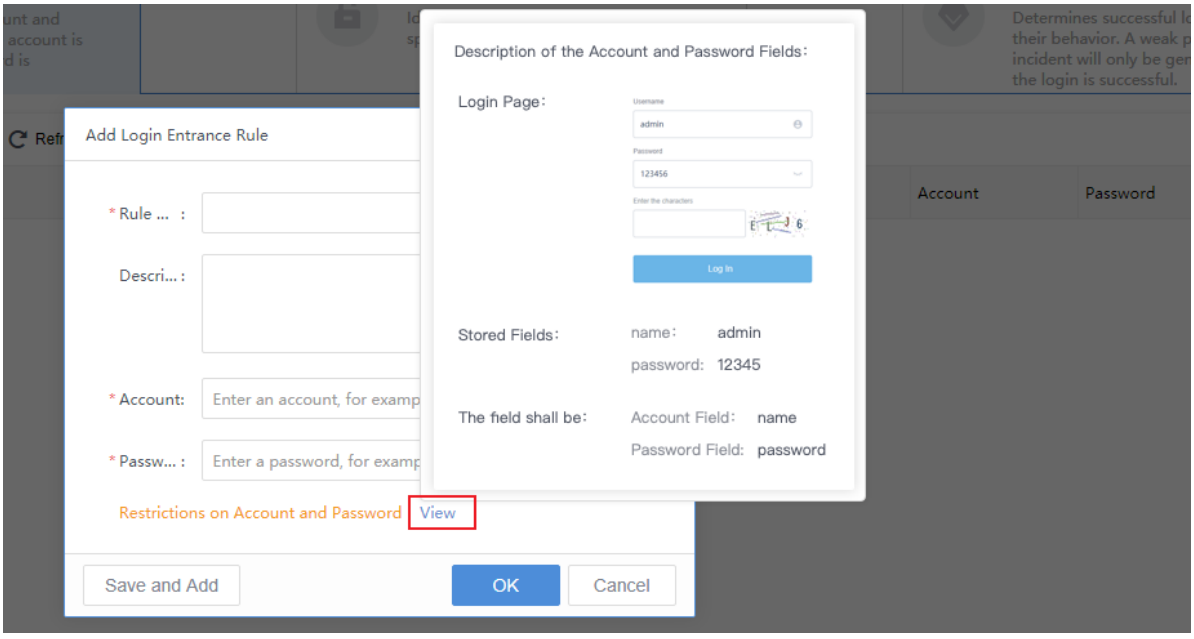
Rule Name: The custom rule name. Digits and letters are supported.

Description: The custom rule description.

Account: Account in the request header or body. You can confirm it with the O&M personnel of the web application.

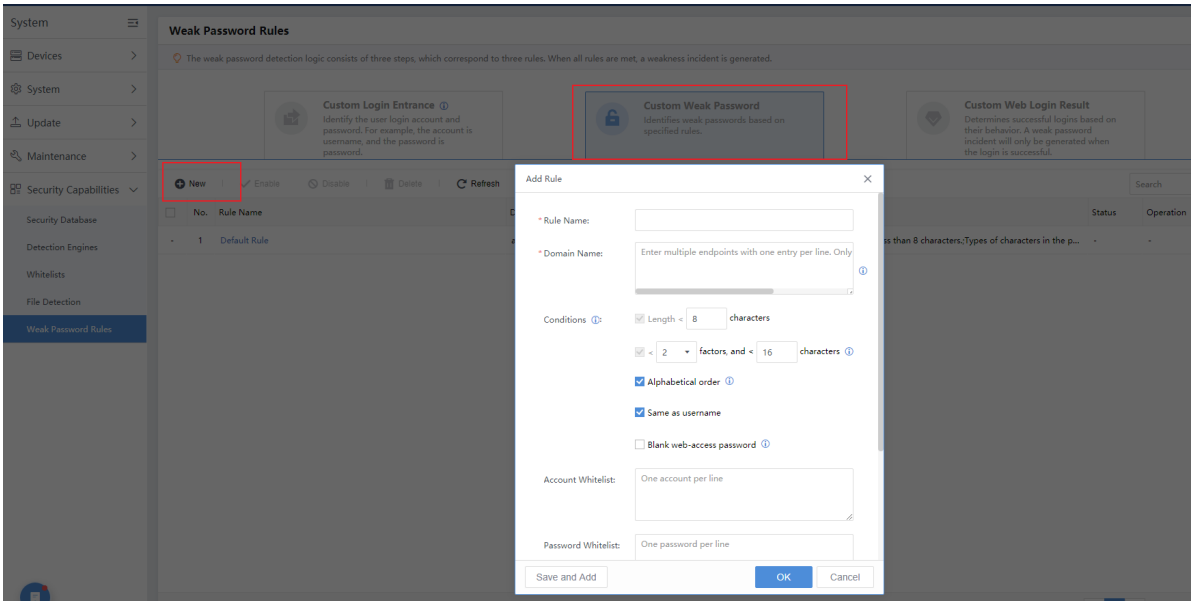
Password: Password in the request header or body. You can confirm it with the O&M personnel of the web application.

You can click <View> to view the sample of account and password fields.

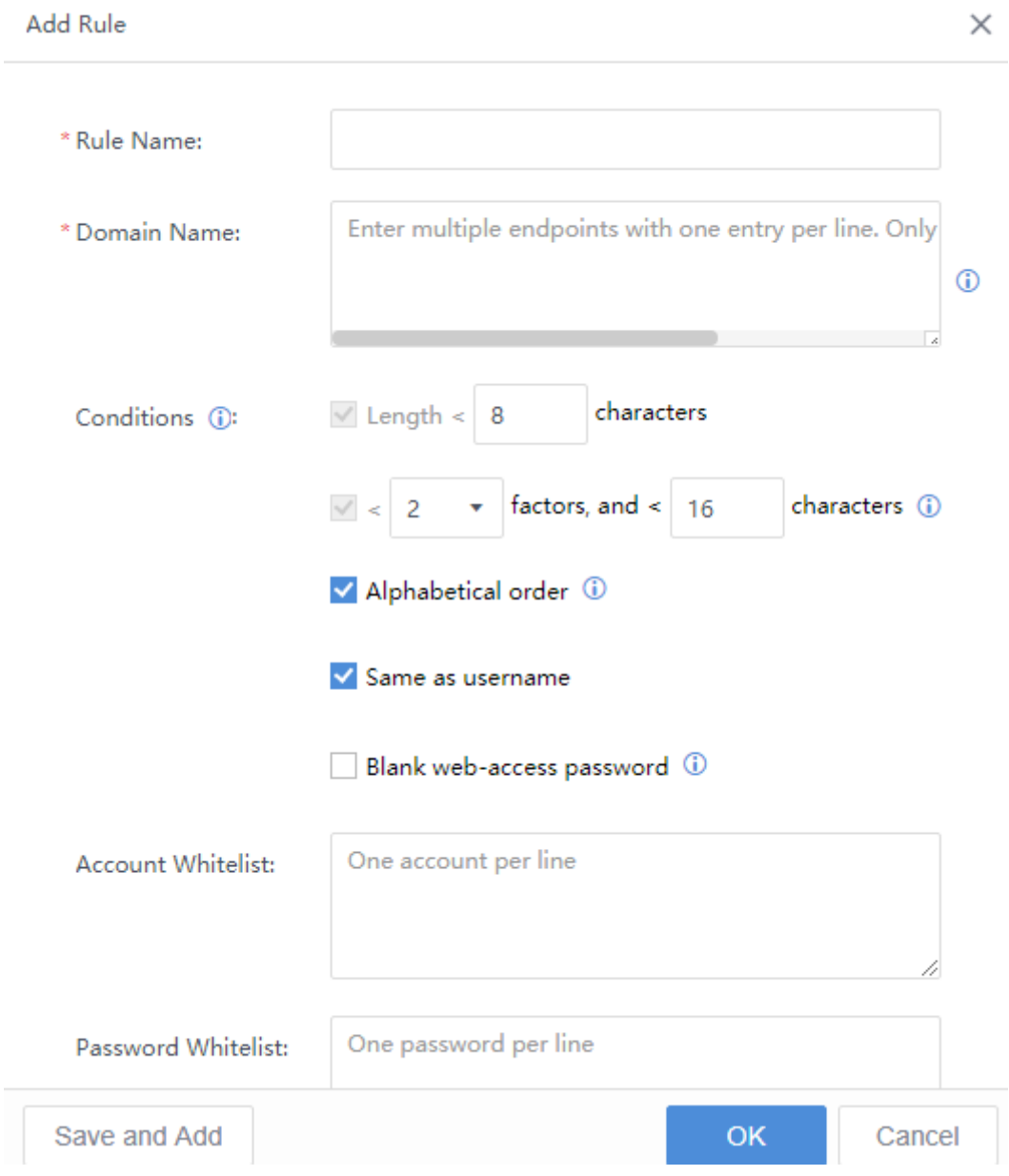


Custom weak password

A default rule is provided. You can also create custom rules on this page. The default rule is used to identify and detect weak passwords of all applications (web and non-web). It cannot be edited, changed, or deleted by default, as shown in the figure below.



You can click <New> to pop up the [Add Rule] dialog box. The custom rule is applicable to web applications. Therefore, you need to specify the domain name, conditions, account whitelist, password whitelist, and weak passwords, as shown in the figure below.



Fields:

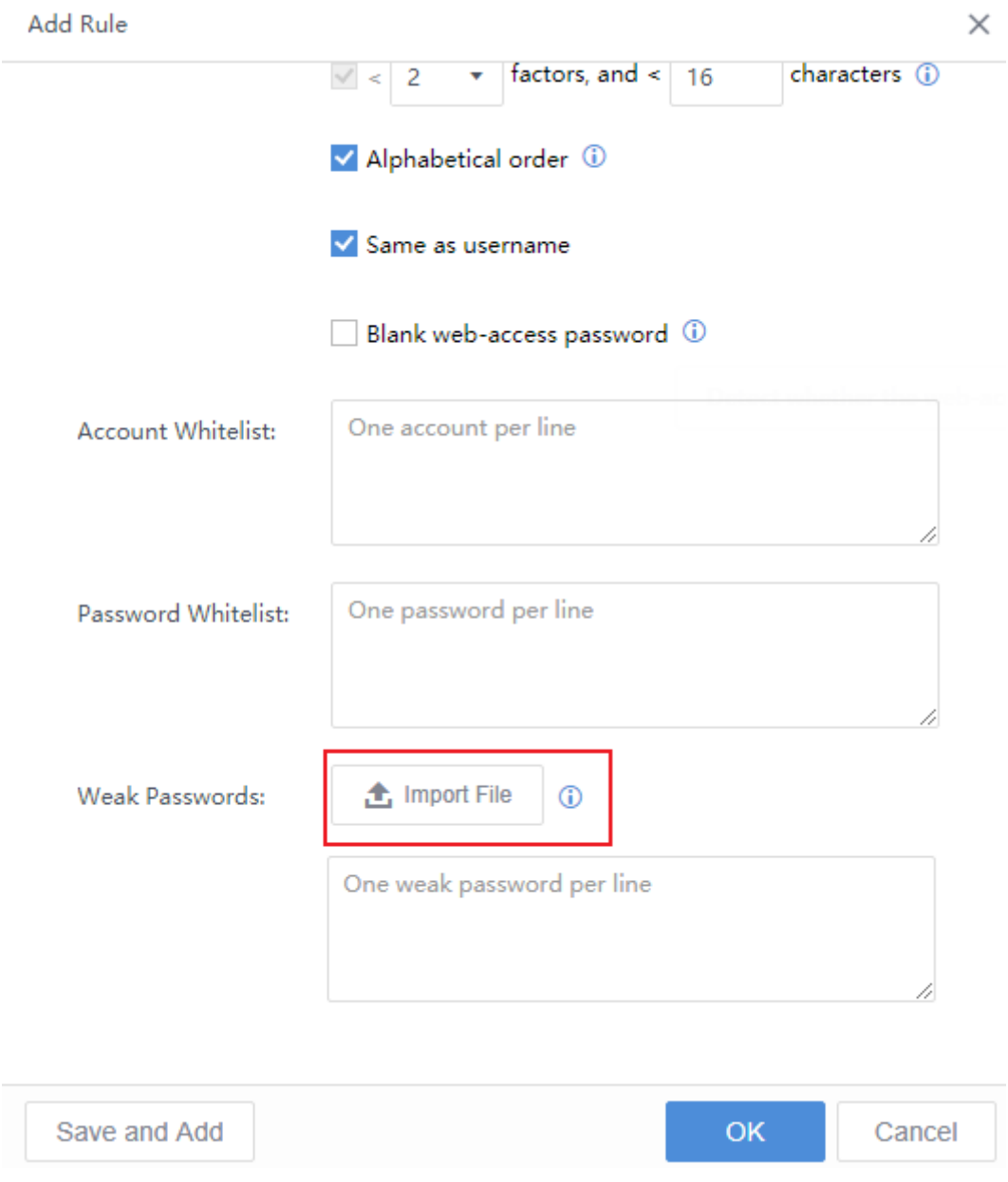
Rule Name: The custom rule name for the weak password rule.

Domain Name: The applicable domain name or URL. Example: http://xxx:80/a/b/c?1=1{.url target="_blank"}. In this URL, http:// indicates the request protocol of the traffic. xxx indicates the endpoint address, which can be the domain name, endpoint name, or endpoint IP address. 80 next to the colon (:) indicates the port number. /a/b/c indicates the resource path. 1=1 next to the question mark (?) indicates the domain name content.
You can refer to the value of Host in the request traffic.

Conditions: The minimum password length, character factors and number, and options of alphabetical order, same as username, and blank web-access password need to be specified.

Account Whitelist: If the weak passwords obtained through the product-side analysis do not meet the customer's service scenario or actual situation requirements, you can customize the whitelist to prevent vulnerability events.

Weak Passwords: If only several weak passwords exist, you can enter them in the text box directly. If there are too many weak passwords, you can import them using a TXT file by clicking <Import File>, as shown in the figure below.

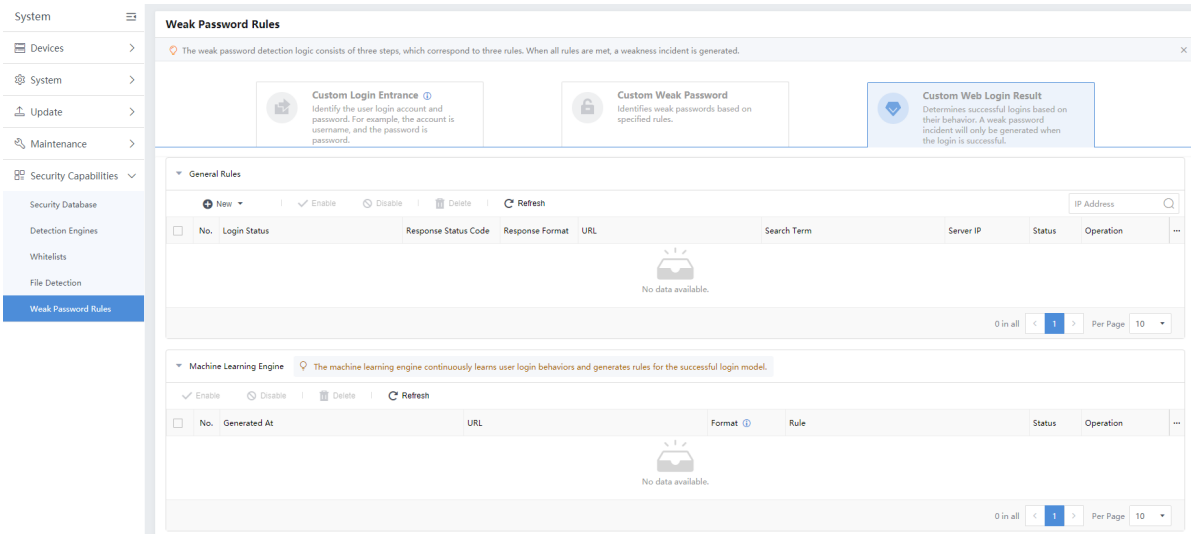


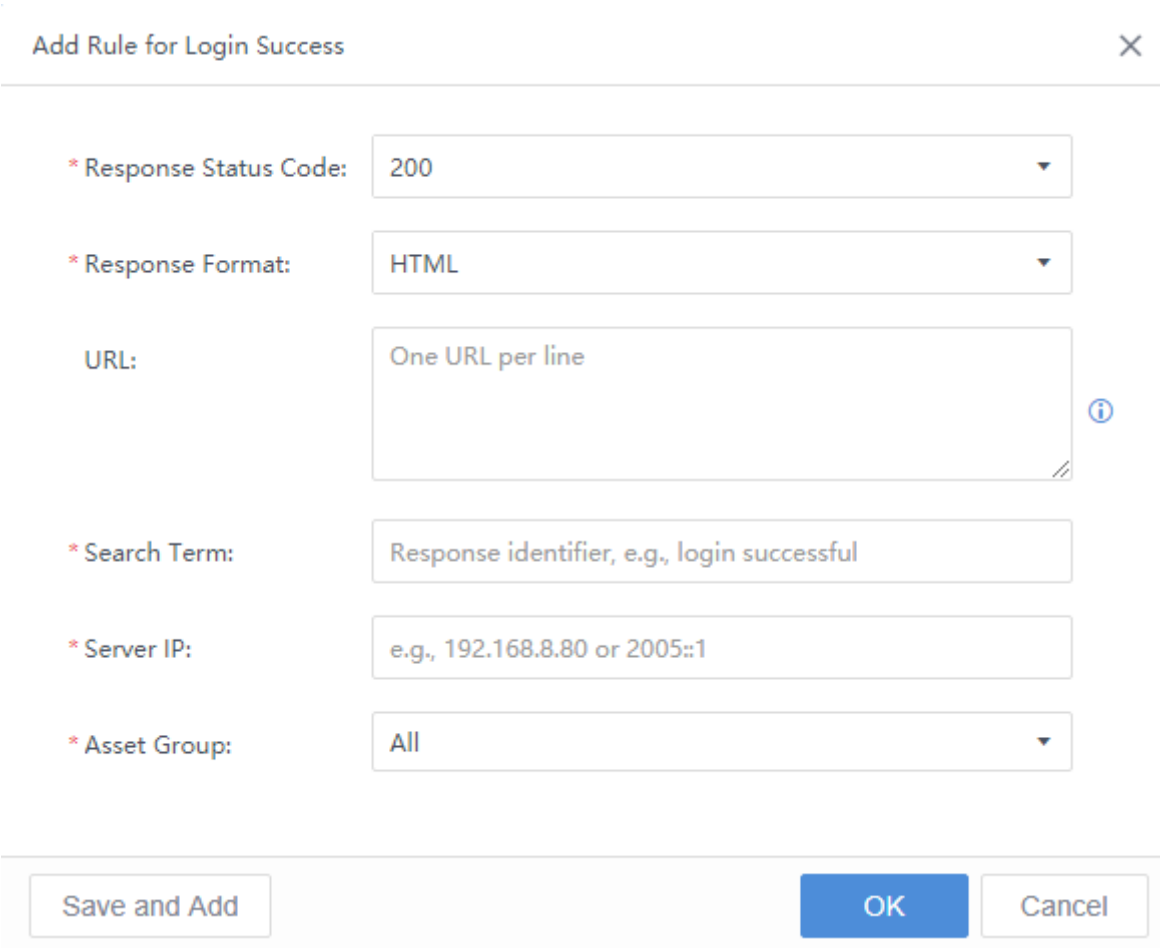
Note

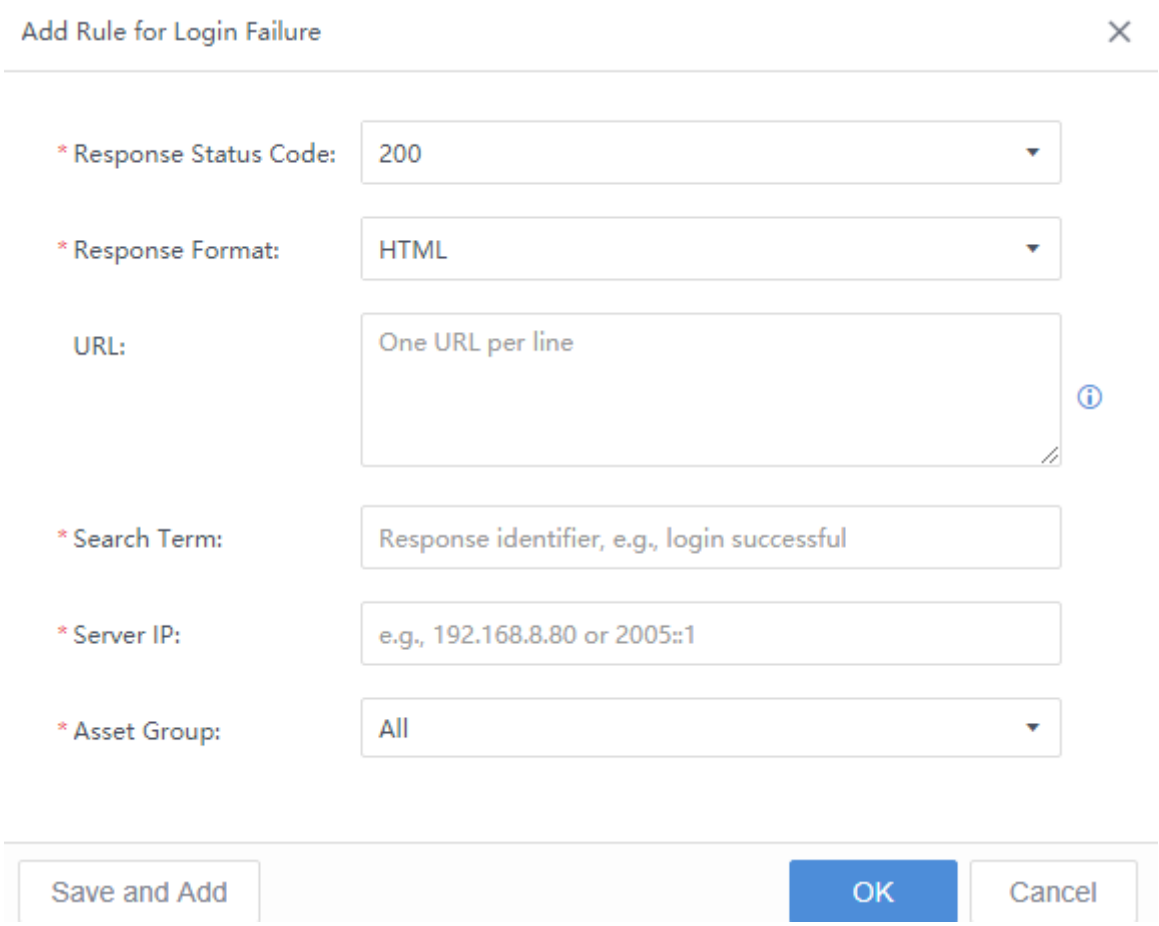
1. A maximum of 50 web domain names or URLs related to the custom weak password rule are allowed.
2. Priority: The custom weak password rule has a higher priority than the default rule. Weak passwords are identified based on the custom rule first and then the default rule.

Custom web login result

Successful login and failed login are two results of web login. The web login rules are used on Nova Command to correct the identification result of the login result if the login result is different from the customer's actual situation. The rules use the status codes of success and redirection in the HTTP protocol to match the content of the successful login and server IP address, as shown in the figure below.





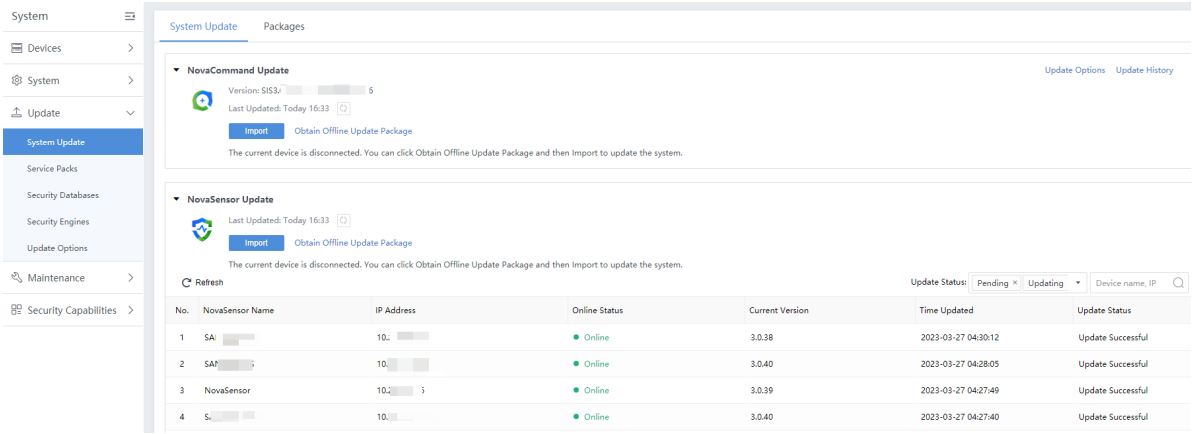


Product and Component Update

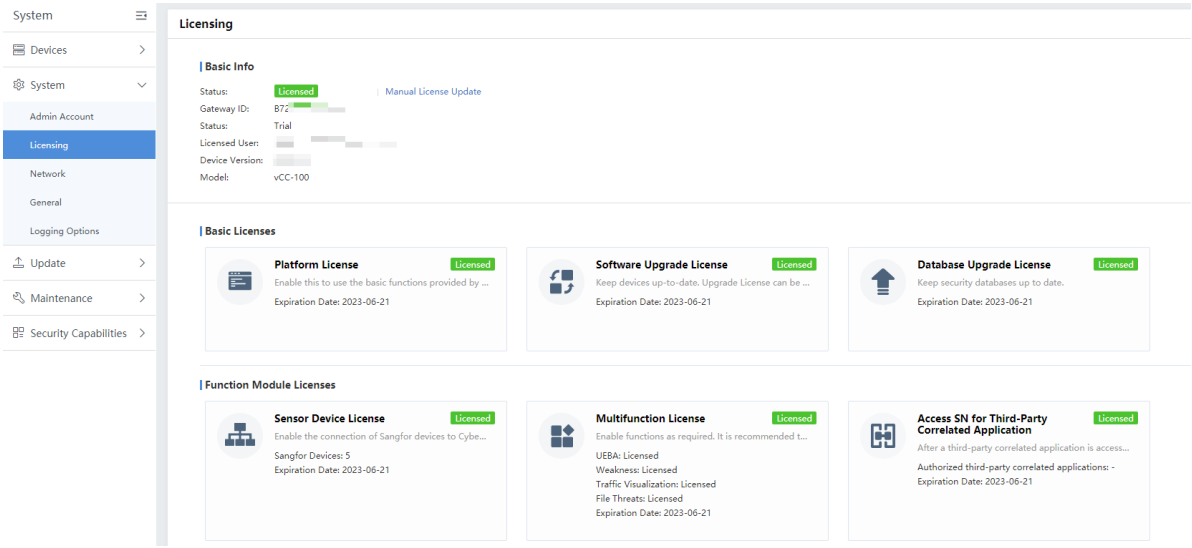
Nova Command Update

Steps of updating Nova Command

1. On the [System/Update/System Update] page, check the current version and status of Nova Command, as shown in the figure below.

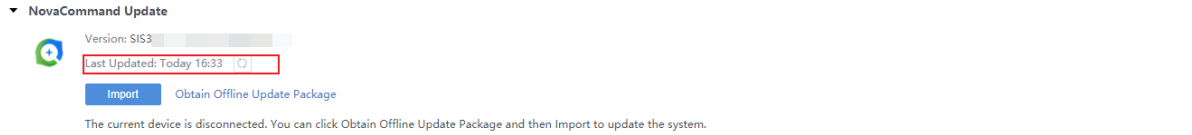


2. On the [System/Licensing] page, check whether the license is valid. If yes, proceed to the next step. Otherwise, please contact Nova Command engineers.



Auto Update

When Auto Update is enabled, Nova Command will be automatically updated without manual intervention when idle resources are available (for example, in the early morning). Nova Command checks for updates from Neural-X every 30 minutes. If there is a new update package, Nova Command will download it to the local path from allowed Neural-X domains, provided that Auto Update is enabled. The value of the Last Updated field indicates the time when Nova Command checks for updates from Neural-X. See the following figure.



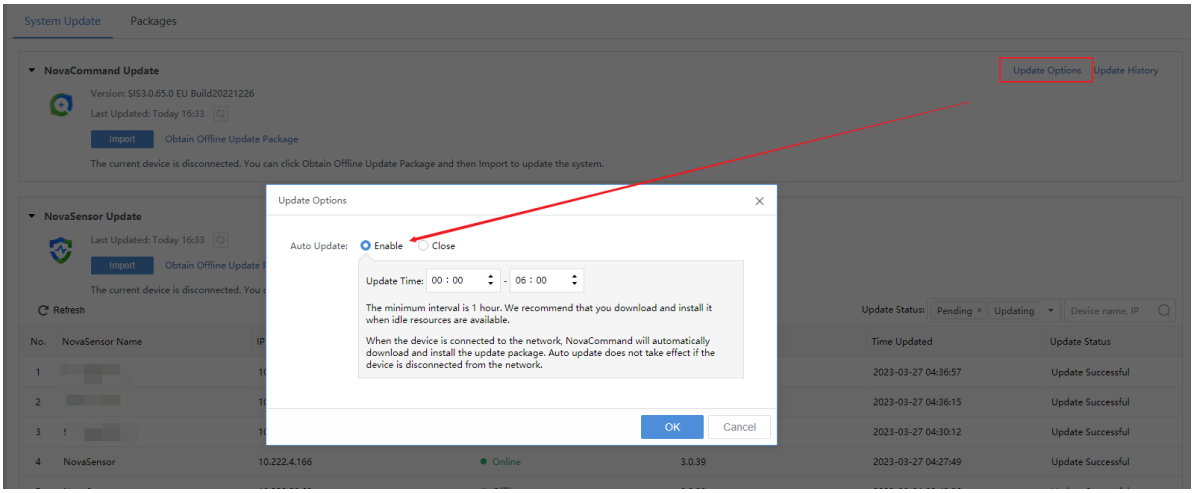
Domains and ports allowed for Nova Command to check for update from Neural-X are listed in the following table.

Table 1 Ports Allowed for Nova Command Auto Update

Component Updated Online	Allowed Domain/IP Address	Port
Nova Command version	sp.forenova.com sp1.forenova.com sp2.forenova.com sp3.forenova.com auth.forenova.com	443

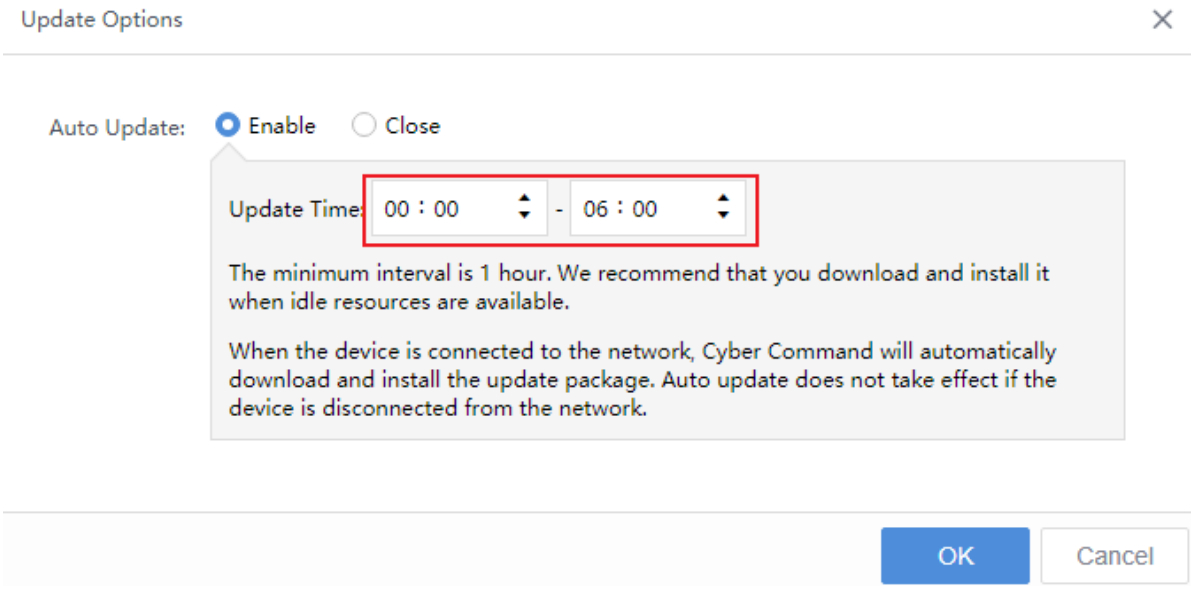
Auto update switch

Auto Update is enabled for Nova Command by default. On the [System/Update/System Update] page, you can click <Update Options> to manually enable or disable Auto Update, as shown in the following figure.



Update time

You can set the time for auto update manually according to the actual situation. When the device is connected to the network, Nova Command will automatically download and install the update package, as shown in the following figure.



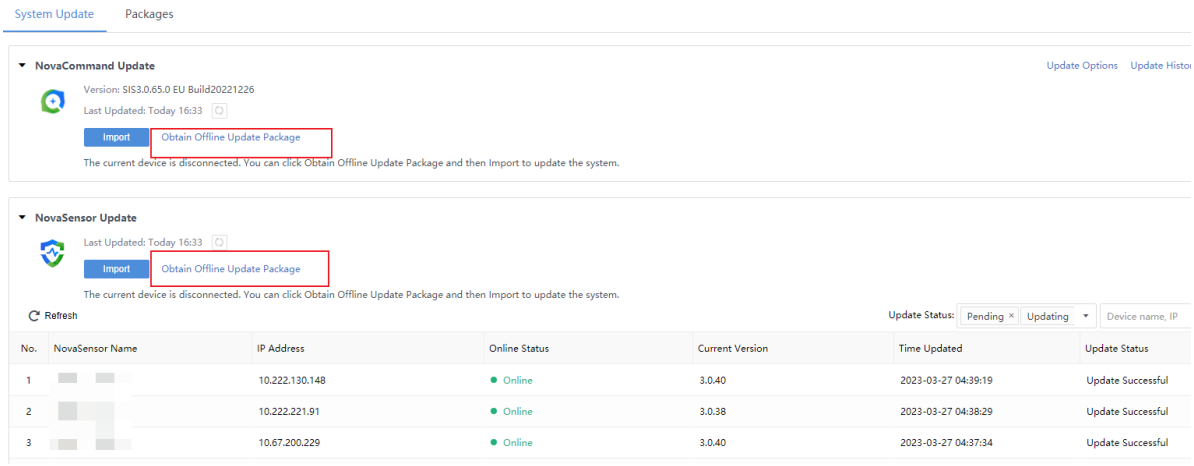
If you do not want to use Auto Update, select <Close>.

Manual Update

In manual update mode, you need to obtain the update package from Sangfor Community, as shown in the following figure.

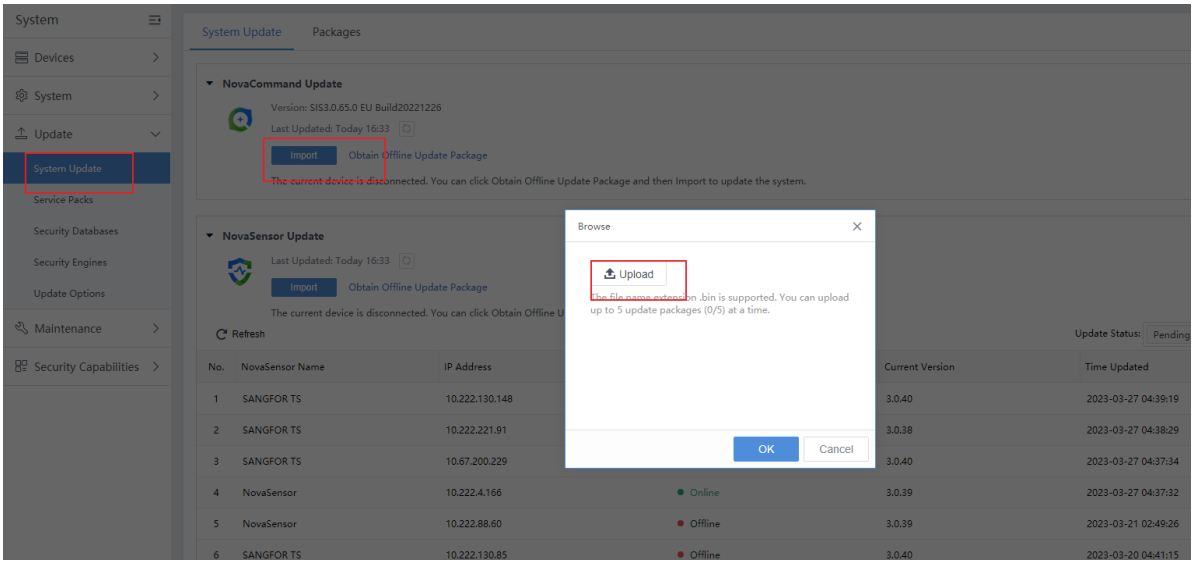
URL: https://download.forenova.com/

Besides, you can click Obtain Offline Update Package and scan the QR code to obtain the offline update package from Neural-X.

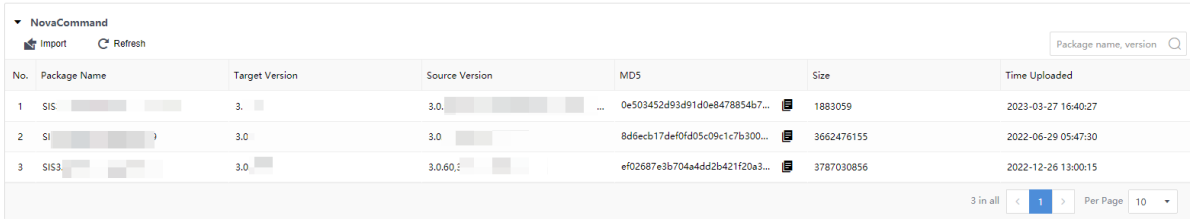


Update package import - method 1

In addition to auto update, you can also manually update Nova Command by importing the update packages. On the [System/Update/System Update] page, you can click <Import> to upload the .bin packages. You can upload up to five update packages at a time, as shown in the following figure.

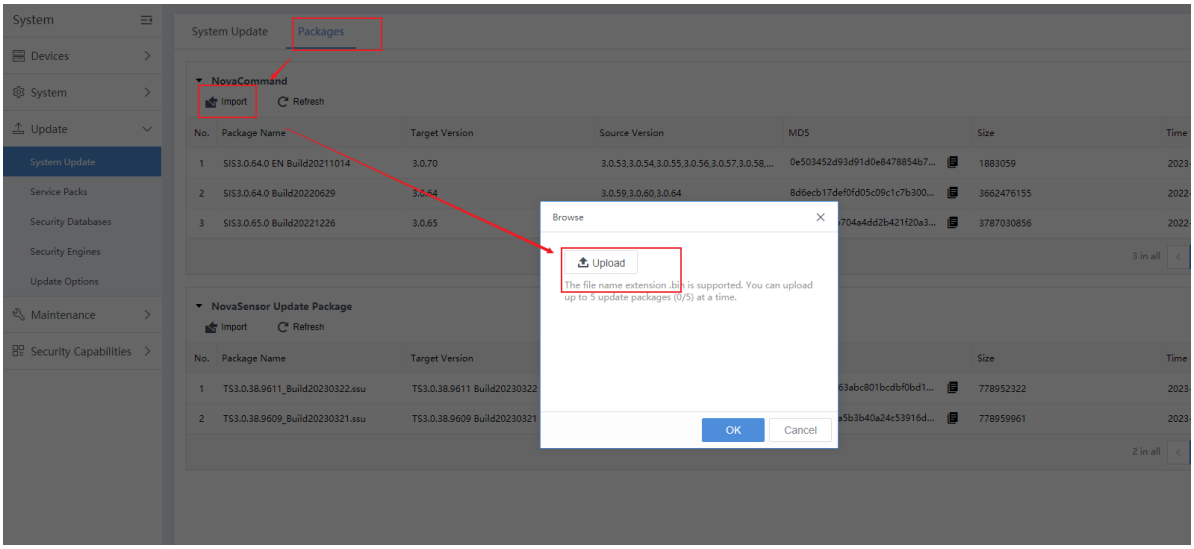


The imported update packages will be displayed on the [System/Update/System Update/Packages] page. The information, such as package name, target version, source version, MD5, size, and upload time, is displayed, as shown in the following figure.



Update package import - method 2

On the [System/Update/System Update/Packages] page, you can also click <Import> below <Nova Command> to import update packages, as shown in the following figure.



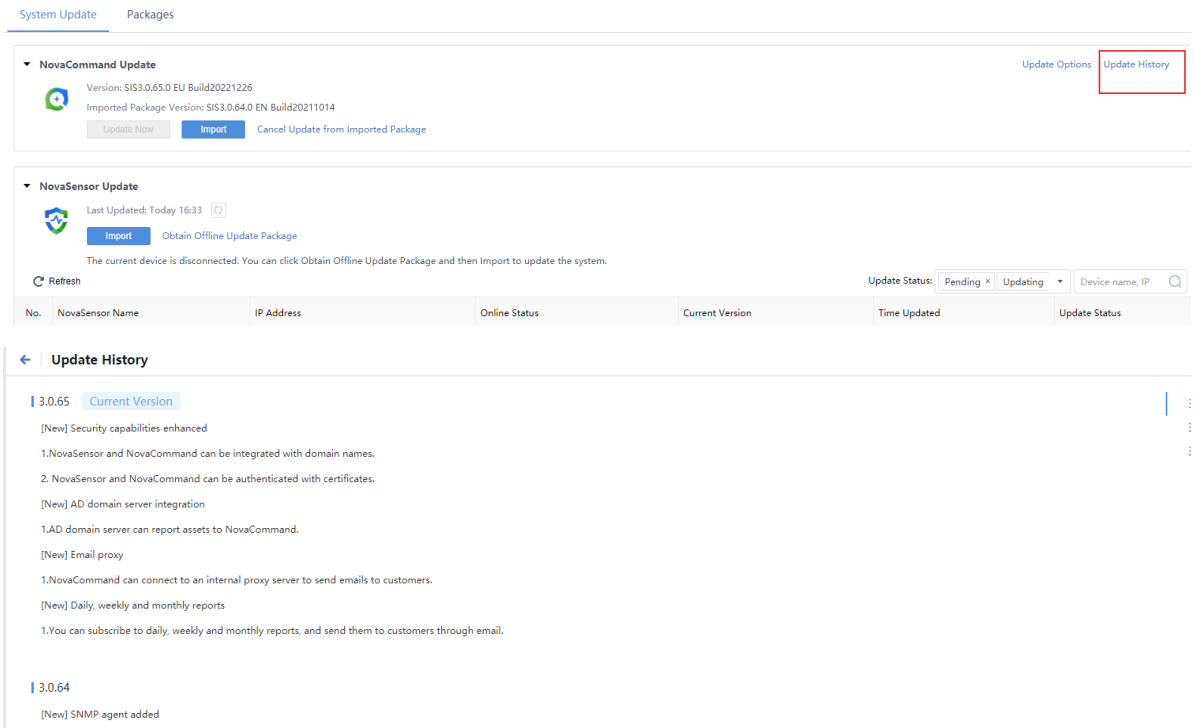
You can click <Update Now> and wait for update to complete.

Obtaining Offline Update Package

Go to the Nova Command module in Sangfor Community (URL: https://download.forenova.com/) to download the update packages and verify the MD5 values.

Viewing Update History

On the [System/Update/System Update/System Update] page, you can click <Update History> to view the update history and features of each version, as shown in the following figures.

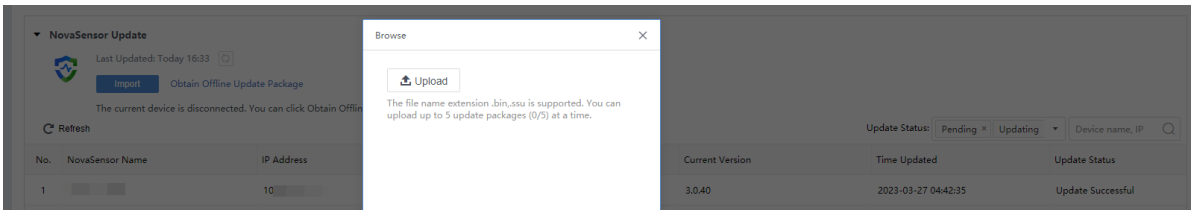


Nova Sensor Update

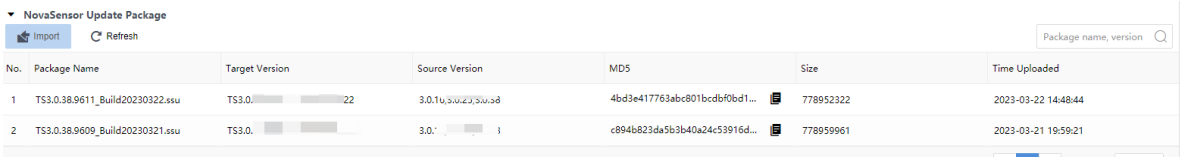
Nova Sensor is an important component of Nova Command. It is advised to automatically obtain update packages by connecting Nova Command to the network. In this way, Nova Sensor can be updated by obtaining update packages from Nova Command. Ports to be allowed are listed in the following table.

Component Updated Online	Allowed Domain/IP Address	Port
Nova Command version	sp.forenova.com sp1.forenova.com sp2.forenova.com sp3.forenova.com auth.forenova.com	443
NS version	Obtained from the IP address of the connected Nova Command	4488

You can also log in to Nova Command and click <Import> below Nova Sensor Update on the [System/Update/System Update/System Update] page to upload Nova Sensor update packages to Nova Command, as shown in the following figure.



After update packages are imported, the details will be displayed on the [System/Update/System Update/Packages] page, as shown in the following figure.



Nova Sensor will check for update from Nova Command every 10 minutes.

Service Packs

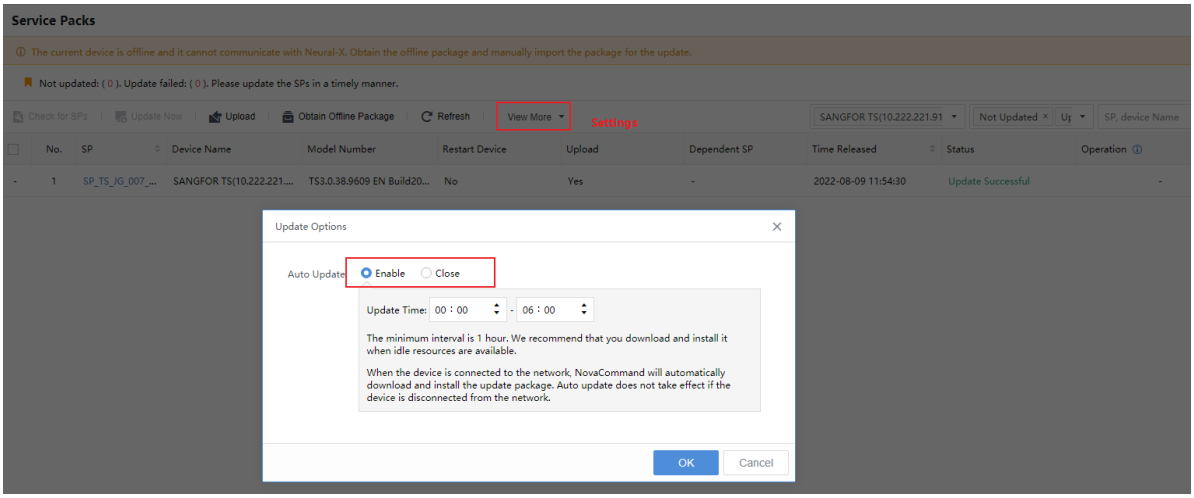
This feature is designed to notify online customers of available service packs. Therefore, customers can install these packs in time. The following part describes two scenarios about how customers can obtain the service packs.

1. When Nova Command is connected to the network

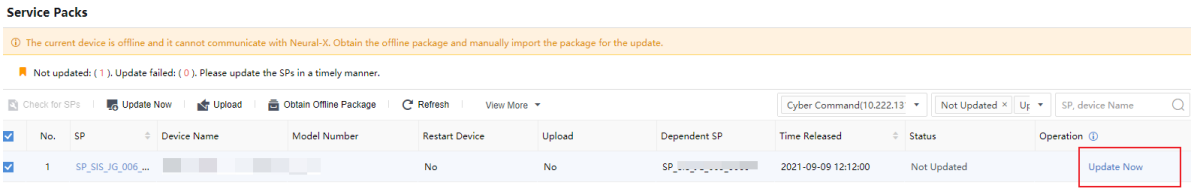
In this scenario, the allowed ports are listed in the following table.

Component Updated Online	Allowed Domain/IP Address	Port
Nova Command service packs	update1.forenova.net update2.forenova.net update3.forenova.net	80
NS service packs	Obtained from the IP address of the connected Nova Command	4488

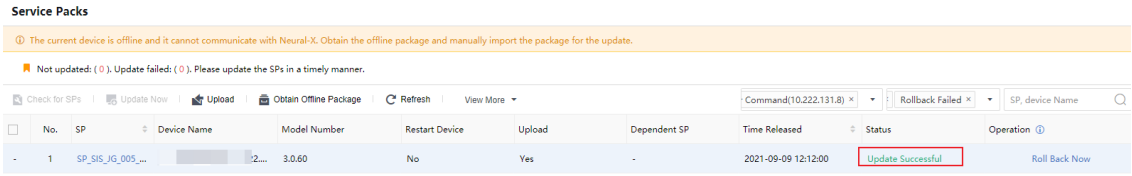
1. Auto update is enabled by default and will be performed from 0:00 to 6:00. You can change the update time.



2. You can click <Check for SPs> to view the service packs to be installed. Then, you can select the target service pack and click <Update Now> to install the service pack immediately.

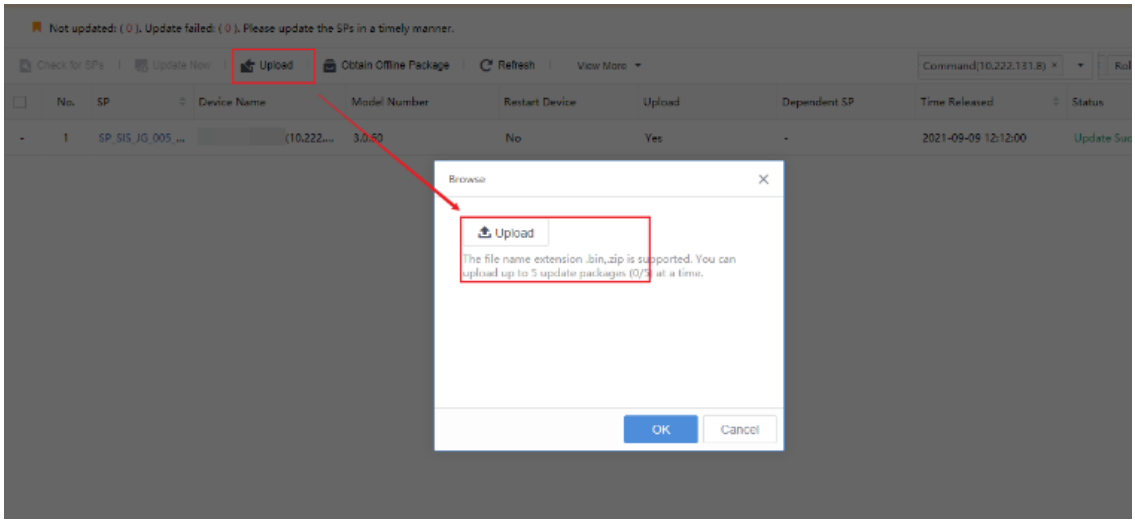


3. When update is done, you can view the status of the service pack on the page. You can filter service packs by status, such as Not Updated, Updating, Update Failed, and Update Successful. You can also search for service packs by service pack name, details, and device name.



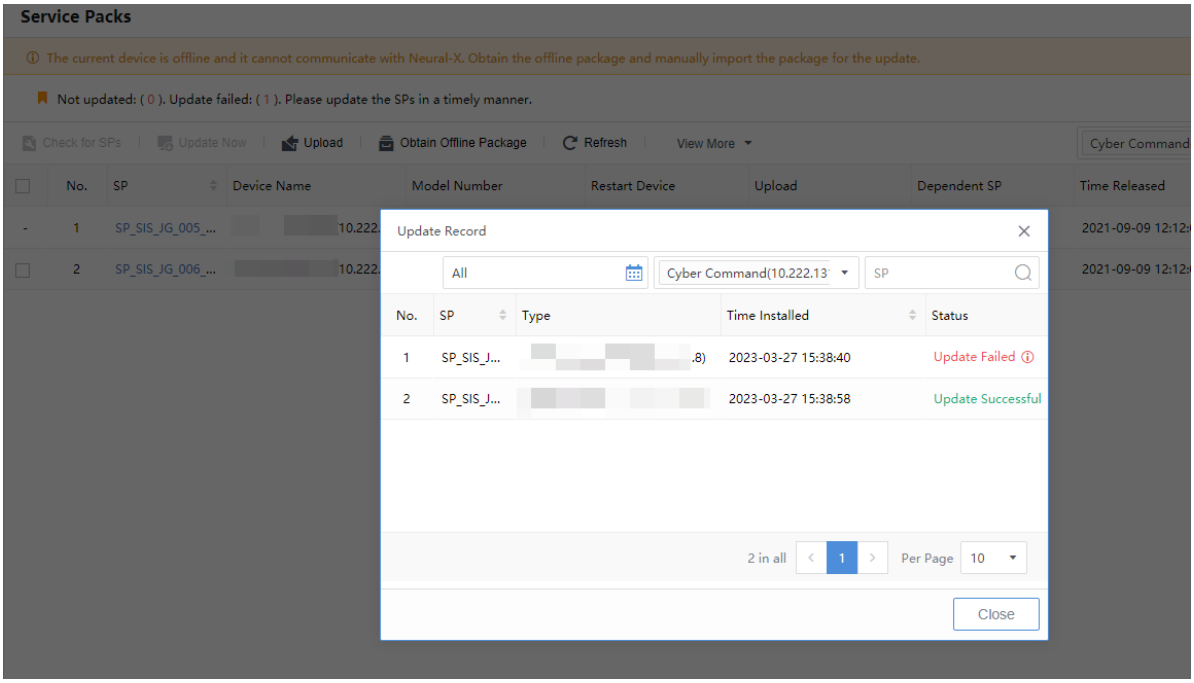
2. When the device is not connected to the network

1. you can also manually update the service packs by click <Upload>.



Update record

On the [System/Update/Service Packs] page, you can click [Update Record] to view more details, including the name and installation time of service packs. You can filter service packs by date and search for service packs by service pack name, details, and device name.



Component Update

Besides system update, security databases and security engines should also be updated in Nova Command.

Security Databases

Security databases of Nova Command include Security Signature Database, File Analytics Model Database, IOC Threat Intelligence, and Whitelist Database. They should be updated on a regular basis through update from cloud, manual update, or update by proxy browser. Auto update is recommended.

Auto Update

Enabling auto update

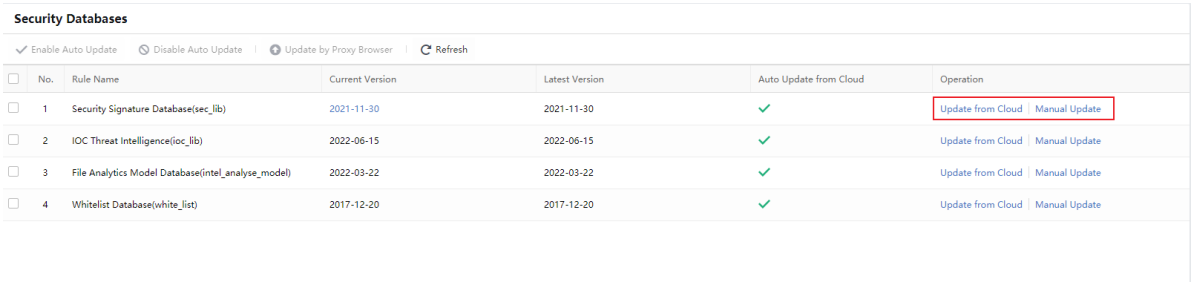
1. Update server settings

On the [System/Update/Security Databases] page, you can select a database and click the icon in the [Auto Update from Cloud] column to enable or disable auto update. You can also select multiple databases and click <Enable Auto Update> at the top to enable auto update. The following ports should be allowed in auto update mode.

Component Updated Online	Allowed Domain/IP Address	Port
Nova Command security databases	update1.forenova.net	80
	update2.forenova.net	
	update3.forenova.net	
	upd.forenova.com	
	download.snagofr.com	
NS security databases	Obtained from the IP address of the connected Nova Command	4488

Viewing security database update status

When auto update is enabled, Nova Command automatically checks for and completes updates from update servers at a regular interval. On the [System/Update/Security Databases] page, you can view the current and latest versions of a database. To update a single database, you can click <Update from Cloud> in the [Operation] column, as shown in the following figure.

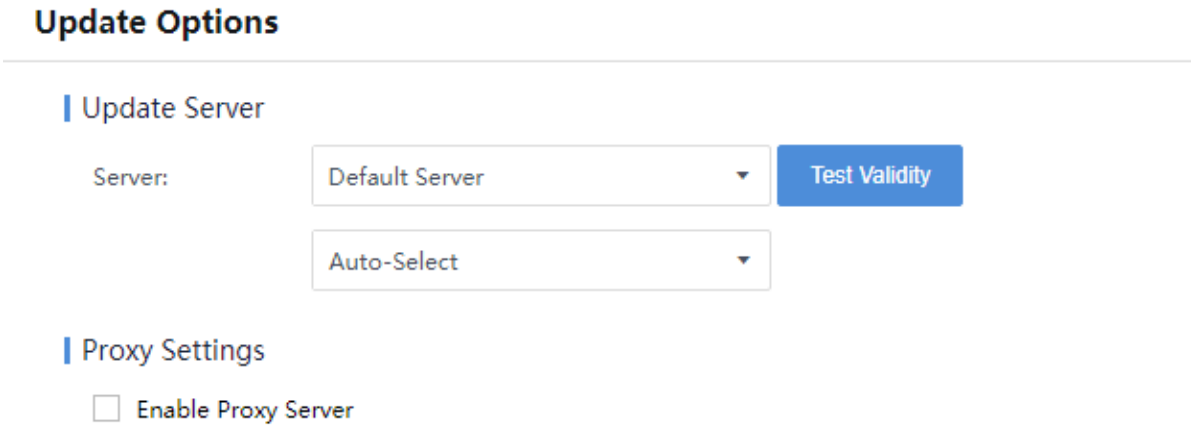


Note:

1. For Security Signature Database, you can click the current version to check the current and latest versions of sub-databases.
2. If the time difference between current version and system time exceeds one month, Nova Command may not be connected to an update server, resulting in update failure. You can go to the [System/Update/Update Options] page to test the connectivity of the update server in the Update Server section.

2. Update server settings

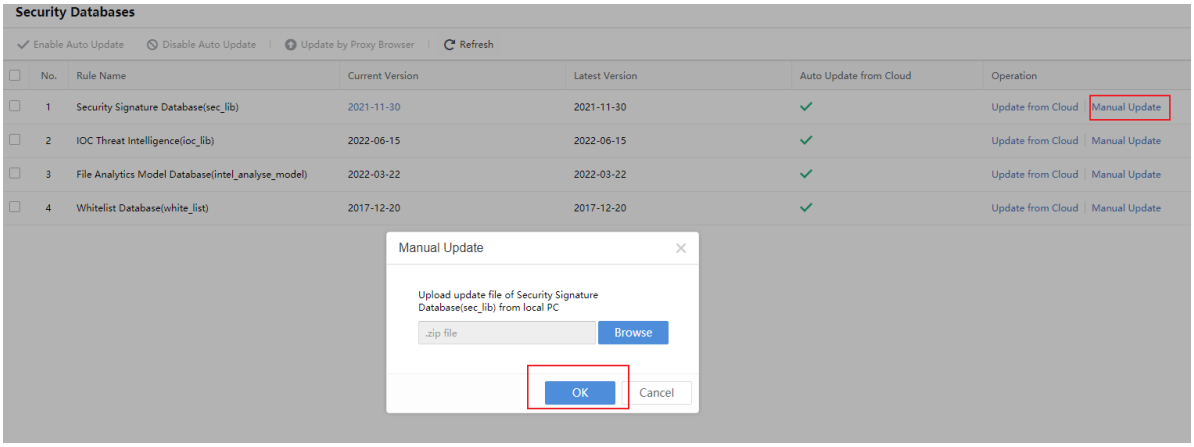
On the [System/Update/Update Options] page, you can click <Test Validity> to check the connectivity of the update server. To access the Internet via HTTP proxy, you can enable proxy server in [Proxy Settings], as shown in the following figure.



Manual Update

You can manually update security databases by following the steps below:

1. Go to Sangfor Community (URL: https://download.forenova.com/) to download the update packages of a security database and verify the MD5 values.
2. Log in to Nova Command. On the [System/Update/Security Databases] page, you can select a database and click <Manual Update> in the [Operation] column to upload the downloaded and verified update packages, as shown in the following figure.



Note:

1. Upload offline update packages in ZIP format for Security Signature Database from the local path.
2. For Security Signature Database, manually update IPS Vulnerability Database, WAF Database, Botnet Database, and Realtime Vulnerability Database only.

Security Engines

Security engines include multiple detection engines, such as
Asset Detection, Net Flow Analytics, and Intelligence Correlation. They should be updated in time through update from cloud, manual update, or update by browser proxy. Auto update is recommended.

Auto Update

Enabling auto update

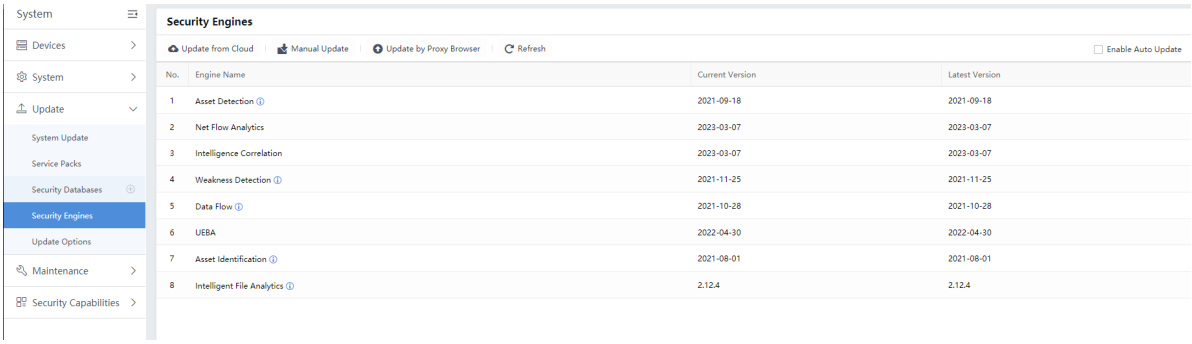
1. Update server settings

On the [System/Update/Security Engines] page, you can select <Enable Auto Update> to enable auto update. Ports that are allowed for auto update are listed in the following table.

Component Updated Online	Allowed Domain/IP Address	Port
Nova Command security engines	update1.forenova.net update2.forenova.net update3.forenova.net	80

Viewing engine update status

When auto update is enabled, Nova Command automatically checks for and completes updates from update servers at a regular interval. On the [System/Update/Security Engines] page, you can view the current and latest versions of an engine. To check for updates for an engine, you can click <Update from Cloud>, as shown in the following figure.

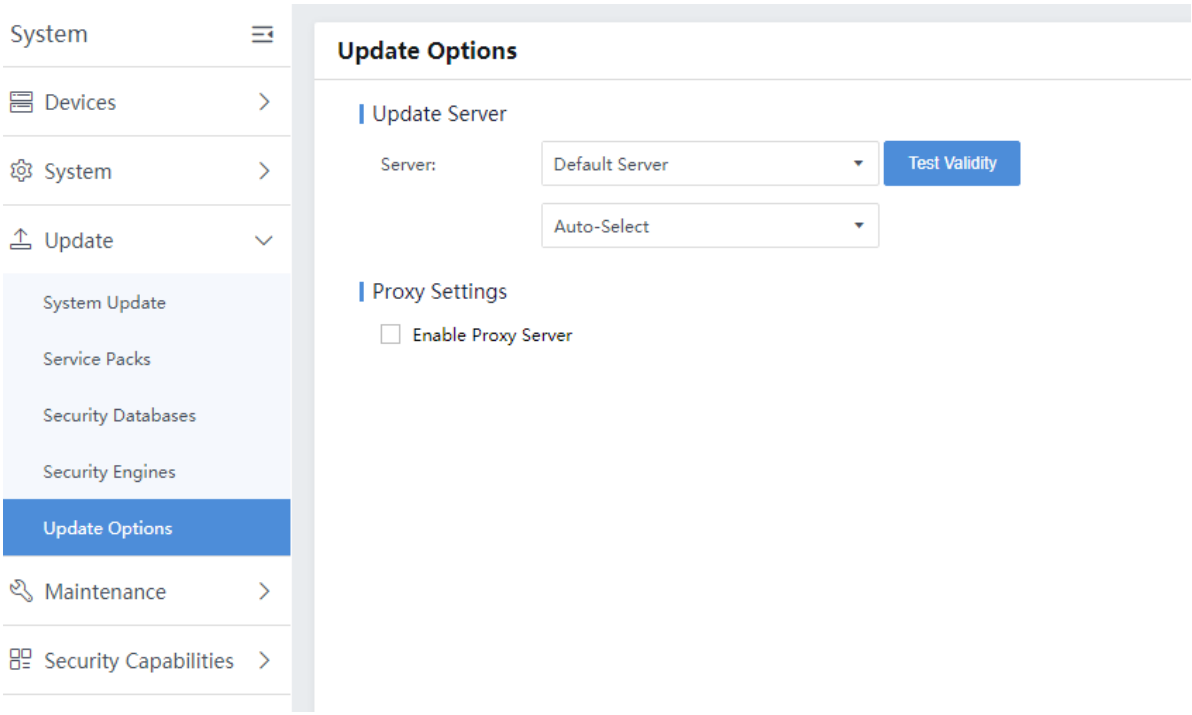


Note:

If the time difference between current version and system time exceeds one month, Nova Command may not be connected to an update server, resulting in update failure. You can go to the [System/Update/Update Options] page to test the connectivity of the update server in the Update Server section.

2. Update server settings

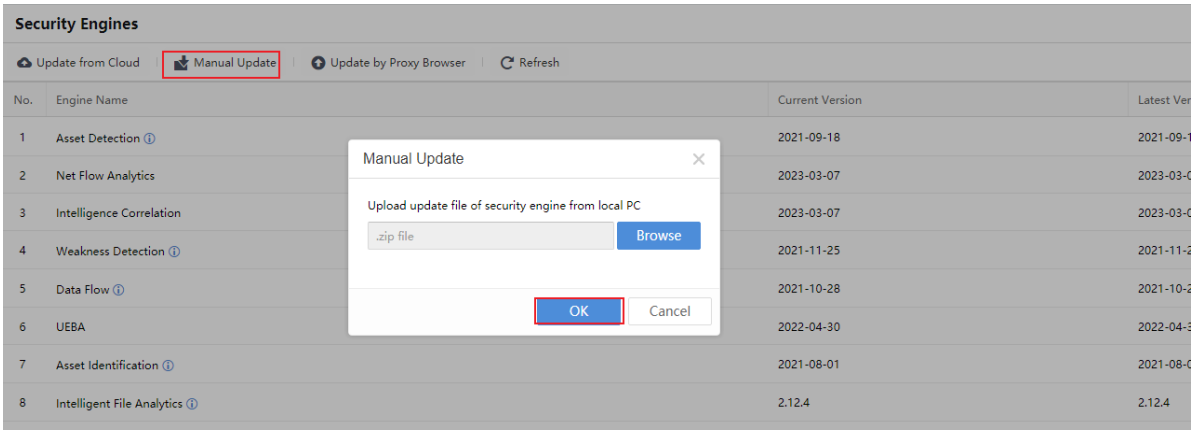
On the [System/Update/Update Options] page, you can click <Test Validity> in the Update Server section to check the connectivity of the update server. To access the Internet using HTTP proxy, you can enable proxy server below [Proxy Settings], as shown in the following figure.



Manual Update

You can manually update security engines by following the steps below:

1. Go to Sangfor Community (URL: https://download.forenova.com/) to download the update packages of a security engine and verify the MD5 values.
2. Log in to Nova Command. On the [System/Update/Security Engines] page, click <Manual Update> to upload the downloaded and verified update packages, as shown in the following figure.

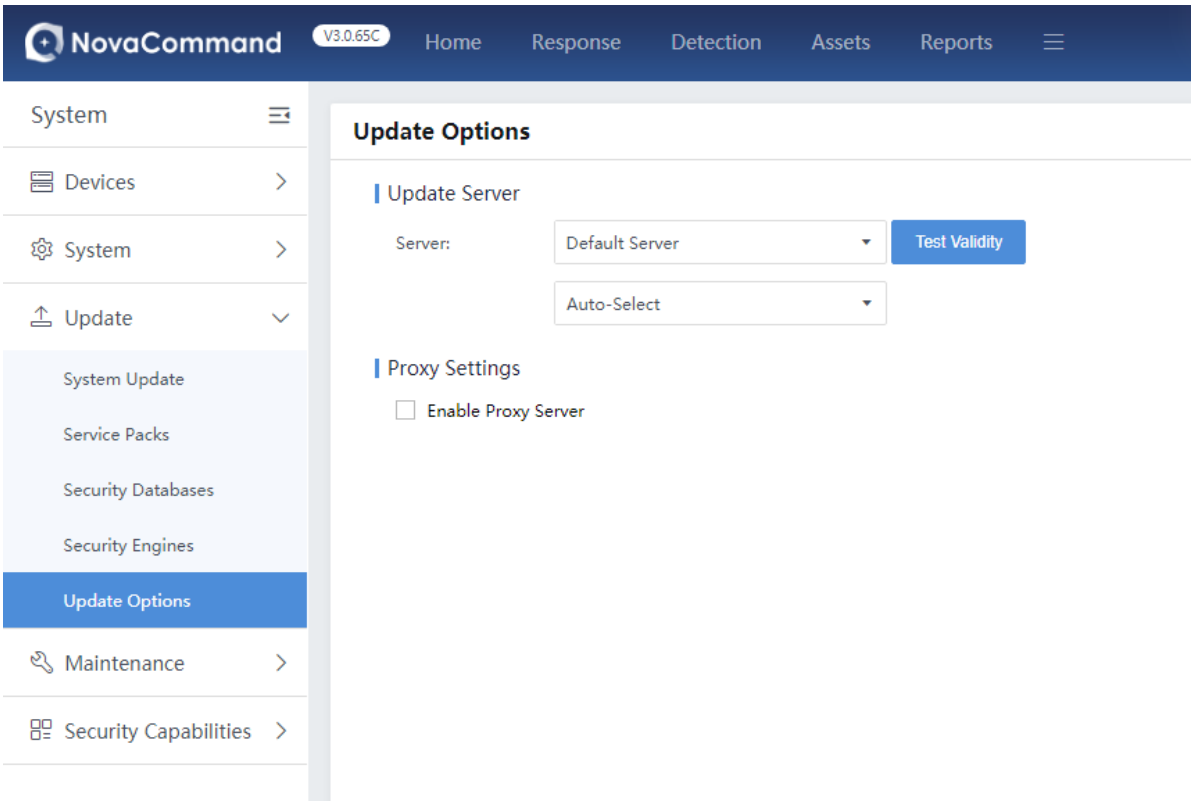


Note:

Upload offline update packages in ZIP format for security engines from the local path.

Update Options

This feature is used to connect Nova Command to update servers. You can click <Test Validity> to test the connectivity of an update server.



Update servers include:

Server1: update1.fornova.net

Server2: update2.fornova.net

Server3: update3.fornova.net

Proxy settings: Select Enable Proxy Server if HTTP proxy servers are used in the network.

Click <OK> to save the settings.

Sangfor Device Connection

NovaGuard

About NovaGuard

Sangfor NovaGuard provides endpoints with granular isolation policies and capabilities of accurate scan, continuous detection, and rapid response throughout the endpoint asset lifecycle. In face of advanced threats, NovaGuard uses coordinated response across cloud-network-endpoint, sharing of threat intelligence, and multi-level response mechanism to help users fix security threats and build a lightweight, intelligent, and responsive next-generation endpoint security system.

1. Notes

To use the correlation feature, add NovaGuard devices on Nova Command.

2. Connection Description

The following table describes connections between NovaGuard and Nova Command of different versions.

NovaGuard Version	Nova Command Version	Feature	Implementation	Port
NovaGuard 2.0	Nova Command 2.5.8 or later	**Log synchronization:** Synchronization of WebShell logs, brute-force attack logs, botnet logs, and micro-segmentation logs	HTTPS protocol	NovaGuard accesses port 7443 of Nova Command
NovaGuard 3.0.2	Nova Command 3.0.2 or later	**Log synchronization:** Antivirus log synchronization	HTTPS protocol	NovaGuard accesses port 7443 of Nova Command
Nova Command 3.0.2 or later	**Correlation:** Endpoint isolation; outbound access blocking; inbound access blocking	HTTPS protocol	Nova Command accesses port 443 of NovaGuard	
NovaGuard 3.2.9	Nova Command 3.0.18 or later	**Correlation:** Endpoint information synchronization; threat scan; file quarantine/ignoring/trusting; single-arm deployment	HTTPS protocol	Nova Command accesses port 443 of NovaGuard
NovaGuard 3.2.9	Nova Command 3.0.21 or later	**Correlation:** After a security incident is fixed on NovaGuard, the status of the security incident changes to "Fixed" on Nova Command.	HTTPS protocol	Nova Command accesses port 443 of NovaGuard
NovaGuard 3.2.13	Nova Command 3.0.23 or later	**Correlation:** The issue of network address translation between NovaGuard and Nova Command is solved.	HTTPS protocol	Nova Command accesses port 443 of NovaGuard
NovaGuard 3.2.15	Nova Command 3.0.39 or later	**Correlation:** Botnet forensics	HTTPS protocol	Nova Command accesses port 443 of NovaGuard
NovaGuard 3.2.33 or later	Nova Command 3.0.53 or later	**Asset information synchronization (new interface)**; **log synchronization (new interface)**	HTTPS protocol	NovaGuard accesses port 7443 of Nova Command
NovaGuard 3.5.6	Nova Command 3.0.57	**Correlation:** Correlated micro-segmentation (port lockout and endpoint isolation)	HTTPS protocol	Nova Command accesses port 443 of NovaGuard

NovaGuard Version	Nova Command Version	Feature	Implementation	Port
NovaGuard 3.5.16	Nova Command 3.0.61	**Optimized asset information synchronization:** Policy recommendation for NovaGuard assets in different scan stages; synchronization of the fixing status of endpoints on NovaGuard	HTTPS protocol	NovaGuard accesses port 7443 of Nova Command

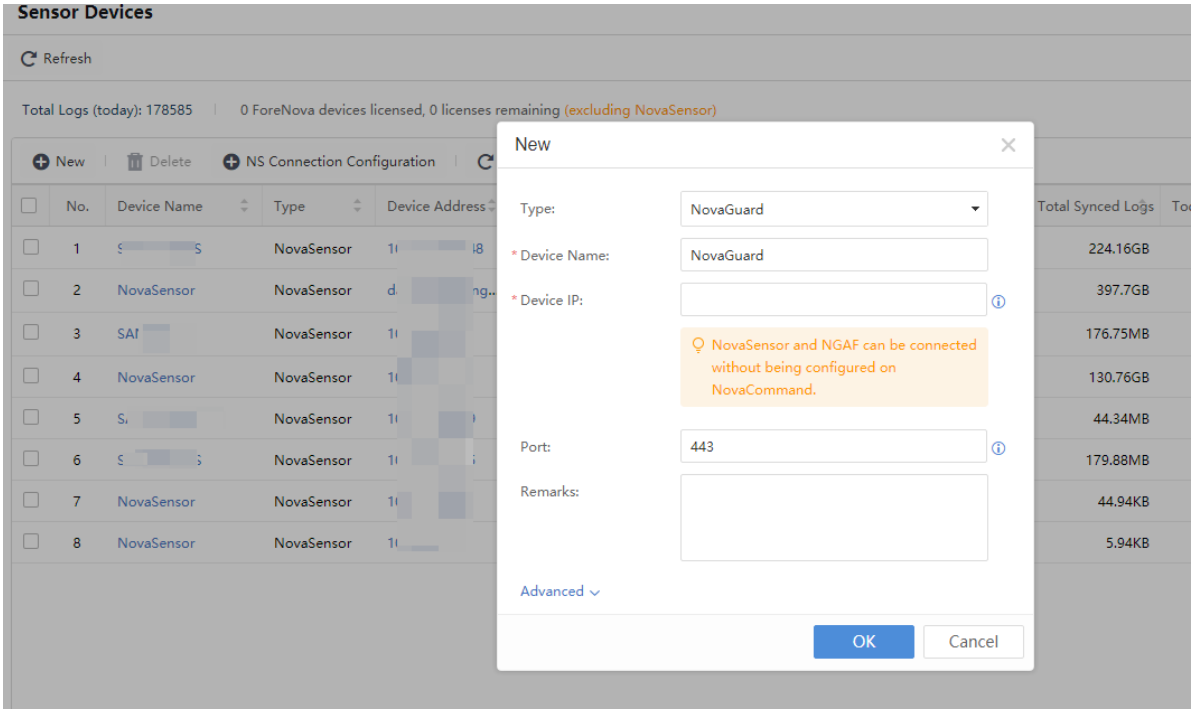
NovaGuard Connection

You can configure NovaGuard connection on Nova Command or NovaGuard following the steps below:

Steps of configuring connection on Nova Command

Step 1. Log in to Nova Command.

Step 2.
Click <New> on the [System/Devices/Sensor Devices] page to import NovaGuard, as shown in the following figure.



Fields:

<Device IP>: If the IP address of the connected device is translated, enter the translated IP address.

<Device Name>: You can specify the device name to distinguish devices of the same type.

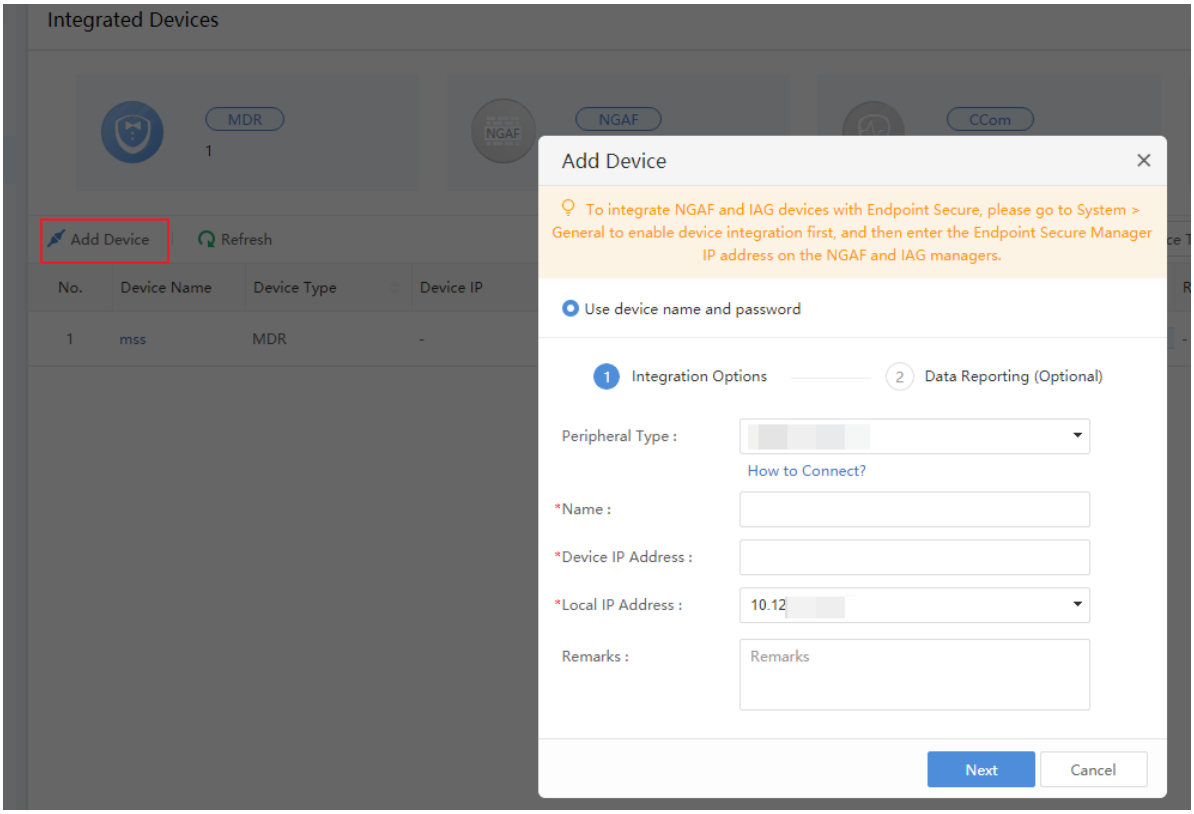
<Port>: The default port is 443. If port mapping is conducted between Nova Command and NovaGuard, enter the mapped port.

<Authentication Required>: Optional. If the username and password are configured, they will be used for NovaGuard authentication when NovaGuard is connected to Nova Command. You can click <Test> to test the username and password. If not configured, they will be automatically generated and configured in the peer device.

Steps of configuring connection on NovaGuard

Step 1. Log in to the MGR platform.

Step 2.
On the [System/Integrated Devices] page, click <Add Device> to connect NovaGuard to Nova Command, as shown in the following figure.



Fields:

<Report Detection Logs>: Select <Enable> to guarantee the integrity of detection logs.