

NSFOCUS ISOP

User Guide



Version: V3.0R011B07 (2023-10-13)

Confidentiality: RESTRICTED

■ Copyright © 2023 NSFOCUS Technologies, Inc. All rights reserved.

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided AS-IS without guarantees of any kind, express or implied. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
 - Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
 - Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).
-

Contents

Preface	1
Organization.....	1
Technical Support.....	2
Documentation Feedback.....	3
1 Product Overview	4
1.1 Introduction	4
1.2 Product Entry	5
1.3 Web-based Management	5
1.3.1 Web Login.....	5
1.3.2 Page Layout of the Web-based Manager.....	5
2 Importing a License	7
3 Situational Awareness	9
3.1 Threat Insight	9
3.2 Environment Insight.....	11
3.3 General Insight	12
3.4 Vulnerability Insight.....	14
3.5 Log Insight	16
3.6 5GC Threat Insight.....	17
3.7 XDR Insight	18
4 Monitoring.....	20
5 Analytics	25
5.1 XDR	25
5.1.1 Viewing Threat Details	26
5.1.2 Switching Response Status	29
5.2 Threat Analysis.....	29
5.2.1 Assessing an Event.....	29
5.3 Intelligence.....	35
5.3.1 Headline Event Alert.....	35
5.3.2 Vulnerability Alert.....	36
5.4 Attribution	41
5.4.1 Querying Logs	41
5.4.2 Traffic Forensics	45

5.4.3 Threat Hunting	45
5.5 Report	47
5.5.1 O&M Report	47
5.5.2 Vulnerability Report	49
5.5.3 5GC Report	50
5.6 Managing Exported Tasks	51
6 Handling	53
6.1 Manual Handling	53
6.1.1 One-Click Responding	53
6.1.2 Ticket Management	57
6.1.3 Alert Notification	59
6.2 Auto Handling	63
6.2.1 Visualized Orchestration	63
6.2.2 Case Management	66
7 Asset	73
7.1 Asset Discovery Task	73
7.1.1 Creating an Asset Discovery Task	74
7.1.2 Managing Asset Discovery Tasks	76
7.1.3 Viewing the Online Report of an Asset Discovery Task	76
7.2 Assets to Be Inventoried	77
7.2.1 Ignoring Assets	78
7.2.2 Registering Assets	79
7.2.3 Manually Typing Assets To Be Inventoried	79
7.2.4 Importing Assets To Be Inventoried	80
7.2.5 Bulk Registering Assets	80
7.3 Inventoried Assets	80
7.3.1 Customizing an Asset Identification Policy	82
7.3.2 Customizing Asset Views	83
7.3.3 Adding Assets	84
7.3.4 Viewing Asset Details	87
7.3.5 Editing Assets	87
7.3.6 Importing Assets	88
7.3.7 Removing/Deleting Assets	88
7.3.8 Vulnerability Management	89
8 Vulnerability	90
8.1 Vulnerability Management	90
8.1.1 Vulnerability O&M	90
8.1.2 Host Vulnerabilities	91
8.1.3 Website Vulnerabilities	98
8.2 Scanning Tasks Management	98
8.2.1 Creating a Task	100

8.2.2 Creating an Import Task.....	112
8.2.3 Viewing a Scanning Report.....	112
8.2.4 Configuring a Plugin.....	115
9 Knowledge Base	116
9.1 Rule Base	116
9.1.1 Intelligence Rules.....	116
9.1.2 Updating Rule Bases.....	117
9.2 Intelligence Database	118
9.2.1 Intelligence Overview	118
9.2.2 Configuring Intelligences.....	119
9.2.3 Querying Intelligences	121
9.2.4 Querying Online.....	121
9.3 Vulnerability Database	121
9.3.1 Vulnerabilities	121
9.3.2 Password Dictionary	123
9.3.3 Vulnerability Database Upgrade	125
9.4 Geodatabase	125
10 More.....	127
10.1 System Configuration.....	127
10.1.1 Theme	127
10.1.2 Storage	128
10.1.3 Allowlist.....	129
10.1.4 Asset Topology.....	131
10.2 Device Manager	133
10.2.1 Device List.....	133
10.2.2 App Store	140
10.2.3 Traffic Forensics	142
A Factory Parameter.....	143
B Message Channel Configuration.....	144
C User Profile.....	145
D Component Configuration.....	146
D.1 Configuring an Asset	146
D.1.1 Managing Policies.....	146
D.1.2 Managing Attributes.....	146
D.1.3 Managing Types	148
D.1.4 Managing Labels.....	149
E Supplementary Information.....	150
E.1 Collaborative Device Access Descriptions	150
E.2 Supported Components.....	151

E.3 Rule Packages.....	152
E.4 Supported Databases.....	152

Preface

This document describes the functions and usage of the web-based manager of NSFOCUS Intelligent Security Operations Platform (ISOP for short).

This document is provided for reference only. It may slightly differ from the actual product due to version upgrade or other reasons.

Organization

Chapter	Description
1 Product Overview	Describes the characteristics and typical deployment mode of ISOP.
2 Importing a License	Describes the license types of ISOP and how to import ISOP licenses.
3 Situational Awareness	Describes displayed items in situational awareness screens and how to configure big screens.
4 Monitoring	Describes how to configure the dashboard and view overall threat information.
5 Analytics	Describes how to view XDR, threat analysis, intelligence data as well as reports, conduct attribution, and perform related configurations.
6 Handling	Describes manual handling and automated handling of events, responses and alerts.
7 Asset	Describes asset security-related management and operations.
8 Vulnerability	Describes vulnerability management and scanning task management.
9 Knowledge Base	Describes how to manage the rule base, intelligence database, vulnerability database and GeoIP database.
10 More	Describes system and device-related configurations and operations.
A Factory Parameter	Describes factory settings of ISOP.
B Message Channel Configuration	Describes how to configure message channels.
C User Profile	Describes user-related configurations and operations.
D Component Configuration	Describes how to manage policies, attributes, types and labels of assets.
E Supplementa	Describes other information to facilitate the usage of ISOP.

Change History

Version	Description
V3.0R01IB07	-

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
 Note	Reminds users to take note.
 Tip	Indicates a tip to make your operations easier.
 Caution	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
 Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong: +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Product Overview

With the comprehensive advancement of Internet +, the application of information technology in national social and economic construction is becoming more and more extensive, and new network security threats are more prominent. The traditional security system based on protection faces great challenges.

The next-generation cybersecurity defense system should pay more attention to security monitoring and response capabilities. For example, the system should be able to use big data analytics and prediction techniques to identify potential threats based on all network traffic, cope with large numbers of unknown security threats.

In answering to these requirements, NSFOCUS introduces Intelligent Security Operations Platform (ISOP).

This chapter contains the following topics:

Topic	Description
Introduction	Describes the overview functions of the ISOP system.
Product Entry	Describes how to access the ISOP platform.
Web-based Management	Describes the login method and page layout of the web-based manager of ISOP.

1.1 Introduction

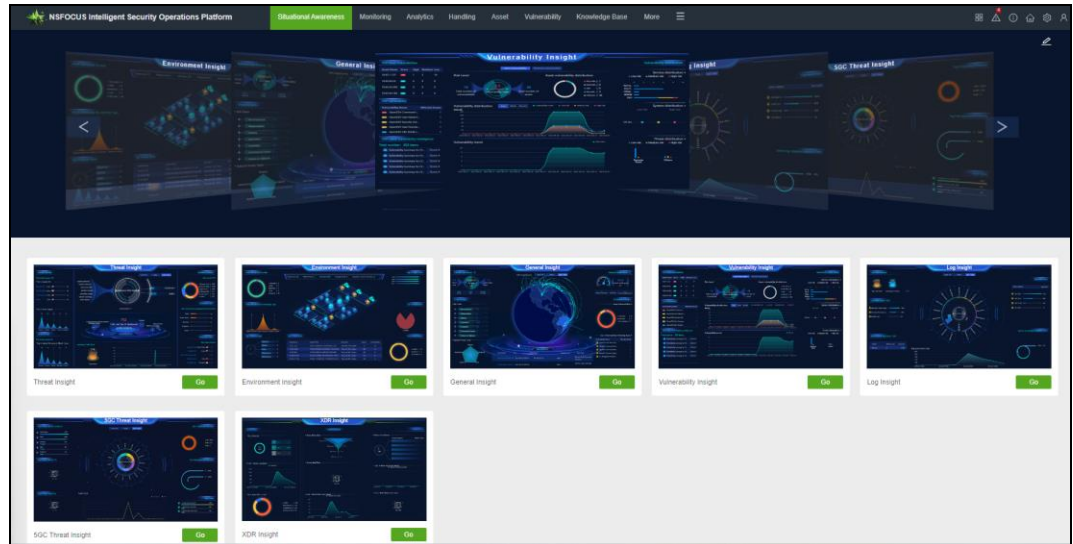
ISOP is a trusted security management platform applicable to all scenarios. Revolving around assets, ISOP is built on the big data architecture to help government and enterprise customers with their day-to-day security operations, putting in practice the concept of NSFOCUS Intelligent Security 3.0.

ISOP aggregates networkwide traffic and heterogeneous log data and incorporates threat intelligence for real-time analysis and intelligent decision-making. It implements lifecycle management of assets and vulnerabilities, achieving closed-loop security controls throughout the process of an incident from investigation, analysis, and traceback to forensics and response. It can also be used as an aid to customers' security orchestration and anomalous behavior analysis in their development and deployment of security operations centers (SOCs), effectively supporting their security operations (management, analysis, and response). By providing customers with an insight into their overall security posture, ISOP helps enterprises develop a benign security ecosystem.

1.2 Product Entry

Upon login to NSFOCUS Big-Data Security Analytics Platform (BSA), click  in the upper-right corner of the page and select **NSFOCUS ISOP**. Then the **Situational Awareness** page of ISOP appears, as shown in [Figure 1-1](#).

Figure 1-1 Situational awareness page



1.3 Web-based Management

The web-based manager of ISOP provides intuitive interfaces for users to manage and configure ISOP. The following sections describe the login method, page layout, and common operations on the web-based manager.

1.3.1 Web Login

Make sure that the network is accessible before login.

Open a browser and use HTTPS to access the administrative IP address (for example, <https://192.168.1.1>). After you accept the normal risk, the web login page appears. Type a valid user name and password; Then click **Login**.

You must load a valid license when you use NSFOCUS ISOP for the first time. For the license loading methods, see [Importing a License](#).

1.3.2 Page Layout of the Web-based Manager

The page layout for all functional module is the same, as shown in [Figure 1-2](#).

[Table 1-1](#) describes the page layout.

	The menus and workspace shown on the page vary with user permissions.
---	--

Figure 1-2 Page layout

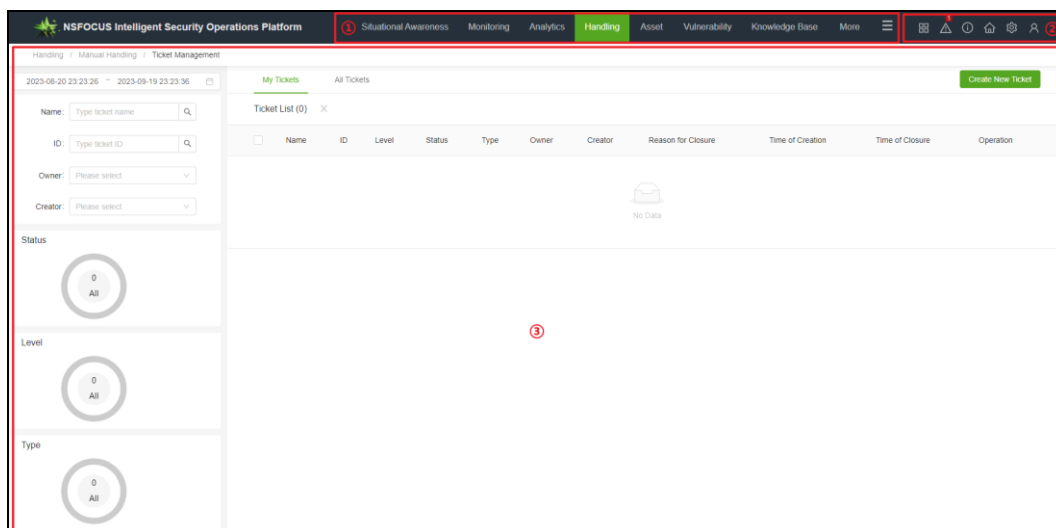


Table 1-1 Page layout description

No.	Area	Description
①	Navigation bar	- First-level menu. Hover the mouse over the menu and the corresponding secondary and tertiary function menus appear. - Click  to display the full menu navigation and open the corresponding page by clicking the corresponding link. The name of the current page is shown in blue in the navigation bar.
②	BSA general menu/Quick access bar	The icons from left to right are described as follows: : allows you to select and open specific solutions. : displays system alerts. The red number indicates the current number of alert messages. : displays information of the products, such as the product version and support information. : returns to the home page of the current system. : opens BSA's general menu bar. Refer to <i>NSFOCUS BSA User Guide</i> for detailed function description. : logs the current account out of the system.
③	Work area	Area where you can perform configurations and operations and view data.

2 Importing a License

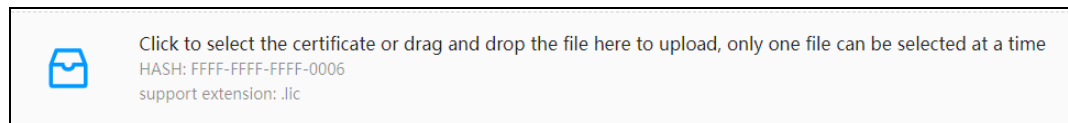
ISOP licenses are classified into two types:

- Trial
 - Trial licenses are mostly used for pre-sale testing.
 - The validity period is expressed with a starting date and end date in the license. After the license expires, all functions of the system are disabled. Besides, you can not log in to the system any more either through the web-based manager or the command line interface (CLI). You can only import a new license through the Web UI.
 - When the license is about to expire, an alert is displayed. You can configure ISOP to not display the alert again. Alternatively, you can click **Buy Now** or scan the QR code to purchase warranty services for the product.
- Paid
 - Official licenses can only be used after payment.
 - The validity period is expressed with a starting date and end date in the license. After the license expires, the purchased modules can continue to be used but cannot be upgraded.

A message is displayed on the web page one month before the license expires. To import a new license, follow these steps:

- Step 1** Make sure that the client host communicates properly with BSA (open port 443 if the traffic needs to go through a firewall).
- Step 2** Open a browser (for example, Firefox) and enter the IP address (for example, https://192.168.1.1) and press **Enter**.
- Step 3** Click **Advanced...** and then **Accept the Risk and Continue** to jump to BSA's web login page.
- Step 4** Type a correct user name and password and click Login.
- a. For initial login, you can use the default administrator account. For details, see [Factory Parameter](#).
 - b. If you log in with the default password for the first time, the system will ask you to change the password. After setting the new password, click **OK**.
- Step 5** Import the license.
- a. If you log in to ISOP for the first time using the admin account, change the password and log in again. The license importing page appears, as shown in [Figure 2-1](#). You must load a valid license to be able to continue to use the product.

Figure 2-1 Prompt box of importing the license



- b. After selecting the correct license file, click **OK** and then **Import** in the pop-up dialog box to complete the license import, as shown in [Figure 2-2](#).

Figure 2-2 License imported successfully

License Information			
Product Name:	BSA	HASH Value:	FFFF-FFFF-FFFF-0006
Authorized Object:	试用证书6725567	License Type:	Trial
License Status:	Normal	Number Of Authorized Nodes:	1
License Start And End Date:	2023-04-17 至 2024-04-17		
Authorization Module			
Name	Start Time	End Date	Expiration Reminder
+ 一体化网络安全管理系统	2023-04-17	2024-04-17	The service will be 247days after stop!
+ NSFOCUS Intelligent Security Operations Platform	2023-04-17	2024-04-17	The service will be 247days after stop!
+ ISOP-SGC	2023-04-17	2024-04-17	The service will be 247days after stop!
+ Threat Intelligence Component	2023-04-17	2024-04-17	The service will be 247days after stop!
+ NSFOCUS Threat Intelligence	2023-04-17	2024-04-17	The service will be 247days after stop!
+ Scenario Model Upgrade Service	2023-04-17	2024-04-17	The service will be 247days after stop!



- Before login, check whether the check box of blocking pop-ups or disabling JavaScript is selected in the browser. If yes, clear the check box.
- You are advised to use the latest Firefox or Chrome browser and set the browser resolution to 1024x768 or higher.
- You can use the default system administrator to log in to the system for the first time.

----End

3

Situational Awareness

Big screens for situational awareness cover the threats, environment, general situation, operation and maintenance responses, vulnerabilities, logs, 5GC threats, and extended detection and response (XDR).

Before using these big screens, you must configure the screen display, cards, chartics library, and screen interface.

This chapter contains the following topics:

Topic	Description
Threat Insight	Describes how to view the Threat Insight screen.
Environment Insight	Describes how to view the Environment Insight screen.
General Insight	Describes how to view the General Insight screen.
Vulnerability Insight	Describes how to view the Vulnerability Insight screen.
Log Insight	Describes how to view the Log Insight screen.
5GC Threat Insight	Describes how to view the 5GC Threat Insight screen.
XDR Insight	Describes how to view the XDR Insight screen.

3.1 Threat Insight

Choose **Situational Awareness** > **Situational Awareness** and click **Go** on the **Threat Insight** gadget.

The Threat Insight screen shows various threat statistics of the last 1 hour, current day, and last 7 days in the current network environment, as shown in [Figure 3-1](#). The time range cannot be customized.

You can customize the display of some gadgets in the screen by clicking  in their upper-right corner. On the panel that appears after you click , titles of gadgets that have been displayed are shown in gray. Gadgets without the  icon are default ones, which cannot be removed or switched.

[Table 3-1](#) describes items displayed on the Threat Insight screen.

Figure 3-1 Threat Insight screen

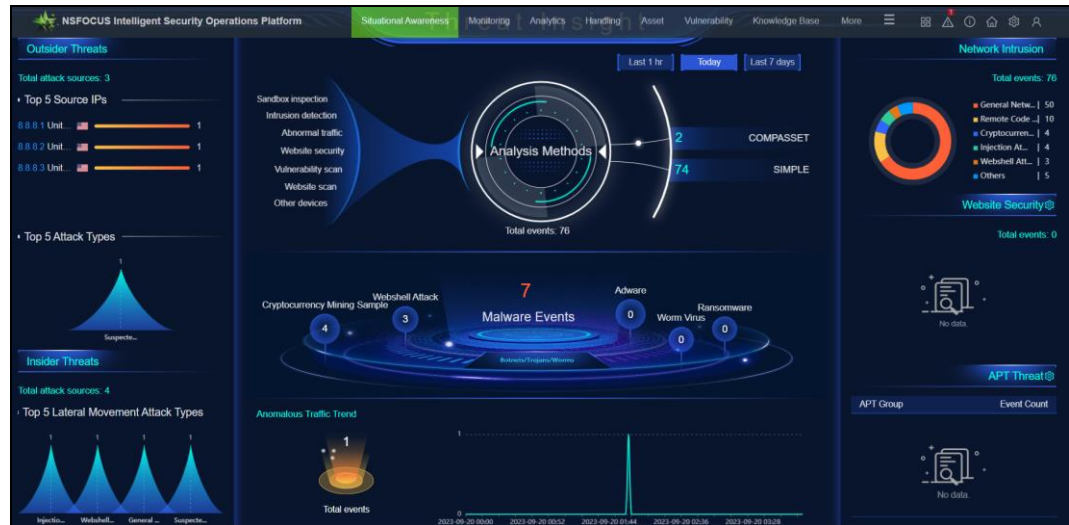


Table 3-1 Threat Insight screen description

Displayed Item		Description
Analysis Methods		Displays the threat analysis methods, the number of incidents detected by each type of rule, and the total number of incidents during the selected time range.
Botnets/Trojans/Worms		Displays the total number of botnet/trojan/worm events and the number of each type of events in the specified time range. You can click a number to go to the Analytics > Threat Analysis > Event Assessment page to view and manage the corresponding category of events. See Assessing an Event for the follow-up operations.
Anomalous Traffic Trend		Displays the total number of anomalous traffic events in the specified time range on the left and illustrates the anomalous traffic posture trend in a chart on the right. Hovering over the chart shows specific statistics. You can click any point of the chart to go to the Analytics > Threat Analysis > Event Assessment page to view and manage the corresponding category of events. See Assessing an Event for the follow-up operations.
Website Security		Displays the total number of network intrusion events in the specified time range and the number of various website security events in a donut chart. Hovering over the chart shows specific statistics.
Outsider Threats	Total attack sources	Displays the total number of external total attack sources in the specified time range.
	Top 5 Source IPs	In the bar chart, the top 5 attack source IP addresses with the most anomalous traffic and attack times within the specified time range are displayed (the country/region/flag where the IP addresses belong can be displayed).
	Top 5 Attack Types	The area chart displays top 5 attack types with the most external attacks within the specified time range.

Displayed Item		Description
Insider Threats	Total attack sources	Displays the total number of internal total attack sources in the specified time range.
	Top 5 Lateral Movement Attack Types	Displays top 5 lateral movement attack types with the most external attacks within the specified time range in a area chart.
Network Intrusion		The total number of network intrusion events in the specified time range and the number of various network intrusion events are displayed in a doughnut chart. Hovering over the chart shows specific statistics.
APT Threat		Displays the APT organization names and the corresponding number of APT incidents in a list. You can customize this gadget by clicking the  icon.

3.2 Environment Insight

Choose **Situational Awareness** > **Situational Awareness** and click Go on the **Environment Insight** gadget.

The Environment Insight screen displays statistics about the current network environment, as shown in [Figure 3-2](#).

The statistical time ranges include **Last 1 hr**, **Today** and **Last 7 days**.

[Table 3-2](#) describes the statistical items displayed in the Environment Insight screen.

Figure 3-2 Environment Insight screen



Table 3-2 Environment Insight screen description

Displayed Item	Description
Overall statistics	Displays the number of hosts, websites, new assets, changed assets, and suspected compromised assets.
Asset Distribution by Risk Level	The distribution of assets by risk level in the current network environment is displayed in the form of a donut chart. You can click the check box leading each legend to hide/display the statistics of the corresponding category in the ring chart, and hover over the donut chart to view specific statistics.
Asset Distribution by Anomaly Type	The distribution of assets by anomaly type in the current network environment is displayed in the form of an area chart. Hovering over the chart shows specific statistics.
Top 5 Device Types	The donut chart shows top 5 device types with the largest number of assets in the current network environment and the number of each type of assets. The device types include the terminal, server, security device, network device, and cloud host.
TOP 10 Open Ports	In the bar chart, top 10 ports opened on the most assets are displayed.
TOP 10 Applications	The area chart displays top 10 applications with the biggest quantities in the current network environment. Hover over the chart to see specific statistics.
Discovered Assets	The distribution of discovered assets in the current network environment is displayed in the form of a donut chart. You can click a discovery source to hide/display its statistics in the chart, and hover over the chart to view specific statistics.
Top 5 Assets by Risk Count	Top 5 assets with the highest number of events in the current network environment are displayed in a list, including the asset name, IP/URL, risk label, number of events, and number of vulnerabilities.

3.3 General Insight

Choose **Situational Awareness** > **Situational Awareness** and click Go on the **General Insight** gadget.

The General Insight screen shows the overall security situation of the current network environment in the last 1 hour, current day, or last 7 day, as shown in [Figure 3-3](#). The time range cannot be customized.

[Table 3-3](#) describes items displayed in the General Insight screen.

Figure 3-3 General Insight screen



Table 3-3 General Insight screen description

Displayed Item		Description
ISOP uptime		Displays how long ISOP runs since it goes live.
Attack Overview (Domestic/International)		A globe shows attacks across the world in the specified time range. Hovering over the attack line in the globe shows the corresponding attack direction and number.
Network Risk Posture		Displays the network's risk level, threat index, vulnerability index, total number of events, logs, and threat intelligence (TI) entries in the specified time range. You can click  to view the calculation methods and scores of the threat index, vulnerability index, and risk level.
Threat Analysis	Kill Chain	Displays the number of events for each stage of the attack chain in the specified time range. You can click the event number to go to the Analytics > Threat Analysis > Event Assessment page to view and manage the corresponding category of events. See Assessing an Event for the follow-up operations.
	Threat Statistics by Scenario	The number of events in each specific threat scenario in the specified time range is displayed in a radar chart. The threat scenarios include network security, application security, endpoint security, business security, and data security. Hovering over the radar chart shows the number of threats of each threat scenario.
Network Health Status		Displays the network health grade, number of online/connected devices, total number of assets, number of host vulnerabilities, and number of website vulnerabilities in the specified time range. You can click  to view the calculation methods and scores of the network health index.
Vulnerability	Asset	The distribution of asset vulnerabilities by severity level in the

Displayed Item		Description
Analysis	Vulnerabilities	specified time range is displayed in the form of a donut chart. You can click a severity level to hide/display the statistics of the corresponding category in the chart, and hover over the chart to view specific statistics.
	Top Vulnerabilities Affecting Asset	5 The list displays top 5 vulnerabilities affecting assets within the specified time range.
Key Events		Displays key events in the specified time range in a scrolling manner, including the event name, time, O&M object, severity level, and event type. You can click the event name to go to the event details page. See Viewing Event Details for the follow-up operations. Data source: Monitoring > Dashboard > Threat .

3.4 Vulnerability Insight

Choose **Situational Awareness** > **Situational Awareness** and click **Go** on the **Vulnerability Insight** gadget.

The Vulnerability Insight screen displays the vulnerabilities of host assets and website assets in the current network environment, as shown in [Figure 3-4](#).

[Table 3-4](#) describes the statistical items displayed in the Vulnerability Insight screen.

Figure 3-4 Vulnerability Insight screen



Table 3-4 Vulnerability Insight screen description

Displayed Item	Description
Top 5 Vulnerable Assets	Lists top 5 host/website assets with the highest vulnerability score, including the asset name, vulnerability score, and numbers of high-, medium-, and low-risk vulnerabilities.

Displayed Item		Description
		- Data source of host vulnerabilities: Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics. - Data source of website vulnerabilities: Vulnerability > Vulnerability Management > Website Vulnerabilities > Asset Statistics.
Top 5 Vulnerabilities Affecting Assets		Lists top 5 vulnerabilities that affect the most hosts/websites, including the vulnerability name and the number of affected assets. - Data source of host vulnerabilities: Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics. - Data source of website vulnerabilities: Vulnerability > Vulnerability Management > Website Vulnerabilities > Asset Statistics.
Top 5 Latest Vulnerability Intelligence		Displays the total number of received vulnerability intelligence and top 5 vulnerabilities with the highest vulnerability score. Data source: Analytics > Intelligence > Vulnerability Alert > Intelligence.
Risk level		Displays the total numbers of vulnerabilities and assets as well as the vulnerability index in the current network environmen.
Asset Distribution by Vulnerability Level		Displays the distribution of assets by vulnerability level in a donut chart. You can click a vulnerability level to hide/display the statistics of the corresponding category in the chart, and hover over the chart to view specific statistics. Asset vulnerability levels include Very vulnerable, Vulnerable, Safe, Very safe, and Unknown.
Vulnerability Trend by Level		Displays the total number of host/website vulnerabilities in the last 12 days, 12 weeks, or 12 months, and the distribution trend of low-/medium-/high-risk vulnerabilities in a curve chart. Hovering over the chart shows specific statistics
Vulnerability Trend by Risk Score		Displays the host/website vulnerability trend by risk score in the last 12 days, 12 weeks, or 12 months in a curve chart. Hovering over the chart shows specific statistics.
Host Vulnerability Distribution	Services	Displays the number of services with the most vulnerabilities and the vulnerability distribution by risk level. You can click a risk level to hide/display the statistics of the corresponding category in the donut chart. Hovering over the donut chart shows specific statistics.
	Systems	Displays the distribution of low-/medium-/high-risk vulnerabilities in operating systems in a scatter chart. You can click a risk level to hide/display the statistics of the corresponding category in the chart, and hover over the chart to view specific statistics.
	Threats	Displays the distribution of low-/medium-/high-risk vulnerabilities by threat types in a bar chart. You can click a risk level to hide/display the statistics of the corresponding category in the chart, and hover over the chart to view specific statistics.

Displayed Item		Description
Website Vulnerability Distribution	WASC Distribution	Displays the number of low-/medium-/high-risk vulnerabilities in a radar chart. You can click a risk level to hide/display the statistics of the corresponding category in the chart, and hover over the chart to view specific statistics.
	OWASP-2013 Distribution	Displays the number of low-/medium-/high-risk OWASP Top 10 (2013) vulnerabilities in a scatter chart. Hovering over the chart shows specific statistics.
	Threats	Displays the distribution of low-/medium-/high-risk vulnerabilities by threat type in a bar chart. You can click a risk level to hide/display the statistics of the corresponding category in the chart, and hover over the chart to view specific statistics.

3.5 Log Insight

Choose **Situational Awareness > Situational Awareness** and click **Go** on the **Log Insight** gadget.

The Log Insight screen displays statistics of logs collected by ISOP in the last 1 hour, current day, and last 7 days, as shown in [Figure 3-5](#).

[Table 3-5](#) describes items displayed in the log Insight screen.

Figure 3-5 Log Insight screen

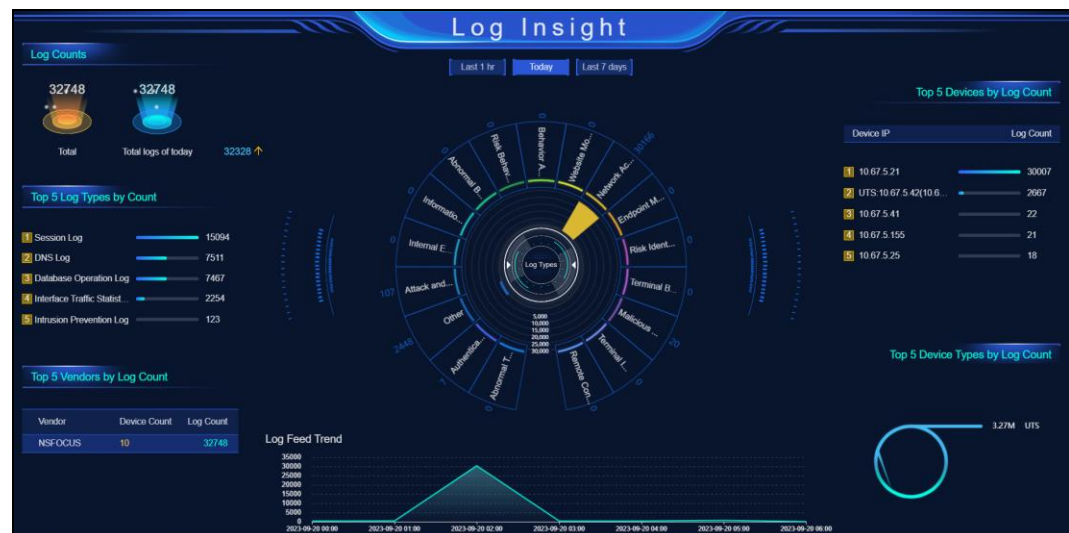


Table 3-5 Log Insight screen description

Displayed Item	Description
Log Types	Displays the log types and the corresponding number of logs in the specified

Displayed Item	Description
	time range. Hovering over a color block in the figure shows the specific data for the corresponding log type.
Log Counts	Displays the total logs, total logs of today, and the number of logs increased or decreased from the previous day within the specified time range.
Top 5 Log Types by Count	Displays top 5 log names with the largest number of access logs in the specified time range in a bar chart.
Top 5 Vendors by Log Count	Displays top 5 vendors with the largest number of access logs within the specified time range in a list, including the vendor name, device count, and log count.
Top 5 Devices by Log Count	Displays top 5 devices with the highest log volume within a specified time range.
Top 5 Device Types by Log Count	Displays top 5 device types with the most access logs within the specified time range in a donut chart.
Log Feed Trend	Displays the number trend of access logs within the specified time range in a curve chart. Hovering over the chart shows the number of the access logs at a specific time point.

3.6 5GC Threat Insight

Choose **Situational Awareness > Situational Awareness** and click **Go** on the **5GC Threat Insight** gadget.

The 5GC Threat Insight screen displays the threat posture of the 5G core network in the last 1 hour, current day, and last 7 days, as shown in [Figure 3-6](#).

[Table 3-6](#) describes items displayed in the 5GC Threat Insight screen.

Figure 3-6 5GC Threat Insight screen



Table 3-6 5GC Threat Insight screen description

Displayed Item	Description
Event Types	Displays the even types and the corresponding number of events within the specified time range. Hovering over a color block in the figure shows the specific data for the corresponding event type.
Top 5 Attack Source Locations	Scroll through the bar chart to display the following: - The top 5 countries/regions with the most 5GC events in the specified time range. - The top 5 provinces/autonomous regions/municipalities with most 5GC events in the specified time range.
Top 5 Attack Source IPs	Displays the top 5 attack source IP addresses with the most 5GC events within the specified time range in a bar chart.
Top 5 Attack Target IPs	Displays the top 5 destination IP addresses with the most 5GC events within the specified time range in a bar chart.
Top 10 Signaling Protocols	Displays the top 10 5GC signaling protocol types with the most vulnerabilities within the specified time range in a ring diagram.
Top 5 Management Protocols	Displays the top 10 5GC management protocol types with the most vulnerabilities within the specified time range in a ring diagram.
Top 5 Slices	Displays top 5 offline slices with the most events and the total number of slices in the specified time range.
Event Trend	Displays the 5GC event trend. Hovering over the chart shows the number of 5GC events and total events within the specified time range.

3.7 XDR Insight

Choose **Situational Awareness** > **Situational Awareness** and click Go on the **XDR Insight** gadget.

The XDR Insight screen displays threat detection and response analysis data at the network, terminal, and cloud levels, as shown in [Figure 3-7](#).

[Table 3-7](#) describes the statistical items displayed in the XDR Insight screen.

Figure 3-7 XDR Insight screen



Table 3-7 XDR Insight screen description

Displayed Item		Description
Extended Statistics	Log Sources	Displays the source distribution and the total number of received logs in a donut chart. Hovering over the chart shows specific statistics. EDR indicates the device-side log, NDR the network-side log, and Other indicates logs other than EDR and NDR logs.
	Last 1 Week Log Trend	Displays the number trend of received logs in the past week in a chart.
	Log Type Distribution	Displays the log type distribution of received logs in a donut chart. You can click a type to hide/display the statistics of the corresponding category in the chart, and hover over the chart to view specific statistics.
Extended Detection	Noise Reduction	Displays the total number of received original logs and the number of alert logs, threat events, and entity events after noise reduction in a funnel chart.
	Associated Data	Displays the number of different types of logs successfully spliced, including logs of alerts, networks, processes, files, users, and others in a rose chart. Hovering over the chart shows specific statistics.
	Last 1 Week XDR Event Trend	Displays the number trend of entity events in the past week in a chart. Hovering over the chart shows specific statistics.
Extended Response	Response Devices	Displays top 5 collaborative devices with the largest number of blocking actions.
	Last 1 Week Response Trend	Displays the response trend of events in the past week in a chart.
	Top 5 Auto Response Cases	Displays the top 5 cases with the largest number of automated responses in a bar chart.

4 Monitoring

The monitoring dashboard shows the overall situation related to operation and maintenance of threats.

Choose **Monitoring > Dashboard > Threat** to view the operation and maintenance data of threats within the last 1 hr, Today or 7 days, as shown in [Figure 4-1](#).

[Table 4-1](#) describes displayed items in the dashboard.

In the statistical chart, click each legend to hide or display the statistics of the corresponding category in the ring chart, and hover the mouse over the ring chart to view the specific statistics.

Click **Refresh** to manually refresh the statistics of the threat overview dashboard. Click **Custom Dashboard** to customize what are displayed in the threat monitoring dashboard.

Figure 4-1 Threat monitoring dashboard

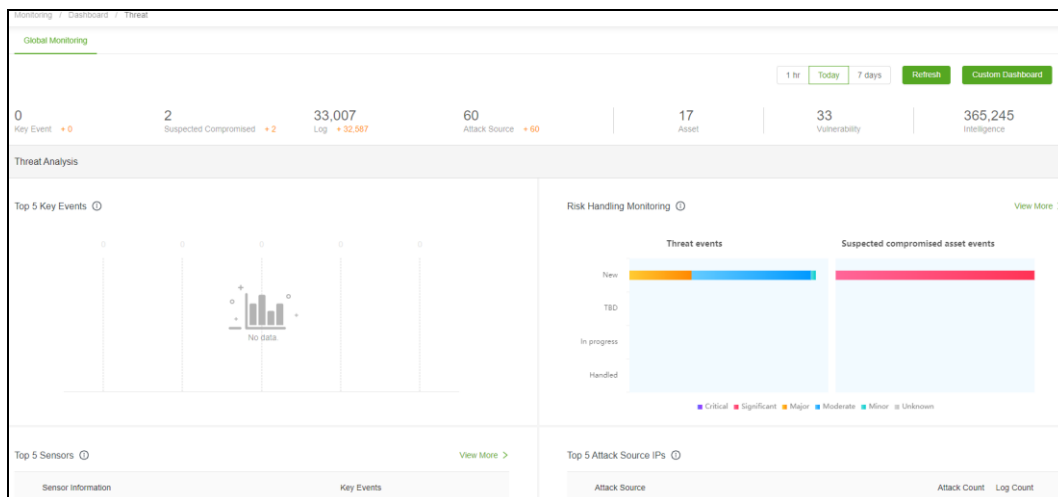


Table 4-1 Threat monitoring dashboard description

Displayed Item		Description	Default Display
Global Monitoring	Key Event	Displays the total number of key events within the specified time range as well as the increments or decrements compared to the last statistical period.	√

Displayed Item		Description	Default Display
	Suspected Compromised	Displays the total number of suspected compromised assets within the specified time range as well as the increments or decrements compared to the last statistical period. Clicking on the total number will navigate to the Analytics > Threat Analysis > Event Assessment page to manage the suspected compromise assets. See Assessing an Event for the follow-up operations.	√
	Log	Displays the total number of logs within the specified time range as well as the increments or decrements compared to the last statistical period. Clicking on the total log number will navigate to the Analytics > Attribution > Log Query page to search for normalized logs. For details, see Querying Logs.	√
	Attack Source	Displays the total number of attack sources within the specified time range as well as the increments or decrements compared to the last statistical period. Clicking on the total attack source number will navigate to the Analytics > Threat Analysis > Event Assessment page to carry out network threat analysis from the perspective of events. For details, see Assessing an Event.	√
	Asset	The total number of assets within the specified time range. Click the asset number and go to the Asset > Asset Security > Inventoried Assets page to manage the assets. See Inventoried Asset.	√
	Vulnerability	Displays the total number of vulnerabilities within the specified time range. Clicking on the total vulnerability number will navigate to Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics to view the statistics of host vulnerabilities. For details, see Asset Statistics.	√
	Intelligence	Displays the total number of intelligences within the specified time range. Clicking on the total intelligence number will navigate to the Knowledge Base > Intelligence Database > Query page to search threat intelligences. For details, see Querying Intelligences.	√
Threat Analysis	Top 5 Key Events	Displays the top 5 key events with the highest number of occurrences within the specified time range in a pictochart.	√
	Risk Handling Monitoring	Displays the operation and maintenance information of various risk events in the	√

Displayed Item		Description	Default Display
		specified time range in the bar charts. The statistics are grouped according to event category, event status and risk level. Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to assess the events. For details, see Assessing an Event .	
	Top 5 Sensors	Displays the top 5 devices (probes) with the highest number of accessed events within the specified time range in a list. The displayed fields include sensor information and key events. Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to assess the events. For details, see Assessing an Event .	√
	Top 5 Attack Source IPs	Displays the top 5 attack sources with the highest number of attacks within the specified time range in a list. The displayed fields include the attack source (IPv4 or IPv6), attack count, and log count. Clicking the attack source IP will navigate to the Analytics > Attribution > Log Query page to carry out advanced searches for the attack source's logs. For details, see Querying Logs .	√
	Top 5 Attack Source Locations	Displays the top 5 countries/regions with the highest number of incidents within the specified time range in a bar chart. Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to assess the events. For details, see Assessing an Event .	-
	Top 5 Threat Event Types	Displays the top 5 event types with the highest number of occurrences within the specified time range in a pictochart. Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to assess the events. For details, see Assessing an Event .	-
	Top 5 Outbound Event Types	Displays the top 5 asset outbound attack event types with the highest number of occurrences within the specified time range in a pictochart. Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to assess the events. For details, see Assessing an Event .	-
	Top 10 Cryptomining Hosts	Displays the top 10 mining hosts with the highest number of mining events in the specified time range in a chart.	
	Top 10 Ransomware-hit	Displays the top 10 ransomware-hit hosts with the highest number of ransomware events in the specified time range in a	

Displayed Item		Description	Default Display
	Hosts	pictochart.	
Asset Analysis	Top 5 Threat Event Types	Displays the top 5 event types with the highest number of attacks on assets for the specified time range in a pictochart. Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to assess the events. For details, see Assessing an Event .	√
	Asset Discovery	Displays the changes of the asset discovery in the specified time range in a bar chart. The displayed fields include Changed and New . Clicking ViewMore will navigate to the Asset Management > Asset Security Management > Asset Discovery Task page to perform management operations of asset scanning tasks. For details, see Asset Discovery Task .	√
	Top 5 High-Risk Assets	Displays the top 5 suspected compromised assets with the highest asset risk score within the specified time range in a list. The displayed fields include asset ID (asset IP), asset risk value and top 3 event type. Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to assess the events. For details, see Assessing an Event .	√
	Asset Vulnerability	Displays the vulnerability distribution of host assets and the top 5 assets with the highest number of vulnerabilities in the specified time range in a ring chart and lists. The displayed fields include asset ID, asset vulnerability score and the number of high-risk vulnerabilities. Clicking ViewMore will navigate to Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics page to view the statistics of host vulnerabilities. For details, see Asset Statistics .	√
Vulnerability Analysis	Vulnerability Monitoring	Displays the host vulnerability monitoring information within the specified time range. The displayed fields include the handled vulnerabilities, to be handled vulnerabilities, total vulnerabilities and the number of vulnerabilities in different handling status. Clicking ViewMore will navigate to Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics page to view the statistics of host vulnerabilities. For details, see Asset Statistics .	√
	Website Monitoring Events	Displays the website monitoring event information within the specified time range. The displayed fields include the processed events, pending events and event count.	√

Displayed Item		Description	Default Display
		Clicking ViewMore will navigate to Analytics > Threat Analysis > Event Assessment page to judge the events. For details, see Assessing an Event .	
	Top Vulnerable Hosts 5	Displays the top 5 host assets with the highest vulnerability values within the specified time range. Clicking ViewMore will navigate to Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics page to view the statistics of host vulnerabilities. For details, see Asset Statistics .	-
	Top High-Risk Vulnerabilities Affecting Assets 5	Displays the top 5 vulnerabilities that have affected the most assets within the specified time range. Clicking ViewMore will navigate to Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics page to view the statistics of host vulnerabilities. For details, see Asset Statistics .	-
	Top Vulnerable Websites 5	Displays the top 5 website assets with the highest vulnerability score within the specified time range. The displayed fields include the website name, URL, and their vulnerability value. Clicking ViewMore will navigate to Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics page to view the statistics of website vulnerabilities. For details, see Asset Statistics .	-

5 Analytics

Analysis center displays details about abnormal data discovered by the monitoring center, facilitating threat analysis, intelligence analysis, and attribution analysis, and generating statistical reports.

This chapter contains the following topics:

Topic	Description
XDR	Describes how to operate the threat detection and event response tool (XDR).
Threat	Describes how to analyze network threats based on events assessment, attacker profile and risk behavior.
Intelligence	Describes how to view threat intelligence statistics and how to manage vulnerability intelligence alerts.
Attribution	Describes attribution related operations, including log query, traffic forensics, and threat hunting.
Report	Describes how to generate and manage O&M reports, vulnerability reports, and 5GC reports.
Managing Exported Tasks	Describes how to manage exported tasks.

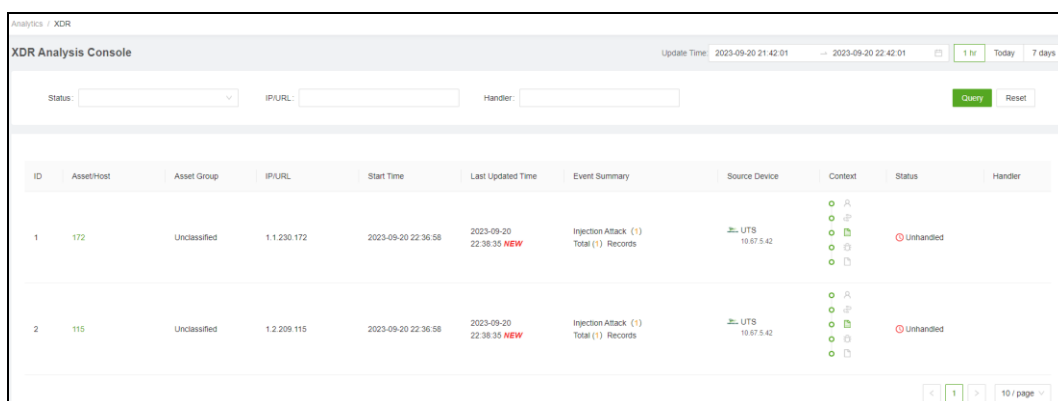
5.1 XDR

Based on the threat detection and data analysis capabilities of NSFOCUS, the XDR analysis console in ISOP utilizes host assets as the anchor point to associate event alerts and establish scoring and triage mechanisms based on the accessed attack telemetry data (including network, endpoint, identity user and third-party data). This approach helps to reduce alert quantity, improve alert accuracy, facilitate rapid response and handling, and enhance the efficiency of security operations.

Choose **Analytics > XDR**. This page displays threat detection and response information reported within the last hour. You can also set search criteria to query host assets, as shown in [Figure 5-1](#).

[Table 5-1](#) describes the XDR list.

Figure 5-1 XDR analysis console



ID	Asset/Host	Asset Group	IP/URL	Start Time	Last Updated Time	Event Summary	Source Device	Context	Status	Handler
1	172	Unclassified	1.1.230.172	2023-09-20 22:36:58	2023-09-20 22:38:35 NEW	Injection Attack (1) Total (1) Records	UTS 19.67.5.42	   	Unhandled	
2	115	Unclassified	1.2.209.115	2023-09-20 22:36:58	2023-09-20 22:38:35 NEW	Injection Attack (1) Total (1) Records	UTS 19.67.5.42	   	Unhandled	

Table 5-1 XDR list description

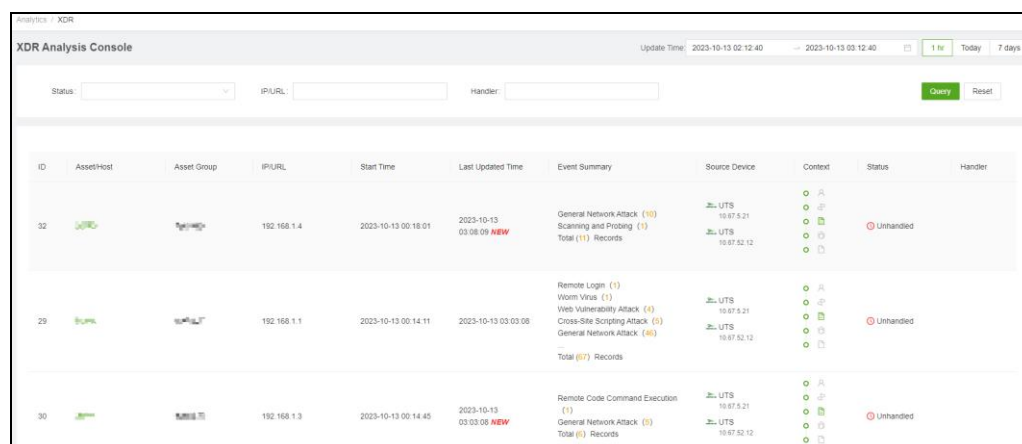
Displayed Item	Description
ID	Unique identification of the XDR event.
Asset/Host	Name of the threatened assets. Click the asset name to go to the threat details page of the asset. Centralized management and centralized response are supported. For details, see Viewing Threat Details .
Asset Group	Asset group to which the asset belongs.
IP/URL Address	IP address of the asset.
Start Time	Time when the first threat event was discovered.
Last Updated Time	Time when the latest threat event was discovered.
Event Summary	Displays the top 10 events by event type.
Source Device	Displays the type and IP address of the device that reports the event.
Context	Color-coded context information for events, including the user files, process, log, vulnerability, and file. The green icon indicates that this information is contained. The gray icon indicates that the information is not contained.
Status	Indicates whether the security threat on the current asset is handled. There are three handling status: Unhandled , Handled , and Ignored . For details, see Switching Response Status .
Handler	It is empty by default. After the status is changed, the handler is automatically updated to the current user.

5.1.1 Viewing Threat Details

In the XDR list, click the name (IP address) of an asset to go to the threat details page of the asset, as shown in [Figure 5-2](#).

[Table 5-2](#) describes the XDR details page.

Figure 5-2 XDR details page



ID	AssetHost	Asset Group	IPURL	Start Time	Last Updated Time	Event Summary	Source Device	Context	Status	Handler
32			192.168.1.4	2023-10-13 00:18:01	2023-10-13 03:08:09 NEW	General Network Attack (10) Scanning and Probing (1) Total (11) Records	UTS 19.87.5.21 19.87.52.12		Unhandled	
29			192.168.1.1	2023-10-13 00:14:11	2023-10-13 03:03:08	Remote Login (1) Worm Virus (1) Web Vulnerability Attack (1) Cross-Site Scripting Attack (1) General Network Attack (46) Total (51) Records	UTS 19.87.5.21 19.87.52.12		Unhandled	
30			192.168.1.3	2023-10-13 00:14:45	2023-10-13 03:03:08 NEW	Remote Code Command Execution (1) General Network Attack (1) Total (2) Records	UTS 19.87.5.21 19.87.52.12		Unhandled	

Table 5-2 XDR details page description

Displayed Item		Description
Basic Information		The top of the page shows the number of events, source device name and IP address, and asset information. The asset information includes the asset name, asset IP address, operating system, application, port, user, and responsible person.
Threat List	Event	The Event tab displays the following contents (See Viewing Event Details for more details): - On the lower-left of the page, the attack status of the current asset is displayed from the attacker's perspective, including the attacker's IP address, generation time (the time when the attacker started the attack), origin region (the attacker's geographical location), and event tags (TOP 10 event types). - Click an attacker on the left. The details about the attack events of the attacker against different targets in a specified time range are displayed in the middle part of the page. Note that one day is divided into four time ranges. You can view more logs (see Viewing More Logs) and quick assessment (see Assessing an Event Quickly). - On the lower-right of the page, the topology of end-network association analysis is displayed.
	Log	Log list of the current asset. Displayed fields include the timestamp, log name, log type, source IP, source port, destination IP, destination port, and device address.
	Vulnerability	List of vulnerabilities discovered by the current asset scan. Displayed fields include the Vulnerability Name, CVE ID, Response Priority, Response Status, Vulnerability Handler, and Vulnerability Source.
	Process	Process list of the current asset. Displayed fields include the Process Name, Process ID, Parent Process ID, Parent Process Path, Source Device, Process Operation, Process Path, Process MD5, Process Creation Time and Investigation Response. For quick response to process threats, see Isolating a Process .
	File	List of files associated with the current asset. Displayed fields include File Directory, File Type, Modified Time, File Size (Bytes), File Hash,

Displayed Item		Description
		File User, Process Behavior, Intelligence Result and Investigation Response. For quick response to file threats, see Isolating a File .
	User	List of users associated with the current asset. Displayed fields include User Name, User Description, User Status, User Belongs to Group, User Type, and Last Modified Time.

Viewing Event Details

On the Event tab, you can view the attack overview, event details, and the topology of end-network association analysis. [Table 5-3](#) describes the event details page of the current asset.

Table 5-3 Event details page of XDR

Displayed Item	Description
Attack overview	Attacks can be sorted by time and attack count. By default, events are sorted by attack count. • Sort by Time: displays attacks in descending order based on generation time (i.e. latest time to farthest time). • Attack Count: displays the number of attacks in descending order (from highest to lowest count). By default, 10 pieces of data are displayed. You can load more data (similar to turning pages). When there are more than 10 pieces of data, click More at the bottom to display 11 to 20 or more pieces of data.
Event details	Click the attack information box on the lower-left of the page. In the middle area, the details of all events from the current attacker are displayed by time range. Displayed fields include the statistical time range, destination IP address, attack count, event name, attack status, confidence, attack time, event tag, response code, and attack characteristics.  Note Here, there are 4 time ranges for each day: 0:00 to 6:00, 6:00 to 12:00, 12:00 to 18:00, and 18:00 to 24:00.
Topology of end-network association analysis	The area on the right displays the end-network association analysis topology, also known as the full attack path. The displayed items include the attacker, the attacked, the process created during the attack, the file, and the user. If an event has a corresponding attack path, click the event and the corresponding path is highlighted.

Assessing an Event Quickly

Click **Quick assessment** in the middle area to view the basic information, payload, request body, and response body of the event. For more information on events and quick analysis, see [Assessing an Event](#).

Viewing More Logs

Click **Detailed log** in the middle area to view the log details of the event, including the time stamp, log type, log name, basic information, source domain, target domain, and analysis. For more information on log and traffic forensics, see [Querying Logs](#) and [Traffic Forensics](#).

Isolating a Process

Click the **Process** tab. In the process list of the current asset, click **Select** in the **Investigation Response** column, then select **Process Isolation**, and configure the investigation response parameters to isolate the process. For configuration methods, see [Adding a Response](#).

Isolating a File

Click the **File** tab. In the file list of the current asset, click **Select** in the **Investigation Response** column, then select **File Isolation**, and configure the investigation response parameters to isolate the file. For configuration methods, see [Adding a Response](#).

5.1.2 Switching Response Status

In the XDR list as shown in [Figure 5-1](#), click the status in the **Status** column. After changing the status, the handler automatically becomes the current login user.

5.2 Threat Analysis

This topic describes how to analyze and assess events.

5.2.1 Assessing an Event

You can handle operation and maintenance (O&M) events in the Event Assessment module.

Choose **Analytics > Threat Analysis > Event Assessment**. By default, the statistics and event list of O&M events from 0:00 to the current time of today are displayed, as shown in [Figure 5-3](#).

[Table 5-4](#) describes the displayed items.

Figure 5-3 Event assessment page

Source IP	Destination IP	Event Name
10.8.22.1	134.224.120.62	10.8.22.1 to 134.224.120.62
10.8.22.1	120.78.176.150	10.8.22.1 to 120.78.176.150
192.168.10.129	185.68.111.122	192.168.10.129 to 185.68.111.122
111.29.107.219	47.243.131.340	111.29.107.219 to 47.243.131.340
192.168.116.149	223.5.5.5	192.168.116.149 to 223.5.5.5

Table 5-4 Event assessment page description

Displayed Item	Description
Query conditions	Basic query supports search by time range and text fuzzy search. By default, the page displays the O&M events from 0:00 of today to the current time in reverse order based on the end time. Advanced search supports the following operations: - Set more query conditions to query O&M events. - Click Add to add more query conditions. - After the query, click Save As Custom Tab to save the current query conditions and search results as a customized tab page on the right of the current tab page for quick search.
Statistics	O&M events statistics include the following types (click  /  to go to previous/next page): - Event Name: displays the top 20 names of the events with the highest number of attack occurrences. - Event Type: displays the top 20 event types with the highest number of attack occurrences. - Source IP: displays the top 20 source IP addresses with the highest number of attack occurrences. - Destination IP: displays the top 20 destination IP that are most frequently attacked. In the above data table, you can click   to filter the displayed data categories for display. For example: - Click  of the destination address 3.1.1.1 to filter out the related event type, event name, and source IP. - Click  of the destination IP 3.1.1.1 to filter out the event types, event names, and source IP addresses whose destination IP address is not 3.1.1.1.
Event List	Displays the total number of O&M events in the specified time range at the bottom of the page. The following operations are supported: Auto refresh: Auto refresh is disabled by default. When this function is enabled, you can set the automated refresh time range and refresh frequency. View event details: Click an event name to view the event details and handle the event. For details, see Viewing Event Details. Export event information: Click Export to directly jump to the offline exported task management list page. For details, see Managing Exported Tasks. Quick assessment: Click Quick Assessment in the Operation column to view the basic information, payload, request body, and response body of the corresponding event. For attack identification events, you can view only basic information. In addition, quick operations including Allowlist, One-Click Response, and Assessment Result are supported. Event handling: For more information, see Bulk Handling.

Operations Scenario Tab

In the upper-right corner of the **Event Assessment** page, click  to add the **Operations Scenario** Tab. After the **Operations Scenario** tab is added, the operations scenario list is displayed. [Table 5-5](#) describes the supported operations.

Table 5-5 Operations scenario operations

Operation	Description
Search for operation scenarios	Fuzzy query of scenario name or rule ID is supported. Multiple IDs are separated by the commas.
View operations scenario details	Hover over the ... at the end of the rule details, and all rule IDs for the scenario are displayed.
Delete/Bulk delete operations scenarios	You can delete/bulk delete operation scenarios.
Import operations scenarios	- Click Import to download an operations scenario template. - Open the template and fill in the operations scenario information as required. Save the template in XLS format. - Click Import to upload the operations scenario file.
Export operation scenarios	Click Export to export the current operations scenario query results as an XLS file.

Viewing Event Details

Click the event name and go to the event **Details** page, as shown in [Figure 5-4](#).

[Table 5-6](#) describes the displayed contents and supported operations of the **Details** page. Events whose details have been viewed are displayed in grey in the O&M event list on the **Event Assessment** page.

Figure 5-4 Event details page

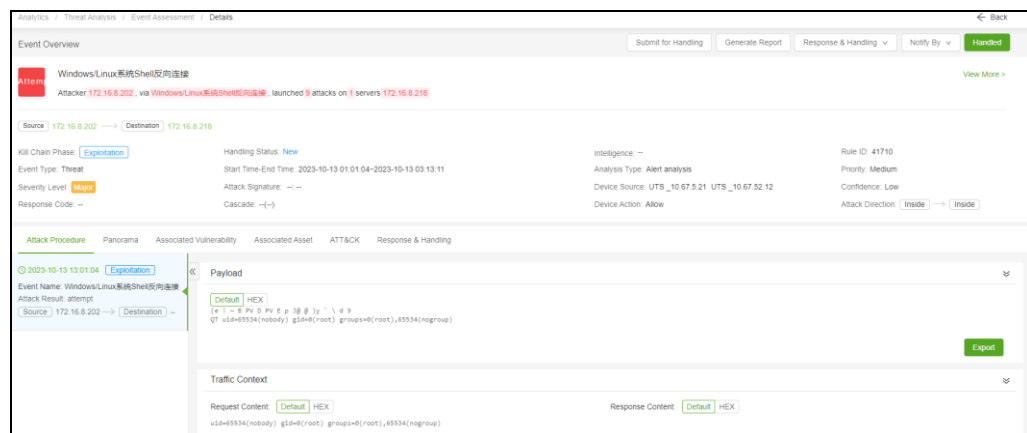


Table 5-6 O&M event details

Displayed Item	Description
Event Overview	Displays basic information of the event, including the attack status, event name, event description (IP address of the attacker, attack mode, attack times, IP addresses and quantity of the victims), and attack information. Click View More to view details of the event. On the Details page, key information is highlighted by color. Hovering over the key information shows the complete information.
Attack Procedure	The attack time, attack type, event name, attack result, IP address of the attacker, and IP addresses of the victims are displayed in the left pane of the page. The content displayed on the right side of the page and supported operations are as follows: • Payload: In addition to viewing attack payload, click Export to download the payload. • Traffic Context: includes request content and response content. • Alert Log: displays alert log details in a list. If the source or destination IP address is an external IP address, the corresponding national flag and country/region name are displayed. - Click + to view the traffic Log List. - Click More to go to the Analytics > Attribution > Log Query page to carry out advanced searches for the event's logs. For more information, see Querying Logs. • Intelligence Extension: displays information of relevant intelligence if the event hits the intelligence database, including the threat index, severity level, threat type, and update time. • Further Investigation: displays investigation information from different perspectives. The information displayed varies depending on the event type. - Event View: displays the alert log type. Click the event type to go to the Analytics > Threat Analysis > Event Assessment page to view all similar attack events. - Attacker View: displays the attacker's IP address. Click the address to go to the Analytics > Threat Analysis > Event Assessment page to view all the attacker's attack events. - Victim View: displays the victim's IP address. Click the address to go to the Analytics > Threat Analysis > Event Assessment page to view all attacked events of the victim. - Asset Perspective: displays the asset name. Click the asset name to go to the Analytics > Threat Analysis > Event Assessment page to view all attack events of the asset. When the event looks like an attack, with related signatures in the payload, request body, or response body, these signatures are highlighted in the payload, request body, or response body.
Panorama	Illustrates the specific location of the event in the seven-phase kill chain.
Associated Vulnerability	Displays the vulnerability information associated with the event. An empty list means that no matching vulnerability has been found.
Associated Asset	Displays basic asset information and asset risk alerts associated with the event. An empty asset risk alert list means that the matched asset has not been scanned for vulnerabilities and no vulnerability information about the asset is available.

Displayed Item	Description
	You can click Fast vulnerability scan to go to the Vulnerability > Scanning Task Management page to create a new scanning task. For more information, see Scanning Tasks .
ATT&CK	Displays the attacker tactics and technical knowledge base associated with the event.
Response Handling &	Displays the response and handling recommendations and the handling history of the event.
Event handling operations	Click buttons in the upper-right corner of the page to handle the event: • Submit for Handling: Set the threat level, handling status, responsible person, and description of the event, and upload attachments as required. • Generate Report: Generate an O&M report in Word format for the current event and download it to a local disk drive automatically. • Response & Handling: The following response handling modes are supported. - One-Click Response: Create a response task for the current event. For details, see Adding a Response. - Generate Ticket: Create a new ticket for this event, see Creating a Ticket. - Allowlist: Customize an allowlist based on the event assessment information and add it to the global allowlist, see Creating a New Whitelist. - Assessment Result: Add an assessment result label to the event. This label will be displayed in the event basic information. Assessment results can be False Positive, Real Attack, or Noncompliant Operation. • Notify By: The event will be notified to the designated personnel by the chosen mode which can be Email or SMS. Each mode supports a maximum of 10 recipients, separated by semicolons. Before manual notification, configure the alert notification channel. For details, see Alert Notification. • Handled: Close the event.

Quick Assessment

Click **Quick Assessment** in the **Operation** column of the O&M event list. Information about the event that needs to be quick assessed is displayed in a drawer. In addition, you can add the event to the allowlist, start response by clicking **One-Click Response**, and add an assessment result label for the event. The events that have been clicked are displayed in gray on the **Event Assessment** page.

After quick assessment of the current event, click **Previous event/Next event** at the bottom of the drawer, you can quickly open the **Quick Assessment** drawer of the previous event/next event.

Viewing Event Assessment Information

Event assessment information includes basic information of the event, the assessment result, the payload, the request body, and the response body. When the event looks like an attack,

with related signatures found in the payload, the request body, or the response body, these signatures are highlighted in the payload, the request body, or the response body.

For the attack identification event, only basic event information is displayed. Click **View More** to view the event details and the supported handling operations. For details, see [Viewing Event Details](#).

Adding to Allowlist

Click **Allowlist** to customize an allowlist based on the event information and add it to the global allowlist. For details, see [Creating a New Whitelist](#).

One-Click Response

Click **One-Click Response** to create a response task for the event. See [Adding a Response](#).

Adding an Assessment Result Label

Click **Assessment Result** to add an assessment result label to the event and display it in the basic information of the event. Assessment results can be **False positive**, **Real attack**, or **Non-compliant operation**.

Bulk Handling Events

	A maximum of 10,000 events can be simulataneously selected. If there are more than 10,000 events, add limiting conditions.
---	--

Click **Event Handling** above the O&M event list to perform bulk processing on the selected events. [Table 5-7](#) describes the processing operations.

Table 5-7 Event bulk handling operation

Operation	Description
Submit for assessment	The status of the selected event changes to TBD .
Prioritize	The status of the selected event changes to TBD , and the corresponding events will be handled with priority.
Confirm	The processing status of the selected event changes to In progress .
Ignore	The processing status of the selected event changes to Ignored , and the corresponding events does not appear in the O&M event list.
False positive	The processing status of the selected event changes to False positive .
Handled	The processing status of the selected event changes to Handled and does not appear in the O&M event list.

Operation	Description
Assessment result	Add an assessment result for the event. Assessment results can be False positive , Real attack , or Noncompliant operation .

Customizing O&M Event List

In the far right of the O&M event list head, click  to set the display column of the O&M event list. **Generation Time**, **End Time**, and **Event Name** are default fields and cannot be removed.

5.3 Intelligence

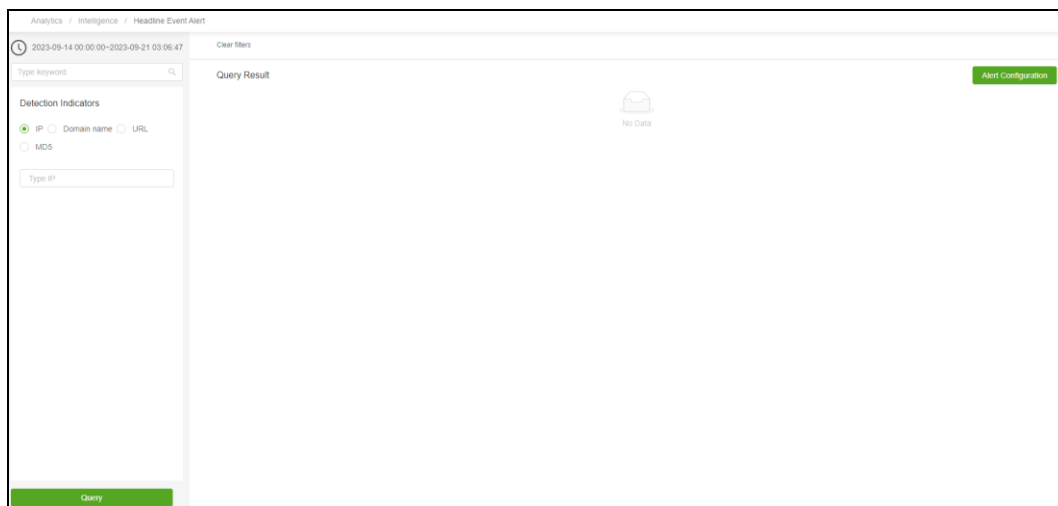
Intelligence is a collection of known information. Intelligence analysis includes **Headline Event Alert** and **Vulnerability Intelligence Alert**.

5.3.1 Headline Event Alert

Headline event intelligence refers to threat intelligence receiving high attention, with high levels of activity and risk. Such intelligence is fed by NSFOCUS Threat Intelligence (NTI).

Choose **Analytics > Intelligence > Headline Event Alert**. This page displays headline intelligences of the last month by default. You can configure a headline event alert policy or filter such intelligence for viewing, as shown in [Figure 5-5](#).

Figure 5-5 Headline event alert page



Configuring a Headline Event Alert Policy

Before configuring a headline event alert policy, email configuration is required. For configurations, see [Message Channel Configuration](#).

Querying Headline Events

On the left side of the page, query conditions can be set to filter headline events. [Table 5-8](#) describes query conditions of headline event alerts.

Table 5-8 Headline event alert query condition description

Condition	Description
Time filter	Specifies a time range when headline event alert is issued.
Keyword	Allows you to type the event name or description for query of related intelligence.
Detection Indicators	Include IP, domain, URL and MD5, which can be used as keywords to query headline events.

Viewing Headline Event Details

The right side of the page displays headline event intelligence. The displayed items include headline event name, first published time, last updated time, tag, link, description and IP/domain name/vulnerability/file/URL list. It supports to switch list display.

5.3.2 Vulnerability Alert

The **Vulnerability Alert** page provides a list of vulnerabilities and alerts, so that users can understand vulnerabilities, track vulnerability lifecycle, and take precautions.

5.3.2.1 Intelligence

Choose **Analytics > Intelligence > Vulnerability Alert > Intelligence** to view the automatically obtained vulnerability intelligence. Manual import and management operations are supported, as shown in [Figure 5-6](#).

[Table 5-9](#) describes the displayed items.

Figure 5-6 Vulnerability intelligence page

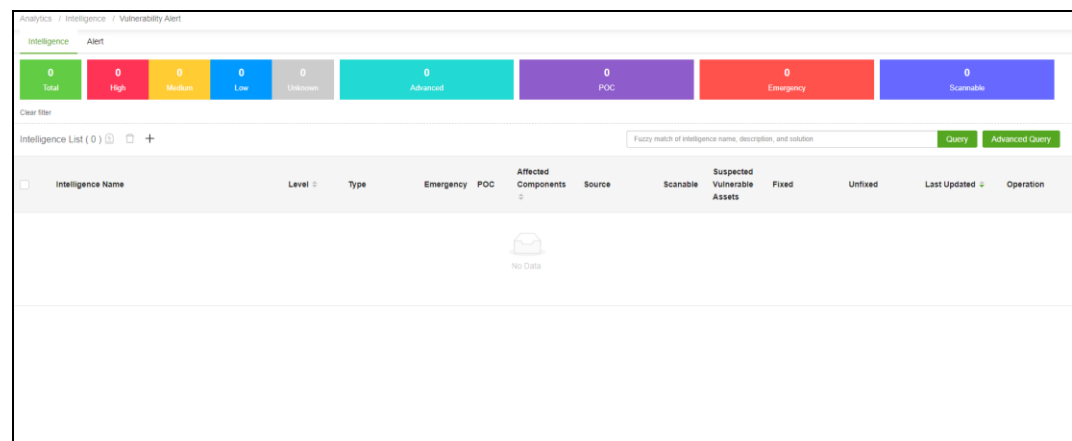


Table 5-9 Vulnerability intelligence page description

Displayed Item	Description
Vulnerability Level	In the upper part of the page shows the quantity of intelligence by vulnerability level. Clicking a vulnerability level lists intelligence of that level below.
Intelligence Type	In the upper part of the page displays the quantity of intelligence of various types. Clicking a type lists intelligence of that type below.
Query Conditions	Above the intelligence list, you can type the intelligence name, description, or solution in the search box for fuzzy query of intelligence. Click Advanced Query and set conditions to query more specific intelligence. Click More Conditions to set more query conditions.
Intelligence List	Displays vulnerability intelligence. You can perform the following operations: - View intelligence details: Click an intelligence name to view vulnerability intelligence details. For details, see Viewing Intelligence Details. - Manually import intelligence: Click  on the top of the intelligence list to manually import intelligence. For details, see Intelligence Entry. - Intelligence alert: When intelligence matches an asset, a new alert is generated. For details, see Intelligence Alert. - Bulk delete intelligence: Click  to bulk delete the selected intelligence. When the intelligence is deleted, all alerts associated with the intelligence are also deleted and cannot be restored.



- ISOP cannot access to intelligence prior to the current month.
- For instructions on NTI working with ISOP, see [Supported Components](#).

Intelligence Entry

To manually enter intelligence, follow these steps:

Step 1 On the page shown in [Figure 5-6](#), click  to open the vulnerability intelligence entry page.

Step 2 Configure basic information of vulnerability intelligence.

[Table 5-10](#) describes the configuration parameters.

Table 5-10 Vulnerability intelligence basic information parameters

Parameter	Description
Intelligence Name	Specifies the name of the intelligence. A maximum of 256 characters are allowed. The name cannot contain the following characters: ` ~ ! @ # \$ % ^ & * + = " ; , \ / ?
Intelligence Description	Enter description for the intelligence. A maximum of 2,000 characters are allowed.
Vulnerability Level	Specifies a vulnerability level for the intelligence. The values include Low , Medium , High , and Unknown .
Emergency	Selecting Yes indicates that the intelligence is of high user concern.

Parameter	Description
Disclose or Not	Selecting Yes indicates that the intelligence is publicly accessible. Non-login accounts can view the intelligence.

Step 3 Configure the advanced information of vulnerability intelligence.

Table 5-11 describes the configurable parameters.

Table 5-11 Vulnerability intelligence advanced information parameters

Parameter	Description
CVE ID/CWE ID/CNNVD ID/APACHE ID/ Bugtrap ID/ CISCO ID/X-Force ID	Type the vulnerability ID recorded in the world-famous vulnerability knowledge base. A maximum of 32 characters are allowed.
CVSS Score	CVSS score of the vulnerability. The value ranges from 0 to 10. It supports floating point numbers and is accurate to a maximum of double digits.
discovery time	Time the vulnerability is disclosed.
Vulnerability Discloser	Author who discloses the vulnerability. A maximum of 128 characters are allowed.
Affected Software	Click Add to configure the asset information affected by the vulnerability. You can add multiple assets.
POC	Whether the vulnerability has a POC.
Solution	Specific solution of the vulnerability. A maximum of 2,000 characters are allowed,
Reference URL	Fill in the reference link for vulnerability information. A maximum of 256 characters are supported. Multiple URLs are supported.

Step 4 Click **OK** to publish the vulnerability information to ISOP's vulnerability intelligence list.

----End

Intelligence Alert

After the intelligence alert operation, the intelligence is automatically matched with the asset, and the alert is generated only after the matching is successful.

- Alert one by one

Click **Alert** in the **Operation** column to perform alert operations on the corresponding intelligence.

- Bulk alert

Click  above the vulnerability intelligence list to perform bulk alert operations for the selected intelligence.

Viewing Intelligence Details

On the page shown in [Figure 5-6](#), click the intelligence name to view the details of the corresponding vulnerability intelligence.

[Table 5-12](#) describes the displayed items.

Table 5-12 Vulnerability intelligence details page description

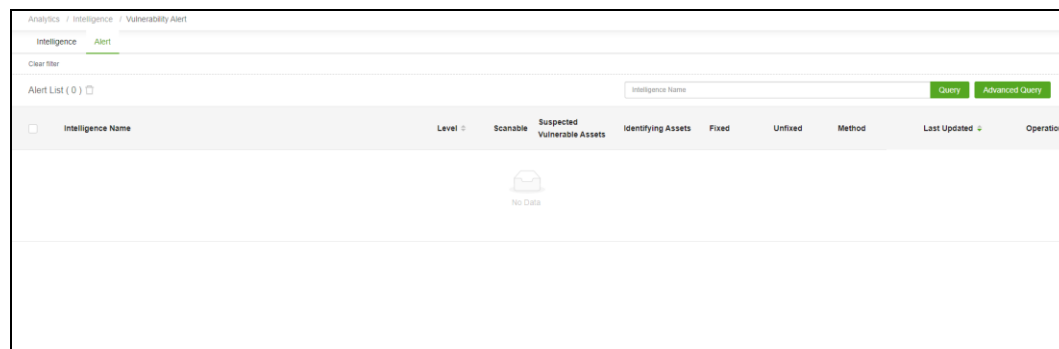
Displayed Item	Description
Life cycle	Displays basic information of vulnerability intelligence and an overview of the intelligence life cycle, where the information is highlighted in different colors. Click Update to manually update the intelligence life cycle information.
Intelligence Details	Displays vulnerability intelligence details, solutions, reference URLs, and impacted component information.
Associated Alert	Displays the Global Trend of Suspected Vulnerable Assets chart and alert list of assets affected by intelligence. Hovering over the trend chart shows the number of affected assets.
Update History	Displays update records of vulnerability intelligence.

5.3.2.2 Alert

ISOP protects assets and discovers the latest vulnerabilities and threat events in the protection target based on specific alert rules.

Choose **Analytics > Intelligence > Vulnerability Alert > Alert**. You can view alerts that match intelligence and query and delete alerts in this page, as shown in [Figure 5-7](#).

Figure 5-7 Alert page



Querying Alert Intelligences

Above the alert list, you can perform fuzzy queries by intelligence name, or click **Advanced Query** to set more criteria for querying.

[Table 5-13](#) describes the advanced query conditions for alert intelligence.

Table 5-13 Advanced query parameters of alert intelligence

Condition	Description
Alert Level	Options include High , Medium , Low , and Unknown . Multiple values are supported.
Intelligence Name	Specifies the name of the intelligence. A maximum of 256 characters are allowed.
Alert Method	Options include Intelligence update , Periodic trigger , and Manual triggering . Multiple values are supported.
Asset Name	Name of the asset. A maximum of 64 characters are allowed.
Asset IP/URL	Asset IP or URL address. A maximum of 256 characters are allowed.
Creation Time	Creation time of the alert intelligence.
Last Updated	Update time of alert intelligence.

Viewing Alert Intelligence Details

Click the intelligence name in [Figure 5-7](#) to view the details of the corresponding alert intelligence.

[Table 5-14](#) describes the displayed items.

Table 5-14 Alert intelligence details description

Displayed Item	Description
Affected Assets	Display information of assets affected by the vulnerability, including the asset name, IP/URL, asset group, state, criticality, and degree of matching. The following operations are supported: • Hover over the matching degree bar  to view the description of matching rules between vulnerability intelligence and the asset. • Click the percentage in the Degree of Matching column to view the matching information between vulnerability intelligence and the affected asset. • Click the asset name to jump to the details page of the asset. For details, Viewing Asset Details. If the vulnerability intelligence has a matching CVE ID, click  to perform scanning verification, and the verification information will be displayed in the scanning verification list.
Intelligence Details	Display vulnerability intelligence details, solutions, reference URLs, and impacted component information.
Alert History	Displays the historical alert record of the vulnerability, including last updated, suspected vulnerable assets, ok the number of assets, alert method, trigger cause.
Verification	If the vulnerability intelligence has a matching CVE ID, after the asset page is scanned and verified, the scanning and verification information will be displayed, including ID, task name, scan targets, suspected vulnerable assets, identifying assets, task status, execution count, start time, end time, and dispatched by.

5.4 Attribution

Attribution is to analyze traffic and threat-related information through normalized logs, helping users improve security analysis and response capabilities.

5.4.1 Querying Logs

ISOP provides the intelligent search function for users to query normalized logs stored on ISOP for investigation and analysis of threats.

Choose **Analytics > Attribution > Log Query**. This page displays no data by default, as shown in [Figure 5-8](#). After you set query conditions, the layout of the log statistics chart is displayed, as shown in [Figure 5-9](#).

[Table 5-15](#) describes the log query page.

Figure 5-8 Log query page (before query)



Figure 5-9 Log query page (after query)

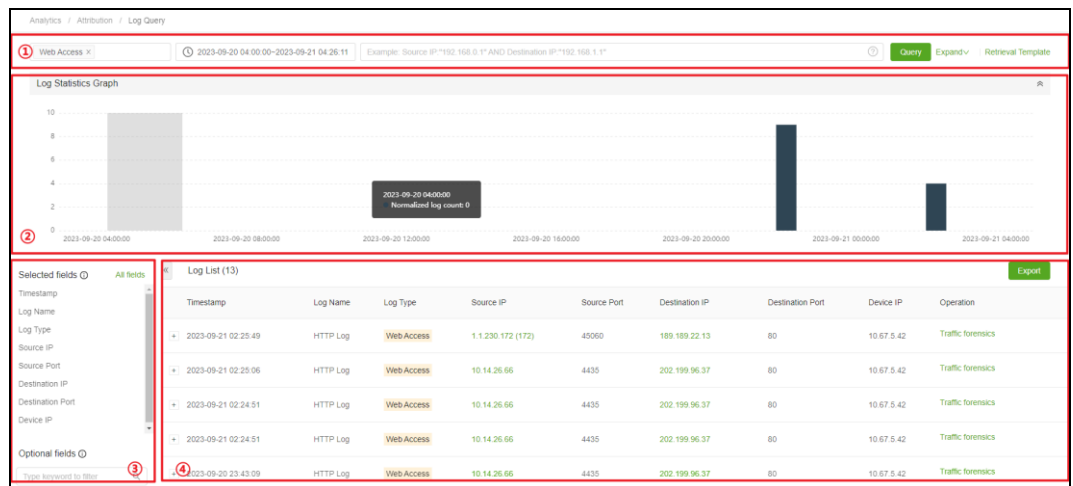


Table 5-15 Log query page layout description

Id	Area	Description
①	Log query box	- Supports common searches by log types, time ranges, and lucene query syntax. Click Expand to perform an accurate search. For details, see Log Basic/Advanced Query. - During accurate log search, click Save as Query Template to save the current query conditions as a template to facilitate subsequent search operations. Click Template to directly invoke the search template and manage it. For details, see Template.
②	Log statistics chart	Displays the time distribution of logs that match the query conditions. Hovering over the chart shows the specific time and the number of corresponding logs. Clicking  hides/displays the log statistics view.
③	Log list field configuration area	This area is divided into the display field area and hidden field area. For details, see Log List Display Fields. Clicking  hides/displays fields configuration area view.
④	Log list	Displays logs that meet the query conditions in a list. For details, see Log List. Click Export to directly jump to the offline export list interface. For details, see Managing Exported Tasks.

Log Basic/Advanced Query

You can search for logs in common and accurate modes. The search parameters are described in [Table 5-16](#).

Table 5-16 Log query parameters

Parameter		Description
Basic Query	Log type	The drop-down list contains all log types. Multiple entries are supported. If you select All , all log types are searched.
	Time range	Click the text box to select a time range. The options can be the last 1 hr , 24 hr or Custom .
	Custom query conditions	Common Elasticsearch query_string functions are supported. Supported keywords: AND OR NOT. Field names in English are supported. You can click  of the query statement to view the help description.
Advanced Query	Source IP/Destination IP	The matching mode can be Equal or Not equal. IPv4 and IPv6 are supported. The details are as follows: - IPv4 - Individual IP query, for example, 192.168.1.1. - Wildcard query, for example, 192.168.1.* 192.168.*.* 192.*.*.*.*. - IP range query, for example, 10.1.1.1-10 or 10.1.1.1-10.2.1.1. - IP address segment query, for example,

Parameter		Description
		192.168.1.1/18. - Mixed mode query, for example, 192.168.1-10.* 192.168-169.*.*. • IPV6 - Individual IP query, for example, abcd::eeee. - Single-node prefix query, for example, abcd::eeee/64. - Multiple IP addresses are separated by the comma or spaces.
	Alerting Device	The matching mode can be Equal or Not equal. Multiple values are supported. For device configuration methods, see Device List.
	URL	The matching mode can be Equal, Not equal, contain, or does not contain. Fuzzy queries are supported.
	Source/Destination Location	The matching mode can be Equal or Not equal. Select a country/region.
	Source /Destination Port	The matching mode can be Equal or Not equal. Multiple ports, separated by the comma, are allowed. The TCP port should be an integer ranging from 0 to 65535.
	Source/Target Asset	The matching mode can be Equal or Not equal. Fuzzy queries are supported. You can switch to the asset view to select assets. For the configuration method of assets and asset views, see Inventoried Asset.
	Intelligence IOC	The matching mode can be Equal or Not equal. Value options include Hit and Not Hit.
	More query conditions	Click Add to add more conditions as query conditions for accurate search.

Template

ISOP supports the reuse of log retrieval templates. You can save commonly used search scenarios for future use to reduce repetitive operations.

Saving a Query Template

Click **Save as retrieval template** to save the current query conditions as a log query template. [Table 5-17](#) describes the parameters of the log query template.

Table 5-17 Log retrieval template parameters

Parameter	Description
Query Condition	Automatically displays all query conditions for this query and do not support

Parameter	Description
	modification.
Template Name	Name of the log retrieval template.
Description	Description information of the log retrieval template.

Accessing the Log Retrieval Template List

Click **Retrieval Template** to access the list of log retrieval templates. Click **Query** in the **Operation** column to quickly retrieve the corresponding template. You can also delete log retrieval templates.

Log List Display Fields

Users can control the display content of the log list by fields. [Table 5-18](#) describes supported operations.

Table 5-18 Log list display field operation

Operation	Description
Selected fields	The selected fields are the headers of the log list, where the timestamp, log_name, log type, source IP, source port, destination IP, destination port, and device address are the default fields and cannot be removed from the selected fields. If you do not want certain fields to appear in the log list, click  next to the fields to move the fields from the selected fields area down to the optional fields area.
Optional fields	Click  next to the optional fields to move the fields up to the selected field area, which will appear in the header section of the log list.
Search fields	In the optional fields area, fuzzy search of fields is supported.
View field value list	Click a field name to display top 5 logs for that field in a horizontal bar chart.
Switch log list display mode	To display all fields in the log list, click All fields to display all fields in the log list. Click List display to restore to log list display.

Log List

Logs that meet query conditions appear in the log list. Displayed fields include the timestamp, log type, log name, basic information, source domain, destination domain, and log analysis. Click + to expand each log to view the corresponding table and JSON. In addition to viewing logs, you can also export the logs in the current list as Excel files.

In the log list, each field supports several operations. [Table 5-19](#) describes the operation icons.

Table 5-19 Log field operation icon description

Operation Icon	Description
	Add the current field to the filtering conditions of logs, with a matching method of Equal . If the icon is gray, it indicates that the current field cannot be used for searching.
	Add the current field to the filtering conditions of logs, with a matching method of not equals . If the icon is gray, it indicates that the current field cannot be used for searching.
	Add the current field to the current log list.

5.4.2 Traffic Forensics

The traffic forensics list records all traffic forensics operations performed in [Querying Logs](#).

Choose **Analytics > Attribution > Traffic Forensics**. On the left display query conditions. The traffic forensics operations that meet the conditions appear in the traffic forensics list on the right side of the page. Click **Download** in the **Operation** column to download the corresponding forensics PCAP package locally, as shown in [Figure 5-10](#).

Figure 5-10 Traffic forensics page

Analytics / Attribution / Traffic Forensics										
Traffic Forensics List (1)										
Session ID: 	No	Creation Time	Session ID	Source IP	Destination IP	Source Port	Destination Port	Protocol	Device Address	Operation
Source IP: 	1	2023-09-20 22:38:49	650bac0e095083a9010b247800	1.1.230.172	1.2.209.115	45060	80	TCP	10.67.5.42(10.67.5.42)	Download
Destination IP: 	< 1 > 10/ page Goto									
Source Port: 										
Destination Port: 										

5.4.3 Threat Hunting

Through threat hunting, users can query corresponding attack, traffic, asset, and intelligence information based on IP, URL, domain name, or MD5.

Choose **Analytics > Attribution > Threat Hunting**. The **Threat Hunting** page is empty by default. Threats can be queried through various conditions and time ranges. [Table 5-20](#) describes the query conditions.

Table 5-20 Threat hunting query conditions

Condition		Description
Time range		Options include Today , Last 24 hr , Last 7 days .
Leads	IP Lead	Supports IPv4 and IPv6 addresses. Supports filling in multiple IPs separated by the comma.

Condition		Description
	URL Lead	Multiple URLs, separated by the comma, are allowed
	Domain name Lead	Multiple domain names, separated by the comma, are allowed.
	MD5 Lead	Multiple MD5 values, separated by the comma, are allowed.

Take the IP lead as an example. Type **1.1.1.1** and click **Query**. The threat hunting result is listed, as shown in [Figure 5-11](#).

[Table 5-21](#) describes the displayed items.

Figure 5-11 Threat hunting query result

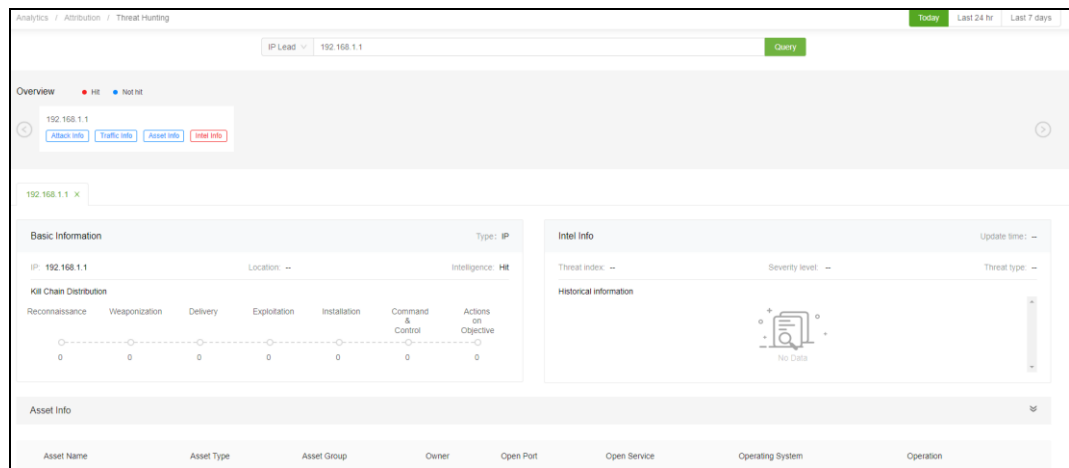


Table 5-21 Threat hunting display content (IP leads)

Displayed Item	Description
Overview	Display relevant information on attacks, traffic, assets, and intelligence that match clues: Hit: indicates that the corresponding type of information has been retrieved by red font. Not hit: indicates that the corresponding type of information has not been retrieved by blue font.
Basic Information	Displays basic information of the lead within the specified time range, including the type, IP, region, hit intelligence, and kill chain distribution.
Intel Info	Displays intelligence and historical information within the specified time range. Intelligence information includes update time, threat index, threat level, and threat type.
IP Recommendation	Displays the captured relevant threat IPs. Click an IP address to use the corresponding IP as a lead for threat hunting queries.

Asset Info		Displays asset-related information within the specified time range in a list, including the asset name, asset type, asset group, responsible person, open port, open service, and operating system. Click View Details in the Operation column to view the detailed information of the corresponding asset, including basic information, host information, service information, and application information.
Associated Attacks	Attack Path Model	Displays top 5 attack paths of the source IP and destination IP addresses associated with the lead within the specified time range in a schematic diagram.
Alert logs		Displays the alert logs associated with the lead within the specified time range. Click Log Retrieval to go to the log search page of the clue and view the detailed alert log information. For more information, see Querying Logs .
Traffic-associated information	Traffic Trend Model	The traffic associated with the lead within the specified time range is displayed in a chart.
	Session Protocol Model	Displays top 5 destination ports associated with the lead with the largest traffic volume in the bar chart within the specified time range.
	Port Model	Display TOP 5 destination ports associated with the clue with the biggest traffic volume in the bar chart within the specified time range.
	Target Outreach Model	Displays top 5 target IP addresses associated with the lead and with the biggest number of access times within the specified time range.
	Access Target Model	Displays top 5 target IP addresses associated with the lead and with the biggest access counts within the specified time range.
Traffic Logs		Displays the traffic log information associated with the lead within the specified time range. Click Log Retrieval to jump to the log search page of the thread to view the detailed traffic log information. For more information, see Querying Logs .

5.5 Report

Statistical reports include O&M report, vulnerability report, and 5GC report.

5.5.1 O&M Report

The O&M report shows statistical data of operation and maintenance responses.

5.5.1.1 Generating a Report

Choose **Analytics > Report > O&M Report**. Configure the parameters and click **Generate Report** to generate an O&M report. See [Managing O&M Reports](#) for the follow-up operations.

[Table 5-22](#) describes parameters for generating O&M reports.

Table 5-22 O&M reports generation parameters

Parameter	Description
Report Template	Select a report template. Options include O&M Report and General Threat Report .
Time Range	Select time range for the generation statistics. It supports 90 days at the most. Options for quick selection are Toady , Last 7 days , and This month .
Asset Range	When the report template is General Threat Report , you need specify the asset range for statistics. You can switch asset views. For asset views and asset configuration methods, see Inventoried Asset .

5.5.1.2 Managing O&M Reports

After the O&M report is generated, click **OK** to go to the report view page. You can query and manage all O&M report and comprehensive threat report tasks. [Table 5-23](#) describes the management operations.

Table 5-23 O&M report management operations

Report Type	Description
O&M report	Supports the following management operations: - View reports online: Click View in the Operation column to view the generated report. - Delete reports: Click More in the Operation column and select Delete to delete the report whose task ends. - Terminate report generation: When the report is being generated, click More in the Operation column and select Terminate task. The report being generated will be terminated and the generation status will change to Failed. - Export reports: Click More in the Operation column and click Export to download the report as a Word, PDF, or HTML file.
Comprehensive threat report	Supports the following management operations: - Delete report: Click More in the Operation column and select Delete to delete reports whose tasks have ended. - Terminate report generation: when the report is being generated, click More in the Operation column and select Terminate task. The report being generated will be terminated and the generation status will change to Failed. - Export report: Click More in the Operation column and click Export to export the report as a WORD file.



ISOP retains a maximum of 1,000 recently generated O&M reports.

5.5.2 Vulnerability Report

The vulnerability report reflects the current security status of the network.

5.5.2.1 Generating a Vulnerability Report

Choose **Analytics > Report > Vulnerability Report** and click **New** to configure the vulnerability report generation parameters. See [Managing Vulnerability Reports](#) for the follow-up operations. [Table 5-24](#) describes the vulnerability report generation parameters.

Table 5-24 Vulnerability report generation parameters

Parameter		Description
Type		Options include Asset Risk Report , Host Scan Comprehensive Report , Website Scan Report , Asset Discovery Report , Vulnerability Handling Report , and Password Guessing Report .
Asset Risk Report	Asset Scope	Select the asset scope for statistics. You can switch asset views. Fuzzy queries for asset views is supported.
	Report Content	The default option is Overview Information , and the optional one is Detailed Information .
	Task Name	Task name of the asset risk report, which defaults to Asset Risk Report + Asset Scope .
	Description	Description information of the asset risk report.
	Report Format	The default format is HTML and cannot be changed.
Host Scan Comprehensive Report/Website Scan Report/Asset Discovery Report	Task Selection	Host Scan Comprehensive Report: Select a system scanning task to generate a report. For system scanning tasks, see Creating a System Scanning Task. Website Scan Report: Select a website scanning task to generate a report. For website scanning tasks, see Creating a Website Scanning Task. Asset Discovery Report: Select an asset discovery task to generate a report. For asset discovery tasks, see Creating an Asset Discovery Task.
	Task Name	Task name for the Host Scan Comprehensive Report/Website Scan Report/Asset Discovery Report which defaults to the same name as the selected task.
	Description	Description information of the host scan comprehensive report, website scan report, or asset discovery report.
	Report Format	The default format is HTML , and the EXCEL option is available.
Vulnerability Handling Report	Handling Status	Select the status of the vulnerability handling for statistics. Multiple values are supported.
	Asset Scope	Select the asset scope of vulnerability handling for statistics. You can switch asset views. Fuzzy queries for asset views are supported.
	Start/End Time	Specify the time range for vulnerability handling.

Parameter		Description
	Task Name	Name of the vulnerability handling report task, which defaults to Vulnerability Handling Report + Asset Scope .
	Description	Description information of the vulnerability handling report.
	Report Format	The default format is HTML and cannot be changed.
Password Guessing Report	Task Selection	Select a password guessing task to generate a report. For details on password guessing tasks, see Creating a Password Guessing Task .
	Task Name	Task name of the password guessing report, which defaults to the same name as the selected task.
	Description	Description information of the password guessing report.
	Report Format	Default HTML , with EXCEL option available.

5.5.2.2 Managing Vulnerability Reports

After the vulnerability report is generated, you can download, query, delete it, and view task details. The format of the vulnerability report download is determined by the originally set format.

5.5.3 5GC Report

The 5GC report shows the threat situation of the 5G mobile network core.

5.5.3.1 Generating a 5GC Report

Choose **Analytics > Report > 5GC Report**, configure the 5GC report generation parameters, and click **Generate Report** to generate a 5GC report. [Table 5-25](#) describes parameters for generating a 5GC report.

Table 5-25 5GC report generation parameters

Parameter	Description
Report Template	Select a report template. Currently only the 5GC threat statistics report is supported.
Execution Mode	Once: Execute the task immediately after a task is created. Periodic execution: Execute the task periodically based on the set frequency.
Time Frame	Specify the time range when the Once mode is selected. The largest time span is 6 months. Quick selection options include Today , Last 7 days , and This month .
Frequency	When the Periodic execution mode is selected, three types of reports are supported: Daily report: The report of the previous day is automatically generated every day at 3:00 AM. Weekly report: The weekly report of the previous week is automatically generated every at 3:00 a.m Monday. Monthly report: The monthly report of the previous month is automatically generated at 3:00 a.m. on the first day of each month.

Parameter	Description
Asset Scope	The default value is Whole and cannot be changed.

5.5.3.2 Managing 5GC Reports

After a 5GC report is generated, click **View** in the report list to view the report. You can also manage 5GC report tasks.

[Table 5-26](#) describes the management operations.

Table 5-26 5GC report management operation description

Report Type	Description
5GC Threat Report	Supports the following management operations: - View reports online: Click View in the Operation column to view the generated reports. - Delete report: Click More in the Operation column and select Delete to delete the report whose tasks end. - Terminate report generation: when the report is being generated, click More in the Operation column and select Terminate task. The report being generated will be terminated and the generation status will change to Failed. - Export report: Click More in the Operation column to export the report as a Word file.

5.6 Managing Exported Tasks

Choose **Analytics > Exported Task Management** to view the events or log tasks that have been executed the export operation, as shown in [Figure 5-12](#). You can view the specific information of the exported tasks, terminate the exported task, and download and clear the exported task files. [Table 5-27](#) describes the displayed items in the exported task list.

Figure 5-12 Exported task management page

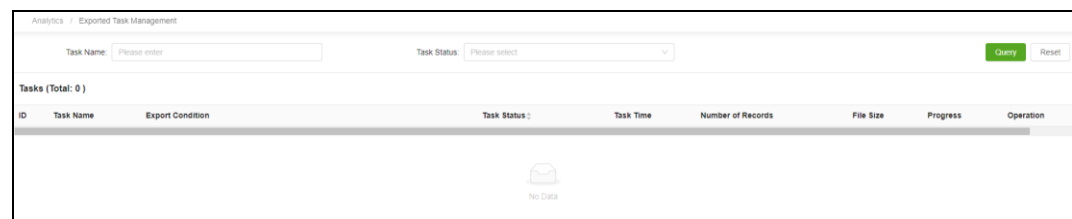


Table 5-27 Displayed items in the exported task list

Displayed Item	Description
Task Name	The task name consists of the task type and the time it was executed.

Displayed Item	Description
Export Condition	Displays the export conditions set when exporting the task.
Task Status	Displays the execution status of the task, including Pending , In progress , Successful , Failed , and Terminated .
Task Time	Start and end time of task execution.
Number of Records	Number of events exported by this task.
File Size	File size generated by the export task.
Progress	Task export progress.
Operation	Supported operations: • Terminate: Terminate the ongoing download task. • Download: Download the generated files for successfully executed tasks to the local location. • File Cleanup: Cleans the generated files of the successfully executed task from the server. • Retry: Execute the task export again.

You can click **Export** in the [Assessing an Event](#) page and [Querying Logs](#) page to jump to the **Exported Task Management** page.

6 Handling

Through the handling center, users can respond to threats manually or automatically.

This chapter contains the following topics:

Topic	Description
Manual Handling	Describes how to manage one-click response, tickets, and alert notifications for manual handling.
Auto Handling	Describes how to manage and visually orchestrate cases/playbooks for automated handling.

6.1 Manual Handling

Manual handling includes response tasks, managing tickets, and setting alert notification rules.

6.1.1 One-Click Responding

One-click response is used to handle response tasks, including adding query response tasks and viewing response history.

[Table 6-1](#) describes the default role permissions of the system.

Table 6-1 Default role permissions

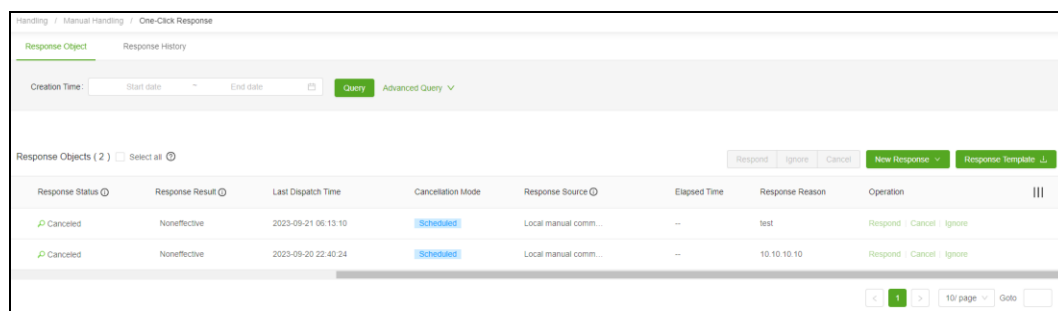
Functional Permissions		Global Permission Domain Security Officer	General Permission Domain Security Officer	Response Approver
Response object	Manually add response	√	√	×
	One-click import responses	√	√	×
	Respond/bulk respond	√	√	×
	Cancel/bulk cancel	√	√	×

Functional Permissions		Global Permission Domain Security Officer	General Permission Domain Security Officer	Response Approver
	Ignore/bulk ignore	√	√	×
Response history		√	√	×

6.1.1.1 Response Objects

Choose **Handling > Manual Handling > One-Click Response > Response Object**. This page displays the query area for manual response objects, the total number of current manual response objects, and the list of response objects, as shown in [Figure 6-2](#).

Figure 6-1 List of response objects for manual handling



Querying Response Objects

Above the response object list, you can query by **Creation Time** or click **Advanced Search** to set more query conditions. [Table 6-2](#) describes the query conditions.

Table 6-2 Response object query conditions

Condition	Description
Creation Time	Creation time of the response object.
Response Object	Name of the response object, which should be a string of up to 256 characters.
Response Result	Options include Effective and Not Effective .
Response Reason	A maximum of 256 characters are allowed.
Last Dispatch Time	Latest dispatch time of the response.
Response Source	Response trigger source. The d2drop-down selection box supports querying.
Response Device	Response device, which can be selected from the drop-down list and supports fuzzy queries.
Response Type	Options include Domain blocking , IP blocking , and Session blocking .
Creator	Creator of the response. A maximum of 256 characters are allowed.

Condition	Description
Response Status	Options include Unresponded , Responding , Failed response , Successful response , Canceled , Failed cancellation , Canceled and Ignored .
Cancellation Mode	Supports both scheduled release and manual release.

Adding a Response Manually

Point to **New Response**, click **Manual**, and configure the response parameters. Then the newly added manual response will also appear in the response object list, as shown in [Figure 6-1](#).

[Table 6-3](#) describes the response parameters.

Table 6-3 Parameters for adding a response

Parameter	Description
Response Type	Options include Session blocking , Domain blocking , and IP blocking .
Response Device	Select the corresponding response device based on the response type and support multiple selections. The response device supports a maximum of 50 devices. For the configuration method of response devices, see Instance List . Device parameters: Response Object: Up to 100 response objects can be typed. Cancellation Time: The default value 0 indicates permanent blocking. Other non-zero digits indicate scheduled cancellation.
Response Reason	Supports a maximum of 256 characters and cannot contain the following special characters: \ " ' % = ; < >

One-Click Importing a Response

To one-click import responses, perform the following steps:

- Step 1** Click **Response Template** to download the response template to a local disk drive.
- Step 2** Open the response template to a local disk drive, type the response information according to the template prompts, and save it as an XLSX file.

When response information is edited locally, Office 2019, Office 365, or WPS 2016 or above must be used.

- Step 3** Above the response objects list, click **New Response > Import**, and follow the prompts on the page to upload the saved response information file.

Only an XLSX file of no more than 5MB can be uploaded at a time.

If the file is successfully imported, the system prompts the import success.

----End

Responding/Bulk Responding

In the response object list, you can click **Respond** in the **Operation** column to block response objects with a status of **Failed response**. Besides, you can redispach response operations to the response objects with status of **Failed response/Responding/Blocking approval rejected**. You can click [Response History](#) to view the response records.

Cancelling/Bulk Cancelling

Response objects that are scheduled to be released can be cancelled one by one or in bulk before the response time expires. Choose [Response History](#) to view the release record.

- In the response object list, click **Cancel** in the **Operation** column to release the corresponding response object.
- Select multiple response objects and click **Cancel** to bulk cancel response objects. Up to 10,000 response objects can be selected simultaneously.

Ignoring/Bulk Ignoring

Support individual/bulk ignoring of response objects with a response status of **Failed Response/Blocking Approval Rejected**. Choose [Response History](#) to view the ignored records.

- In the response object list, click **Ignore** in the **Operation** column to ignore the corresponding response object.
- Select multiple response objects and click **Ignore** to bulk ignore response objects.

Customizing Response Object List

At the far right above the response object list, you can click  to select/deselect the columns to be displayed on the response object list. However, you cannot deselect the default options, including **Event Name**, **Response Object**, **Response Type**, **Response Status**, **Cancellation Mode**, and **Response Reason**.

6.1.1.2 Response History

Choose **Handling > Manual Handling > One-Click Response > Response History** to set query conditions to view all manual response history records, customize the fields to be displayed on the list, and export history query results to an XLSX file. [Table 6-4](#) describes the response history query conditions.

Table 6-4 Conditions for querying the response history description

Parameter	Description
Select Date	Start and end time of the response object.
Response Object	Name of the response object. A maximum of 256 characters are allowed.
Device Name	Name of the responding device. A maximum of 256 characters are allowed.
Response Source	Options include Local manual command , SOAR engine , Assessment operations , Predictive engine , Attacker monitoring , Attacker profile , Risky asset , and Local bulk operation .
Response Type	Options include Session blocking , Domain blocking , and IP blocking .

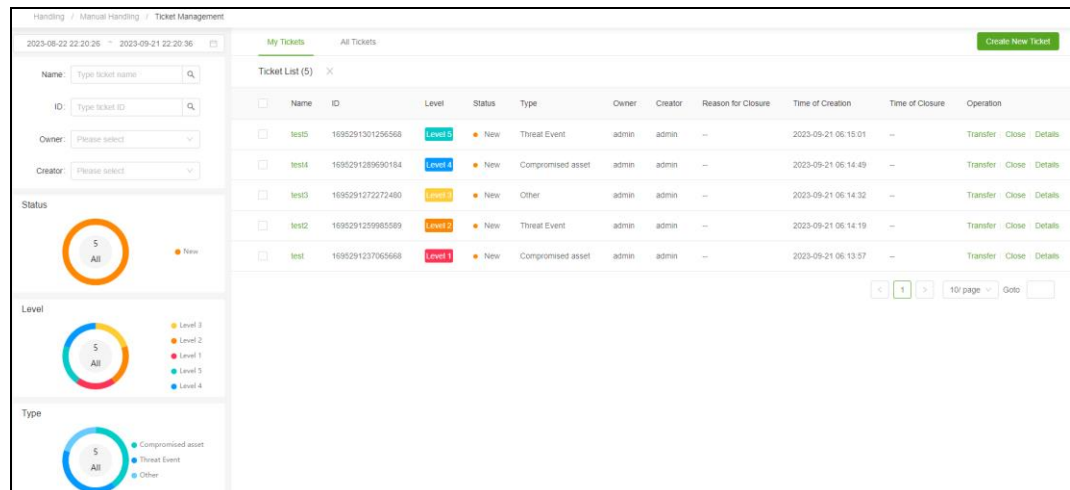
Parameter	Description
Response Status	Options include New , Successful response , Failed response , Response approved , Response disapproved , Response cancellation approved , Cancellation disapproved , Canceled , and Failed cancellation . You can select one or more options.

6.1.2 Ticket Management

A ticket refers to a service request composed of one or more tasks, which can handle security incidents discovered by users during the use of ISOP and arrange corresponding work. It is a closed-loop management process.

Choose **Handling > Manual Handling > Ticket Management**. This page displays the query conditions area for manual handling tickets, ticket statistics, and my tickets list, as shown in Figure 6-2.

Figure 6-2 Manual handling ticket management



Creating a Ticket

Click **Create New Ticket** and configure the manual handling ticket parameters to create a new manual handling ticket. The ticket owner can log in to ISOP and choose **Handling > Manual Handling > Ticket Management** page to view and dispose of the tickets. Table 6-5 describes the manual handling ticket parameters.

Table 6-5 Manual handling ticket parameters

Parameter	Description
Name	Name of the ticket. The value ranges from 3 to 32 characters and cannot contain the following special characters: # ^ @ / % = ; < > : ' \
Type	Type of the ticket. Options include Compromised asset , Threat event , and Other .
Level	Level of the ticket. Options include 5 levels. The lower the level is, the more important the ticket is. For example, if the ticket is at

Parameter	Description
	Level 1 , it indicates the highest importance.
Owner	User in the role of a security officer as the ticket owner. Multiple users are supported. Up to 10 owners can be selected for each ticket.
Notify by Email	After switching to on , the owner will receive a ticket notification email. Before enabling this function, you must make email settings, see Message Channel Configuration .
Description	Information for the ticket. Supports up to 256 characters and cannot contain the following characters #^@/% =-;<>:\
Associated Event	Click Select to add the events that require the responsible person's attention. Each ticket supports a maximum of 20 related events.

Viewing Manual Handling Ticket Details

Choose **Handling > Manual Handling > Ticket Management > My Tickets**. This page displays a ticket list with the owner being the current login user. Click the ticket name or click **Details** in the **Operation** column to view the corresponding manual handling ticket details.

Choose **Handling > Manual Handling > Ticket Management > All Tickets**. This page displays a ticket list that the current logged in user has viewing permissions. Click the ticket name to view the corresponding manual handling ticket details.

[Table 6-6](#) describes the details page.

Table 6-6 Manual handling ticket details

Displayed Item	Description
Basic information	Displays the ticket's ID , Type , Status , Age , Owner , Creator , Resting Time , and Level . The level color with different levels.
Ticket Handling	For tickets with handling permissions, the following two operations can be performed: Transfer: See Transferring a Manual Handling Ticket. Close: See Closing a Manual Handling Ticket.
Handling History	Displays the handling history of the current manual handling ticket, including Handling Time , Handler , Owner , Time taken , and Description .
Traceback – Associated Events	If the current manual handling ticket is associated with an operations and maintenance event ticket, click Details in the Operation column to navigate to the Analytics > Threat Analysis > Event Assessment page to view the details of the event for event tracing purposes. See Assessing an Event for further instructions.

Transferring a Manual Handling Ticket

Choose **Handling > Manual Handling > Ticket Management > My Tickets** and click **Transfer** in the **Operation** column. Configure the ticket transfer parameters, and then transfer the corresponding ticket to the designated owner. [Table 6-7](#) describes the parameters for transferring a manual handling ticket.

Table 6-7 Manual handling ticket transfer parameters

Parameter	Description
Owner	Select the user in the role of security as the ticket owner. Multiple owners are supported. Each ticket supports the selection of up to 10 owners.
Notify by Email	After switching to on , the owner will receive a ticket notification email. To enable this function, email configuration is required. See Message Channel Configuration for the configuration.
Description	Name of the ticket. The value ranges from 3 to 32 characters and cannot contain the following special characters: # ^ @ / % = ; < > : ' \

Closing a Manual Handling Ticket

Choose **Handling > Manual Handling > Ticket Management > My Tickets** and click **Close** in the **Operation** column. Configure the ticket closing parameters to close the corresponding ticket. [Table 6-8](#) describes parameters for closing a manual handling ticket.

Table 6-8 Manual handling ticket closure parameters

Parameter	Description
Reason for Closure	Options include Resolved and Unresolved .
Description	Description for closing the ticket. It supports up to 256 characters and cannot contain the following special characters: # ^ @ / % = ; < > : ' \

6.1.3 Alert Notification

ISOP can accurately send event information to users based on the alert object, notification method, and notification frequency set in the alert notification rules.

Choose **Handling > Manual Handling > Alert Notification**. This page allows you to configure alert notification channels and customize alert notification rules.

Configuring a Notification Channel

The alert notification channel refers to the method of sending alert notifications. After you open the corresponding alert notification channel and configure basic parameters, ISOP can send alert notifications normally according to the alert notification rules. Currently, ISOP supports the following two notification channels:

- Email
- SMS

Click **Notification Channel Configuration**. Initially, the two channels are in a **Close** state.

Email

Open the Email notification channel, configure the email notification channel parameters, and click **Send Test Mail** to test whether the parameters are correct. [Table 6-9](#) describes the parameters for configuring the email notification channel.

Table 6-9 Email notification channel parameters

Parameter	Description
Domain/IP	IP address or domain name of the email server.
Sending Port	Sending port number of the Email server. The value range is 1–65535.
Sender	Sender name of the alert notification.
Sender Email	Email address of the sender of the alert notification.
Authenticate Sender	Controls whether to verify the sender's account/password.
Use Nname/Password	When Yes is selected for Authenticate Sender , fill in the user name/password for logging in to the Email server.
SSL Link	Whether the Email notification channel is encrypted for transmission.

SMS

Open the SMS notification channel, configure the SMS notification channel parameters, and click **Send Test Message** to test whether the parameters are correct. [Table 6-10](#) describes the SMS notification channel parameters.

Table 6-10 SMS notification channel parameters

Parameter	Description
URL	Interface address of the SMS operator.
Request Data Type	Identifies the sending type of the request parameter. Options include application/json , application/x-www-form-urlencoded , and multipart/form data .
Number Field Name (key value)	Field name of the mobile phone number.
Content Field Name (key value)	Field name for the SMS message content.
Check Field Key	Field name of the combined validation field.
Check Field	This field is the combination content of the verification field, including the combination method and connector of the field. The verification field key is enclosed in curly braces, and multiple keys are separated by a specified separator as required by the document and filled in the keys by the order required by the document.
Check Field Encryption Method	Specifies an encryption method for check fields, which can only be md5 currently.
Interface Request Fields	Name of field to be used for calling the interface, as indicated in the vendor's interface document. Multiple fields should be separated by the comma (mobile number field and message content field are excluded).

Parameter	Description
All Parameters (Key-Value)	Names and values of all fixed-value parameters, such as the account name and message type. Click + to add multiple parameters.
Proxy	Proxy IP and port number.

Creating a Notification Rule

To create a new alert notification rule, perform the following steps:

Step 1 Click **New**.

Step 2 Configure alert object parameters. [Table 6-11](#) describes the alert object parameters.

Table 6-11 Alert object parameters

Parameter		Description
Rule name		Name of the alert notification rule. The name cannot contain the following characters #'^@/% =;<>:\
Alert object		Only Event is supported.
Default parameters	Event Name	Used to set rules. The matching mode can be equals , not equals , contains , or not in .
	Event Type	Used to set rules. The matching mode can be equals or not equals .
	Attack Result	Used to set rules. The matching mode can be equals or not equals .
	Alerting Device	Used to set rules. The matching mode can be equals or not equals .
	Source IP	Used to set rules. The matching mode can be equals or not equals .
	Destination IP	Used to set rules. The matching mode can be equals or not equals .
	Source Location	Used to set rules. The matching mode can be equals or not equals .
	Destination Location	Used to set rules. The matching mode can be equals or not equals .
	Source Asset	Used to set rules. Supports switching asset views. The matching mode can be equals or not equals .
	Destination Asset	Used to set rules. Supports switching asset views. The matching mode can be equals or not equals .
	Confidence	Used to set rules. The matching mode can be equals or not equals .
	Intelligence	Used to set rules based on IP, URL, domain name, or MD5 matching. The matching mode can be Hit or Not hit .
	Asset Criticality	Set rules based on asset importance. The matching mode can be equals or not equals .
Custom	Common	Used to set rules. The options include Event Rule ID , Threat Level , Source

Parameter		Description
parameters	Fields	Port, Destination Port, and Event Count.
	Analysis	Used to set rules. The options include Analysis Type, Kill Chain, Attack Signature, Response Code, Load, r_body, r_body, and Attack Direction.
	Operations	Used to set rules. The options include Event Type, O&M Object, Event Handling Status, Priority, and Handling Result.



- The rule contains at least one (default or custom) condition.
- Please try to configure the rules as accurately as possible to avoid receiving a large amount of notification information.

Step 3 Configure alert notification method parameters. [Table 6-12](#) describes the parameters for configuring an alert notification method.

Before enabling the notification method, you must configure the alert notification channel, as shown in [Configuring a Notification Channel](#).

Table 6-12 Alert notification method parameters

Parameter	Description
Email	After enabling email notification, you need to configure the following parameters: • Recipient: supports multiple email addresses, separated by the semicolon. • Send Attachment: After it is enabled, email notification allows sending attachments.
SMS	After enabling email notification, you need to fill in the mobile number that receives alert short messages. You can type multiple mobile numbers, separated by the semicolon.

Step 4 Configure alert notification frequency parameters. [Table 6-13](#) describes the parameters for configuring the alert notification frequency.

Table 6-13 Alert notification frequency parameters

Parameter	Description
Notification Mode	• Real time: sends notifications in real time after the alert is triggered. • Periodic: counts the events that meet the rules within the alert cycle and sends notifications according to the configured cycle. For example, if the notification cycle is 1 hour, a bulk of alerts will be sent every hour, with data collected from the previous hour to the current time. Click Preview to support online preview of the selected notification title and details.
Cycle	When you set Notification Mode to Periodic , you need to configure the recurring frequency of sending notifications.
Notification Time	Time range for sending notifications. No notifications will be sent for events occurring not within the notification time range. When the notification time is reached, notifications will be sent for these

Parameter	Description
	events.
Apply or not	Controls whether to enable the rule.
Remarks	Description of the rule.

Step 5 Click **Complete** to save the alert notification rule.

----End

Managing Alert Notification Rules

Alert notification rules, after being created, can be queried, edited, enabled (one by one or in bulk), disabled (one by one or in bulk), and deleted (one by one or in bulk).

6.2 Auto Handling

Automated handling includes visual orchestration and case management.

6.2.1 Visualized Orchestration

By creating a case or scenario through visual orchestration, which includes multiple assessment responses (assessment and evidence collection/feature extraction/blocking and isolation/tickets/notification and alert/general scenarios, etc.), complex event response processes and tasks can be transformed into consistent and repeatable work flows, thereby achieving automated response and handling of threats.

Scripts are divided into the following categories:

- **Custom playbook:** A newly created playbook by the user.
- **Case playbook:** The case playbook is automatically generated when creating a new case.

Cases can use built-in playbooks and custom playbooks.

Choose **Handling > Automated Handling > Visualized Orchestration** to create cases or playbooks. After saving a case, it can be viewed and managed on the **Case Overview** page, see [Case Overview](#); After saving the playbook, it can be viewed and managed on the **Playbook Overview** page, see [Playbook Overview](#).

6.2.1.1 Creating a Case

Creating a case refers to the process of organizing end-to-end data sources, threat analysis, automated response, and other case processes through a visual interface.

Case Process Block Description

A case contains several process blocks, which can be generated by dragging and dropping them from the toolbox on the canvas, as shown in [Figure 6-3](#). [Table 6-14](#) describes the process block.

Table 6-14 Visualized orchestration – case process block

Process Block	Description
Start	Starting point of a case, which indicates the beginning of a case. After you drag a tool to the canvas, it will automatically appear on the canvas by default.
TRIGGER	Used to trigger the execution of a case (process). Only one trigger is supported within the same case process. There are currently two modes: - Data pattern triggering (based on O&M events/attackers) - Task mode triggering (scheduled/manual tasks)
INFORMATION ACQUISITION	Used for information supplementation, enhancement, and forensics. The built-in information acquisition includes log acquisition, intelligence acquisition, asset acquisition, and vulnerability acquisition.
RESPONSE	Used to perform a specific response action (ticket issuance, notification and alert, IP blocking, etc.).  ISOP can collaborate with the application store, thereby can expand the responses to over a hundred types. For how to obtain the application, see App Store.
SYSTEM TOOLS	Built-in system tools, including feature extraction, general playbooks, logic assessment, custom scripts, APIs, and data merging.
End	End point of a case, which indicates the end of a case. After you drag a tool to the canvas, it will automatically appear on the canvas by default.

Case Creation Method

There are two entries for creating a case:

- Entry 1: Choose **Handling > Auto Handling > Visualized Orchestration** and click **Create Case** to start creating a case.
- Entry 2: Choose **Handling > Auto Handling > Case Management > Case Overview** and click **Create Case** to start creating a case.

As shown in [Figure 6-3](#), on the left side of the visualized orchestration page is a toolbox (supporting fuzzy queries), including tools of **Trigger**, **Information Acquisition**, **Response**, and **System Tools**. Click **More** to display all tools; Click the tool icon and drag it onto the canvas to draw an automated handling case; After drawing, click **Save** to view and manage the case overview page. For the follow-up operations, see [Case Overview](#).

[Table 6-15](#) describes the tools and operation icons used in the case drawing process.

Figure 6-3 Visualized orchestration page of the auto handling case

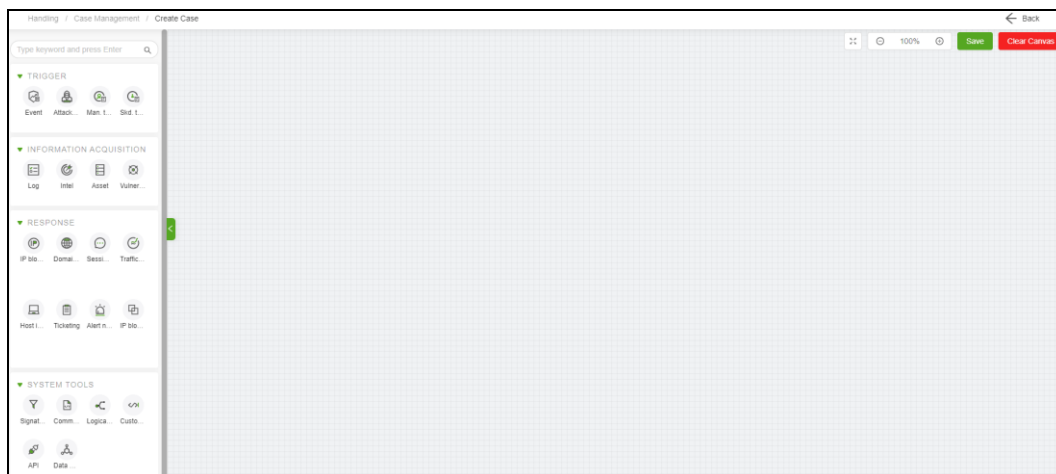


Table 6-15 Case drawing tools and icons description

Area	Icon/Button	Description
Toolkit		Collapses/Expands the toolkit area. For more tool instructions, see Case .
Canvas area	Connecting line/connection point	 Starting point of the connecting line.
		 Starting point of the upstream connecting line of the Logical decision system tool.
		 Starting point of the downstream connecting line of the Logical decision system tool.
		 Ending point of the connecting line.
		 Hover the mouse over the connecting line, and this icon appears. Then, you can click it to delete the current connecting line.
	Information Acquisition/Response/System tools	 Copies the current node.
		 Edits the current node parameters. After editing, it is necessary to reconfigure the connected downstream nodes. Other descriptions are as follows: - The Man. task trigger does not support this function. - When editing the conditions of the Logical decision system tool, you can click Log forensics Field Configuration Guide to view the configuration instructions.
		 Deletes the current node.
	Press and drag the mouse in the blank area on the canvas to move the case process as a whole.	
Operation area		Switches the canvas between full screen mode and operation mode.

Area	Icon/Button	Description
		Zooms in and out the canvas display ratio (100% by default).
	Save	Saves the case. Before performing this operation, ensure that the connecting lines, process blocks, and their configurations in the canvas are complete.
	Clear canvas	Clears the existing canvas content with one click and restore the canvas to the initial state.

6.2.1.2 Creating a Playbook

Creating a play refers to orchestrating palybooks of automated responses through a visual interface.

There are two entries for creating playbooks:

- Choose **Handling > Auto Handling > Visualized Orchestration** and click **Create Playbook** to start creating the playbook.
- Choose **Handling > Auto Handling > Case Management > Playbook Overview** and click **Create Playbook** to start creating a playbook.

The method for creating a playbook is the same as that for creating a case. For details, see [Creating a Case](#).

6.2.2 Case Management

Case management includes responses, case overview, case template, playbook execution, playbook overview, and custom script.

6.2.2.1 Case Response

Choose **Handling > Auto Handling > Case Management > Responses**. This page displays the statistical data and response list of automated handling cases, as shown in [Figure 6-4](#). [Table 6-16](#) describes the displayed items.

Figure 6-4 Automated handling case response page

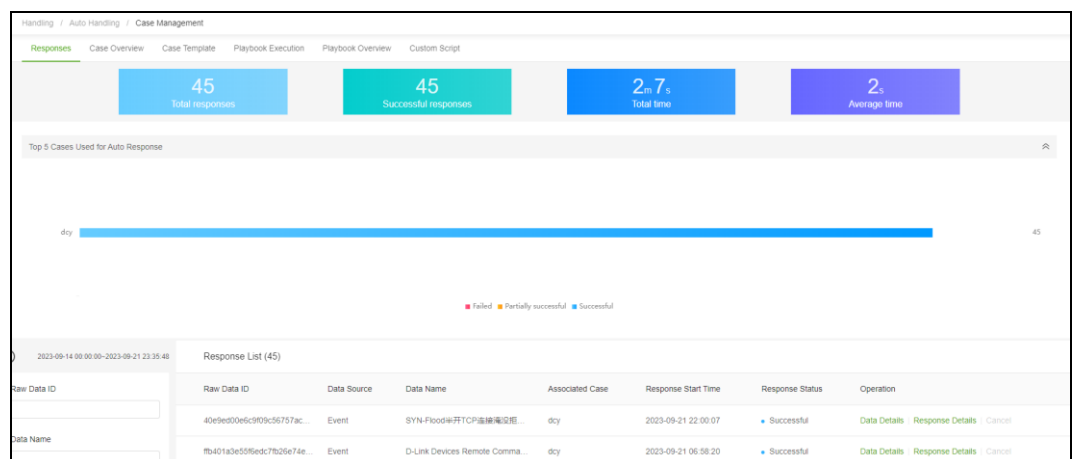


Table 6-16 Automated handling case response page description

Displayed Item	Description
Automated handling case response overview	The top of the page displays the following four items: • Total responses: total number of O&M events handled by all automated handling cases. • Successful responses: total number of O&M events handled successfully by automated handling cases. • Total time: total time taken for all automated handling cases to handle O&M events. • Average time: average time taken for all automated handling cases to handle O&M events.
Top 5 Cases Used for Auto Response	The bar chart shows the top 5 cases with the largest number of events in different automated handling response status. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the specific chart to view response details in a specific category. Click  to hide the statistical chart, and click again to restore it.
Automated case query conditions	The lower left of the page is the query area of the automated handling response list. You can query by Time Range, Raw Data ID, Data Name, Data Source, Response Status, Case Name or Message Body. The query conditions are displayed at the top of an automated handling response list.
Automated handling response list	Displays automated handling response information for the past 7 days by default. The list also supports the following operations: • Viewing data details: Click Data Details to go to the event details page associated with the response, where you can conduct event assessment. See Viewing Event Details for the follow-up operations. • Viewing response details: Click Response Details to view the details of the response, including response status, original data ID, associated case, response start/end time, response playbook, failed action, response flow chart and response list. For failed responses and responses in progress, both the failed action and the response list are empty. • Cancelling responses: Only responses in in progress status can be cancelled. Click Cancel to cancel the ongoing response process.

6.2.2.2 Case Overview

Choose **Handling > Auto Handling > Case Management > Case Overview**. This page displays the statistical data and case list of automated handling cases, as shown in [Figure 6-5](#). [Table 6-17](#) describes the displayed items.

Figure 6-5 Automated handling case overview

Handling / Auto Handling / Case Management

Responses

Case Overview

Case Template

Playback Execution

Playback Overview

Custom Script

4

Total cases

4

Enabled cases

0

Disabled cases

Case Name

Case Status

Associated Playbook

Case List (4)

Create Case

Case Name	Creation Time	Priority	Associated Playbook	Case Handling Result				Action with Most Failures	Status	Operation
				Total	Successful	Partially Successful	Failed			
dcy	2023-09-21 06:56:07	Medium	dcy	46	46	0	0	--		Edit Generate template Delete
Case1	2023-09-21 06:53:06	Medium	Case1	0	0	0	0	--		Edit Generate template Delete
test2	2023-09-21 06:44:51	Medium	test2	0	0	0	0	--		Edit Generate template Delete
test1	2023-09-21 06:34:04	Medium	test1	0	0	0	0	--		Edit Generate template Delete

<

1

>

1/1 page

Goto

Table 6-17 Automated handling case overview page description

Displayed Item	Description
Automated handling case overview	The top of the page displays the following three items: Total cases: Total number of automated handling cases. Enabled cases: Total number of currently enabled automated handling cases. Disabled cases: Total number of currently disabled automated handling cases.
Query conditions for automated handling case list	On the left side of the page is the query area for automated handling cases. The query conditions include Case Name, Case Status, and Associated Playbook which are displayed at the top of the automated handling case list.
List of automated handling cases	By default, all automated handling case information is displayed. Supported operations include: - Creating a case: Click Create Case to enter the Create case page, see Case Creation Method. - Enabling/disabling a case: Controls the status of the case. - Editing a case: Redraw the corresponding case. - Deleting a case: Delete the corresponding case. - Generating a template: Automatically generate a case template for the corresponding case. See Case Template for subsequent operations. - Executing a case: Manually trigger the corresponding case.

6.2.2.3 Case Template

For common reusable orchestration scenarios, users can generate templates from existing cases.

Choose **Handling > Auto Handling > Case Management > Case Template**. This page displays statistical data and a list of automated handling case templates, including built-in templates and custom templates, as shown in [Figure 6-6](#). [Table 6-18](#) describes the displayed content.



Built-in case templates cannot be deleted or exported.

Figure 6-6 Automated handling case template page

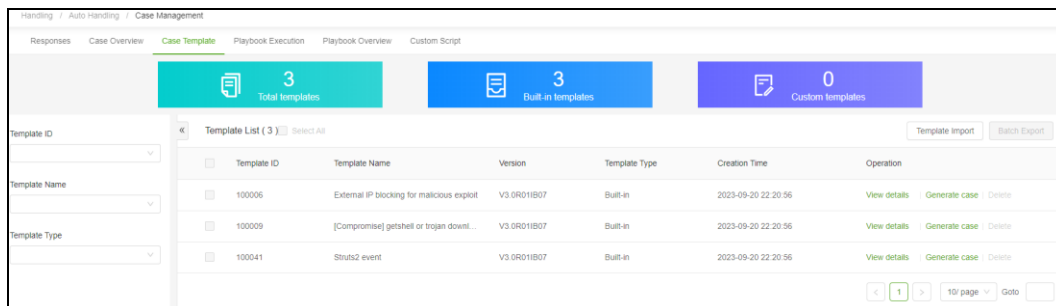


Table 6-18 Automated handling case template page description

Displayed Item	Description
Automated handling case template overview	The top of the page displays the following three items: Total templates: total number of current automated handling case templates. Built-in templates: total number of built-in automated handling case templates. Custom templates: total number of custom automated handling case templates.
Query conditions for automated handling case template	On the left side of the page is the query area for the automated handling case templates. The query conditions include Template ID, Template Name, and Template Type which are displayed at the top of the automated handling case template list.
Automated handling case template list	By default, all automated handling case template information is displayed, and the following operations are supported: - Viewing template details: Click View details to display the corresponding case template flowchart. - Generating a case: Click Generate case to enter the Create Case page, where you can draw and save the current case template as a case. For details, refer to Case Creation Method. - Importing a template: Click Template Import to import a custom case template (Only one DAT file of no more than 10 MB can be imported at a time). - Exporting a template: Only custom case templates can be exported one by one or in bulk. - Deleting a template: Only custom case templates can be deleted.

6.2.2.4 Playbook Execution

Choose **Handling > Auto Handling > Case Management > Playbook Execution**. This page displays the statistical data and automated handling case list, as shown in [Figure 6-7](#). [Table 6-19](#) describes the displayed content.

Figure 6-7 Automated handling playbook execution page

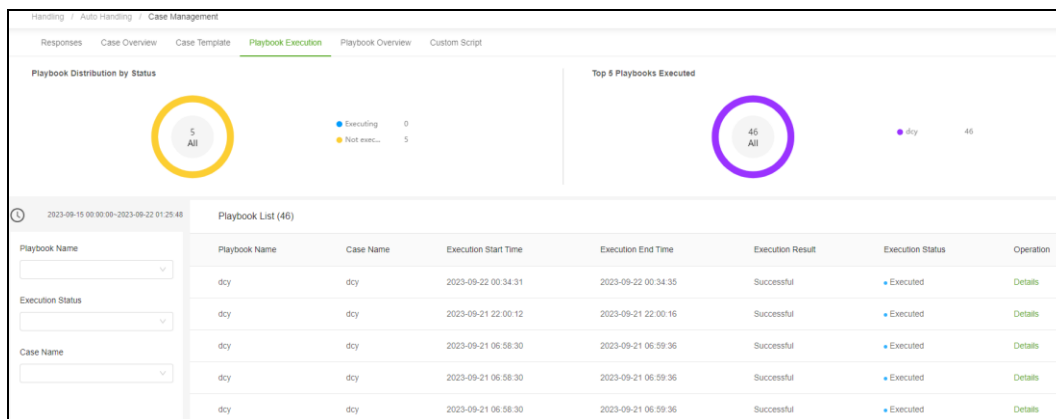


Table 6-19 Automated handling playbook execution page description

Displayed Item	Description
Playbook Distribution by Status	Displays the number of playbooks in different states and the total number of playbooks in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view execution details in a specific category.
Top 5 Playbooks Executed	Displays the top 5 executed playbooks and their execution times in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view execution times in a specific category.
Automated handling playbook list query conditions	At the bottom left of the page is the query area for the automated handling playbooks. The query conditions include Playbook Name , Execution Status , and Case Name which are displayed at the top of the automated handling list.
Automated handling playbook list	By default, the execution information of all automated handling playbooks is displayed. Click Details in the Operation column to view the execution status and results of the corresponding playbooks.

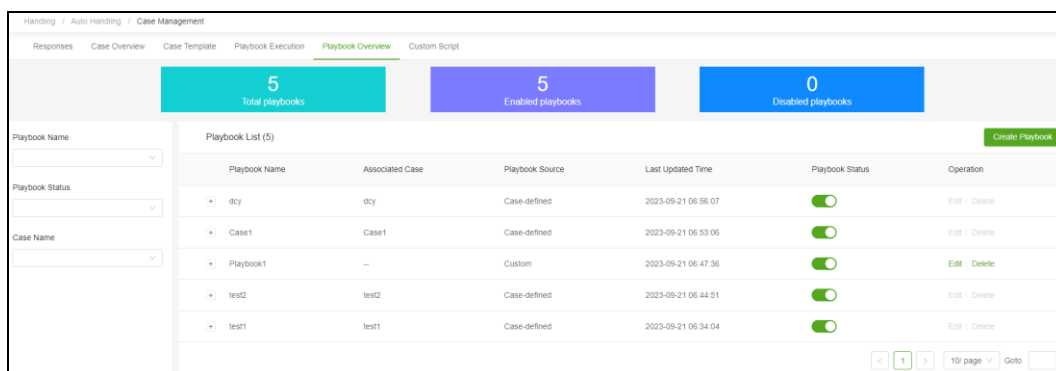
6.2.2.5 Playbook Overview

Choose **Handling > Auto Handling > Case Management > Playbook Overview**. This page displays statistical data and the automated handling playbook list, including case defined playbooks and custom playbooks, as shown in [Figure 6-8](#).

[Table 6-20](#) describes the displayed content.

	- Case-defined playbooks cannot be deleted or edited. - Custom playbook referenced by the case does not support deletion.
---	--

Figure 6-8 Automated handling playbook overview



Playbook Name	Associated Case	Playbook Source	Last Updated Time	Playbook Status	Operation
dcy	dcy	Case-defined	2023-09-21 06:56:07	Enabled	Edit Delete
Case1	Case1	Case-defined	2023-09-21 06:53:06	Enabled	Edit Delete
Playbook1	---	Custom	2023-09-21 06:47:36	Enabled	Edit Delete
test2	test2	Case-defined	2023-09-21 06:44:51	Enabled	Edit Delete
test1	test1	Case-defined	2023-09-21 06:34:04	Enabled	Edit Delete

Table 6-20 Automated handling playbook overview page description

Displayed Item	Description
Automated handling playbook overview	The top of the page displays the following three items: - Total playbooks: total number of current automated handling playbooks. - Enabled playbooks: total number of currently enabled automated handling playbooks. - Disabled playbooks: total number of currently disabled automated handling playbooks.
Automated handling playbook list query conditions	On the left side of the page is the query area for the automated handling playbook list. The query conditions include Playbook Name, Playbook Status, or Case Name which are displayed at the top of an automated handling playbook list.
Automated handling playbook list	By default, all automated handling playbook information is displayed, and the following operations are supported: - Creating a playbook: Click Create Playbook to open the playbook creating page. - Enabling/disabling a playbook: Control the status of the playbook by turning on/off the switch. - Editing a playbook: Redraw the corresponding playbook. - Deleting a playbook: Delete the corresponding playbook.

6.2.2.6 Custom Script

ISOP supports referencing custom playbooks in cases, and script input parameters can be references to upstream data.

Choose **Handling > Auto Handling > Case Management > Custom Script** and click **New** to configure the custom script parameters, which can be referenced as a system tool when creating cases or playbooks.

Table 6-21 describes the script parameters.

After creating a custom script, it can be deleted and imported more than once for editing.

Table 6-21 Custom script parameters

Parameter		Description
Basic Information	Script Name	Name of the custom script.
	Programming Language	Programming language for the custom script. Options include Python and JavaScript .
	Entry Function	Depends on the selected programming language. It cannot contain the following special characters: % " = ; < > : ' \ # ^ @ /
	Script Description	Brief description of the custom script.
Input/output Parameter Configuration	No.	Sequence number automatically assigned by ISOP, which cannot be modified.
	Name	Name of the input/output parameter.
	ID	ID of the input/output parameter.
	Type	Type of the input/output parameter. Options include string , ip , int , domain , path , raw , url , md5 , and port .
	Mandatory or Not	Control whether the corresponding input/output parameter is mandatory.
	Default Value	Default value of the input/output parameter.
	Description	Brief description of the input/output parameter.
Custom Script Import		Click  to import a script file (such as IP regular matching). Only a single DAT file is supported.

7 Asset

The Asset module provides lifecycle management of known assets, covering management of assets discovery tasks, assets to be inventoried, and inventoried assets.

This chapter contains the following topics:

Topic	Description
Asset Discovery Task	Describes how to manage asset discovery tasks.
Assets to Be Inventoried	Describes how to analyze and manage assets to be inventoried.
Inventoried Assets	Describes how to analyze and manage inventoried assets.

7.1 Asset Discovery Task

Choose **Asset > Asset Security > Asset Discovery Task**. By default, the left side of the page displays the statistical chart of asset discovery, and the right side of the page displays information on newly discovered assets in the past week, as shown in [Figure 7-1](#). [Table 7-1](#) describes displayed items.

Figure 7-1 Asset discovery task page

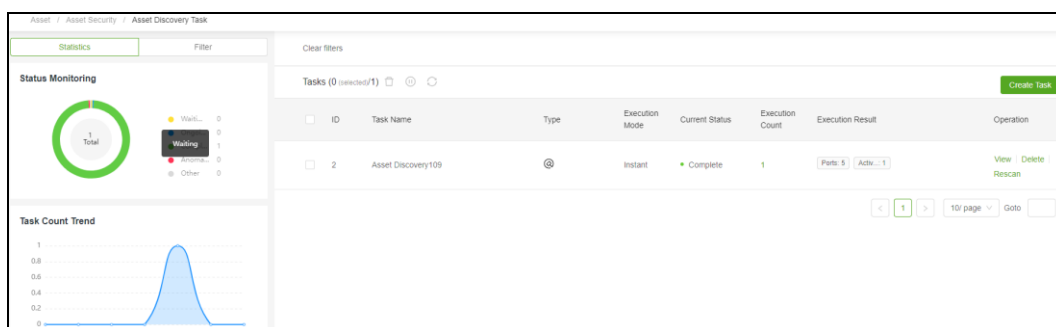


Table 7-1 Asset discovery task page description

Displayed Item	Description
Statistics	The following content is displayed on the left side of the page: Status Monitoring: displays the total number of asset discovery tasks and the

Displayed Item	Description
	number of asset discovery tasks in different status in a pie chart. Task Count Trend: displays the trend of asset discovery tasks in a chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart/chart to view data details.
Filter	You can switch the tab on the left side of the page and enter the Filter area. You can query assets by time range, task name, and task ID, and the query conditions are displayed at the top-right of the page. This area supports advanced search, with the following conditions: Status: Options include Waiting, Ongoing, Complete, Anomalous, and Other. You can select one or more options. Execution Mode: Options include Instant, Scheduled, Periodic, and Import. You can select one or more options.
Asset discovery task list	Displays asset discovery information and allows you to perform the following operations: - Creating a task: See Creating an Asset Discovery Task. - Viewing asset details: Click View in the Operation column to view the corresponding asset details, including basic information, software information, and open service information of the asset. - Deleting a task: Click Delete in the Operation column to delete the corresponding asset discovery task. Besides, you can select multiple tasks and delete them in bulk. Supports bulk deletion. - Rescanning a task: Click Rescan in the Operation column to rescan the corresponding asset discovery task. Besides, you can select multiple tasks and rescan them in bulk. You can stop ongoing scanning.

7.1.1 Creating an Asset Discovery Task

To create an asset discovery task:

Step 1 Click **Create Task**.

Step 2 Configure basic information of the asset discovery task. [Table 7-2](#) describes parameters for configuring the asset discovery task.

Table 7-2 Parameters of basic information of an asset discovery task

Parameter	Description
Task Name	Name of the asset discovery task, which cannot be empty or duplicate. A maximum of 60 characters are allowed.
Execution Mode	Instant: After the task is created, execute the asset discovery task immediately. Scheduled: The asset discovery task will be executed at a scheduled time according to the Time settings. Periodic: The asset discovery task will be executed according to the Time settings.
Time	When Execution Mode is set to Scheduled or Periodic , it is necessary to configure a

Parameter	Description
	fixed or periodic (daily, weekly, or monthly) time to execute the asset discovery task.
Target Type	Type of the discovered asset. Options include IPv4 , IPv6 , and Domain Name . Only when ISOP successfully connects to NSFOCUS Threat Intelligence (NTI) can Domain Name be selected.
Target	• Select: Click the text box and select the asset in the pop-up box. You can switch views and select one or more views. • Type: Type asset information manually. You can type multiple targets. Hover the mouse over the text box to view the format requirements.
Device	Specifies the method for executing the scanning task on ISOP. • Auto: ISOP automatically distributes tasks to scanners based on task types. • Manual: You need to select one or more scanning device connected to ISOP from the drop-down list. • NSFOCUS Threat Intelligence: This option can only be selected if ISOP successfully connects to the NSFOCUS Threat Intelligence Center (NTI).

Step 3 Configure the port and liveness configuration for asset discovery tasks.

Table 7-3 Parameters for configuring the port and status test for an asset discovery task

Parameter	Description
Scan Scope	• Standard port scan: only scans the ports corresponding to commonly used services. • Fast port scan: only scans ports 1 to 1024. • Full port scan: scan ports 1 to 65535. • Specified port scan: only scans ports within the specified range, with multiple ports separated by the comma.
Scanning Speed	The slower the scanning speed is, the more accurate the port opening information obtained is, and the longer the time it may take.
TCP Port Scan Method	• CONNECT: controls whether the port is open by directly establishing a complete TCP connection. This method is fast and accurate. • SYN: sends SYN packets to the target port, and controls whether the port is open based on whether the other party responds to the ACK message.
Host Status Test	After this function is enabled, a data packet will be sent to the target host to determine its active status based on its response, and ICMP Ping, UDP Ping, UDP Scan, TCP Ping, and TCP Ping Port need to be configured. Only active hosts can perform password guessing.
UDP Scan	Once this function is enabled, UDP ports will be scanned. Enabling UDP scanning greatly increases scanning time, so you are advised not to enable this option.
ICMP Ping	After Host Status Test is enabled, you need to choose whether to enable ICMP Ping to test the active status of the host.
UDP Ping	After Host Status Test is enabled, you need to choose whether to enable UDP Ping to test the active status of the host.

Parameter	Description
TCP Ping	After Host Status Test is enabled, you need to choose whether to enable TCP Ping to test the active status of the host.
TCP Ping Port	After TCP Ping is enabled, test ports need to be configured with multiple ports separated by the comma.

Step 4 Click **OK** to save the task.

----End

7.1.2 Managing Asset Discovery Tasks

In the asset discovery task list, you can manage asset discovery tasks one by one or in bulk. [Table 7-4](#) describes operations supported in asset discovery task management.

Table 7-4 Asset discovery task management operation

Operation	Description
View	Views online reports corresponding to asset discovery tasks, including the summary, asset list, audit logs, and task configuration.
Delete	Deletes the corresponding asset discovery task. Click  to bulk delete tasks.
Rescan	Rescans the corresponding asset discovery task. Click  to bulk rescan tasks. After you perform a rescan, the execution count increases by 1. Click the numerical link in the Execution Count column to view the historical scan records of the corresponding task.
Stop	You can stop ongoing rescanning. Click  to bulk stop rescanning.

7.1.3 Viewing the Online Report of an Asset Discovery Task

In the asset discovery task list, click **View** in the **Operation** column to view the online report of a task. [Table 7-5](#) describes the online report parameters.

Table 7-5 Online reports page of an asset discovery task

Displayed Item		Description
Summary	Basic information	Displays the scanning target, number of active hosts, scanning start and end time, and duration of this scanning task.
	Operating System Distribution	Displays the distribution of the operating system scanned in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the specific data of the corresponding operating system.
	Asset Type Distribution	Displays the distribution of asset types scanned in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the specific

Displayed Item		Description
		data of the corresponding asset type.
	Top 5 Ports	Displays the ports with top 5 occurrences in this scan in a list.
	Top 5 Services	Displays the services with top 5 occurrences in this scan in a list.
Asset List		Displays the asset information scanned this time in a list. Click View in the Operation column to view the basic information, software information, and open service information of the corresponding asset.
Audit Log		Displays the audit logs of this scanning task.
Task Configuration		Displays Basic Settings for Asset Discovery , Port Scan-related Settings , and Host Status Test-related Settings for this scanning task.

7.2 Assets to Be Inventoried

By managing assets to be inventoried, you can view and manage assets discovered in different ways. At present, the sources of asset discovery results include the following categories:

- Traffic Analysis: UTS log traffic discovery
- Discovery by Endpoints: UES Agent asset discovery
- Active Scan: RSAS asset discovery; and NTI asset discovery
- Manual Entry: assets manually entered into ISOP

 Note	• The source equipment of asset discovery includes NSFOCUS Remote Security Assessment System (RSAS), NSFOCUS Threat Intelligence (NTI), NSFOCUS Unified Threat Sensor (UTS) and NSFOCUS Unified Endpoint Security (UES). • If ISOP is required to access assets discovered by UTS log traffic, click  and choose Setting > Data Source Management. Click View in the Operation column of the isoc_uts entry and make sure the isoc_uts data source has asset log parsing rules. • If ISOP is required to access the UES Agent assets, please install the UES component package. For the installation method, see <i>NSFOCUS UES Installation and Deployment Guide</i>.
---	--

Choose **Asset** > **Asset Security** > **Assets to Be Inventoried**. By default, this page displays asset statistics and information newly discovered in the past week, as shown in [Figure 7-2](#).

[Table 7-6](#) describes the displayed content.

Figure 7-2 Assets to Be Inventoried page

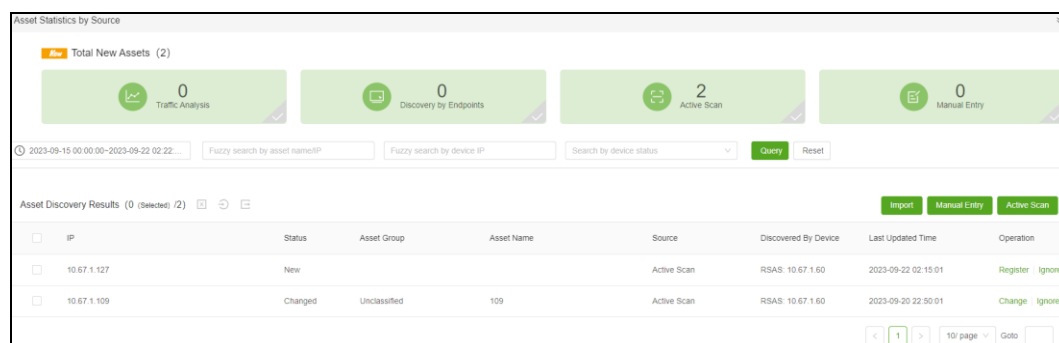


Table 7-6 Assets to be inventoried management page description

Displayed Item	Description
Asset Statistics by Source	Displays the total number of newly discovered assets and the number of newly discovered assets from the perspectives of traffic analysis, endpoint discovery, active scan, and manual entry.
Query conditions	Specifies the time range, asset name, device IP, and device status for querying an asset. ISOP supports fuzzy query by asset name.
Asset Discovery Results	Displays newly discovered asset information and supports the following operations: - Ignore: The discovered assets, once ignored, will not be managed or rediscovered. For details, see Ignor. - Register: Completes basic information for assets to be inventoried. For details, see Regist. - Manual Entry: Types the information of assets to be inventoried. For details, see Manually Typing Assets To Be Inventoried. - Active Scan: Click Active Scan to create an asset discovery task. For details, see Creating an Asset Discovery Task. - Import: Imports the information of assets to be inventoried, see Importing Assets To Be Inventoried. - Export: Click  to bulk export the asset discovery results. - Bulk inventory: Bulk import discovered assets for management. See Bulk Registering Asset.

7.2.1 Ignoring Assets

In the asset discovery results list, click **Ignore** in the **Operation** column. After confirmation, the corresponding asset can be ignored and will not be included in asset management. Furthermore, the asset will be ignored from the discovery results the next time it is discovered.

An asset, after being ignored, cannot be restored.

Click  to bulk ignore assets.

7.2.2 Registering Assets

In the asset discovery results list, click **Register** in the **Operation** column to enter the details page of assets to be inventoried. You can confirm the basic information of assets, discovery source information, and compared information, configure asset inventory parameters. Click **Register** to complete asset registration.

Table 7-7 describes asset inventory parameters.

Table 7-7 Asset registration parameters

Parameter	Description
Asset Name	Name of the asset. It supports a maximum of 30 characters and can contain spaces, tabs, and the following special characters: # - _.(): \ / + &
Asset Group/Business/Organization/Industry	Asset group/business/organization/industry to which the asset belongs. Asset Group is mandatory. For how to configure these fields, see Customizing Asset View .
Asset Criticality	Criticality of the asset. Options include Minor , Common , Important , Critical , and Core .
MLPS Level	MLPS level of the asset. For details.
Latitude/Longitude	Longitude and latitude of the asset geolocation. Longitude and latitude are separated by the comma. For format requirements, see the tooltip on the page.
Description	Brief description of the asset. It supports a maximum of 10,000 characters and can contain spaces, tabs, and the following special characters: # - _.(): \ / + &
Asset Label	Default labels are Key and Anomalous . You can add multiple labels. Click Add to customize more asset labels. A maximum of 30 characters are allowed. A label cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - _.(): \ / + &
Contact	Contact name of the asset. It supports a maximum of 30 characters and can contain spaces, tabs, and the following special characters: # - _.(): \ / + &
Contact Mobile	Only one mobile number is supported.
Contact Email	Only one email is supported.
Medium Type	Medium type of the asset. Options include Hardware device , Virtual machine , Software applications , and Other .

7.2.3 Manually Typing Assets To Be Inventoried

Click **Manual Entry**, configure the parameters of asset information to be inventoried, and click **Submit** to enter the asset information. Table 7-8 describes the parameters for manually typing asset information.

Table 7-8 Manually enter asset information parameters

Parameter	Description
Ip	Fill in the IP address of the asset. Only IPv4 is supported.
System Type	Fill in the operating system type of the asset.
System Version	Fill in the operating system version information of the asset.

7.2.4 Importing Assets To Be Inventoried

The steps to import asset information are as follows:

- Step 1** Click **Import** to enter the asset information import page and click **Download Import Template** to download the asset information template locally.
- Step 2** Open the asset information template locally, enter the asset information according to the template prompts, and save it as an **XLSX** file.
- When editing asset information locally, Office 2019, Office 365, or WPS 2016 or higher versions must be used.
- Step 3** Click **Import** above the asset discovery results list and follow the prompts on the page to upload the saved asset information file.
- Step 4** The page prompts that the bulk import is successful.

----End

7.2.5 Bulk Registering Assets

In the asset discovery results list, select the assets to be inventoried and click  to configure the asset register parameters. Click **OK** to bulk register selected assets and include them in asset management.

[Table 7-7](#) describes the bulk register parameters.



- When an asset is found to have multiple information sources, it is stored according to the following priority: **Discovery by Endpoints** > **Active scan** > **Traffic Analysis**.
- The register operation commits the asset changes corresponding to the selected asset discovery results into the asset database, and reduced assets will be deleted from the asset database.
- The register attribute is only valid for assets with a status of **New**, while the basic attributes of assets with a status of **Changed** remain unchanged.

7.3 Inventoried Assets

Choose **Asset** > **Asset Security** > **Inventoried Assets**. This page displays the statistical data and asset information of all inventoried assets, as shown in [Figure 7-3](#).

[Table 7-9](#) describes the displayed content in this page.

Figure 7-3 Inventoried assets management page

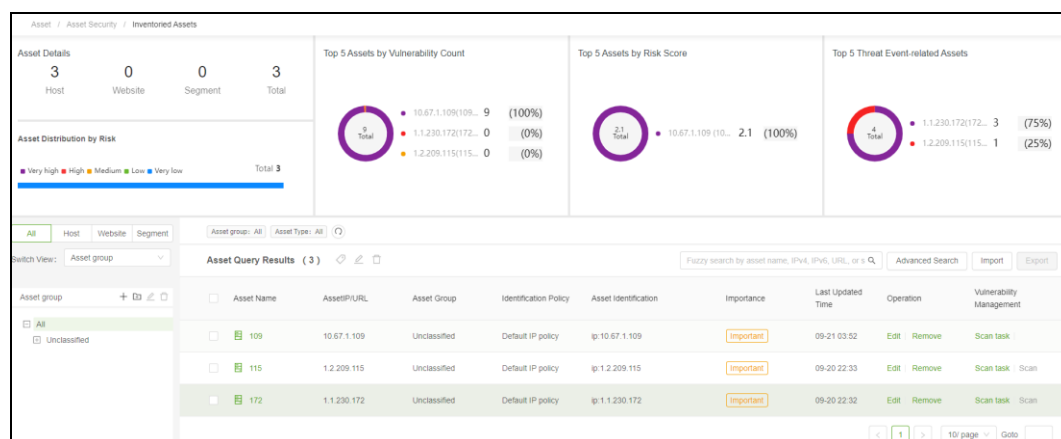


Table 7-9 Inventoried assets management page description

Displayed Item	Description
Asset Details	Displays the number of Host , Website , Segment , and Total Inventoried Assets.
Asset Distribution by Risk	Displays the risk distribution of assets in a bar chart.
Top 5 Assets by Vulnerability Count	Displays the top 5 assets with the most vulnerabilities and the total number of vulnerabilities in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the specific data of the corresponding asset.
Top 5 Assets by Risk Score	Displays the top 5 assets with the highest degree of vulnerability and the sum of vulnerability values in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the specific data of the corresponding asset.
Top 5 Threat Event-related Assets	Displays the top 5 assets with the highest number of threat events and the total number of threat events in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the specific data of the corresponding asset.
Asset Classification View	According to the asset classification view at the lower left of the page, you can filter assets according to the following classifications: - Asset type: All, Host, Website, Segment. - Asset view: Asset group, Geographic, Business, Organization, and Industry. For the configuration method of the asset view, see Customizing Asset View.
Asset List	In addition to displaying asset information of inventoried assets, the following operations are supported: - Assets query: supports fuzzy queries of asset name, IPv4, IPv6, URL, and network segments. Click Advanced Search to set more conditions for accurate asset queries. - View asset details: asset types may vary slightly in asset details. For details,

Displayed Item	Description
	refer to Viewing Asset Details. - Edit asset information: the editable asset information varies slightly depending on the asset type. See Editing Asset. - Import assets: import assets to be included in management. For details, refer to Importing Asset. - Add asset tags: click  to bulk add asset tags, with a maximum of 10,000 assets supported each time. - Asset removal/deletion: delete the asset which will no longer be included in management. For details, refer to Removing/Deleti. - Vulnerability management: issue scanning tasks to corresponding assets and view vulnerability information. For details, refer to Vulnerability Management.

7.3.1 Customizing an Asset Identification Policy

In order to solve the problem of duplicate assets, ISOP introduces an asset identification policy that can identify a unique set of properties for assets. The asset identification policy description is as follows:

- Each policy corresponds to at least one asset property.
- Each policy cannot have duplicate property fields, and the fields are displayed and used in the order they are selected.
- The relationship between properties is **And**, which means that all fields in the policy are completely consistent in the asset and log before being recognized as matching the current asset in the log.
- There cannot be a policy with the same fields.

To create a new asset identification policy:

- Step 1** Click  on the shortcut toolbar of ISOP and choose **Setting > Asset Setting** to display the built-in asset identification policy. The **Default domain policy** and the **Default IP policy** are enabled by default and cannot be disabled or deleted.
- Step 2** Click **Add Policy** to configure asset identification policy parameters, and you can customize the new policy based on actual scenarios. [Table 7-10](#) describes the asset identification policy parameters.

Table 7-10 Asset identification policy parameters

Parameter	Description
Policy Name	Name of the asset identification policy. Cannot have the same name as an existing policy. The name supports a maximum of 30 characters and cannot contain the following characters: "% =<>:\.
Asset Field	Select the asset fields to be identified by this policy. Cannot duplicate asset fields with other policies. Multiple values are supported.
Status	Choose whether to enable this policy.
Priority	The value is an integer ranging from 1 to 100. Cannot duplicate the priority of other policies.

Parameter	Description
Description	Fill in the explanatory information of the asset identification policy.

Step 3 After creating an asset identification policy, adjust the strategy status according to the actual situation. Only the enabled asset identification policy can be selected when configuring asset information.

Support the simultaneous activation of up to 10 asset identification policies. If there are more than 10 active policies, some of them need to be disabled.

----End

7.3.2 Customizing Asset Views

In the initial state, the asset view includes **Asset Group**, **Geographic**, **Business**, **Organization**, and **Industry**. The default sub group of the asset group is **Unclassified**, and switching views allows for adding and filtering assets from different dimensions.

Asset View Management Description

The root node of each asset view is **All**. Click the icon to customize the group and add new assets under the root node. [Table 7-11](#) describes the icons.

Table 7-11 Asset view management icon description

Icon	Description
	Add assets in the selected group. For specific operation methods, see Adding Assets .
	Create a first level subgroup under the root node All and a subgroup under the selected group. The configuration of subgroup parameters varies depending on the asset view. Asset group: For specific operation methods, see Customizing Asset Group and Other Views. Geographic: Select a country/region name. Business/Organization/Industry: Simply configure node names. Supports up to 10 characters and can contain spaces, tabs, and the following characters: #-_.():\+&. Cannot have the same name as an existing group under the same parent node.
	Asset group: Modify the parameters of the selected asset group. When modifying, check the parameter to synchronously apply the modification results to the sub node asset groups. Geographic: The group name does not support modification. Business/Organization/Industry: Modify the selected group name.
	Delete the selected group. The precautions are as follows: - The built-in Unclassified primary device group does not support deletion. - If the device group to be deleted contains a device, the device is moved to the Unclassified device group by default.

Customizing Asset Group and Other Views

The built-in **Unclassified** asset group does not support adding sub groups.

Click  to configure asset view parameters to add sub groups under the corresponding groups.

[Table 7-12](#) describes the asset view parameters.

Table 7-12 Asset view parameters

Parameter		Description
Asset group	Node Name	Name of the asset group. A maximum of 10 characters are allowed. Can include spaces, tabs, and the following characters: #-_.():\V+&
	Contact Person	Contact name for the asset. A maximum of 30 characters are allowed. Can include spaces, tabs, and the following characters: #-_.():\V+&
	Email	Only one email is supported.
	Mobile Number	Only one mobile phone number is supported.
	Geographic Location	Select a country/region. Please configure the geographic labels in the geographic view in advance.
	Longitude/Latitude	Longitude and latitude of the geographic location where the asset group is located. Longitude and latitude are separated by the comma. See the prompts on the page for the formatting.
	Value	Select the asset importance of the asset group. Options include Minor , Common , Important , Critical , and Core .
	Description	Description information of the asset group. A maximum of 30 characters are allowed. Can include spaces, tabs, and the following characters: #-_.():\V+&
	Device	Select the device that discovered the asset, and the asset discovered by the selected device will automatically be assigned to the asset group. Multiple values are supported. For device configuration methods, see Device Manage .
Geographical	Geographical Tag	Select a country/region.
Business	Node Name	Name of the business view. A maximum of 10 characters are allowed. Can include spaces, tabs, and the following characters: #-_.():\V+&
Organization	Node Name	Name of the organization. A maximum of 10 characters are allowed. Can include spaces, tabs, and the following characters: #-_.():\V+&
Industry	Node Name	Name of the industry. A maximum of 10 characters are allowed. Can include spaces, tabs, and the following characters: #-_.():\V+&

7.3.3 Adding Assets

Click  to add hosts, websites, or network segments in the selected group.

Taking hosts as an example, ISOP supports addition of a single host and bulk addition of hosts. To add an asset, perform the following steps:

Step 1 Configure basic information parameters of an asset.

Table 7-13 Basic information parameters of an asset

Parameter	Description
Mandatory IP	When a single host is added, options include IPv4 , IPv6 , and IPv4 & IPv6 .
IPv4/IPv6	When adding a single host, you should fill in the IP of the host.
IPv4 Range	When adding hosts in bulk, you should fill in the IP range of the hosts (only IPv4 is supported). Up to 1,000 assets can be added at a time.
Asset Name	- When adding a single host, you should fill in the host name, which cannot exceed 30 characters and can contain spaces, tabs, and the following characters: # - _ . () : \ / + & - When you add hosts in bulk, names of the hosts to be bulk inventoried are the IP addresses of the hosts by default.
Asset Group/Geographic Location/Business View/Organization/Industry	Specifies the asset group/geographic location/business view/organizational structure/industry to which the host asset belongs. Asset Group is a mandatory field. For configuration methods for asset groups and other views, see Customizing Asset View.
Asset Identification Policy	- When adding a single host asset, select an asset identification policy. Multiple values are supported. - When adding host assets in bulk, it defaults to the built-in asset identification policy and does not support selection. For the configuration method of asset identification policy, see Customizing an Asset Identification Policy.
Asset Criticality	Select the importance of the host assets. Options include Minor , Common , Important , Critical , and Core .
MLPS Level	Select the security level for the host asset.
Asset Label	The default labels are Key and Anomalous. Multiple labels can be added. Click Add to customize more asset tags. An asset label cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - _ . () : \ / + &
Longitude/Latitude	Longitude and latitude of the geographic location where the host is located. Longitude and latitude are separated by the comma. Format requirements can be seen in the pop-up tooltip.
Description	Brief description of the host. It cannot exceed 10,000 characters and can contain spaces, tabs, and the following special characters: # - _ . () : \ / + &
Proxy IP/Port	Proxy IP and proxy port of the host.
Tenant ID	Tenant ID of the host. It cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - _ . () : \ / + &
Medium Type	Medium type of the host. Options include Hardware device , Virtual machine , Software application , and Other .
Contact Person	Contact name of the host. It cannot exceed 30 characters and can contain

Parameter	Description
	spaces, tabs, and the following special characters: # - _ . () : \ / + &
Mobile Number	Only one mobile number is supported.
Email	Only one email is supported.

Step 2 (Optional) Configure the host information of a single asset. [Table 7-14](#) describes the parameters.

Table 7-14 Asset host information parameters

Parameter		Description
System Information	Operating System	Specifies the operating system for the host. You can select an option from the drop-down list or type a custom value. Only a single operating system is supported.
	Operating System Version	Specifies the operating system version number of the selected operating system. You can select an option from the drop-down list or type a custom value. Only a single version number is supported.
Device Information	Device Type	Specifies the device type of the host asset. The primary device categories include Terminal , Network device , Security device , Cloud host , and Server .
	Device Vendor	Device vendor name of the host. It cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - _ . () : \ / + &
	Device Model	Device model of the host. It cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - _ . () : \ / + &
Login Information	Login IP	Login IP of the host. Only a single IPv4 address is supported.
	Login Protocol	Specifies the network protocol for logging in to the host. Options include Samba , SSH , Telnet , and RDP .
	Login Port	Login port for the host. The value range is 1–65535.
	Login Account	Login account for the host. It cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - _ . () : \ / + &
	Login Password	Login password for the host. It cannot exceed 30 characters.
Associated Address	URL	URL of the host. Multiple URLs can be added.

Step 3 Configure service information of a single asset and click **Add** to add multiple services.

Table 7-15 Asset service information parameters

Parameter	Description
Port Number	Service port number of the host. The value range is 1–65535.

Parameter	Description
Protocol	Specifies the network protocol for this service port. Options include TCP and UDP .
Service Name	Service name of the service port. It cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - . () : \ / + &
Update Time	Specifies the update time of this service port.
Description (Banner)	Brief description of the service port.

Step 4 Configure application information of a single asset and click **Add** to add multiple applications.

Table 7-16 Asset application information parameters

Parameter	Description
Application Name	Specifies the application for the host. You can select an option from the drop-down list or type a custom value.
Application Version	Specifies the application version number based on the selected application. You can select an option from the drop-down list or type a custom value.
Vendor	Vendor name of the application. It cannot exceed 30 characters and can contain spaces, tabs, and the following special characters: # - . () : \ / + &
Description	Brief description of the application.

Step 5 Click **Create** to complete the asset addition.

----End

7.3.4 Viewing Asset Details

Click the asset name to view asset details based on different asset categories:

- Host: basic information, host information, service information, and application information.
- Website: basic information, website information, website components.
- Segment: basic information.

7.3.5 Editing Assets

When editing assets, you cannot edit URLs and asset identification policies of websites or IP ranges and asset identification policies of segments.

- Edit assets one by one
In the list of inventoried assets, click **Edit** in the **Operation** column to edit the corresponding asset.
- Bulk edit assets

Click  to bulk edit assets, with a maximum of 10,000 assets supported each time.

7.3.6 Importing Assets



When importing assets in bulk, the maximum number of assets allowed by ISOP is one million.

In addition to manually adding assets, ISOP supports bulk import of assets. To import assets, perform the following steps:

- Step 1** Click **Import** above the asset list and click **Download Import Template** to download the asset information template to a local disk drive.
- Step 2** Open the asset information template on the local disk drive, enter asset information as prompted by the template, and save the template as an XLSX file.

When editing asset information on the local disk drive, you must use Office 2019, Office 365, or WPS 2016 or above.
- Step 3** Back to the asset list, click **Import**, and follow the prompts on the page to upload the saved asset information file.

Then, the **Import data analysis** page appears.
- Step 4** Click **Next** to go to the **Import result processing** page for importing assets and configure the storage policy. The import principles are as follows:
 - a. The assets imported by the current account belong to the current account.
 - b. If assets with the same IP or URL already exist in the asset list, you can change storage policies of the assets, which will overwrite the existing asset information and properties.
 - c. If the assets/properties do not exist, the assets/properties will be created after importing
 - d. Do not delete assets that do not exist in the asset file but are already in the asset list.
 - e. For more detailed import instructions, see prompts on the page.
- Step 5** Click **Next** to go to the **Import result display** page.
- Step 6** (Optional) Click **Continue import** and repeat the above steps to import other asset files.
- Step 7** Click **Back** to return to the **Inventoried Asset** page.

----End

7.3.7 Removing/Deleting Assets

Asset withdrawal means deleting assets under inventory management to exclude the corresponding assets from management. Please remove/delete assets with caution as this operation cannot be undone.

- Remove/delete assets one by one
In the asset list of inventoried asset management, click **Remove** in the **Operation** column, and confirm to delete the corresponding asset.
- Bulk remove/delete assets
Click  to bulk delete assets, with a maximum of 300,000 assets supported each time.

7.3.8 Vulnerability Management

You can issue scanning tasks to inventoried assets and view vulnerability information in inventoried assets.

In the list of inventoried assets, click **Scan task** in the **Operation** column to create a scan task. For assets that have completed scanning, you can view vulnerability information. For how to create a scan task, see [Creating a Task](#).

8 Vulnerability

Through vulnerability management, ISOP can accurately detect various vulnerability issues in assets, including security vulnerabilities, security configuration issues, and noncompliant behaviors.

This chapter contains the following topics:

Topic	Description
Vulnerability Management	Describes how to view and manage host and website vulnerabilities.
Scanning Tasks	Describes how to create and manage scanning tasks.

8.1 Vulnerability Management

Vulnerability management is mainly aimed at network O&M personnel, providing functions such as vulnerability O&M, host vulnerability management, and website vulnerability management.

8.1.1 Vulnerability O&M

Vulnerability O&M refers to the operations and maintenance of vulnerabilities and hazard events discovered in assets.

Choose **Vulnerability > Vulnerability Management > Vulnerability O&M**. The left side of the page displays the statistical chart of asset vulnerabilities, and the right side of the page displays vulnerabilities and hazard events, as shown in [Figure 8-1](#).

[Table 8-1](#) describes the displayed content on the page.

Figure 8-1 Vulnerability O&M page

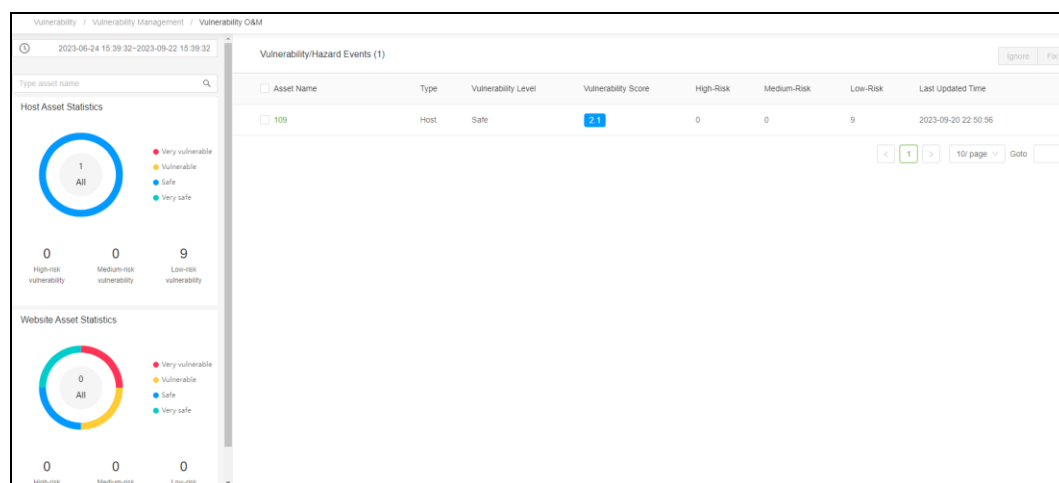


Table 8-1 Vulnerability O&M page description

Displayed Item	Description
Query conditions	You can query asset vulnerabilities/hazard events by time range or asset name.
Statistical data	The following content is displayed on the left side of the page: - Host asset statistics: displays the distribution of host assets by vulnerability level in a donut chart and the number of high-risk, medium-risk, and low-risk vulnerabilities in digits. Host asset vulnerability levels include Very vulnerable, Vulnerable, Safe, and Very safe. - Website asset statistics: displays the distribution of website assets by vulnerability level in a donut chart and the number of high-risk, medium-risk, and low-risk vulnerabilities in digits. Website asset vulnerability levels include Very vulnerable, Vulnerable, Safe, and Very safe. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to see the number of the assets in a specific category.
Vulnerability/Hazard Events	This area displays the information of host assets and website assets containing vulnerabilities. The following operations are supported: - View vulnerability handling information: Click the asset name to navigate to the vulnerability handling page for that asset. - Ignore: Click Ignore to ignore the selected vulnerability/hazard event. - Fix: Click Fix to fix the vulnerabilities in the selected vulnerability/hazard event.

8.1.2 Host Vulnerabilities

ISOP conducts statistics, analysis, and management of system vulnerabilities in host assets to reflect the vulnerability of host assets.

8.1.2.1 Asset Statistics

Choose **Vulnerability > Vulnerability Management > Host Vulnerabilities > Asset Statistics**. This page displays the information of host assets with vulnerabilities, as shown in [Figure 8-2](#).

[Table 8-2](#) describes the content displayed in the page.

Figure 8-2 Host vulnerabilities (Asset statistics)

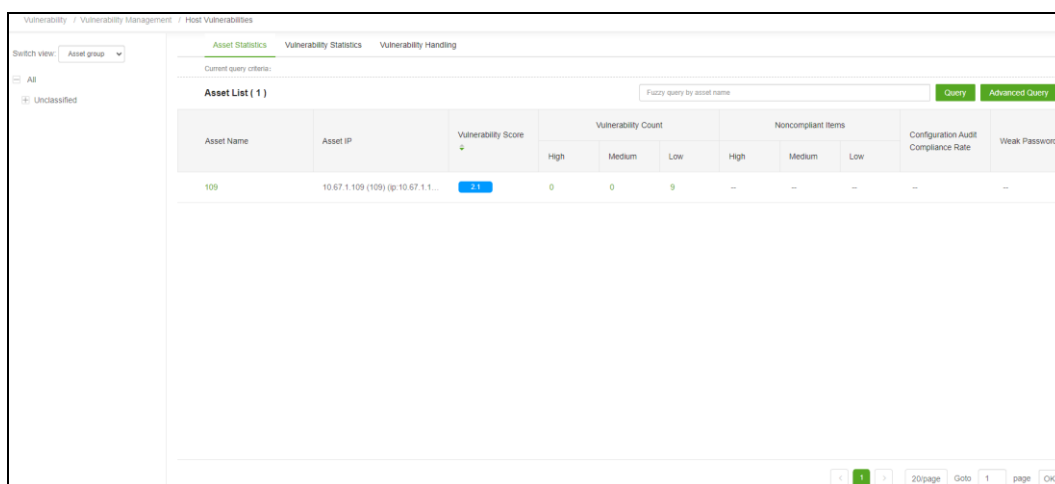


Table 8-2 Host vulnerability asset statistics page description

Displayed Item	Description
Asset view by category	You can filter assets by asset view. For the configuration method of the asset view, see Customizing Asset View .
Asset List	DisplayS asset statistics of host vulnerabilities and supports the following operations: - Query assets: ISOP supports fuzzy query by asset name. Click Advanced Query to accurately query assets by asset owner, asset IP, or asset name. - View host vulnerability details: Click the asset name to navigate to the Vulnerability Handling page and click the number in the Vulnerability Count column to navigate to the Vulnerability Handling page corresponding to the vulnerability level of the host asset. Host asset vulnerability statistics: Click the number in the Vulnerability Score column to navigate to the vulnerability assessment page of the host asset. Table 8-3 describes the detail of the page.

Table 8-3 Vulnerability details of host assets

Displayed Item	Description
Asset Analysis	Asset properties Displays the Asset Name , Asset IP , and and MLPS level of the current asset. Click the asset name to navigate to the Asset Details page, see Viewing Asset Details .

Displayed Item		Description
	Distribution Summary	Displays the distribution of current assets in the following aspects: vuln: displays the total number of vulnerabilities by risk level (high, medium, and low) in a donut chart. risk: displays vulnerability scores in a dashboard diagram. weakPwd: displays the number of existing weak passwords. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the the number of the assets in a specific category.
	Trend analysis	Displays the trend of the number of high-risk, medium-risk, and low-risk vulnerabilities and vulnerability scores of the current asset in the last 10 days, weeks or months in a line chart. Click the legend to cancel/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the number of the assets in a specific category.
	Vulnerability distribution	Uses a bar chart to display the distribution of high-risk, medium-risk, and low-risk vulnerabilities from the perspective of current asset services, application, system, threat, time, and CVE year. Click the legend to cancel/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the number of the assets in a specific category.
	Vulnerability TOP 5	Displays the top 5 vulnerabilities with the highest asset risk level in a list. Click the vulnerability name to view the corresponding vulnerability details.
	Configuration risk distribution	Displays the distribution of operating system configuration risks in current assets in a bar chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the number of the assets in a specific category.
	Configuration risk classification	Displays the compliance statistics of operating systems with asset configuration risks from the perspective of different operating systems in a bar chart. Click the legend to cancel/display the statistics of the corresponding category in the chart. Hover the mouse over the chart to view the number of the assets in a specific category.
Vulnerability Statistics		- Display s the vulnerabilities of the current assets in a list and supports fuzzy query by vulnerability name. - Click the vulnerability name to view the corresponding vulnerability details. - Click the digit in the Number of occurrences column to view the list of ports affected by the corresponding vulnerability.
Weak password statistics		Displays the vulnerable account status of the current asset application in a list and supports the following operations: - View weak passwords: Click Authentication in the Password column and type the ISOP login password. After password verification, you can view the login password of the asset. - View forensics logs: For weak passwords discovered through traffic logs, click View Forensic in the Password column to go to the log search page and view the forensics details. For the follow-up

Displayed Item	Description
	operations, see Querying Logs .

8.1.2.2 Vulnerability Statistics

Choose **Vulnerability > Vulnerability Management > Host Vulnerabilities > Vulnerability Statistics**. This page displays the vulnerability status of host assets, as shown in [Figure 8-3](#). The method for viewing vulnerability statistics is the same as that for viewing asset statistics. For details, see [Asset Statistics](#).

Figure 8-3 Host vulnerabilities (vulnerability statistics)

Vulnerability / Vulnerability Management / Host Vulnerabilities				
Asset Statistics Vulnerability Statistics Vulnerability Handling				
Current query criteria:				
Vulnerability List (7)				
Fuzzy query by vulnerability name				
Query Advanced Query				
Vulnerability Name	Vulnerability Score	Affected Assets	Occurrences	Source
ICMP timestamp Request Response Vulnerability	2.1	1	1	NSFOCUS scanner
Traceroute Detection	2.1	1	1	NSFOCUS scanner
SSL Cipher Suites Supported	2.1	1	1	NSFOCUS scanner
SSH Version Information Retrieval Vulnerability	2.1	1	2	NSFOCUS scanner
WWW Service Information Disclosure over HTTP	2.1	1	1	NSFOCUS scanner
Detection of Algorithms Supported by SSH Server	2.1	1	2	NSFOCUS scanner
SSL Encryption Protocol Detected to Be Supported by Server [Thorough Scan]	2.1	1	1	NSFOCUS scanner

8.1.2.3 Vulnerabilities Handling

Choose **Vulnerability > Vulnerability Management > Host Vulnerabilities > Vulnerability Handling**. On this page, you can handle scanned or imported host vulnerabilities, thereby achieving closed-loop vulnerability management process, as shown in [Figure 8-4](#).

[Table 8-4](#) describes the content on this page.

Figure 8-4 Host vulnerabilities (vulnerability handling)

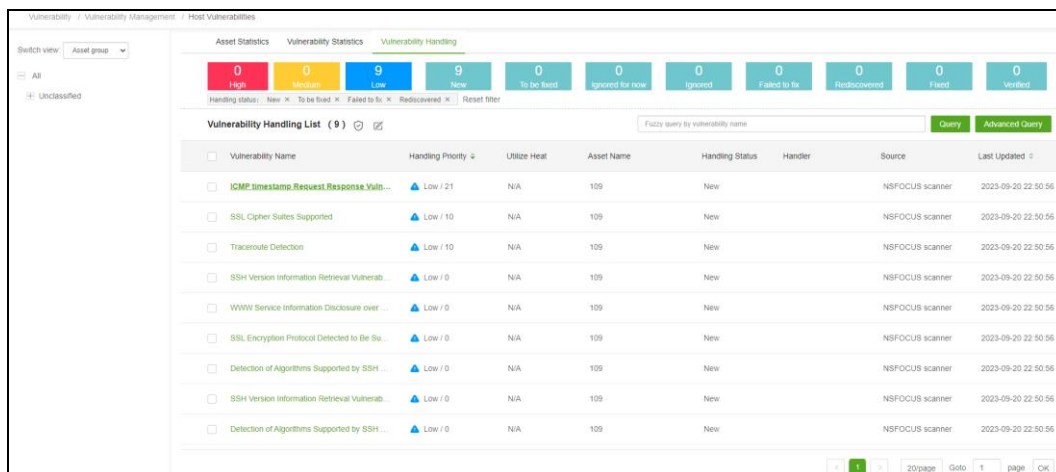


Table 8-4 Host vulnerability handling page description

Displayed Item	Description
Asset view by category	The Asset group view is displayed on the left side of the page by default and can be switched to Geographic , Business , Organization , Industry , and Device type for asset filtering. For the configuration method of the asset view, see Customizing Asset View .
Vulnerability level	The number of vulnerabilities with High , Medium , and Low is displayed above the vulnerability handling list on the right side of the page. Click a vulnerability level to perform vulnerability filtering.
Vulnerability status	The number of vulnerabilities is displayed by handling status above the vulnerability handling list on the right side of the page. Click a specific vulnerability status to filter vulnerabilities For an explanation of vulnerability status, see Vulnerability Status Description .
Query conditions	In the upper-right corner of the vulnerability handling list, fuzzy query by vulnerability name is supported. Click Advanced Query to perform a fuzzy or exact query of vulnerabilities by vulnerability name, popularity, handling priority, vulnerability level, vulnerability status, vulnerability handler, or asset IP/name.
Vulnerability handling list	Displays the vulnerability handling status of the selected asset group. Click the vulnerability name to open the vulnerability details page which supports the following operations: - View vulnerability details: see Viewing Host Vulnerability Details. - Handle vulnerabilities: Click the vulnerability name to open the vulnerability details page, on which you can handle a single vulnerability or click  to bulk handle the selected vulnerabilities. - Verify vulnerabilities: Click the vulnerability name to open the vulnerability details page, on which you can handle a single vulnerability or click  to bulk verify the selected vulnerabilities. For details, see Vulnerability Verification. - Generate tickets: see Generating a Ticket. - One-Click response: see One-Click Respon.

Vulnerability Status Description

Table 8-5 describes the vulnerability status.

Table 8-5 Vulnerability status description

Handling Status	Vulnerability Status	Description
Unprocessing status	New	When a vulnerability is first discovered, ISOP sets the status of the vulnerability to New .
	To be fixed	If a vulnerability needs to be fixed, the status of the vulnerability can be manually set to To be fixed .
	Failed to fix	If a vulnerability with the status of Fixed is discovered again during rescanning, ISOP sets the vulnerability status to Failed to fix .
	Rediscovered	If a vulnerability with the status of Verified , is discovered again during rescanning, ISOP sets the vulnerability status to Rediscovered .
Processing status	Ignored	During rescanning, ISOP will not change this status and will not calculate the risk value of the vulnerability.
	Ignored for now	After a vulnerability is ignored, the risk value of the vulnerability will not be calculated this time. If the vulnerability is found again during rescanning, ISOP will set the vulnerability status to To be fixed .
	Fixed	After completing the vulnerability repair, you can manually set the status of the vulnerability to Fixed .
	Verified	If a vulnerability with the status of Fixed , does not exist during rescanning, ISOP sets the vulnerability status to Verified .

Viewing Host Vulnerability Details

Click the vulnerability name to open the host vulnerability details page. Table 8-6 describes the content in the page.

Table 8-6 Host vulnerability details page description

Displayed Item	Description
Vulnerability information	Displays the Affected Asset , Port/Protocol , Affected Service , Source , Protection Status , Handling status , Handling Priority , Handler , Discovery Time , Update Time , and Dwell Time of the current vulnerability. Click the name of the affected asset to view the corresponding asset details.
Vulnerability description	Brief description of the current vulnerability.
Vulnerability solution	Solution to the current vulnerability.
Operation history	Displays the handling history of the current vulnerability in a list. Click the task name in the Operation Content column to view the online report of the

Displayed Item	Description
	corresponding scanning task.

Handling Disposal

You can dispose of vulnerabilities one by one or in bulk. The following just describes how to dispose of a single vulnerability.

When viewing vulnerability details, you can click **Disposal** and configure vulnerability disposal parameters to dispose of the current vulnerability. The disposal record will be automatically added to the operation history list of the vulnerability. [Table 8-7](#) describes vulnerability disposal parameters.

Table 8-7 Vulnerability disposal parameters

Parameter	Description
Handling status	Specifies a handling status from Table 8-5 .
Handler	You can assign vulnerabilities to the selected responsible person for handling through email. Before sending email notifications, you need to configure the email server and the email addresses of system users. For details, see Message Channel Configuration and User Profile .
Asset Protection	Enabling this option indicates that the asset has been protected by security devices. ISOP lowers the default priority value of vulnerability handling tickets, and the priority value will be automatically adjusted to 1 and cannot be changed.
Priority Update Mode	After disabling Asset Protection , you need to specify the priority value of the vulnerability handling ticket. Options include Automatic and Manual .
Priority Value	When Priority Update Mode is set to Manual , you need to configure the priority value, which ranges from 1 to 100.

Vulnerability Verification

Vulnerability verification means that ISOP issues a system scanning task for fixed vulnerabilities to detect the vulnerability and verify vulnerability repair status. This function is available only for vulnerabilities with the status of **Fixed**.

You can verify vulnerabilities one by one or in bulk. The following just describes how to verify a single vulnerability.

When viewing vulnerability details, you can click **Verify** and configure vulnerability verification parameters to issue a system scanning task.

[Table 8-8](#) describes the vulnerability verification parameters.

Table 8-8 Vulnerability verification parameters

Parameter	Description
Task Name	Name of the system scanning task, which cannot be empty or duplicate and cannot

Parameter	Description
	exceed 60 characters.
Target Type	Asset target type of vulnerability verification. Options include IPv4 and IPv6 .
Select Devices	Specifies the device selecting method for performing the scanning task. • Auto: ISOP automatically distributes tasks to scanners based on task types. • Manual: Select a scanning device that has been connected to ISOP from the drop-down list. You can select one or more devices.

Generating a Ticket

When viewing vulnerability details, you can click **Generate Ticket** to configure ticket parameters and then click **OK** to generate a vulnerability handling ticket. The ticket owner can log in to ISOP and choose **Handling > Manual Handling > Ticket Management > My Tickets** to manually dispose of the assigned vulnerability tickets. For how to generate and dispose of tickets, see [Ticket Management](#).

One-Click Response

When viewing the vulnerability details, you can click **One-Click Response** to configure one-click response parameters and then click **OK** to generate a response object task. Users with relevant permissions can log in to ISOP and choose **Handling > Manual Handling > One-Click Response > Response Object** to manually respond to pending tasks. For how to create response tasks and manual responses, see [Response Object](#).

8.1.3 Website Vulnerabilities

Choose **Vulnerability > Vulnerability Management > Website Vulnerabilities**. This page allows for displaying. On this page, you can see the corresponding website vulnerability details by switching asset views. The viewing method for viewing website vulnerabilities is basically the same as that for viewing host vulnerabilities, please refer to see [Host Vulnerabilities](#).

8.2 Scanning Tasks Management

Choose **Vulnerability > Scanning Task Management**. On the left side of the page displays the statistical chart of the scanning task by default, and on the right side displays the scanning task list, as shown in [Figure 8-5](#).

[Table 8-9](#) describes the displayed content in this page.

Figure 8-5 Scanning task management page

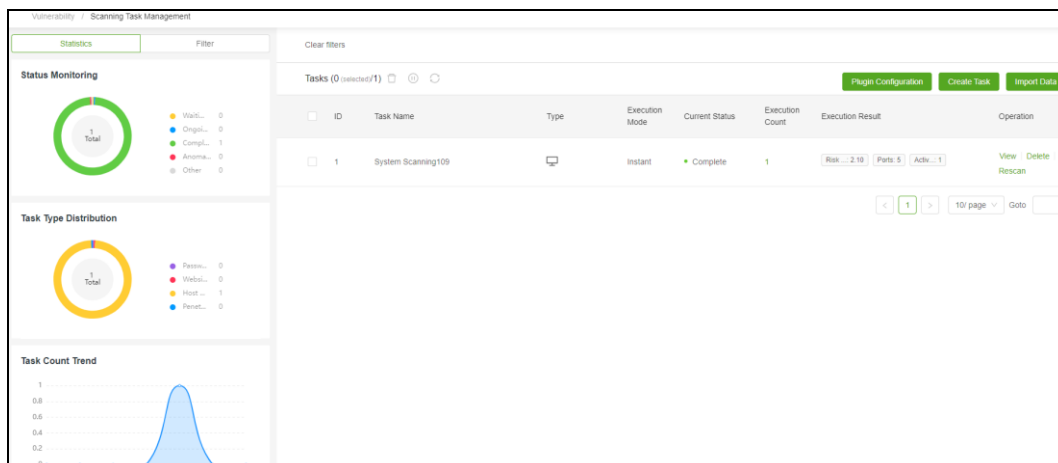


Table 8-9 Scanning task management page description

Displayed Item	Description
Statistical Data	The following three items are displayed on the left side of the page: Status Monitoring: Displays the number of scanning tasks by task status and the total number of scanning tasks in a doughnut chart. Task Type Distribution: Displays the number of scanning tasks by task types and the total number of tasks in a doughnut chart. Task Count Trend: Displays the trend of scanning tasks in an area chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the number of the assets in a specific category.
Scanning Task List	The scanning task list displays all scanning tasks and supports the following operations. Create task: Support the creation of five types of scanning tasks. For details, see Creating a Task. Import data: Support the import of scanning tasks from RSAS and WVSS and third-party vulnerability reports. For details, see Creating an Import Task. View scan results: View the scan results of tasks with the status of Complete. For tasks in other status, the scan result is empty. For details, see Viewing a Scanning Report. View historical tasks: For tasks other than Penetration Test, click the number in the Execution Count column to open the Execution Records page, where you can view and manage the historical execution of tasks. Rescan: supports rescanning of newly created scanning tasks on ISOP. Click  to bulk rescan tasks. Stop: supports stopping scanning tasks during task execution. Click  to bulk stop rescanning. Delete: After deleting the scanning task, it cannot be restored. Click  to bulk delete tasks. Configure plugin: Click Plugin Configuration to add parsing plugins from other vendors, which can be used to parse vulnerability scanning reports from

Displayed Item	Description
	these vendors. For details, see Configuring a Plugin .

8.2.1 Creating a Task

Click **New Task** to create a new task. See the following topics for methods of creating each type of scanning tasks.

- [Creating a System Scanning Task](#)
- [Creating a Password Guessing Task](#)
- [Creating a Website Scanning Task](#)
- [Creating a Penetration Test Task](#)

 Note	When creating a scanning task, multiple scanning types can be selected, as explained below: • For system scanning tasks, it supports simultaneous selection of configuration verification and password guessing. • For configuration verification tasks and password guessing tasks, only the simultaneous selection of system scan types is supported. • For website scanning task and penetration test task, it is not supported to select other scanning types at the same time.
---	--

8.2.1.1 Creating a System Scanning Task

Through system scanning tasks, ISOP can perform system vulnerability scanning and host configuration scanning on scanning targets, thereby discovering system vulnerabilities and configuration non-compliance information in assets.

Take a single task type as an example. The operation steps for creating a new system scanning task are as follows:

- Step 1** Click **Create Task** to enter the scanning task type selection page.
- Step 2** Select **System Scanning** and click **OK** to open the system scanning task creation page.
- Step 3** Configure basic information of the system scanning task.

[Table 8-10](#) describes the parameters for the system scanning task.

Table 8-10 Basic information parameters of system scanning task

Parameter	Description
Task Name	Name of the system scanning task, which cannot be empty or duplicate. A maximum of 60 characters are allowed.
Execution Mode	• Instant: After being created, the task is executed immediately. • Scheduled: executed at a scheduled time according to the time setting. • Periodic: executed according to the recurring settings.
Time	When the Execution Mode is Scheduled or Periodic , it is necessary to configure a fixed time or choose Daily/Weekly/Monthly to execute the system scanning task.

Parameter	Description
Target Type	Type of asset target scanned. Options include IPv4 and IPv6 .
Target	• Select: Click the text box and select the asset in the pop-up box. You can switch the view and select multiple assets. For asset views and asset configuration methods, see Inventoried Asset. • Type: Manually input the scanning target information. You can type multiple targets. Hover over the text box to view the formatting requirements. To manage vulnerabilities in the scanning results on ISOP, manually synchronize asset risks on the task details page after the task is completed.
Device	After the scanning device is connected to ISOP, select the method of selecting the device to execute the scanning task. • Auto: ISOP automatically distributes tasks to scanners based on task types. • Manual: Select a scanning device that has been connected to ISOP from the drop-down list. Multiple values are supported.
Login Check	Whether to perform pre-login or configuration verification on the target system. • Enable: ISOP will perform a login scan on the target host. • Disable: ISOP performs remote version scanning on the target host.

Step 4 (Optional) Configure the login parameters for the scanning target.

[Table 8-11](#) describes the parameters for configuring scanning target.

Table 8-11 System scanning task login configuration parameters

Parameter		Description
Basic Information	IP	Displays the IP address of the scanning target. It has been configured in the previous step and modification is not supported here.
	User Name/Password	Login user name and password of the scanning target.
	Login Protocol	Select the login protocol for the scanning target. Options include SMB , SSH , Telnet , RDP , and Select none .
	Port	Port number used by the remote login scanning target based on the selected login protocol. • SMB: default port number is 445. • SSH: default port number is 22. • Telnet: default port number is 23. • RDP: default port number is 3389.
	Host Jump	When the login protocol is SSH or Telnet, it is necessary to configure whether to enable host redirection. The host redirection parameters are explained as follows: • Jump Host IP: IP address of the target host for the redirection. • User Name/Password: user name and password of the target host to be redirected. • Login Protocol: protocol for logging in to the target host, with

Parameter		Description
		options such as SSH and Telnet. • Port: Port is 22 using SSH protocol for redirection. Port is 23 using Telnet protocol for redirection.
Vulnerability Scanning Policy	ORACLE	After enabling ORACLE, the following parameters need to be configured: • User Name/Password: user name and password for logging into Oracle. • Port: port used for logging into Oracle for scanning, with a default value of 1521. • SID: security identifier of the account.
WEB LOGIC Policy	WEBLOGIC	After enabling WebLogic, the following parameters need to be configured: • Operating System Type: operating system type of the host where WEBLOGIC is located. • Weblogic Version: Version information of WEBLOGIC. • WebLogic User: User name for access to WebLogic. • WebLogic WLS Path: Installation path of WebLogic WLS.

Step 5 (Optional) Configure the system parameters of the scanning target.

[Table 8-12](#) describes the system parameters.

Table 8-12 System scanning task system configuration parameters

Parameter	Description
Scheduling Priority	The scanning device will determine the execution order of scanning tasks based on the scheduling priority value and background algorithms.
Debug Mode	After being enabled, the scanning device will record the execution information of the scanning task. When the scanning task performs abnormally, the abnormal information can be exported and sent to NSFOCUS technical support personnel for error analysis.
Scanning Depth	The larger the value, the more information the scanning device may obtain and the longer the scanning time. You are advised to use the default configuration.
Dangerous Plugin Scan	Such plugins may cause system crashes or service interruptions of assets. It is usually recommended to disable this feature and only enable it in specific situations (such as product assessment).
Oracle Deep Scan	• Disable: The scanning device only reports Oracle-related service identification and principle scanning vulnerabilities. • Enable: The scanning device reports all vulnerabilities, including the aforementioned vulnerabilities and local Oracle vulnerabilities.
Key Network Device Deep Scan	When enabled, it may cause certain specific models of network devices to malfunction during scanning. Please use it with caution.
Plugin Timeout	If a single plugin does not end normally within the timeout limit of the plugin, it will

Parameter	Description
(s)	be forcibly terminated.
Socket Timeout (s)	The maximum timeout to wait when obtaining scan data from the network layer. This option has a relatively great impact on the scanning speed and accuracy. The recommended value is 5 seconds for a local area network (LAN) or 15 seconds for an asymmetric digital subscriber line (ADSL) network. Socket timeout limits can be configured based on network speed. If the network speed is slow, the socket timeout limit needs to be configured larger.

Step 6 (Optional) Configure the port and liveness parameters of the scanning target. [Table 8-13](#) describes the parameters.

Table 8-13 System scanning task port and liveness configuration parameters

Parameter	Description
Scan Scope	Standard port scan: only scans the ports corresponding to commonly used services. Fast port scan: only scans ports 1 to 1024. Full port scan: The scanned port range is 1 to 65535. Specified port scan: only scans ports within the specified range, with multiple ports separated by the comma.
Scanning Speed	The slower the scanning speed, the more accurate the port opening information obtained, and the longer the time it may take.
TCP Port Scan Method	CONNECT: determines the port's openness by directly establishing a complete TCP connection. This method is fast and accurate. SYN: sends SYN packets to the target port, and determines the port's opening status based on whether the other party responds to the ACK message.
Host Status Test	After activation, a data message will be sent to the target host to determine its liveness based on its response. Only live hosts can perform password guessing. ICMP Ping, UDP Scan, TCP Ping, and UDP Ping ports need to be configured after the activation.
UDP Scan	After being enabled, UDP ports will be scanned. Enabling UDP scanning greatly increases scanning time, so you are not advised to enable this option.
ICMP Ping	After the Host Status Test is enabled, ICMP Ping is enabled by default to test the host liveness.
UDP Ping	After the Host Status Test is enabled, you need to choose whether to enable UDP Ping to test the host liveness.
TCP Ping	After the Host Status Test is enabled, you need to choose whether to enable TCP Ping to test the host liveness.
TCP Ping Port	After TCP Ping is enabled, test ports need to be configured with multiple ports separated by the comma.

Step 7 Click **OK** to save the task.

----End

8.2.1.2 Creating a Password Guessing Task

Through password guessing tasks, ISOP can attempt to log in to the target host using a user name and password. If the login is successful, it indicates that there is a vulnerable account in the target host.

Take creating an individual task as an example. The operation steps are as follows:

- Step 1** Click **Create Task** to enter the scanning task type selection page.
- Step 2** Select **Password Guessing** and click **OK** to enter the new password guessing task page.
- Step 3** Configure the basic information of the password guessing task.

[Table 8-14](#) describes the configurable parameters.

Table 8-14 Basic information parameters of password guessing task

Parameter	Description
Task Name	Name of the password guessing task, which cannot be empty or duplicate. A maximum of 60 characters are allowed.
Execution Method	Instant: After being created, the task is executed. Scheduled: executed at a scheduled time according to the time settings. Periodic: executed according to the time settings.
Time	When the execution method is Scheduled or Periodic , it is necessary to configure a fixed time or a certain time of Daily/Weekly/Monthly to execute the password guessing task.
Target Type	The type of asset target to be scanned. Options include IPv4 and IPv6 .
Target Method	Select: Click the text box and select the asset in the pop-up box. You can switch views and select multiple assets. For asset views and asset configuration methods, see Inventoried Asset. Type: Manually input the scanning target information. You can type multiple targets. Hover over the text box to view the formatting requirements. To manage vulnerabilities in the scanning results on ISOP, manually synchronize asset risks on the task details page after the task is completed.
Device	After the scanning device is connected to ISOP, select the method of selecting the device to execute the scanning task. Auto: ISOP automatically distributes tasks to scanners based on task types. Manual: Select a scanning device that has been connected to ISOP from the drop-down list. Multiple values are supported.

- Step 4** Configure the system parameters of the scanning target.

[Table 8-15](#) describes the configurable parameters.

Table 8-15 Password guessing task system configuration parameters

Parameter	Description
Scheduling Priority	The scanning device will determine the execution order of scanning tasks based on the scheduling priority value and background algorithms.
Debug Mode	After being enabled, the scanning device will record the execution information of the scanning task. When the scanning task performs abnormally, the abnormal information can be exported and sent to NSFOCUS technical support personnel for error analysis.

Step 5 Configure the host liveness parameters for scanning targets, including the following two parts:

a. Host Status Test

Send data packets to the target host and determine whether the target is alive based on its response. Only live hosts can perform password guessing.

Enable host liveness test, select the method for liveness test. **ICMP Ping** is enabled by default. Other methods include **UDP Ping** or **TCP Ping**. If you choose **TCP Ping**, you also need to configure the **TCP Ping Port**.

b. UDP Scanning

Whether to perform UDP scanning on the target host.

Step 6 Configure password guessing parameters for scanning targets.

[Table 8-16](#) describes the configurable parameters.

Table 8-16 Password guessing task password guessing parameters

Parameter		Description
Guessing Times		Number of times password guessing is performed on a single host, with 0 indicating no limit on the number of times.
Max Concurrent Threads		Number of concurrent threads in performing the password guessing task on a single service on a single host. The value range is 1-10, and the larger the value, the faster the detection speed.
Frequency (s)		Time interval between two guesses of the same protocol password on the scanned target. The value range is 0-600 seconds.
Timeout (min)		Maximum running time of the password guessing plugin. The plugin terminates after reaching the specified time. The value range is 1-10080 minutes.
New password guessing configuration (optional)	Service Type	Service type to which the password guessing configuration belongs.
	Mode	The mode of password guessing can be either Combined or Standard .
	User Name	Target user name for password guessing.
	Password	Target user password for password guessing.

Step 7 Click **OK** to save the task.

----End

8.2.1.3 Creating a Website Scanning Task

Through website scanning tasks, ISOP can continuously crawl, analyze, and match the target site's pages based on user needs, thereby discovering web vulnerabilities in the target site.

Take a single task type as an example. The operation steps for creating a new website scanning task are as follows:

- Step 1** Click **Create Task** to enter the scanning task type selection page.
- Step 2** Select **Website Scan** and click **OK** to enter the new website scanning task page.
- Step 3** Configure the basic information of the website scanning task.

[Table 8-17](#) describes the configurable parameters.

Table 8-17 Basic information parameters of website scanning task

Parameter	Description
Task Name	Name of the website scanning task, which cannot be empty or duplicate. A maximum of 60 characters are allowed.
Execution Method	• Instant: After being created, the website scanning task is executed immediately. • Scheduled: executed at a scheduled time according to the time settings • Periodic: executed according to the time settings.
Time	When the Execution Method is Scheduled or Periodic , it is necessary to configure a fixed time or choose Daily/Weekly/Monthly to execute the website scanning task.
Target Method	• Select: Click the text box and select the asset in the pop-up box. You can switch views and select multiple assets. For asset views and asset configuration methods, see Inventoried Asset. • Type: Manually input the scanning target information. Support entering multiple targets. Hover the mouse over the text box to view the formatting requirements. To manage vulnerabilities in the scanning results on ISOP, manually synchronize asset risks on the task details page after the task is completed.
Scan Scope	Select the scope for crawling and scanning. • Whole Website: scans all URLs under the parent domain and each of its subdomainsight. • Subdomains: only scan the subdomain name and all URLs under the sub domain name configured here. • Subdomains skipped: scan all URLs under the parent domain name and other subdomainsight except those under the subdomain configured here. • Current directory and related subdirectories: only scan URLs in the scanning target and all subdirectories. • Current link: only scan URLs in the scanning target.
Device	After the scanning device is connected to ISOP, select the method of selecting the device to execute the scanning task. • Auto: ISOP automatically distributes tasks to scanners based on task types. • Manual: Select a scanning device that has been connected to ISOP from the drop-down list. Multiple values are supported.

Step 4 (Optional) Configure the website authentication parameters for the scanning target.

Table 8-18 describes the configurable parameters.

Table 8-18 Website scanning task website authentication parameters

Parameter		Description
Protocol Authentication		Scans the authentication protocol used by the target.
Protocol Authentication Username/Password		Scans the User name/Password of the authentication protocol used by the target.
Login Scan		After activation, NSFOCUS Threat and Vulnerability Management Platform (TVM) will use the configured login information to log in and scan the target, and a cookie needs to be configured to record the login session ID. For example: action=login&username=admin&password=admin88
Authentication Agent Configuration	Enable/Disable	Controls whether to use a proxy server to connect to the scanning target.
	Proxy Type	Type of proxy server.
	Authentication Protocol	Authentication protocol used by the proxy server.
	Server Address/Port	Address/port of the proxy server. The server address can be an IP address or domain name.
	User Name/Password	Specifies the user name and password used to log in to the proxy server. You must configure both the user name and password.

Step 5 (Optional) Configure the website access parameters for the scanning target.

Table 8-19 describes the parameters for configuring the website access.

Table 8-19 Website scanning task website access parameters

Parameter	Description
Number of concurrent threads	Number of concurrent scanning threads of the scanning plugin during website scanning. The larger the value, the faster the scanning speed. The default is 100, with a value range of 1-100.  Note When configuring, it is necessary to consider network bandwidth and server processing capacity. Excessive values can affect the normal operation of the target server.
Time out limit (seconds)	Specifies the maximum time allowed for scanning a page. The default is 30 seconds, with a value range of 1-300 seconds.
Max Request Attempts	Maximum number of allowed requests for website access after a failed request.
Web Encoding	Specifies the web page encoding method used by the scanning target. The value

Parameter	Description
Method	must be correct so that ISOP can properly access the target. Auto: ISOP automatically matches the web page encoding method. Manual: You need to specify the web page encoding method used by the specified scanning target.
Custom User-Agent	Use the specified browser or search engine to access the scanning target.

Step 6 (Optional) Configure the website detection parameters for the scanning target.

[Table 8-20](#) describes the parameters to configure website detection.

Table 8-20 Website scanning task website detection parameters

Parameter	Description
Directory Guess Scope	Specifies the guess scope of common sensitive directories and files in each directory. The default is 1, with a value range of 0 to 3, where 0 means no guessing.  Note The larger the value, the wider the guess range, and the more directories and files may be guessed, but the scanning time will also be longer.
Directory Guess Depth	The guessing depth of sensitive directories and files. This value cannot be greater than the value of Directory Depth in the web crawling parameters. The default is 3, with a value range of 0–30.
Backup File Check Type	Which types of files need to be checked for backup files, and multiple types should be separated by the comma.
Backup File Check Extensions	The backup file extension that needs to be checked is used in conjunction with the Backup File Check Type , with multiple extensions separated by the comma.

Step 7 (Optional) Configure website crawling parameters for scanning targets.

[Table 8-21](#) describes the parameters for configuring website crawling.

Table 8-21 Website scanning task website crawling parameters

Parameter	Description
Crawling order	URL acquisition method used during the scanning process.
Number of files per directory	Maximum number of files scanned in each directory when the Link deduplication strategy is enabled. An integer with a value range of ≥ -1, where -1 indicates unrestricted.
Directory depth	Specifies the number of directory levels that will be crawled. The default is 15, with a value range of -1 to 30, and -1 indicates unrestricted.

Parameter	Description
	 The depth of directory hierarchy refers to the number of / in the URL, starting from the root directory. A greater depth value indicates a wider scan scope and a longer scan time. Therefore, you need to set a proper value.
Total number of links	Maximum number of URLs obtained. The value can be -1 or any integer that is ≥ 1. The value cannot be filled with 0.
Case sensitivity	Whether to distinguish between uppercase and lowercase letters in URLs during the scanning process.
Custom links	URLs that must be scanned and they can be external links. Multiple URLs are separated by the comma or carriage returns.
Exclude links	URLs that do not require crawling.
Custom directories	The directory scope for crawling analysis. Separate multiple directories with commas or carriage returns. Special characters are not allowed, and the range of special characters should be based on the page prompts.
Exclude directories	A directory that does not need to be crawled. Separate multiple directories with commas or carriage returns. Special characters are not allowed, and the range of special characters should be based on the page prompts.
Exclude filenames	File name of a file that does not need to be crawled. Separate multiple file names with commas.
Exclude extensions	Suffix name of a file that does not need to be crawled. Multiple suffixes are separated by the comma.
Parse Flash Files	Controls whether to scan Flash files. Currently, only files of Flash earlier than V10 can be parsed.
Execute JavaScript	Whether to execute the JavaScript playbook code in the page to obtain the URL when crawling the page. - If Yes is selected, JavaScript will be executed and simulate various events. - If No is selected, JavaScript will not be executed, which will improve the scanning speed but miss out some links.
Link deduplication strategy	Specifies the level of URL deduplication policy, with options of 0, 1, 2 and 3. The default is 2. Generally, a URL is a quintuplet that consists of the page, method, query-name, query-value, and post-data. The URL deduplication level determines the elements based on which ISOP distinguishes URLs. Takes http://www.nsfocus.com/test.php?login=admin as an example: - Page=http://www.nsfocus.com/test.php (page = protocol + domain name + path file) - method=GET - query-name=login - query-value=admin - post-data=NULL

Parameter	Description
	For the link deduplication strategy levels: • 0: sensitive to page • 1: sensitive to page and method • 2: sensitive to page, method, and query-name • 3: sensitive to page, method, query-name, and query-value.  Note A higher deduplication level means more factors in the URL address need to be identical during scanning. When the level is set to 0, as long as the pages of two URLs are the same, it is considered that these two URLs are the same URL, without considering subsequent parameter values.
Form scanning	Controls whether to scan a form on the target page to discover more vulnerability information.
Add form	When there is a form on the page, should more forms be added to obtain more URLs and discover more vulnerability information. Once enabled, click to add multiple fill in information. 

Step 8 Click **OK** to save the task.

----End

8.2.1.4 Creating a Penetration Test Task

Through penetration test tasks, ISOP can simulate and insightpect security risks in the network.

Take a single task type as an example. The operation steps for creating a new penetration test task are as follows:

Step 1 Click **Create Task** to open the scanning task type selection page.

Step 2 Select **Penetration Test** and click **OK** to enter the new penetration test task page.

Step 3 Configure the basic information of penetration test tasks.

[Table 8-22](#) describes the parameters for configuring basic information.

Table 8-22 Basic information parameters of penetration test task

Parameter	Description
Task Name	Name of the penetration test task, which cannot be empty or duplicate. A maximum of 60 characters are allowed.
Target Type	Type of target asset to be scanned. Options include IPv4 , IPv6 , and URL .
Target	• Select: Click the text box and select the asset in the pop-up box. You can switch views and select multiple assets. For asset views and asset configuration methods, please refer to Inventoried Asset. • Type: Manually input the scanning target information. You can type multiple targets. Hover over the text box to view the formatting requirements. To

Parameter	Description
	manage vulnerabilities in the scanning results on ISOP, manually synchronize asset risks on the task details page after the task is completed.
Test Time	The start time of the penetration test task.
Tester Name	A maximum of 60 characters are allowed.
Tester Contact Method	A maximum of 60 characters are allowed.
Risk Level	Drag the mouse to select the risk level of the scanning target. The value range is 1-10.

Step 4 Configure the port and liveness parameters of the scanning target.

[Table 8-23](#) describes the parameters for configuring the port and liveness.

Table 8-23 Configuration of vulnerability information for penetration test tasks

Parameter	Description
Vulnerability Name	Name of vulnerability used in the penetration test.
Port	Port for penetration test scanning.
Protocol	Select the scanning protocol. Options include TCP , UDP , and ICMP .
Discovery Time	Select the discovery time for this vulnerability.
Vulnerability Score	Drag the mouse to select the vulnerability score.
Service	Service information for the vulnerability.
Operating System	Select the operating system targeted by this vulnerability.
Operating System Version	Select the operating system version targeted by this vulnerability.
Application Name	Select the application name targeted by the vulnerability.
Application Version	Select the application version targeted by this vulnerability.
Vulnerability Description	Description information of the vulnerability.
Vulnerability Details	Detailed information of the vulnerability.
Vulnerability Solution	Solution for this vulnerability.
Attachment Upload	Upload relevant attachments.

Step 5 (Optional) Import vulnerability.

- c. Click **Import Vulnerabilities** to display the import vulnerabilities side window.
- d. Import the vulnerability file in the specified area, and click **OK** to complete the import operation. Only a single **XLXS** file is supported, and the file size cannot exceed 20 MB.

Step 6 Click **Complete** to save the task.

----End

8.2.2 Creating an Import Task

ISOP supports importing scanning tasks from NSFOCUS Remote Security Assessment System (RSAS) and NSFOCUS Web Application Vulnerability Scanning System (WVSS), as well as importing data from third-party vulnerability reports.

Click **Import Data** and configure the import task/data parameters to import scanning tasks or vulnerability data. [Table 8-24](#) describes the import task/data parameters.

Table 8-24 Import task/data parameters

Parameter	Description
Task Type	Select the data/task source. Options include RSAS , WVSS , and 3rd-party vulnerability report import .
Task Name	Based on the selected task type, the system automatically generates a task name, which can also be customized.
Report Parser	When the task type is 3rd-party vulnerability report import , the corresponding vulnerability report parsing plugin needs to be selected. For the configuration method of the report parsing plugin, see Configuring a Plugin .
Importing a file	Upload the scanning task file or vulnerability report in the designated area, and click Import to complete the file import. Only a single ZIP file is supported, and the file size cannot exceed 20 MB .

8.2.3 Viewing a Scanning Report

In the scanning task list, click **View** in the **Operation** column to view the scanning report with the current status of **Completed**.

[Table 8-25](#) and [Table 8-26](#) describe the displayed content.

For tasks in other states, the scan report is empty.

Table 8-25 Scanning report content description (RSAS scanning task)

Displayed Item		Description
Summary	Risk score	Displays the number of active, inactive and unscanned IP addresses, and the risk score automatically calculated by the system (different colors indicate different system risks).
	Operating System Distribution	Displays the distribution of scanned operating systems and the total number of operating systems in a donut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the number of the assets in a specific category.
	Risk Distribution	Displays the risk distribution of different dimensions scanned in a bar chart. The dimension options include Threat , Service , CVE Year , System , Time , and Application . Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the specific statistics in a specific category.

Displayed Item		Description
	Host Risk Distribution	Displays the scanned host risk distribution and total number of hosts in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the specific statistics in a specific category.
	High/Medium-Risk Vulnerabilities	Displays the distribution of vulnerability levels and the total number of vulnerabilities scanned in a doughnut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the specific statistics in a specific category.
Host Information		Displays IP address, operating system, number of vulnerabilities, total vulnerabilities, vulnerability score, and synchronization status of the scanned hosts in a list. The following operations are supported: - View asset details: Only assets with a risk value greater than 0 are supported. Click the asset IP to view the host overview, port information, vulnerability information, and other information of the asset. - Sync risk: - For hosts in Not synchronized state, both single synchronization risk and bulk synchronization risk are supported, which synchronizes the vulnerability information in this task to the existing assets of the selected asset group. You need to create corresponding assets first if there are no matching assets in the selected asset group. For the creation method, see Inventoried Asset. - For hosts that have completed risk synchronization, click the asset name in the Synchronization Status column to jump to the vulnerability assessment page of the host asset. Table 8-3 describes the content displayed in the page.
Vulnerabilities		Displays the number of High-risk , Medium-risk , and Low-risk vulnerabilities and the scanned vulnerability information in a list. The following operations are supported: - View vulnerability information: Click the vulnerability name to view detailed information about the vulnerability. - View the host information affected by the vulnerability: Click the number in the Affected Hosts column to view the list of hosts affected by the vulnerability. Click the asset IP to view the corresponding asset details.
Audit Log		Displays audit logs of the scanning task in a list.
Task Configuration		Displays the basic configuration information of the scanning task.
Reference Criteria		Displays the reference standards for system scanning, including single-vulnerability risk level metrics, single-configuration risk level metrics, host risk level metrics, network risk level metrics, and security recommendations.

Table 8-26 Scanning report content description (WVSS scanning task)

Displayed Item		Description
Summary	Risk score	Displays the number of active addresses scanned, the number of inactive addresses, and the risk score automatically calculated by the system (different colors indicate different system risks). Click the number of active sites to download the TXT file of the active site IP list locally.
	High/Medium/Low-Risk Vulnerabilities	Displays the distribution of vulnerability levels and the total number of vulnerabilities scanned in a donut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the specific statistics in a specific category.
	Site Risk Distribution	Displays the scanned site risk distribution and total number of sites in a donut chart. Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the specific statistics in a specific category.
	Risk Distribution	Displays the risk distribution of different dimensions scanned in a bar chart. Dimension options include THREAT , WASC , and OWASP . Click the legend to hide/display the statistics of the corresponding category in the chart. Hover over the chart to see the specific statistics in a specific category.
Site List		Displays the website name, scan time, discovered links, scanned links, discovered files, files with vulnerabilities, vulnerability risks (count), risk score and the synchronization status of the scanned websites in a list. The following operations are supported: - Synchronize Risks: For sites with a Synchronization Status of Not Synchronized, both single synchronization risk and bulk synchronization risk are supported, which synchronizes the vulnerability information in this task to the existing assets of the selected asset group. You need to create corresponding assets first if there are no matching assets in the selected asset group. For the creation method, see Inventoried Asset. - View site risk situation: Click the website IP to view the risk profile and risk distribution list of the site, including risk level, number of high-risk/medium-risk/low-risk vulnerabilities, number of discovered links, number of scanned links, and website vulnerability details.
Vulnerability List		Displays the number of high-risk, medium-risk, and low-risk vulnerabilities and the scanned vulnerability information in a list. The following operations are supported: - View vulnerability information: Click the vulnerability name to view detailed information about the vulnerability. - View the site information affected by the vulnerability: Click the number in the Occurrences column to view the list of hosts affected by the vulnerability.
Audit Log		Displays audit logs of the scanning task in a list.
Task Configuration		Displays the basic configuration information of the scanning task.
Reference Criteria		Displays reference standards for website scanning, including

Displayed Item	Description
	single-vulnerability risk level metrics, page risk level assessment metrics, site risk level assessment metrics, and security recommendations.

8.2.4 Configuring a Plugin

Click **Plugin Configuration** to add parsing plugins from other vendors, which can be used to parse vulnerability scanning reports from these vendors, as shown in [Figure 8-6](#).

Click **New Plugin** to import the parsing plugin file in the specified area (only a single DAT file is supported, and the file size cannot exceed 20MB). Click **Upload** to complete the addition of the parsing plugin. After the parsing plugin is added, operations such as deleting and importing vulnerability scanning reports from corresponding vendors can be performed.

Figure 8-6 Plugin configuration page

Plugin List (0)						Back	New Plugin
Plugin ID	Plugin Name	Plugin Type	Description	Associated Devices	Upload Time	Operation	
 No Data							

9 Knowledge Base

The knowledge base of ISOP provides rules, intelligence, vulnerability sets, and IP geographic information.

This chapter contains the following topics:

Topic	Description
Rule Base	Describes how to configure and upgrade various rules.
Intelligence Database	Describes how to configure the intelligence database.
Vulnerability Database	Describes how to configure the vulnerability databases.
Geodatabase	Describes how to configure the IP geodatabase.

9.1 Rule Base

The rule base of ISOP basically meets daily protection requirements. You can customize rules and upgrade them according to actual situations.

9.1.1 Intelligence Rules

Choose **Knowledge Base > Rule Base > Intelligence Rules**. Select one or more intelligence types and click **OK** for intelligence pushing.

[Table 9-1](#) describes the intelligence rule parameter.

Table 9-1 Intelligence rule parameters

Parameter	Description
Valid Intelligence Type	Select from all intelligence types whose meta type is Detection . Multiple selection is supported. For intelligence type configuration methods, see Configuring Intelligences .



Note

The intelligence type here is not real-time push, and the push cycle is 1 hour.

9.1.2 Updating Rule Bases

Before upgrading the rule base, it is necessary to contact the technical support personnel of NSFOCUS to obtain an upgrade package file in *.dat format.



Uploading upgrade packages by multiple users simultaneously are not allowed. Otherwise, the upgrade may fail.

9.1.2.1 Upgrading the System

The upgrade steps for the ISOP system are as follows:

- Step 1** Choose **Knowledge Base > Rule Base > Rule Base Upgrade > System Upgrade**.
- Step 2** Upload the upgrade package file in the **System Upgrade** area. After successful upload, a message appears, prompting that the upgrade package is successfully uploaded and upgrade package information is recorded.
- Step 3** Click **Upgrade** to perform an ISOP upgrade. The system will automatically display the upgrade progress.
- Step 4** After the upgrade is successful, follow the prompts on the page to wait for the web server to restart, and do not close the page during the restart. After the web server restarts, the upgrade is complete.
- Step 5** (Optional) Click **View Upgrade History** to view the history of system upgrades, including the upgrade date, source version, target version, and upgrade result.

----End

9.1.2.2 Upgrading a Rule Base

The rule base currently only contains the parsing rule packages.

Choose **Knowledge Base > Rule Base > Rule Base Upgrade > Rule Base Upgrade**. The upgrade method can be manual or auto upgrade. After the upgrade is complete, click **View Upgrade History** to view the history of rule base upgrade, including the upgrade date, source version, target version, and upgrade result.

Upgrading the Rule Base Manually

In the **Manual Upgrade** area, after configuring the manual upgrade rule parameters, click **Upgrade** to complete the upgrade of the selected rule package.

[Table 9-2](#) describes the manual upgrade parameters.

Table 9-2 Manual upgrade parameters

Parameter	Description
Rules To Upgrade	Select the Parsing Rules option as needed. The parsing rule package is used for log parsing of accessed data. When the data access component is not installed or enabled, the Parsing Rule option is not visible.
Current Version	Displays the current version of the selected rule package.
Upload Upgrade Package	Upload the upgrade package file in the System Upgrade area. After successful upload, it prompts that the upgrade package is successfully uploaded and upgrade package information is recorded at the same time.

Upgrading Automatically

In the automated upgrade area, configure the automated upgrade parameters and click **Save** to perform the automated upgrade according to the settings.

Table 9-3 describes the auto upgrade parameters.

Table 9-3 Auto upgrade parameter

Parameter	Description
Enable For	Select the Parsing Rules option as needed. Multiple values are supported. For more details, see Table 9-2.
Upgrade Site	Fill in the upgrade website for automated upgrade. Hover the mouse over the box to display the default upgrade site: https://update.nsfocus.com . It is recommended to type the default site as the upgrade site.
Detection Frequency	The following three detection frequencies are supported: 1 day: The detection time is at 2:00 every day. 1 week: The detection time is at 2:00 every Monday. 1 month: The detection time is at 2:00 on the 1st of each month.
Detect Now	After configuring the above parameters, click Detect Now to verify the connectivity of the upgrade site.

9.2 Intelligence Database

The intelligence database provides intelligence overview, intelligence configuration, intelligence search, and online search functions.

9.2.1 Intelligence Overview

Choose **Knowledge Base > Intelligence Database > Overview**. The page displays the type ID, type name, metatype, quantity, disk usage, and update time of pulled intelligence in ISOP.

9.2.2 Configuring Intelligences

Intelligence configuration includes feed configuration, type management, and intelligence import.

9.2.2.1 Configuring Intelligence Feeds

Choose **Knowledge Base > Intelligence Database > Configuration > Feed Configuration**. This page displays the currently connected built-in intelligence feeds. You can also create custom intelligence feeds, and edit and delete them.

Adding an Intelligence Feed

Click **New** and configure the intelligence feed parameters. After saving, you can create a new ISOP intelligence feed.

[Table 9-4](#) describes the intelligence feed parameters.

Table 9-4 Intelligence source parameters

Parameter	Description
Feed Name	Specifies the name of the intelligence.
Priority	Specifies the priority of the feed. It is an integer ranging from 1 to 100. A higher value means a higher priority of the intelligence.
Description	Description of the intelligence.
Associated Intelligence Types	Select the type of intelligence you want to obtain. Multiple values are supported. For associated intelligence type configuration methods, see Managing Intelligence Types .

Testing Connectivity

This feature is only available for built-in intelligence feeds.

Click **Connect** in the **Operation** column, ISOP will immediately attempt to connect to the corresponding intelligence feed and return connectivity information.

Updating Now

This feature is only available for built-in intelligence feeds.

Click **Update** in the **Operation** column, ISOP will immediately attempt to issue update instructions to the corresponding intelligence feed and return the update results.

Editing an Intelligence Feed

Click **Edit** in the **Operation** column. Different parameters can be edited for different intelligence feed types:

- Built in intelligence feeds: intelligence key, priority, address, timeout period, update time, automated synchronization, and associated intelligence types.
- Custom intelligence feeds: intelligence key, priority, and associated intelligence types.

Deleting an Intelligence Feed

Click **Delete** in the **Operation** column to delete custom intelligence feed.

The system's built-in intelligence feed cannot be deleted.

9.2.2.2 Managing Intelligence Types

Choose **Knowledge Base > Intelligence Database > Configuration > Type management**. You can import and create new intelligence types on this page.

Creating an Intelligence Type

Click **New** and configure the intelligence type parameters. After saving, you can create a new intelligence type. [Table 9-5](#) describes the intelligence type parameters.

After creating an intelligence type, you can view and delete it.

Table 9-5 Intelligence type parameters

Parameter		Description
Name		Specifies the name of the intelligence type. The length is 2-20 characters.
Table Name		Cannot start with a number. The length is 2-30 characters.
Priority		Specifies the priority of the intelligence type. It is an integer ranging from 1 to 100. A higher value means the higher priority of the intelligence.
Metatype		Options include Detection and Analysis .
Custom Fields	Field Name	Cannot start with a number. The length is 2-20 characters.
	Type	Options include int , bigint , varchar and text . If you choose varchar , you also need to set the upper limit of the length.
	Allow Empty	Select whether the field is allowed to be empty.
	Description	Description information of the field.
Observable Field		When Metatype is set to Detection , a custom field must be selected as the observable field.
Observable		When Metatype is set to Detection , select the content to be detected. Multiple values are supported. Options include ip , url , domain , md5 , 1k_hash and name .
Intelligence Index Field		When Metatype is set to Analysis , a custom field must be selected as the Intelligence Index Field .
Intelligence Feed		Select the source of intelligence. Multiple values are supported. For intelligence feed configuration methods, see Configuring Intelligences .

Selecting a File

Click **Select File** to import custom intelligence types. The file format is .dat. After successful import, it can be viewed in the intelligence type list.

9.2.2.3 Importing Intelligences

Choose **Knowledge Base > Intelligence Database > Configuration > Intelligence Import**. [Table 9-6](#) describes the intelligence import parameters.

Table 9-6 Intelligence import parameters

Parameter	Description
Select intelligence feed	Select the target intelligence feed for importing intelligence. The importing method varies between the built-in intelligence feed and custom intelligence feed. • Built-in intelligence feed: Click Select File, select the intelligence file package locally, and click Upload to import the intelligence. • Custom intelligence feed: After selecting the intelligence type for the custom intelligence feed, import the intelligence.
Select intelligence type	When you create a custom intelligence feed as the target intelligence feed, you also need to select the intelligence type and click Import to import the intelligence. If you want to adjust the intelligence type before importing, you can click New to edit the values of each field.

9.2.3 Querying Intelligences

Choose **Knowledge Base > Intelligence Database > Query**. You can query intelligences by time range, metatype, intelligence source, intelligence type, object of observation, observation object type. The displayed intelligence query results vary with the meta type and intelligence type.

9.2.4 Querying Online

Choose **Knowledge Base > Intelligence Database > Online Query**. Click **Go** in the pop-up box to redirect you to the NSFOCUS Threat Intelligence Center (NTI) for more detailed intelligence inquiries.

9.3 Vulnerability Database

The vulnerability database can manage all vulnerabilities found in the current network environment assets.

You can use vulnerability database to manage host and website vulnerabilities, vulnerability templates, vulnerability classification, configuration templates, and password dictionaries.

9.3.1 Vulnerabilities

Vulnerabilities in the vulnerability database of ISOP include website vulnerabilities and host vulnerabilities.

9.3.1.1 Website Vulnerabilities

Website vulnerabilities are web vulnerabilities discovered in website assets.

Choose **Knowledge Base > Vulnerability Database > Vulnerabilities > Website Vulnerabilities**. The page displays vulnerability query conditions area, the total number of vulnerabilities in the current website vulnerability database, and the vulnerability list by default. The vulnerability list displays the vulnerability name, vulnerability score, discovery date, vendor source, and threshold.

Querying Website Vulnerabilities

At the top of the website vulnerability list, you can query vulnerabilities by vulnerability name or click **Advanced Query** to set more criteria for query. [Table 9-7](#) describes the query conditions for website vulnerabilities.

Table 9-7 Website vulnerabilities query conditions

Condition	Description
Vulnerability Name	The name of the website vulnerability. Fuzzy queries are supported.
Source	Source of website vulnerabilities. Only NSFOCUS is supported.
Risk Level	The risk level of website vulnerabilities. Options include Low , Medium , and High .
Vulnerability Description	Description of website vulnerabilities. Fuzzy queries are supported.
Discovery Time	Time the vulnerability is discovered. Quick selection options include the last 3 days , 5 days , and 7 days .
Disclosure Time	Time the vulnerability is released. Quick selection options include the last 3 days , 5 days , and 7 days .

Viewing Website Vulnerability Details

In the website vulnerability list, click **Details** in the **Operation** column to view the corresponding vulnerability details, including the vulnerability name, detailed description, vulnerability source, solution, dangerous plugins, discovery date, release date, CVE number, CNNVD number, CNCVE number, BUGTRAQ, NSFOCUS, CVSS score, and CNVD code.

Setting the Vulnerability Threshold

According to the vulnerability threshold and corresponding algorithms, ISOP can automatically calculate the vulnerability handling priority.

You can set the threshold of a website vulnerability or bulk set thresholds of multiple website vulnerabilities.

- Set a threshold: In the website vulnerability list, click **Threshold** in the **Operation** column to set the corresponding vulnerability threshold.
- Bulk set thresholds: Above the website vulnerability list, click  to bulk set the thresholds for the selected vulnerability. You can select all vulnerabilities across pages to bulk set their thresholds.

[Table 9-8](#) describes the threshold parameters for website vulnerabilities.

Table 9-8 Website vulnerability threshold parameters

Parameter	Description
Vulnerability Threshold	The value is an integer ranging from 1 to 100.

Solution for a Vulnerability

In the website vulnerability list, click **Solution** in the **Operation** column to pop up a list of corresponding vulnerability solutions (🔑 representing system solutions). Click **Add Solution** to create a new custom solution.

You can choose the created solution and set it as the default solution for this vulnerability.

Table 9-9 describes the parameter of the website vulnerability solution.

After creating a custom solution, you can edit and delete it.

Table 9-9 Website vulnerability solution parameter

Parameter	Description
New Solution	A maximum of 10,000 characters are allowed.

9.3.1.2 Host Vulnerabilities

Host vulnerabilities are system vulnerabilities discovered in host assets.

The management and operation methods for host vulnerabilities are basically the same as those for website vulnerabilities. For details, see [Website Vulnerabilities](#).

9.3.2 Password Dictionary

During the scanning process, the security device attempts to log in to and examine the target device to identify vulnerabilities based on the content in the password dictionary. If the login user name and password of the target device match the content in the password dictionary, it is considered that the target device has a vulnerable account.

There are system password dictionaries and custom password dictionaries in ISOP.

Choose **Knowledge Base > Vulnerability Database > Password Dictionary**. The page displays the system password dictionaries by default. Click **View** in the **Operation** column to view the details of the password dictionary, including the dictionary name, category, and content.



The system password dictionary contains some common vulnerable accounts that cannot be edited or deleted.

Creating a Password Dictionary

You can create a password dictionary in one of the following methods:

- Save password dictionary as: On the **Password Dictionary Details** page, click **Save as** to customize the dictionary parameters and content based on the corresponding password dictionary for quick creation.
- New template: Click **Add** to configure password dictionary parameters. [Table 9-10](#) describes the password dictionary parameters.

Table 9-10 Password dictionary parameters

Parameter	Description
Dictionary Name	Name of the password dictionary. A maximum of 64 characters are allowed.
Category	• User name: weak user names that pose risks in password guessing tasks for SMB, TELNET, FTP, SSH, POP3, Microsoft SQL Server, MYSQL, Oracle, Sybase, and DB2 protocols. • Password: passwords used in SMB, TELNET, FTP, SSH, POP3, Microsoft SQL Server, MYSQL, Oracle, Sybase, DB2, and SNMP protocols, as well as CISCO devices. You can use them to configure passwords with risks in password guessing tasks. • User name/Password: user names and passwords used in SMB, TELNET, FTP, SSH, POP3, Microsoft SQL Server, MYSQL, Oracle, Sybase, and DB2 protocols. You can use them to configure risky user names and passwords for password guessing tasks.
Dictionary Content	Click  to add dictionary content for the selected category. Supports up to 60,000 records. • User name: one user name per line. • Password: one password per line. • User name/Password: one entry per line in the format of user name: password, for example, administrator: nsfocus.
Dictionary File	Click Please select a dictionary file (.txt) to import .text files. The requirements are as follows: • The file name should consist of lowercase and uppercase letters, digits, hyphens (-), and/or underscores (_). • The content requirements are the same as the dictionary content. UTF-8 and ASCII encoded files are supported.  Note If the content of the imported dictionary file is incorrect, the user name/password in the dictionary will not be guessed during task execution.
Description	Description of the password dictionary.

Customizing a Password Dictionary List

At the top of the password dictionary list, you can customize the display of the password dictionary list by selecting different **Category** and **Type** options.

9.3.3 Vulnerability Database Upgrade

Currently, vulnerability database only supports manual upgrades. Contact the technical support personnel of NSFOCUS to obtain the vulnerability database upgrade package, save it locally, and then upgrade the vulnerability database.

Choose **Knowledge Base > Vulnerability Database > Upgrade**. This page displays the version numbers of the existing configuration template database, website vulnerability database, and host vulnerability database. Click **Select Upgrade Package (*.dat)** to complete the upgrade of the vulnerability database according to the page prompts.

9.4 Geodatabase

The geodatabase is used to perform unified management of geographic information for custom IPs.

Choose **Knowledge Base > Geodatabase > Custom GeoIP Database**. On the **Custom GeoIP Database** page, you can add, bulk import, export and delete IP geographic information. Here only the methods of adding and importing IP geographic information are described.

Adding IP Geographic Information

Click **Add GeoIP Information** and configure IP geographic information parameters to add single or bulk add IP geographic information. After adding IP geographic information, click **Apply** to make the IP geographic information take effect.

[Table 9-11](#) describes the geographic information parameters.

Table 9-11 IP geographic information parameters

Parameter	Description
IP Address	IP address.
Nation	Select the country to which the address belongs.
Province/City/Area	When Nation is China , you need to type Province , City , and Area .
IP Geographic Information List	After typing the above information, click Add to automatically add it to the IP geographic information list. You can continue to add more IP geographic information. Click Delete in the Operation column to delete the corresponding IP geographic information.

Importing IP Geographic Information

To import IP geographic information, follow these steps:

- Step 1** Click **Export Template** to download the IP geographic information template locally.
- Step 2** Open the IP geographic information template locally, type the IP geographic information according to the template prompts, and save it as an .xlsx file or .xls file.

Step 3 Click **Import** and follow the prompts on the page to upload the saved IP geographic information file.

Step 4 After uploading, click **Import** to complete the import of IP geographic information.

----**End**

10 More

More modules include basic configurations related to operations and management.

This chapter contains the following topics:

Topic	Description
System Configuration	Describes how to configure system themes, storage, allowlist, and asset topology.
Device Manage	Describes how to configure device lists, application stores, and traffic forensics devices.

10.1 System Configuration

System configuration includes configurations for theme, storage, allowlist, and asset topology.

10.1.1 Theme

Through theme configuration, users can customize the ISOP login page, the product name and logo image on the login page, as well as the situational awareness screen name.

Choose **More > System Configuration> Theme** to configure the system theme. [Table 10-1](#) describes the theme parameters.

Table 10-1 System theme parameters

Parameter	Description
Product Name/Logo	- Product name: The default is NSFOCUS Intelligent Security Operation Management Platform. A maximum of 33 characters are allowed. - Product logo: Upload a product logo image. Only png and jpeg formats are supported, and the image size cannot exceed 1 MB. - Click OK and after the configuration takes effect, the product name and logo will be automatically updated in the upper left corner, upper right corner , and browser tab of the system. - Click Restore Default and confirm to restore the default settings for the product name and logo.
Large Screen	Configure the name/title for the situational awareness big screen.

Parameter	Description
Renaming	Click Restore Default to restore the default name/title of the corresponding big screen.

10.1.2 Storage

Through storage configuration, users can configure the system's remaining space cleanup strategy, retention time for data and access files, intelligence attribution, and ES queries.

Choose **More > System Configuration > Storage**. This page allows you to configure the system's storage strategy (including the remaining space cleanup strategy, data retention time, access file retention time, intelligence traceability and ES query). [Table 10-2](#) describes the system storage parameters.

Table 10-2 System storage parameters

Parameter	Description
Disk Usage Cleanup Policy	When the disk space exceeds the set threshold percentage, ISOP automatically cleans up the data with the longest storage time. - Disk Usage Cleanup: When turned On, ISOP will automatically clean up space according to the set data cleaning threshold. - Cleanup Threshold: Drag the icon  with the mouse to set the threshold. The value range is 75-90 %.
Data Retention Period	Configure the retention time for ISOP access data. - Alert Log Retention Period: Alert logs that exceed the set time will be automatically deleted by the system. The default value is 180 days. - Event Retention Period: Events that exceed the set time will be automatically deleted by the system. The default value is 180 days. - Traffic Log Retention Period: Traffic logs that exceed the set time will be automatically deleted by the system. The default value is 30 days. 3rd-Party Log Retention Period: Any third-party logs that exceed the set time will be automatically deleted by the system. The default value is 180 days.
Connected File Retention Period	Configure the retention time for ISOP access data. - Enable Retention Policy: After enabling, files accessed by ISOP will be retained; Otherwise, it will be automatically deleted by the system. - Retention Period: Configure the retention days for access files. The value range is 1-180 days.
Intelligence Traceback Configuration	Configure intelligence backtracking time. ISOP backtracks historical log data based on the IP address in the uploaded. csv backtracking file, generate hit IP logs and one-click response templates. It supports to download the backtracking results. - Backtracking Time: The value range is 1-30 days. - Upload File: Click Template, fill in the IP address that needs to be traced according to the template format, and then upload the file.
ES Query Mode	There are two ES query modes:

Parameter		Description
Configuration		- Type: Manually configure the number of days for the Current Log Search Period (days). - Auto assessment: Use intelligent evaluation algorithms to automatically evaluate the time span where a log can be queried.
	Current Log Search Period (days)	Configure the maximum time span days for log search. The value range is 3-90 days.
	EPS	When the mode is Auto assessment , it is necessary to configure the average storage rate of the platform log. The value range is 1,000-1,000,000 items/second . To view the total storage rate of platform log, click  on the shortcut toolbar of ISOP and choose Setting > Data Source Management . This page allows for a query of storage rate.
	Number of ES Cluster Nodes	When the mode is Automated assessment , it is necessary to configure the ES number of data nodes in the cluster. The value range is 1-100 . To view the number of ES data nodes, click  on the shortcut toolbar of ISOP and choose System > Facilities > Facility Management to view the details of Elasticsearch .
	Log Queryable Period (days)	When the mode is Auto assessment , based on the above ES query parameters, click Compute , and the system will automatically calculate the maximum supported span days for the log query. Exceeding this value may affect the platform's Elasticsearch stability. Therefore, it is recommended to configure the Current Log Search Period (days) based on this calculated value.

10.1.3 Allowlist

Events matched to the allowlist are filtered and not displayed or statistically analyzed.

Choose **More > System Configuration > Allowlist**. This page allows you to create a new allowlist and perform operations such as query, edit, import, export, and delete allowlist. Below introduce the methods of adding and importing allowlist.

Creating a New Whitelist

Click **New Allowlist** to configure the whitelist parameters. [Table 10-3](#) describes the whitelist parameters.

Table 10-3 Allowlist parameters

Parameter	Description
Name	Name of the allowlist. Cannot duplicate an existing name.
Source IP	Configure the source IP allowlist. The filling format is as follows: Support input of single IP, IP range, and IP network segment.

Parameter	Description
	- Support filling in multiple IPs separated by the comma. - Support IPv4 and IPv6 addresses.
Source Port	Configure the port of the source IP. Support filling in multiple ports separated by the comma.
Destination IP	Configure the destination IP allowlist. The filling format is as follows: - Support input of single IP, IP range, and IP network segment. - Support filling in multiple IPs separated by the comma. - Support IPv4 and IPv6 addresses.
Destination Port	Configure the port for the destination IP. Support filling in multiple ports separated by the comma.
Rule ID	Configure rule ID allowlist. Support filling in multiple IDs separated by the comma.
URL/Domain	Configure URL/domain allowlist. Support multiple URLs/domains separated by the comma, with a maximum length of 10 K bytes for the total length of URLs/domains.
Global IP	Configure a global IP allowlist that does not distinguish between source IP and destination IP for one-click response and exception assets. The format of the one-click response is as follows (see page prompts for details): IPv4: Support input of single IP, IP range, and IP network segment and configuration of multiple IPs separated by the comma. IPv6: Support single node (e.g. abcd::eeee). The format of abnormal assets is as follows (see page prompts for details): IPv4: Support input of single IP, wildcards, IP ranges, and IP network segments and configuration of multiple IPs separated by the comma. The number of individual IP nodes after parsing cannot exceed 1,000.
Period of Validity	The time range for this allowlist to be in effect.
Description	Description information of the allowlist.
Scope of Validity	Select the functional module for the allowlist to take effect. Support multiple selections. Support fuzzy query of functional module names.  Note - For allowlists that are not configured in the Global IP, One-click response and Abnormal asset analysis do not take effect even if checked. - For the global allowlist that are configured in the Global IP, One-click response and Abnormal asset analysis must be checked to take effect.
Whether to enable	Yes: After configuration, the allowlist takes effect immediately. No: After configuration, the allowlist needs to be manually activated to take effect.

Importing an Allowlist

The steps to import an allowlist are as follows:

- Step 1** Click **Import** above the global allowlist list.
- Step 2** In the allowlist importing dialog box, click **Template** to download the allowlist import template locally.
- Step 3** Open the allowlist import template, enter the allowlist information according to the template prompts, and save it as an **XLSX** file or **XLS** file.
- Step 4** In the allowlist importing dialog box, follow the prompts on the page to upload the saved allowlist file.

If **Overwrite existing data** is checked, it means that the original allowlist information will be overwritten during import.

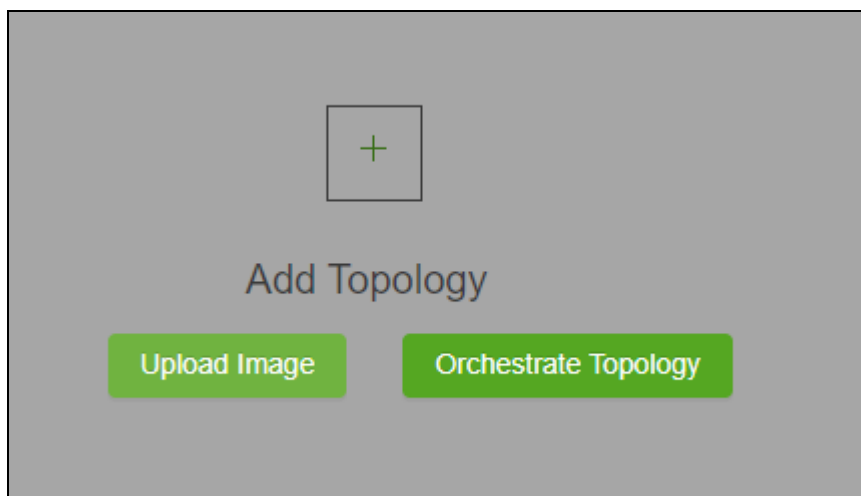
----End

10.1.4 Asset Topology

In order to facilitate users to quickly and intuitively understand the overall security risk situation of assets in various regions of the system, ISOP supports uploading or self organizing network asset topology maps. The uploaded custom topology map will also be displayed on the environmental awareness screen.

Choose **More > System Configuration > Asset Topology**. Hover the mouse over the **Add Topology** area to upload the topology map and perform topology layout operations, as shown in [Figure 10-1](#).

Figure 10-1 Topology management



Uploading a Topology Map

On the page as shown in [Figure 10-1](#), click **Upload Image** to go to the upload topology map page. Click **Select Image** to select the edited topology map locally, and then click **Apply** to apply it to the environmental awareness screen.

The format requirements for topology map files are as follows:

- Only **jpg**, **png**, and **gif** files are supported.
- The file size cannot exceed **10 MB**.

- The file pixels cannot exceed **2180 × 1292**.

Topology Orchestration

On the page as shown in [Figure 10-1](#), click **Orchestrate Topology** to go to the topology map editing page, as shown in [Figure 10-2](#).

On the topology map editing page, by dragging and dropping basic elements, asset node, custom node, and connections and using the shortcut buttons in the upper right corner of the page to draw the topology map yourself. During and after the drawing process, the following operations can be performed:

- Click  on the **Custom Nodes** to add more categories of node elements which support editing and deleting.

Click **Preview** to preview the topology map and follow the prompts on the page to pan, zoom, and rotate the image.

- Click **Save** to define the name of the current topology map and temporarily store it on the asset topology configuration page, with a status of **Not Applied**.
- Click **Apply** to apply the current topology map to the environmental awareness screen.

Figure 10-2 Topology orchestration



Managing Topology Maps

On the asset topology configuration page, you can perform the following operations on the orchestrated topology:

- Click  to edit the corresponding topology map.
- Click  to define the name of the corresponding topology map and apply it to the environmental awareness screen.
- Click  to cancel the application of the corresponding topology map in the environmental awareness screen.
- Click  to delete the corresponding topology map.

10.2 Device Manager

Device management includes the configuration of device list, app store, and traffic forensics devices.

10.2.1 Device List

Choose **More > Device Manager > Device List**. In the initial state, the device list is empty. Users can create new device groups and add devices. After adding a device, you can perform operations such as querying, viewing device details, viewing device monitoring information, editing device information, deleting devices, synchronizing devices, enabling/disabling devices, logging in to devices, viewing certificates, and exporting device reports. The layout of the device list page is as shown in [Figure 10-3](#). [Table 10-4](#) describes the layout.

Figure 10-3 List of devices connected to ISOP

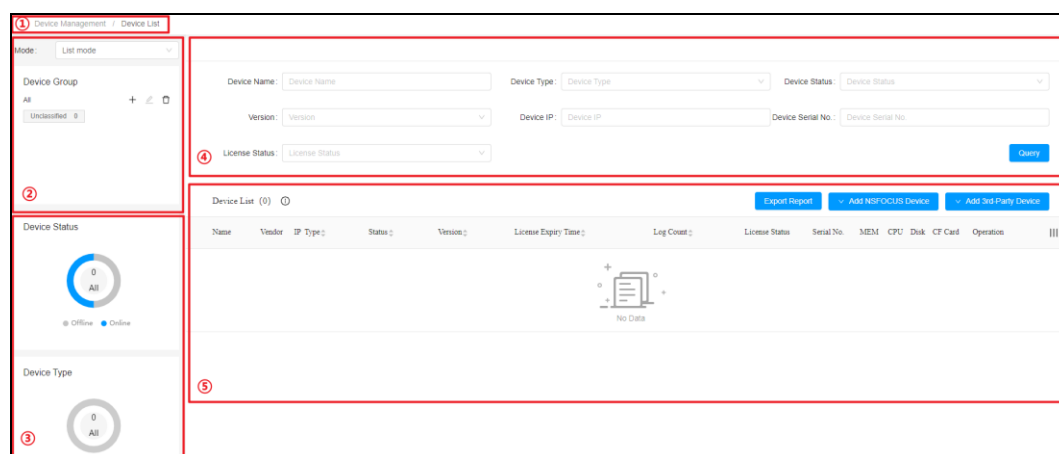


Table 10-4 Device list page layout description

Number	Area	Description
①	Display Mode	ISOP supports two device display modes: - List mode: The default is list mode. Display device information in the device management area in a list. - Card mode: Display device information in the device management area in cards.
②	Device Group Management Area	The management area for device groups supports creating, editing, and deleting device groups. You can also click the device group name to filter device groups for device queries. For device configuration methods, see Managing Device Group .
③	Device Status/Type Statistics Chart	Real time display of the current device status and type in a pie chart. The automated refresh frequency is 20 seconds. Click the legend to hide/display the statistics of the corresponding category in the chart.
④	Device Query Area	Support setting query conditions for device search, as well as clearing all query conditions. For device querying methods, see Querying Device .

Number	Area	Description
⑤	Device Management Area	The automated refresh frequency of the device list is 20 seconds. All device management operations are carried out here: - Add NSFOCUS devices, see Adding NSFOCUS Devices. - Add third-party devices, see Adding 3rd-Party Device. - Customize the display columns of the device list, see Customizing a Device List. - Export all device reports, see Exporting a Device Report. - For more management operations for each device, see Managing Devices.

10.2.1.1 Managing Device Groups

Device group is the logical classification of devices. In the initial state, the built-in root device group of the system is **All**, and the built-in primary device group is **Unclassified**. You can continue to create device groups, with a maximum of two-level device groups supported. However, a device can only belong to one device group.

[Table 10-5](#) describes the operation icons for managing device groups.

Table 10-5 Device group management icon

Icon	Description
	When no device group is selected, clicking the icon can create a first level device group; When selecting a primary device group, click the icon to create a secondary device group under that group. The length of device group name is 3-10 characters. Cannot have the same name as an existing device group.
	When selecting a device group, click the icon to modify the device group name.
	The precautions for deleting device groups are as follows: - The built-in Unclassified primary device group does not support deletion. - If the device group to be deleted contains a device, the device is moved to the Unclassified device group by default.

10.2.1.2 Adding NSFOCUS Devices

When adding NSFOCUS devices on the ISOP platform, it is necessary to select the device group to which the device belongs. By default, the devices that have initiated a connection request to ISOP are put under the **Unclassified** device group.

There are two ways to add NSFOCUS devices:

- Online addition: Add NSFOCUS devices on the ISOP platform.
- Offline addition: Enter the IP address of the ISOP platform on the NSFOCUS device to connect.

Adding NSFOCUS Devices Online

To add NSFOCUS devices on the ISOP platform:

- Step 1** Select a device group on the left panel of [Figure 10-3](#).
- Step 2** Click **Add NSFOCUS Device** on the lower left panel and select **Online addition**.
- Step 3** Configure NSFOCUS device parameters in the pop-up panel.
- Group: Displays the device group selected in step 1.
 - Device IP: The IP address of the newly added NSFOCUS device, supporting **IPv4** and **IPv6**.
- Step 4** Click **Add** to complete the device addition, and the newly connected NSFOCUS devices will display in the device list.
- End

Adding NSFOCUS Devices Offline

To add NSFOCUS devices on the ISOP platform:

- Step 1** Select a device group on the left panel of [Figure 10-3](#).
- Step 2** Click **Add NSFOCUS Device** on the lower left panel and select **Offline addition**.
- Step 3** Configure the parameters of the NSFOCUS device. [Table 10-6](#) describes the parameters.

Table 10-6 Offline addition parameters

Parameter	Description
Device IP	IP address of the newly added device, supporting IPv4 and IPv6 .
Device Hash value	HASH value for the newly added device. See the corresponding product manual for the viewing method of device HASH values.
Device Type	Device type. A maximum of 10 characters are allowed.
Device Name	Name of the device.
Device Serial No	Serial number of the device.

- Step 4** Click **Add** to complete the device addition, and the newly connected NSFOCUS devices will display in the device list.
- End

10.2.1.3 Adding 3rd-Party Devices

When adding 3rd-party devices on the ISOP platform, it is necessary to select the device group to which the device belongs. If not selected, it defaults to belonging to the **Unclassified** device group.

There are two ways to add 3rd-party devices:

- Online addition: Add 3rd-party devices on the ISOP platform.

- Offline addition: Add 3rd-party devices offline without accessing the status logs of 3rd-party devices.

Adding 3rd-Party Devices Online

To add 3rd-party devices on the ISOP platform:

- Step 1** Click  on the shortcut toolbar of ISOP and choose **Setting > Device Management > Third Party Device Plugin**. In the third-party device plugin page, confirm the status collection methods of third-party device plugins, which can be divided into active collection and passive reception.
- Step 2** Select a device group on the left panel of [Figure 10-3](#).
- Step 3** Click **Add 3rd-Party Device** above the device list and select **Online addition**.
- Step 4** The page for adding 3rd-party devices varies depending on the collection method confirmed in step 1.
- Step 5** Configure the parameters of the 3rd-party device. [Table 10-7](#) describes the parameters.

Table 10-7 3rd-Party device online addition parameters

Parameter	Description
Device IP	When the device is connected through NAT, fill in the IP address before NAT, supporting IPv4 and IPv6 addresses.
Device Hash Value	HASH value in the device alert log. If it does not exist, click Automatically Generate Hash and the system will automatically generate it.
Device Name	Name of the device.
Device Vendor	Select the manufacturer of the device.
Device Type/Device Version	Select the device type and device version based on the selected device manufacturer.

- Step 6** Click **Save** to complete the device addition, and the newly connected 3rd-party devices will display in the device list.

----End

Adding 3rd-Party Devices Offline

To add 3rd-party devices offline on the ISOP platform:

- Step 1** Select a device group on the left panel of [Figure 10-3](#).
- Step 2** Click **Add 3rd-Party Device** above the device list and select **Offline addition**.
- Step 3** Configure the parameters of the 3rd-party device. [Table 10-8](#) describes the parameters.

Table 10-8 3rd-Party device offline addition parameters

Parameter	Description
Device IP	IP address of the newly added device, supporting IPv4 and IPv6 .
Device Hash Value	Fill in the HASH value for the newly added device. If it does not exist, click Automatically Generate Hash and the system will automatically generate it.
Device Name	Name of the device.
Device Vendor	Name of the device manufacturer.
Device Type	Type of the device.
Device Version	Version number of the device.

Step 4 Click **Save** to complete the device addition, and the newly connected 3rd-party devices will display in the device list.

----End

10.2.1.4 Querying Devices

Above the device list, you can set query conditions for device queries.

[Table 10-9](#) describes the device query conditions.

Table 10-9 Device query conditions

Condition	Description
Device Name	By default, it consists of device type and device IP.
Device Type	Device type includes NSFOCUS devices and 3rd-party devices. Support multiple selections.
Device Status	For NSFOCUS devices, multiple selections are supported. There are two device status: - Online: There are more device status logs accessed, and the device alert log accessed within the same day is not 0. - Offline: No device status log access. For third-party devices, the device status can be divided into the following two types: - Online: There is device status log or alert log access. - Offline: No device status log or alert log access.
Version	The version information of the device. Support multiple selections.
Device IP	The IP address of the device, supporting IPv4 and IPv6 .
License Status	The certificate status of the device includes Unknown , Effective , and Expired . Support multiple selections.

10.2.1.5 Customizing a Device List

At the right end of the device list header, click  to set the display column for the device list. Among them, **Device Name** is the default option and does not support cancellation.

10.2.1.6 Exporting a Device Report

Click **Export Report** above the device list to export the current status of all connected devices as a **Word** file. The report content includes device online status, certificate status, version status, device certificate details, device version details, device fault details, next week's plan and supplementary information.

10.2.1.7 Managing Devices

You can manage devices through options provided in the **Operation** column. The following takes the **List Mode** as an example to introduce it.

Editing Device Information

Only editing 3rd-party device information is supported, and NSFOCUS device information does not support editing.

Click **Edit** in the **Operation** column to edit the device information, including device name, manufacturer, device type, and device version.

Deleting a Device

Click **Delete** in the **Operation** column and confirm to delete the corresponding device from the device list. Once deleted, ISOP will no longer receive logs from corresponding devices.

Device Sorting/Device Alert

In the device list, click the header **Type**, **Status**, **Version**, **License Expiry Time**, and **Log Count** to sort the devices in ascending or descending order.

When the utilization rate of **MEM**, **CPU**, **Disk**, and **CF Card** exceeds the default threshold of 90% in devices with an **Online** status, the device entries are displayed in red and automatically set to the top. The device placed on top does not take part in the sorting.

Viewing Device Details

Click **Details** in the **Operation** column to view the basic and version information of the corresponding device, as well as edit some device parameters. [Table 10-10](#) describes the editable parameters.

Table 10-10 Editable device parameters

Parameter	Description
Device Name	Edit the device name. The length is 3-30 characters.
NAT IP	Edit the NAT IP of the device.
Remark	Edit the remark information of the device. A maximum of 255 characters are allowed.

Parameter	Description
Belonging Group	Modify the device group to which the device belongs. For example, before deleting a device group, you can transfer the device to another device group as needed.
Scan Scope	Only scanning devices can configure this field.

Viewing Device Monitoring Information

Click **Monitor** in the **Operation** column to view the performance indicator information of the device for **Today**, the past **7 Days**, the past **30 Days**, and the past **90 Days**. [Table 10-11](#) describes device monitoring information. In the trend chart, the following operations can be performed:

- Hover over the chart to see the specific statistics in a specific category.
- Click the legend to hide/display the statistics of the corresponding category in the chart.

Table 10-11 Device monitoring information

Displayed Item	Description
CPU/Memory trend chart	Displays the usage trend of device CPU and memory in an area chart.
Traffic usage trend chart	Displays the total upstream/downstream traffic trend of the device in an area chart.
Device traffic monitoring trend chart	Displays the upstream/downstream traffic trend of the specified interface of the device in an area chart. Interfaces support multiple selections.

Viewing Device Configuration Information

This feature only supports devices with a status of **online**.

Click **More** in the **Operation** column and select **Configuration** to view the network interface configuration information of the device.

In the device interface configuration information list, click **Details** on the **Operation** column to view the configuration details of the corresponding interface.

Synchronizing Devices

Click **More** in the **Operation** column and select **Sync Device** to synchronize device version information, including system rule database version, firmware version, engine version, URL classification database version, virus feature database version, etc.

Disabling/Enabling a Device

Click **More** in the **Operation** column, select **Enable** or **Disable** to enable/disable the corresponding device.

Login Device

Click **More** in the **Operation** column and select **Login** to open the login page for the corresponding device. For the login and usage methods of the device, see the corresponding device manual.

Viewing a Certificate

Click **More** in the **Operation** column and select **License** to view the certificate information of the corresponding device.

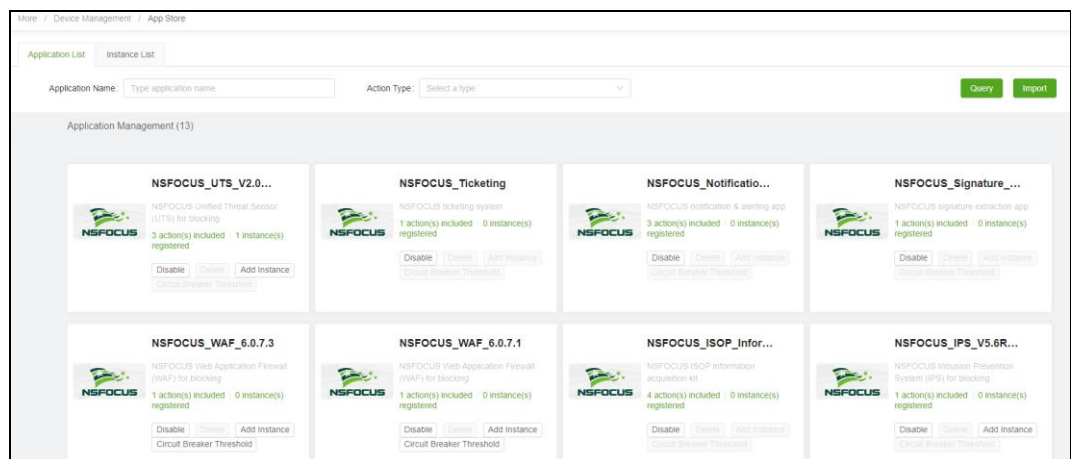
10.2.2 App Store

ISOP supports linking the automated handling case/playbook module with App store, which expands response to over a hundred types.

10.2.2.1 Application List

Choose **More > Device Manager > App Store > Application List**. This page displays the built-in applications of ISOP in the initial state, and supports importing more applications. You can add instances, disable/enable, query, delete instances, and view instruction documents.

Figure 10-1 Application list



Importing/Upgrading Applications

Click **Import** to import more applications for automated responses. Only single DAT file is supported and the file size cannot exceed **50 MB**. When importing, it is supported to check **Upgrade** to upgrade existing applications.

Adding an Instance

Before referencing applications in automated handling cases/playbooks, instances must be added first. Adding an instance means adding response devices to the application for performing response tasks during manual and automated processing. An application supports adding multiple instances.



Some built-in applications do not require adding instances, including **NSFOCUS_Ticketing**, **NSFOCUS_Notification_&_Alerting**, **NSFOCUS_Signature_Extraction** and **NSFOCUS_ISOP_Information_Acquisition**, and **NSFOCUS_API**.

Click **Add Instance**, configure instance parameters, and **Add** response devices to the corresponding application. Successfully added instances can be managed in the instance list. [Table 10-12](#) describes the instance parameters.

Table 10-12 Instance parameters

Parameter	Description
Device address	Select http , https , ssh , ftp , or snmp protocol, and fill in the corresponding response device IP and port number. Supports IPv4 , IPv6 , and domain names . Examples: - UTS device: 192.168.1.1:8805, protocol https. - ADS device: 192.168.1.1, protocol https. - WAF device: 192.168.1.1:8443, protocol https. - NF device: 192.168.1.1:8090, protocol https. - IPS device: 192.168.1.1:8081, protocol https. - UES device: 192.168.1.8, protocol https.
Description	Description information of the response device. Supports up to 256 characters and cannot contain the following characters: \'"%=<>
User Name/Password	When adding instances to some applications, it is necessary to configure authenticated username and password.

Disabling/Enabling an App

All applications are enabled by default.

Click **Disable** to disable the corresponding application and cannot be referenced in automated handling cases/playbooks.

Deleting an App

Click **Delete** to delete the corresponding application from the App store.

The built-in application does not support deletion.

Viewing Instance Documents

Click **View Document** to view the corresponding product documentation, including the linkage configuration manual and the current supported function description.

10.2.2.2 Instance List

Choose **More > Device Manager > App Store > Instance List**. The instance list page allows for editing and deleting response devices for manual and automated response handling.



If the **Device Status** of the instance is **Unavailable**, automated handling will fail in this device node.

10.2.3 Traffic Forensics

Currently, ISOP only supports UTS as a traffic forensics device.

Choose **More > Device Manager > Traffic Forensics Devices**. Click **Add** to configure the parameters of the traffic forensics device to add new traffic forensics devices. [Table 10-13](#) describes the traffic forensics device parameters.

After creating a new traffic forensics device, editing and deletion operations can be performed.

Table 10-13 Traffic forensics device parameters

Parameter	Description
Device Name	The name of the UTS device.
IP Address	The IP address of the UTS device.
User Name/Password	The API user name and password of the UTS device.

A Factory Parameter

This section describes the factory parameters of ISOP.

Role	User Name	Password
system administrator	admin	admin
auditor (not enabled by default, and should be manually enabled by the admin user)	auditor	The initial password is set by the admin user.

B Message Channel Configuration

Messages of automated orchestration use the notification channel of BSA, while messages of other modules use the notification channel of ISOP.

To configure the notification channel for BSA, perform the following steps:

Step 1 Click  on the shortcut toolbar of ISOP and choose **System > Message Channel > Channel Configuration**. All outgoing message channels are closed by default.

Step 2 Open the message channel, configure the corresponding message channel parameters, and then click **Send Test Message** to test whether the parameters are correct.

For details, see [Configuring a Notification Channel](#).

Step 3 (Optional) To send a manual handling alert message by ISOP, choose **Handling > Manual Handling > Alert Notification** and configure alert notification channels and customize alert notification rules.

For details, see [Alert Notification](#).

----End

C User Profile

To create ISOP system users, perform the following steps:

- Step 1** Click  on the shortcut toolbar of ISOP and choose **System > Privileges > Users**. On the left side of the page displays the user group structure and on the right side displays the user list.
- Step 2** Except for the **admin** account in the user list, all other accounts are in the disabled states by default. They need to be manually enabled by the admin account.
- Step 3** Click  on the left pane of the page, configure system user parameters, and click **Create**.

For descriptions of system user parameters, see *NSFOCUS BSA User Guide*.

By default, the state of the newly created system user is **Enabled**.

----**End**

D Component Configuration

ISOP components can be configured through the shortcut toolbar of ISOP.

D.1 Configuring an Asset

Before configuring assets, you need first configure the attributes, types, labels, and asset identification policies for the asset.

D.1.1 Managing Policies

Click  on the shortcut toolbar of ISOP and choose **Setting > Asset > Asset Setting > Policy Management**. This page displays the built-in asset identification policies by default. For more information on the management and operation methods, see [Customizing an Asset Identification Policy](#).

D.1.2 Managing Attributes

In addition to the basic information of assets, users can customize asset attributes based on actual situations, which can be used to edit more information of assets.

Click  on the shortcut toolbar of ISOP and choose **Setting > Asset > Asset Setting > Property Management**. This page displays the system's built-in asset attributes (including asset groups, geographic views, business views, organizational structure, and industries) in the initial state. Users can customize asset attributes and manage them, as shown in [Figure D-1](#).

Figure D-1 Asset attributes management

Asset attribute > Property Management				
Policy Management		Property Management	Type Management	Label Management
Attribute list (7)		Asset clear Attribute sorting Add attribute		
☐	Property Name	Attribute type	View properties	Action
☐	Asset group	Tree Attribute	Yes	Edit Remove
☐	Geographic	Tree Attribute	Yes	Edit Remove
☐	Business	Tree Attribute	Yes	Edit Remove
☐	Organization	Tree Attribute	Yes	Edit Remove
☐	Industry	Tree Attribute	Yes	Edit Remove
☐	Proxy IP	Text Attribute/String	No	Edit Remove
☐	Proxy Port	Text Attribute/String	No	Edit Remove

	- Asset attributes (including built-in and custom attributes) can support up to 20. - The built-in asset attributes can only be edited and cannot be deleted; The Text attribute cannot be edited. - After deleting an asset attribute, the configuration of that attribute in the asset is also deleted. - Custom asset attributes do not support restoration after deletion.
---	--

Creating Asset Attributes

Click **Add Property** and configure the asset attribute parameters to create a new asset attribute. [Table D-1](#) describes the asset attribute parameters.

Table D-1 Asset attribute parameters

Parameter	Description
Property type	Options include Text and Tree .
Property name	Supports Chinese, English, numbers, or a combination of them, and can include #_().\:/+& as well as spaces and tab characters. The name supports up to 32 characters and cannot be duplicated with existing attributes.
Property value type	When the attribute type is Text , the attribute value can be set to the following: - Integer: positive integer, 0, or negative integer. - Character: include Chinese characters, English characters, numbers, and other ASC II characters, which can include #_().\:/+& as well as spaces and tabs; The name length supports up to 30 characters. - Boolean: Yes or No. - Floating point: A number with a decimal part.

Sorting Attributes

Click **Property sorting** and drag asset attributes up and down in the attribute sorting box to rearrange their display order on the [Inventoried Asset](#) page.

Editing Attributes

In the asset attribute list, click **Edit** in the **Operation** column to edit the corresponding built-in attributes.

Removing Attributes

In the asset attribute list, click **Delete** in the **Operation** column to delete the corresponding custom asset attributes.

Clearing Assets

Click **Asset clear** and confirm to delete all assets in the asset database. Please operate with caution.

D.1.3 Managing Types

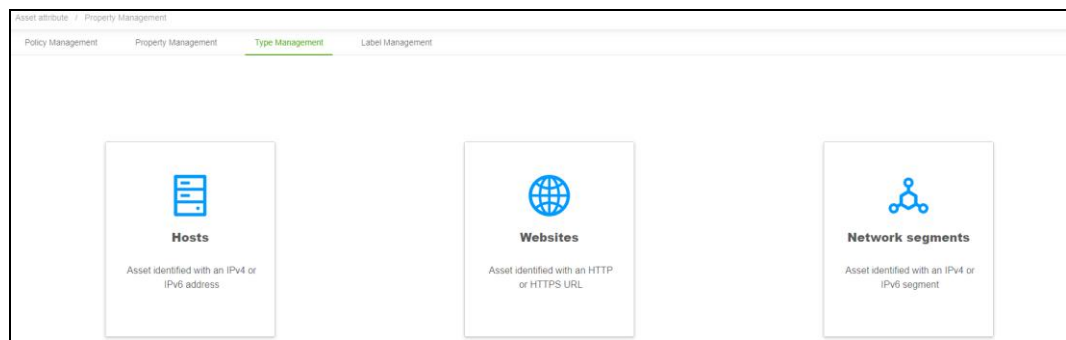
Through type management, asset attributes can be bound to assets. Tree attributes bound to the asset will be displayed in the asset management view.

- Hosts: Assets with **IPv4** and **IPv6** as the flag attribute.
- Websites: Assets with **https** and **http website URLs** as the flag attribute.
- Network segments: Assets with **IPv4** or **IPv6 network segments** as their flag attributes.

Taking the host asset as an example, the operation method for type binding is as follows:

- Step 1** Click  on the shortcut toolbar of ISOP and click **Setting > Asset > Asset Setting > Type Management**. The page is as shown in [Figure D-2](#).

Figure D-2 Asset type selection



- Step 2** Hover the mouse over the **Hosts** card.

- Step 3** Click  to enter the asset type editing page.

- Step 4** Configure the asset type parameters. [Table D-2](#) describes parameters for configuring the asset types.

Table D-2 Asset type parameters

Parameter	Description
Asset type name	The default is Hosts and cannot be modified.
Description	Displays the default description information of the host asset type which cannot be modified.
Tree attribute	By default, all built-in tree attributes are bound. Multiple selections are supported. For the configuration method of tree attributes, see Manag.
Text attribute	By default, all text attributes are bound. Multiple selections are supported. For the configuration method of text attributes, see Manag.

Step 5 Click **Confirm Set** to complete the attributes binding with assets and return to the asset type selecting page.

----End

D.1.4 Managing Labels

Through label management, asset labels created in [Asset](#) can be deleted in bulk.

Click  on the shortcut toolbar of ISOP and choose **Setting > Asset > Asset Setting > Label Management**. This page displays all asset labels that have been created. You can select and delete the labels one by one or in bulk. After the asset labels are deleted, they cannot be restored.

E Supplementary Information

This chapter describes the collaborative devices, components, rule packages, and databases that ISOP supports for access. For access methods, see *NSFOCUS ISOP Installation and Upgrade Manual*.

E.1 Collaborative Device Access Descriptions

The following table lists the supported collaborative devices of ISOP.

Supported Device	Version
NF (NSFOCUS Next Generation Firewall System)	V6.0R01F03 and above
AES (NSFOCUS Attack Entrapment System)	V5.0F00R00
UES (NSFOCUS Unified Endpoint Security Management System)	V1
NTA (NSFOCUS Network Traffic Analysis System)	V4.5
IPS/IDS (NSFOCUS Network Intrusion Prevention System/NSFOCUS Network Intrusion Detection System)	V5.6R10F00, V5.6.9 and below, V5.6.11F00
TAC (NSFOCUS Threat Analytics)	V2.0R01F00SP01
WAF (NSFOCUS Web Application Firewall)	V6.0.6.0 and above
UTS (NSFOCUS Unified Threat Sensor)	V2.0R00F00 and above V2.0R00F02 V2.0R00F03 and above
SSE (NSFOCUS Next-Generation Firewall Security Service Edge)	Any version
WEBSAFE (NSFOCUS WEB Security Monitoring System)	Any version

E.2 Supported Components

The following table lists the supported components in ISOP.

Component Name	Version	Component Type
Storage management	V2.0R01F05SP02.230510.ba227b9	Support
System alert	V2.0R01F05SP02.230517.f65356e	Support
Data access	V2.0R01F05SP01.230331.beac0a5	Support assembly
Report engine	V2.0R01F05.230309.fe3bf3d	Support
Asset management	V2.0R01F07.0be147c	Support
Device management	V2.0R01F05.230309.042e69e	Support
Northbound interface	V2.0R01F05.230309.3ca2f54	Support
Intelligence component	V3.0R01F07.b688333	Capability
Listening engine	V3.0R02F01SP02.81fe709	Capability
Threat and deduction	V3.0R01F07.71f0984	Capability
Predictive engine	V3.0R01F07.15c3cbc	Capability
Business common service	V3.0R01F07.8346c57	Capability
Allowlist	V3.0R01F07.70bc90a	Capability
Notification channel	V3.0R01F07.90e81c5	Capability
Assessment operations	V3.0R01F07.1706e05	Capability
Vulnerability management database	V3.0R01F06.53047	Capability
Alert analysis	V3.0R01F07.5efe26d	Capability
One-click response	V3.0R01F07.6231	Capability
Ticket management	V3.0R01F07.681d466	Capability
Vulnerability management	V3.0R01F07.33ab9a4	Capability
Extended detection and response	V3.0R01F07.537ed61	Capability
SOAR engine	V3.0R01F07.6214	Capability
Visual big screen	V3.0R01F07.f538419	Capability
Cascade management	V2.0R01F07.a972c59	Capability
Security governance	V3.0R01F06.52995	Capability
Scenario	V3.0R01F04.39644	Capability
5GC	V3.0R01F07.a5846e4	Capability
Toolbox	V3.0R01F06SP01.bbc1db3	Capability
NSFOCUS Intelligent Security Operations Platform (ISOP)	V3.0R01F07.1686194674	Application

E.3 Rule Packages

The following table lists the rule packages referenced by ISOP.

Rule Package Name	Version
Parsing rule	3.0.8.2956
Attack identification rule	1.0.0.1.1060048
Behavior analyzing rule	1.0.0.0.59665

E.4 Supported Databases

The following table lists the supported databases of ISOP.

Vendor	Device Type	Version
PostgreSQL	Database	9.X
SQL Server	Database	2000
SQL Server	Database	2005
SQL Server	Database	2008
DB2	Database	DB2 9.7.0
Oracle	Database	11g
Oracle	Database running logs	11g
Oracle	Database running logs	11.2.0.4