

HIRSCHMANN IT

A **BELDEN** BRAND

User Manual

Web UI

RAVEN4000 Intrusion Detection System

Web UI
Release 1.0 10/2020

Technical Support
<https://www.belden.com.cn>

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2020 Belden Singapore Pte Ltd

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Belden according to the best of the company's knowledge. Belden reserves the right to change the contents of this document without prior notice. Belden can give no guarantee in respect of the correctness or accuracy of the information in this document.

Belden can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann IT product site (<https://hirschmann-it.support.belden.com>).

Safety agreement

Safety location

By default, device should be placed in certain location that is safe, stable and reliable; all physical operators should be authorized; the operation CLI scripts should be properly kept, updated and reviewed.

Safety channel

Hirschmann IT devices support multiple managing methods, including Telnet, SSH, HTTP, HTTPS and so forth. All un-encrypted management protocols are not recommended. We highly recommend that our user only use SSH and HTTPs as the way to operate the devices, in order to ensure all management traffic is encrypted.

Safety storage

The login credentials, device configuration and status data should be kept in an appropriate place and be updated regularly and this information can only be accessed and managed by authorized people.

Contents

Safety agreement	3
1 About the Home	8
1.1 Overview	8
1.2 Login system	8
1.3 UI and elements	9
1.3.1 Menus.....	9
1.3.2 Toolbar.....	10
1.3.3 List.....	10
1.3.4 Common icons	11
1.4 Introduction to menu classification.....	11
1.5 Toolbar	12
1.5.1 Display menu.....	13
1.5.2 Full screen switch.....	13
1.5.3 Change skin	13
1.5.4 Important message.....	14
1.5.5 Personal information	14
1.6 Administrator default account	16
2 Home	17
2.1 Introduction to home	17
2.2 System resource status	17
2.3 Overall.....	18
2.4 DoS	18
2.5 Port scanning	18
2.6 Worm.....	18
2.7 Trojan	19
2.8 Attack type statistics.....	19
2.9 Feature detection Top 5	20
2.10 Flow curve trend	20
3 Known detection	22
3.1 Overview	22
3.2 Feature detection	22
3.2.1 Feature detection	22

3.2.2	Event details	24
3.2.3	Retrospective analysis	25
3.2.4	Virus detection.....	26
3.3	File detection.....	27
4	Flow statistics	28
4.1	Macro flow.....	28
4.1.1	Analysis	28
4.1.2	Alarm parameter config	34
4.2	Micro flow	40
4.2.1	Analysis	41
4.2.2	Alarm parameter config	47
4.2.3	Policy config	52
5	Statistical analysis.....	64
5.1	Report task configuration	65
5.1.1	New report task	65
5.1.2	Import a report task	72
5.1.3	Export a report task	73
5.1.4	Edit a task report	74
5.1.5	Delete a report task	75
5.1.6	Manually execute a report task	76
5.1.7	Related report file	76
5.1.8	Send reports by email	76
5.2	Report execution result.....	77
5.2.1	Query the report result	77
5.2.2	Delete a report directory.....	78
5.2.3	View the HTML file	79
5.2.4	Download a PDF file.....	80
5.2.5	Download a WORD file	80
5.2.6	Download an EXCEL file	81
5.2.7	Change IE's settings for opening the downloaded files directly	82
6	Detection configuration	83
6.1	Feature detection configuration	83
6.1.1	Overview	83
6.1.2	Policy set operation	83

6.1.3	New policy set	85
6.1.4	Import a policy set	86
6.1.5	Open a policy set.....	87
6.1.6	Edit a policy set	88
6.1.7	Derive a policy set	99
6.1.8	Export a policy set	100
6.1.9	Delete a policy set.....	101
6.1.10	Policy template	101
6.1.11	Customize the feature event	107
6.1.12	Customize a secondary event.....	122
6.1.13	DoS and scanning events	135
6.1.14	Weak password configuration	138
6.1.15	Event merging	140
6.2	Asset config.....	141
6.2.1	Key Web server.....	141
6.2.2	IP-MAC address binding	146
6.3	Device management.....	147
6.3.1	New device	147
6.3.2	Authorization configuration	148
6.3.3	Device status.....	150
6.3.4	Dynamic engine configuration.....	152
6.3.5	Superior status	153
6.4	File detection configuration	154
6.4.1	Blacklist	154
6.4.2	Whitelist.....	157
6.5	Virus detection configuration	158
7	System management.....	163
7.1	Response method.....	163
7.1.1	Syslog configuration	163
7.1.2	SNMP configuration	164
7.1.3	Email configuration.....	165
7.1.4	Firewall linkage.....	168
7.2	System maintenance	170
7.2.1	Upgrade management	170

7.2.2 System upgrade	172
7.2.3 Storage and maintenance	173
7.3 General config.....	176
7.3.1 Time config	176
7.3.2 Proxy config.....	177
7.3.3 Attention degree config	178
7.4 Running log.....	181
7.4.1 Running log	181
8 User management	182
8.1 User list	182
8.1.1 New user	183
8.1.2 Edit a user	185
8.1.3 Delete a user.....	185
8.1.4 Lock and unlock a user	185
8.1.5 Authorization.....	186
8.1.6 Security configuration.....	186
8.1.7 Lock and unlock configuration.....	188
8.2 Role list	191
8.2.1 New role	191
8.2.2 Edit a role	191
8.2.3 Delete a role	192
8.2.4 Authorization.....	192
8.3 Audit log	193
8.3.1 Query the audit log	193
8.3.2 Export the audit log	193
8.3.3 Clear the audit log	194
8.3.4 Change IE's settings for opening the downloaded files directly.....	194
8.3.5 Page up and down	194
Annex Engine configuration	196

1 About the Home

1.1 Overview

Any computer can access the system through a browser using HTTP or secure HTTPS. It is recommended to use IE 11.0/Firefox 3.x+/Google Chrome or later, with a minimum screen resolution of 1366 x 768.

This product requires Adobe Flash Player 9.0.124 or later. If the plug-in is not installed correctly, a prompt is displayed.

For better user experience, Firefox or Chrome browsers are recommended.



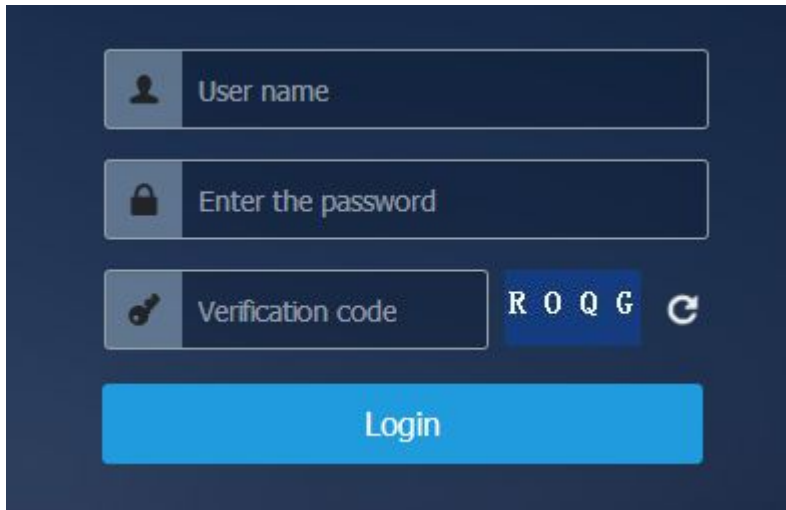
When using the IE 11 browser appears slowly response page or incomplete data display, please use Firefox or Google Chrome browsers instead .

1.2 Login system

Web login: The port 80 is used for HTTP-based login and the port 443 is used for HTTPS-based login. The system default IP address is **192.168.0.200**.

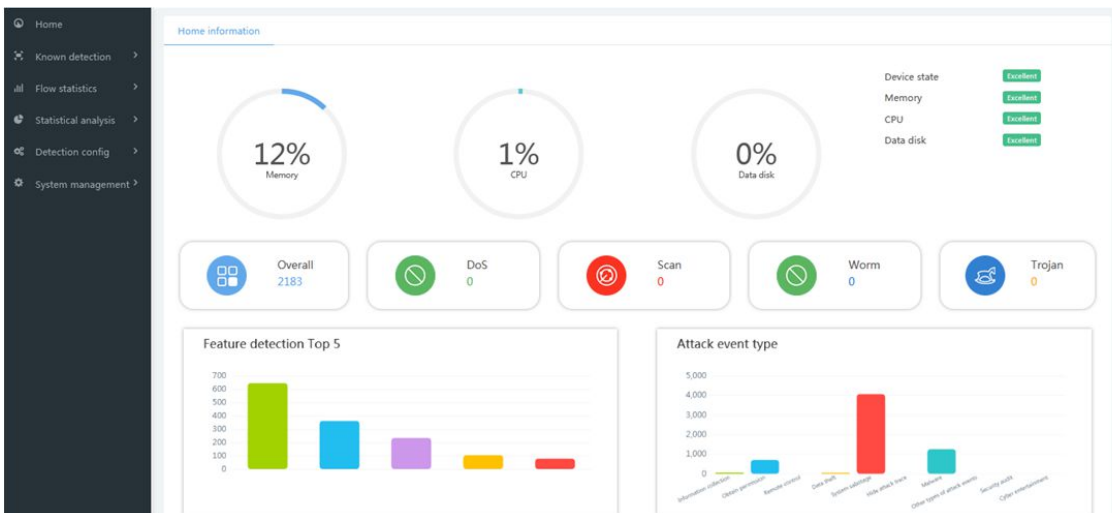
Enter the correct user name and password, press Enter or click the [**Login**] button to enter the system. The system default user name is **adm** and the default password is **Raven.public**.

If the password is entered incorrectly for a certain number of consecutive times, the system locks the host IP address attempting to log in for a period of time. At this time, no matter whether the entered password is correct or not, system access fails until the locking time expires or the user administrator manually unlocks the IP address.



1.3 UI and elements

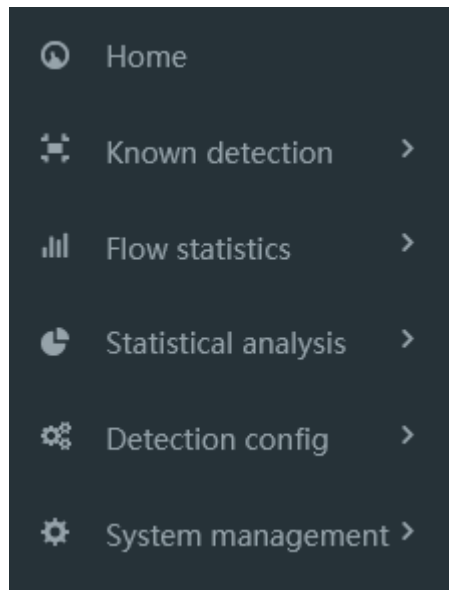
The UI of the RAVEN Intrusion Detection and Management System (hereinafter referred to as "System") consists of menus, toolbars, and display areas. You can click a menu to display sub-menus and then click sub-menus to switch between pages.



1.3.1 Menus

The menus provide configuration options for the system. Most functions need to be switched to the corresponding pages through the menus. The menu bar of the page

displays the first-level menu.


















1.3.2 Toolbar

The toolbar provides quick links to some functions.



1.3.3 List

Many management configuration pages are displayed in the form of lists, such as device management and feature detection configuration.

Policy set		Policy template	Feature event	Secondary event	DoS and scan type	Weak password config	Event merging
TYPE	NAME	DESCRIPTION	CREATION TIME	OPERATION			
system	Hot Event Set	Contains only the latest and most popular e	2017-02-02 00:00:00	    			
system	Intranet Event Set	All events other than online entertainment	2017-02-02 00:00:00	    			
system	Medium and High level Event Set	Contains only medium and high level event	2017-02-02 00:00:00	    			

The rightmost column in a list is generally the operation column, and operation buttons are provided to perform corresponding operations on the entry. Usually, operation buttons are provided above the list for the entire list, such as the **[New]** button, which can be used to add entries.

1.3.4 Common icons

The icons on pages help you with configuration. When the mouse hovers over an icon, a prompt message is usually displayed. The following table describes some common icons.

Icon	Name	Description
	Edit	Edits configurations.
	Delete	Deletes an entry.
	Deliver	Delivers a policy or content.
	Export	Exports a policy or content.

1.4 Introduction to menu classification

Home: View the current status of the system memory, CPU, data disk and authorization, display the statistics on the whole system, denial of service (DoS), port scanning, worms, and Trojan viruses on the day, and view feature detection Top 5 statistics, attack type statistics, and flow curve in the last 24 hours.

Known detection:

Feature detection: View the feature detection logs, virus detection logs.

File detection: View the file detection logs.

Flow statistics:

Macro flow: View the macro flow analysis results and configure macro flow alarm parameters.

Micro flow: View the micro flow analysis results and configure micro flow alarm parameters and policies.

Statistical analysis:

Task list: Formulate various data reports, display report tasks, and view and download report execution results.

Execution result: View the download execution reports, select download format, and

delete the reports.

Detection configuration:

Feature detection configuration: Customize the policy sets, policy templates, feature events, secondary events, DoS and scan type, weak passwords, and event merging rules.

Asset configuration: Configure the Key Web server and IP-MAC binding.

Device management: Add and edit equipment devices, including dynamic engine configuration, and view the connection status of the superior.

File detection configuration: Configure a blacklist/whitelist for file detection.

Virus detection configuration: Configure the virus detection protocol and file type of the intrusion detection and management system.

System management:

Response mode: Edit the Syslog, SNMP, email, and firewall linkage configuration.

System maintenance: The upgrade management module which is used for function upgrade of each module and the storage maintenance module which is used for data maintenance and alarm configuration.

General config: Including time, proxy, and attention degree configuration.

Running log: Display the running logs and export the system diagnosis logs.

User management:

This module is only visible to user administrators. It can be used to add, modify and delete configuration administrators, restricted administrators and custom roles, lock their accounts and modify passwords.

Audit log:

Auditors can view and edit the system operating audit logs.

1.5 Toolbar



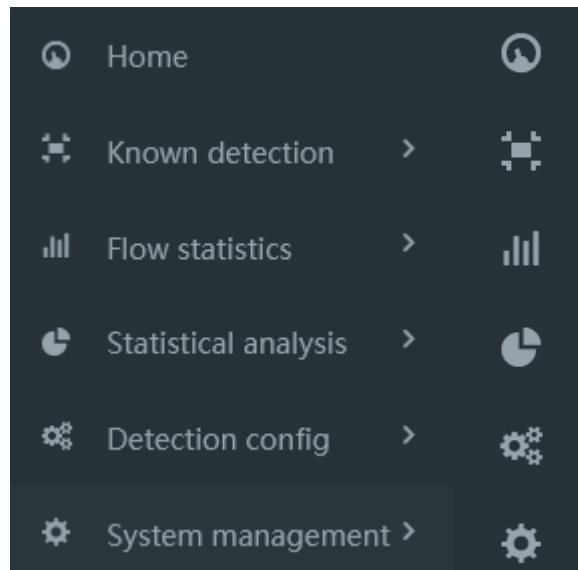
The tools from the left to the right are:

Display menu, full screen switch, change skin, important message, personal information

(Change password, About us, Power-off, and Logout).

1.5.1 Display menu

Perform overall contraction of the menu to reduce the proportion of pages occupied by the menu bar.



1.5.2 Full screen switch


Switch between the full screen mode and non-full screen mode.

1.5.3 Change skin

Change the skin color of web pages. Optional colors include: fresh green, night sky, classic blue, and elegant black.

 Fresh green

 Night sky

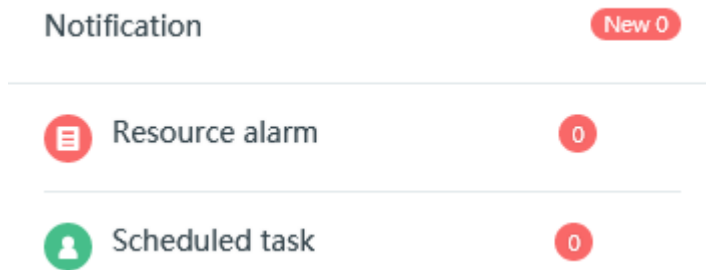
 Classic blue

 Elegant black

1.5.4 Important message

Message prompting function is provided on the page. When important messages are generated, users are prompted by the number of messages. After important messages are confirmed, the number is zeroed. You can click the icon to enter the new message list. You can query and export important message logs and result logs.

The important message prompt is located in the upper-right corner of the page. Two important messages are provided: resource alarms and scheduled tasks.



You can click the real-time important message resource alarm display icon to display the new message page.

Important message log query Export log query results

Query	Export	Confirm all	Delete in batches	All	One day	One week	One month	Customize
<input type="checkbox"/>	Message subject	Message type	Message content	Message state	Creation time	Operation		
<input type="checkbox"/>	Export feature detection	Scheduled task	Export feature det...	Confirmed	2018-12-01 13:51:54			
<input type="checkbox"/>	Scheduled task	Scheduled task	Feature analysis L...	Confirmed	2018-12-01 13:51:49			

1.5.5 Personal information

The **Personal information** tab consists of four buttons: **Change password**, **Abut us**, **Power-off**, and **Logout**.



 Change password

 About Us

 Power-off

 Logout

Change password:

This button allows the currently logged-in user to modify its password. The user administrator (admin), audit administrator (audit), and configuration administrator accounts can only change the password through this function.

Change password

*Login ID:	<input type="text" value="adm"/>
*Initial password:	<input type="text" value="Mandatory"/>
*New password:	<input type="text" value="required Password,length 6-20 place,need containLetters_ Numbers"/>
*Enter the password again:	<input type="text" value="It must be the same as the new password."/>
<input type="submit" value="Submit"/>	

Initial password: Enter the administrator's old password.

New password: Enter a new password for the administrator.

Enter the password again: Confirm the new password you entered.

About us:

This module mainly displays the product name, all rights reserved, product technical support, product and sales information, and copyright information. You can click the corresponding link to browse our product technical support, website, list of branches

and offices, and other related information, and you can also send your valuable comments and suggestions to our company by email.

Power-off:

This button is used to power-off the system.



The system can only be power-off through the " power-off " function on the Web page. Power cable plug-out and forced power-off by using the back panel button are considered abnormal operations, which may lead to system log loss, system configuration damage, and other failures.

Logout:

This button is used to exit the web login status.

1.6 Administrator default account

The default user administrator account of the system is **admin** and the password is **Raven.private**. The account is used to add, modify and delete configuration administrators.

The default audit administrator account of the system is **audit** and the password is **Raven.audit**. The account is used to view the operation logs of the user administrator and configuration administrator.

The default configuration administrator account of the system is **adm**, and the password is **Raven.public**. The configuration administrator can log in to the system and configure various security operations.

2 Home

2.1 Introduction to home

The home information page is divided into five areas for display:

System resource status: Display in graphics the percentage of the current memory usage, CPU usage, and data disk usage of the system, the device status rating, and authorization status.

Overall: Make statistics on all events occurring in the system.

DoS: Make statistics on the number of DoS and DDOS events that occurred on the day.

Port scanning: Make statistics on security scanning and exhaustive detection events occurring on the day.

Worm: Make statistics on the number of worm events that occurred on the day.

Trojan: Make statistics on Trojan back door events that occurred on the day.

Attack type statistics: Make statistics on threat events in the last 24 hours.

Feature detection Top 5: Make statistics on Top 5 Internet abuse or security threat events in the last 24 hours.

Flow curve (last 24 hours): Display the total flow, email flow, web flow, database flow, P2P flow, and other flow curves of the engine in the last 24 hours.

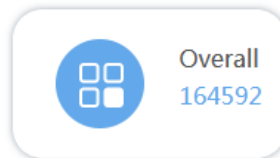
2.2 System resource status

Display in graphics the percentage of the current memory usage, CPU usage, data disk usage of the system and the device status.



2.3 Overall

Make statistics on all events occurring in the system.



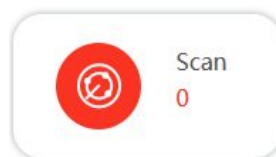
2.4 DoS

Make statistics on the number of DoS and DDOS events that occurred on the day.



2.5 Port scanning

Make statistics on security scanning and exhaustive detection events occurring on the day.



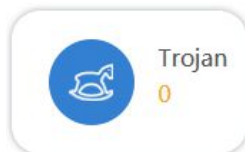
2.6 Worm

Make statistics on the number of worm events that occurred on the day.



2.7 Trojan

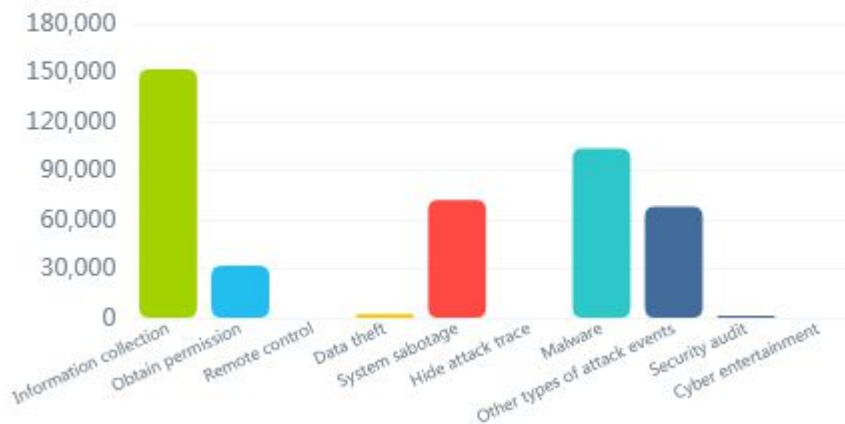
Make statistics on Trojan back door events that occurred on the day.



2.8 Attack type statistics

Record the threat events that occurred in the last 24 hours, and classify the statistics according to the attack type. The specific attack types include information collection, obtain permission, remote control, data theft, system sabotage, hide attack trace, other types of attack events, security audit, and Cyber entertainment. You can hover the mouse over a graph to display the number of attacks that have occurred in the last 24 hours.

Attack event type



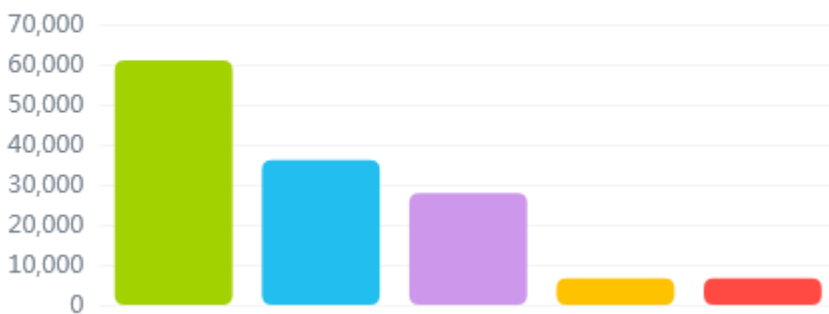
When you click the graph, the page is redirected to the log query page of the corresponding attack type event.

Feature detection		Virus detection							
Parameter config		Query	Export	Classification statistics		One day	One week	One month	Customize
Event level	Security type	Attack type	Prevalence	Event name	Source IP	Destination IP	Engine		
Medium risk	null	Information collec...	Not popular	HTTP_Sensitive_file_and_directo...	192.168.3....	219.234.94....	192.168.13.8		
Medium risk	null	Information collec...	Not popular	SCAN_ICMP_Scanning_Explorati...	192.168.1....	Merged	192.168.13.8		
Medium risk	null	Information collec...	Not popular	FINGER_Root_User_Query	10.0.0.158	10.0.0.163	192.168.13.8		
Medium risk	null	Information collec...	Not popular	TCP_EasyScan_Vulnerability_Scan	192.168.5....	192.168.5.18	192.168.13.8		
Medium risk	null	Information collec...	Not popular	HTTP_Sensitive_file_and_directo...	192.168.3....	219.234.94....	192.168.13.8		
Medium risk	null	Information collec...	Not popular	SCAN_ICMP_Scanning_Explorati...	192.168.1....	Merged	192.168.13.8		
Medium risk	null	Information collec...	Not popular	TCP_EasyScan_Vulnerability_Scan	192.168.5....	192.168.5.18	192.168.13.8		

2.9 Feature detection Top 5

The top 5 attack events detected by the system in the last 24 hours are displayed with a bar chart. In the following figure, the abscissa is the top ranking, and the ordinate is the number of events. When you hover the mouse over the bar chart, the specific event name is displayed.

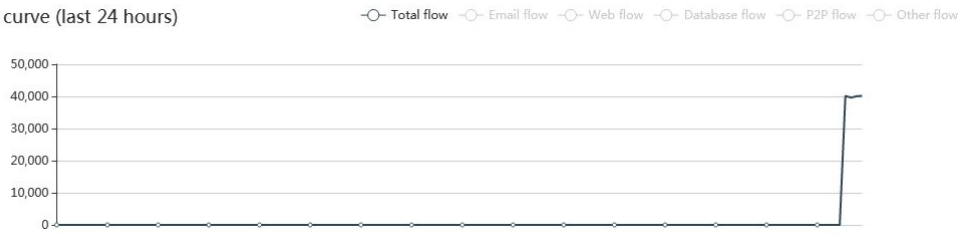
Feature detection Top 5



2.10 Flow curve trend

Statistics on the flow detected by the engine is made and displayed as a curve. In the total flow curve, the total network flow in the last 24 hours is displayed.

flow curve (last 24 hours)



3 Known detection

3.1 Overview











This function is used to display information such as feature detection and file detection that match known features.

3.2 Feature detection

This function is used to display the threat events and virus logs recently detected by the system. It is used to know the current threats to the network and ensure timely tracking, locating, and monitoring when the system suffers from large-scale attacks and virus attacks. Features matched include feature events in the event library and custom feature events.

3.2.1 Feature detection

The feature detection log displays the following information: event level, security type, attack type, prevalence, event name, source IP address, destination IP address, engine, occurrence time, event ID, protocol type, and operation.

Feature detection		Virus detection						
Parameter config	Query	Export	Classification statistics	One day	One week	One month	Customize	
Event level	Attack type	Prevalence	Event name	Source IP	Destination IP	Engine	Occurrence time	Operation
High risk	Malware	Popular	HTTP_XSS_Injection	192.168.3...	219.234.94....	192.168.13.8	2018-12-01 14:15:11	 
High risk	Malware	Popular	HTTP_XSS_Attack	192.168.3...	219.234.94....	192.168.13.8	2018-12-01 14:15:11	 
Medium risk	System sabota...	Not popular	HTTP_/etc/passwd_Access	192.168.3...	219.234.94....	192.168.13.8	2018-12-01 14:15:06	 
High risk	Malware	Popular	HTTP_XSS_Injection	192.168.3...	219.234.94....	192.168.13.8	2018-12-01 14:15:01	 
High risk	Malware	Popular	HTTP_XSS_Attack	192.168.3...	219.234.94....	192.168.13.8	2018-12-01 14:14:53	 

Parameter description:

Event level: High-risk, medium-risk, low-risk, and non-attack.

Security type: Events are classified by security type.

Attack type: Events are classified by attack type.

Prevalence: Popular, not popular and no threat.

Operations include parameter configuration, query, export and classified statistics.

Parameter configuration:

Users can customize the data columns displayed in the event log as required.

Configuration items include: event level, security type, attack type, prevalence, event name, source IP address, destination IP address, engine, occurrence time, event ID, protocol type, and operation.

Display column Event level Security type Attack type Prevalence Event name Source IP address Destination IP address Engine Occurrence time Event ID Protocol type Operation

Query:

Click the **[Query]** button to filter the log list as required. Query configuration items include:

Event level: Non-attack, low-risk, medium-risk, and high-risk.

Attack type: Network entertainment, information collection, access rights, security audit, remote control, data theft, system damage, hiding attack traces, harmful programs, malicious websites, and other types of attacks.

IP address and IP address range: Filter and query events by IP address or IP address range.

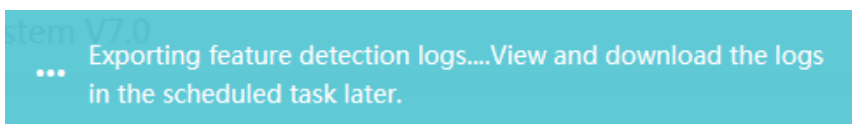
Event name: Manually enter the event name for filtering query.

Engine: All engines and stand-alone engine.

Event level : Non-a... Low risk Mediu... High ri...
Attack type : Cyber ... Inform... Obtain... Remot... Securit... Data t... Syste... Hide a... More
IP : IP
Event name :
Engine : All engines

Export:

When the **[Export]** button is clicked, the export operation is performed in the background. After successful export, important messages are prompted. You can click a scheduled task to enter the export result log query module, and click the **[Download]** button in the operation column to export the logs.

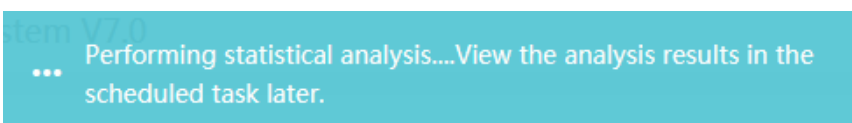


Important message log query Export log query results

SN	File name	File description	Creation time	Operation
1	temp_1543645060632.zip	Export feature detection logs successfully	2018-12-01 14:17:40	⬇️ 🗑️
2	temp_1543643514029.zip	Export feature detection logs successfully	2018-12-01 13:51:54	⬇️ 🗑️

Classified statistics:

You can click the **[Classified statistics]** button to perform classified statistics on the log results. After the statistics are successful, important messages are prompted. You can click a scheduled task to enter the message log, and click a message to view the results of classified statistics. Statistics on attacks can be made in terms of high-risk, medium-risk, low-risk, non-attack and total number.



Important message log query Export log query results

Query Export Confirm all Delete in batches **All** One day One week One month Customize

<input type="checkbox"/>	Message subject	Message type	Message content	Message state	Creation time	Operation
<input type="checkbox"/>	Scheduled task	Scheduled task	Feature analysis I...	Confirmed	2018-12-01 14:17:57	🗑️

3.2.2 Event details

You can double-click a reported event or click the **[Details]** button in the operation column to open the event details window, which displays the event details.

Event details description ×

Event name: HTTP_XSS_injection
 Event alias: Detected XSS injection attacks

Basic event information

Occurrence time: 2018-12-01 14:19:01
 Event level: High risk
 Security type:
 Number of occurrences: 255
 Prevalence: Popular
 Affected system: Web server

	IP address	Retrospective analysis	Port	MAC address
Destination	219.234.94.233	Destination IP address analysis	Merged	00:50:BA:CB:95:D0
Source	192.168.3.50	Source IP address analysis	Merged	00:0D:60:FB:19:4B

Event description

XSS (Cross-Site Scripting) means inserting malicious codes in the html codes of a remote WEB page; users regard the page reliable by mistake, and when the users open the page, the browser will automatically download the malicious codes and run the scr


Event response parameter

```

nic=1;
xss=URL:2;<
script>
alert(\*
```

Through event details, you can quickly view the basic event information, event description, and event response parameters. You can click the destination IP address analysis (source IP address analysis) in retrospective analysis to view the characteristic event log of the corresponding destination IP address (source IP address).

3.2.3 Retrospective analysis

You can click the **[Retrospective analysis]** button  in the event log operation column to go to the retrospective analysis page.

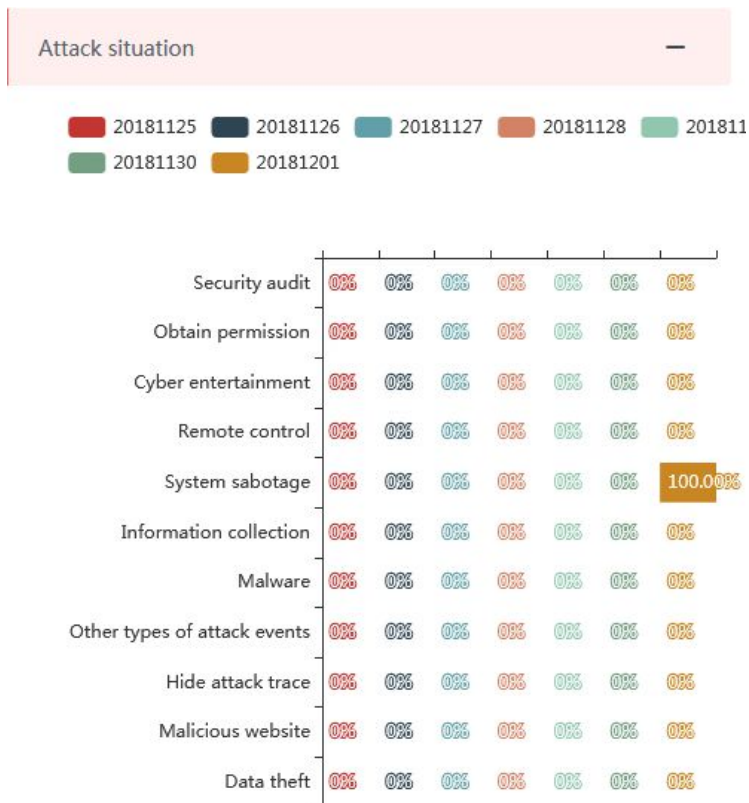
Event perspective: Display the details of this event log.

Attacker perspective: Display the fingerprint, threat intelligence, and attack situation statistics of the assets of the source IP address.

Prospective of the attacked: Display the fingerprint, threat intelligence, and attack situation statistics of the assets of the destination IP address.

Asset fingerprint: Unrecorded asset information is displayed as N/A.

Attack situation: Display the statistics on the number of attacks of each type from this IP address in the last 7 days.



3.2.4 Virus detection

The virus detection log displays the virus name, infected file, protocol type, source IP address, destination IP address, engine, and time of occurrence.

Query:

You can click the **[Query]** button to filter the log list as required. Query configuration items include: source port, destination port, virus name, packet capturing port, engine, source IP address, source IP address range, destination IP address, and destination IP address range.

Export:

When the **[Export]** button is clicked, the export operation is performed in the background. After successful export, important messages are prompted. You can click a scheduled task to enter the export result log query module, and click the **[Download]** button in the operation column to export the logs.

Details:

You can double-click a virus detection log to display the virus log details.

Feature detection		Virus detection				
Query	Export	All	One day	One week	One month	Customize
Virus name	Infected file	Protocol type	Source IP	Destination IP	Engine	Occurrence time
AdWare/Win32.Agent.a..	[http]time-2013-7-1..	FTP	192.168.14.201(54759)	192.168.14.207(21)	192.168.13.8	2018-12-15 15:12:30
AdWare/Win32.Agent.a..	[http]time-2013-7-1..	FTP	192.168.14.201(54759)	192.168.14.207(21)	192.168.13.8	2018-12-15 15:12:23
AdWare/Win32.Agent.a..	[http]time-2013-7-1..	FTP	192.168.14.201(54759)	192.168.14.207(21)	192.168.13.8	2018-12-15 15:12:17
AdWare/Win32.Agent.a..	[http]time-2013-7-1..	FTP	192.168.14.201(54759)	192.168.14.207(21)	192.168.13.8	2018-12-15 15:12:11

3.3 File detection

The file detection log is used to record the results of static detection and dynamic detection of network files. The data columns displayed by default for malicious sample events include the result, time, source IP address, destination IP address, sample name, sample type, detection method, protocol type, capture device, and operation column.

Query:

You can click the **[Query]** button to filter the log list as required. Query configuration items include: sample name, MD5 value, source IP address, destination IP address, protocol, detection result, sample type, and test method.

Export log:

You can click the **[Export log]** button to directly export the network sample detection log to an .xls file.

Operation column:

Details: You can click the **[Details]** button of a sample log to display the log details, including the sample information, detection mode, and protocol information.

View report: The button is displayed only when a dynamic detection result log is available. You can click the **[View report]** button to display the sample dynamic detection report.

More: Provide more operation functions, including report download (only for dynamic detection logs), file download, blacklisting, and whitelisting.

4 Flow statistics

4.1 Macro flow

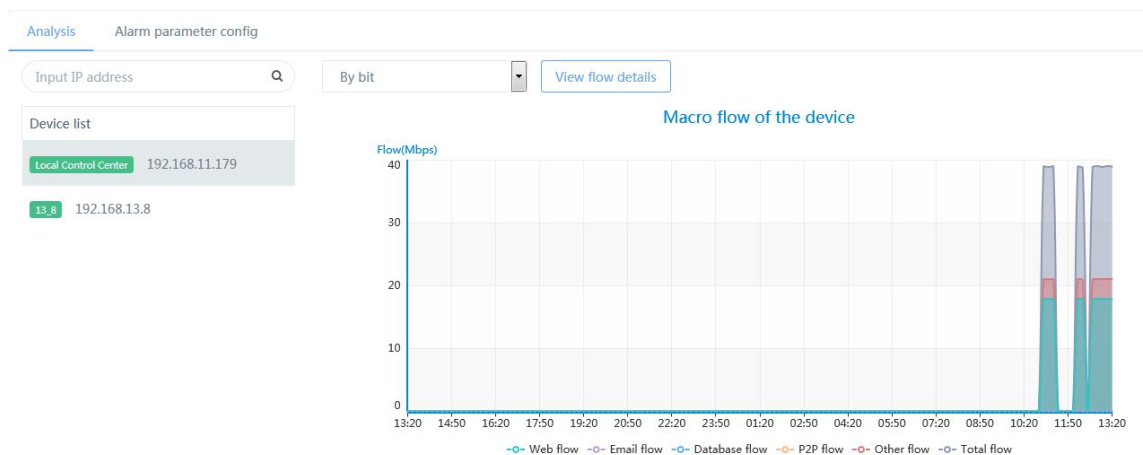
The macro flow module mainly displays the flow information of each engine of the system, including macro flow analysis and macro flow alarm parameter settings. The macro flow analysis function is mainly used to make statistics on the flow of the last 24 hours, the flow of the last 30 days, the real-time distribution of the flow, and the alarm information list.

Flow is measured every 10 minutes and the minimum unit of measurement is bps, that is, bits per second. You can choose to display flow by number of bits or by number of packets.

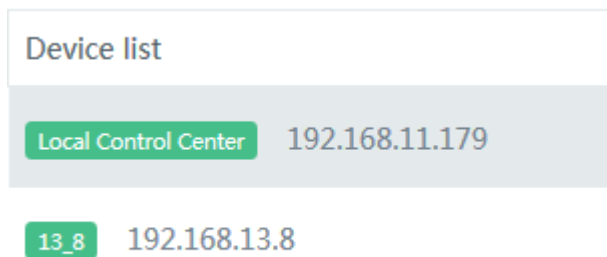
Flow alarm can be based on threshold contrast analysis or automatic machine analysis. According to the analysis results, it can be judged that flow is low anomaly, slightly high anomaly, moderately high anomaly, and severely high anomaly.

4.1.1 Analysis

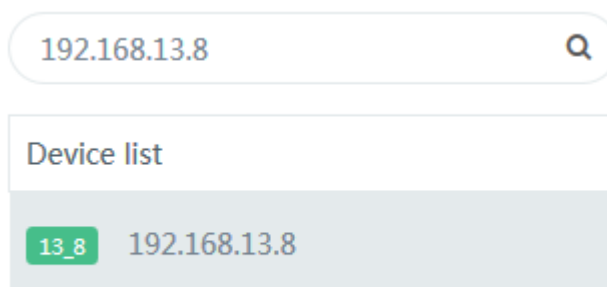
The first macro flow statistics page displays the total flow information of all engines in the system, including the web flow, email flow, database flow, P2P flow, other flow, and total flow.



The device list is listed on the left side of the page, including the control center at the current level and the engines mounted under this control center.

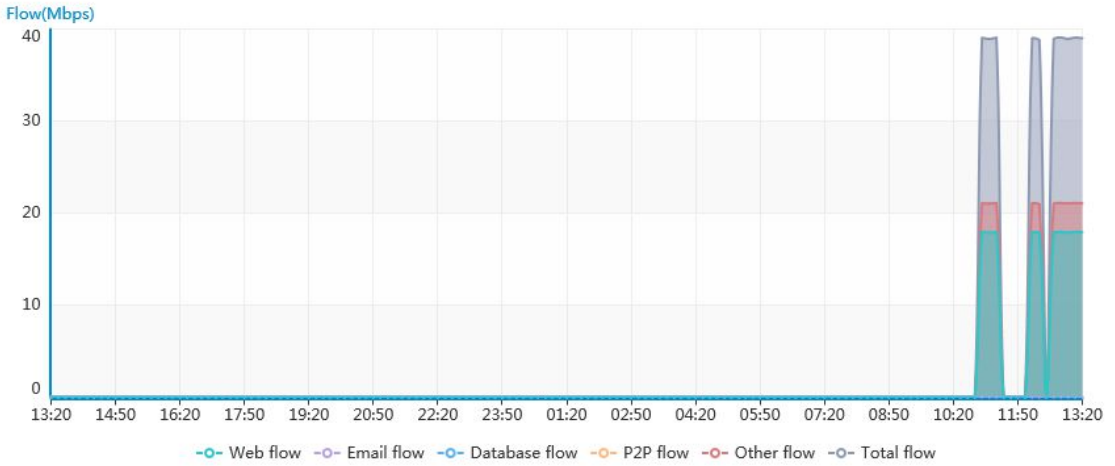


You can enter the engine IP address in the query column below the device list to locate the engine.



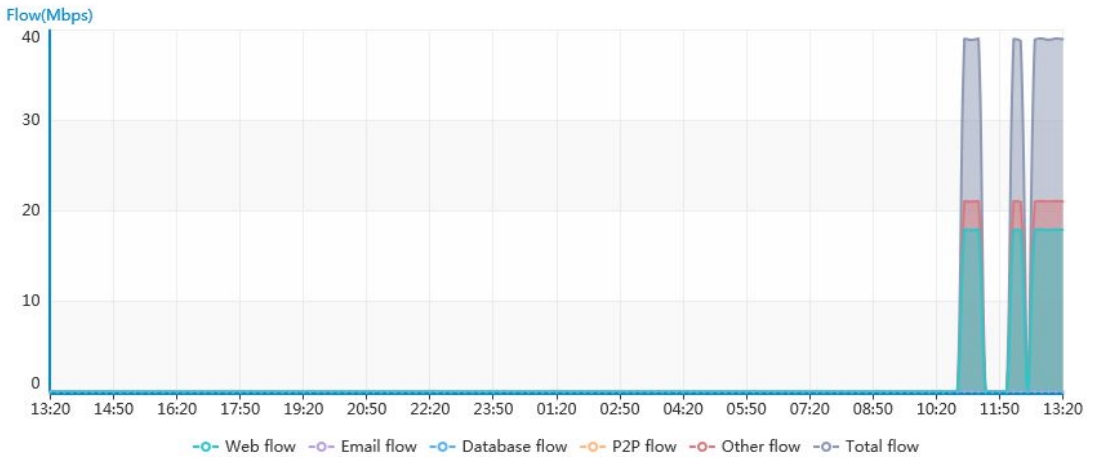
The right side of the page displays the macro flow area map of the selected engine or control center (flow change area map from 00:00 to the current time, one point every 10 minutes). The content includes: the Web flow, email flow, database flow, P2P flow, other flow, and total flow. The current flow value is displayed in bytes (bps).

Macro flow of the device

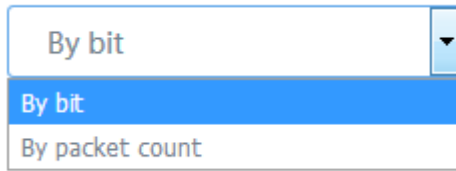


You can hover the mouse over the area map of the corresponding time point to view the flow at that time point.

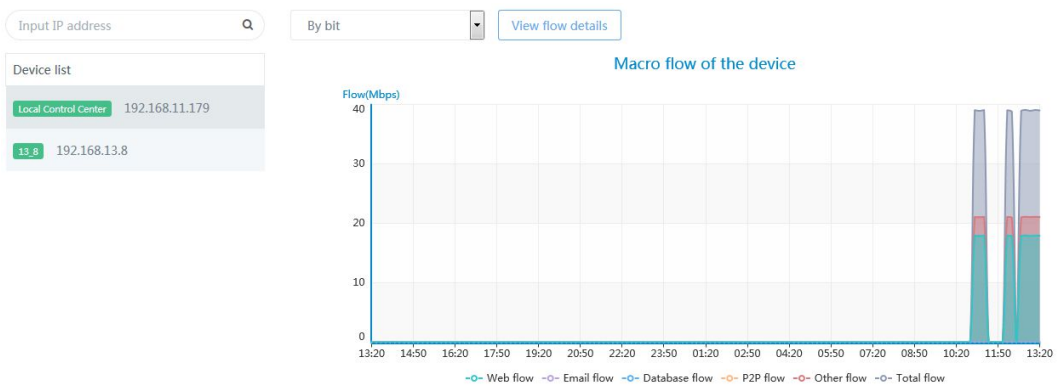
Macro flow of the device



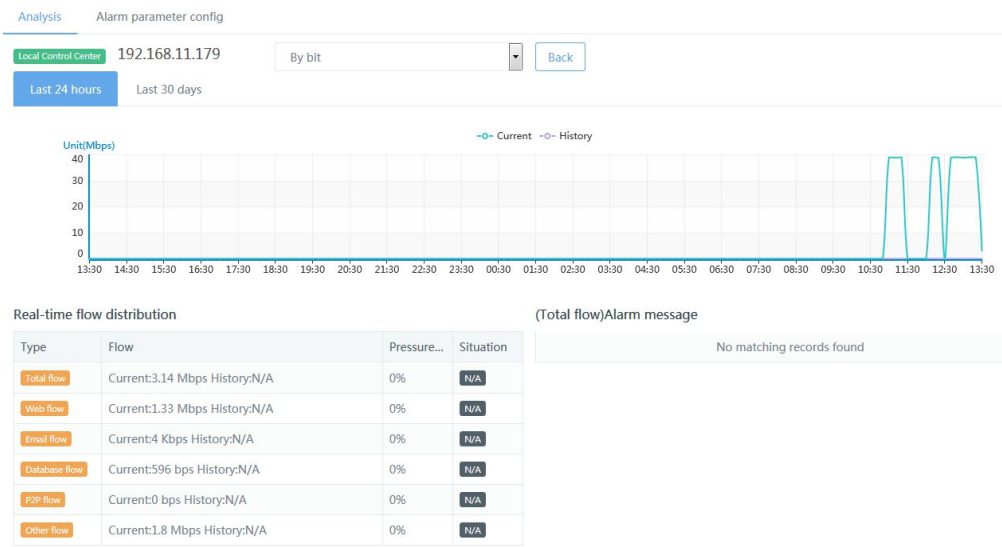
You can click to switch the display mode at the top of the page to select to display the current flow of each device by the number of packets (pps) or by the number of bits (bps).



You can click a device in the device list to display the macro flow of the device on the right of the page. For example, if you want to view the macro flow of the engine 192.168.11.179, click 192.168.11.179 in the device list.



You can click the **[View flow details]** button at the top of the page to enter the macro flow detailed analysis page.



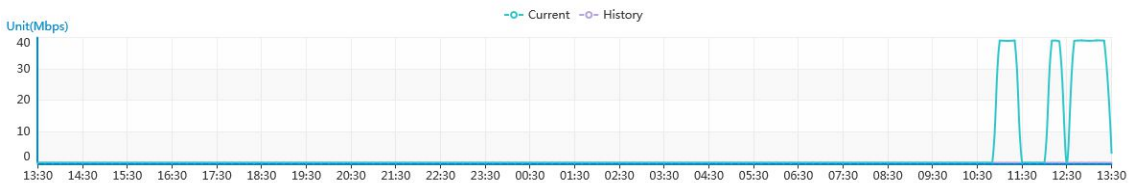
You can click the **[Back]** button on the flow analysis details page to return to the macro

flow analysis page.

The macro flow detailed analysis page mainly displays the flow in the last 24 hours, the flow in the last 30 days, the real-time flow distribution, and alarm message.

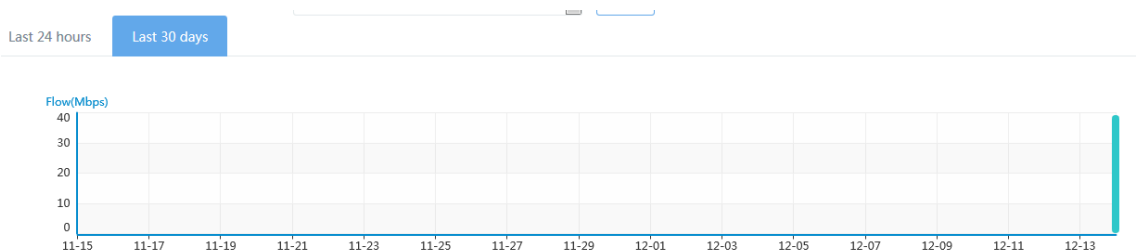
Flow in the last 24 hours:

This module displays the macro flow statistics in the last 24 hours every 10 minutes. When the mouse is hovered over the corresponding flow curve at the time point, the corresponding flow is displayed, with the green curve representing the current flow situation and the purple curve representing the historical flow situation.

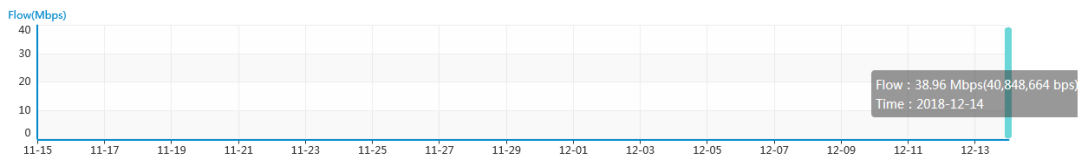


Flow in the last 30 days:

You can click the "**Last 30 days**" tab on the page to display the average daily flow of the current device in the last 30 days.



You can hover the mouse over a certain point time to display the flow for the day.



Real-time flow distribution:

The flow distribution list displays the flow type, the flow value of the corresponding type, the flow pressure, and the running situation, and the running situation tab displays the current running status. There are six types of flow: total flow, web flow, email flow,

database flow, P2P flow, and other flow.

Real-time flow distribution

Type	Flow	Pressure...	Situation
Total flow	Current:3.14 Mbps History:N/A	0%	N/A
Web flow	Current:1.33 Mbps History:N/A	0%	N/A
Email flow	Current:4 Kbps History:N/A	0%	N/A
Database flow	Current:596 bps History:N/A	0%	N/A
P2P flow	Current:0 bps History:N/A	0%	N/A
Other flow	Current:1.8 Mbps History:N/A	0%	N/A

Click on different flow types, and other display modules will switch to corresponding flow display. For example, click on the total flow icon in the real-time distribution of flow, the last 24 hours of flow, the last 30 days of flow and alarm information will show the operation situation of the total flow.

Alarm message:

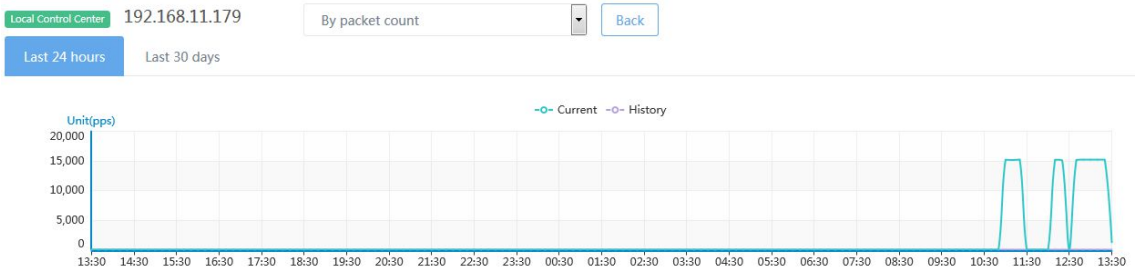
This module displays the comparison of various flow at various time points with the set threshold or historical flow in the same period.

(Total flow)Alarm message

No matching records found

After you click the display mode switch button at the top of the page, the flow display mode (by the number of bits or by the number of packets) is switched. If you choose to display by the number of packets, the flow in the last 24 hours, the flow in the last 30

days, real-time flow distribution, and the alarm message modules will display the running situation of the Web flow.



4.1.2 Alarm parameter config

You can choose **Flow statistics > Macro flow > Alarm parameter config** to view six types of macro flow analysis parameters. By default, the system displays the comparison result of historical flow in the same period and performs automatic machine analysis. Default system parameters are: low coefficient: 50; slightly high coefficient: 150; moderately high coefficient: 200; and severely high coefficient: above 200.

Flow type	Analysis method	Response method	Configuration type	Update time	Operation
Total flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
Web flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
Email flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
Database flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
FTP flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
Other flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎

Showing 1 to 6 of 6 entries Show 10 entries 1

You can click the **[Edit]** button after a flow type in the operation column to display the flow alarm parameters of this type, for example, the Web flow.

Alarm parameter Total flow ×

Configuration type: ✓ Default config Custom config

Exception analysis: ✓ Comparison based on data in the same period Threshold comparison

Low:	<input style="width: 95%;" type="text" value="0"/>	<input style="width: 95%;" type="text" value="50"/>	%
Slightly high:	<input style="width: 95%;" type="text" value="100"/>	<input style="width: 95%;" type="text" value="150"/>	%
Moderately high:	<input style="width: 95%;" type="text" value="150"/>	<input style="width: 95%;" type="text" value="200"/>	%
Severely high:	<input style="width: 95%;" type="text" value="200"/>	<input style="width: 95%;" type="text" value="∞"/>	%

Response method:

Log

Low Slightly high Moderately high Severely high

Submit

To use the custom config mode, you can click the configuration type setting switch button to enter the custom config mode.

Configuration type: ✓ Default config Custom config

Alarm parameter Total flow ×

Configuration type: Default config ✓ Custom config

Exception analysis: ✓ Comparison based on data in the same period Threshold comparison

Low:	<input style="width: 95%;" type="text" value="0"/>	<input style="width: 95%;" type="text" value="50"/>	%
Slightly high:	<input style="width: 95%;" type="text" value="50"/>	<input style="width: 95%;" type="text" value="150"/>	%
Moderately high:	<input style="width: 95%;" type="text" value="150"/>	<input style="width: 95%;" type="text" value="200"/>	%
Severely high:	<input style="width: 95%;" type="text" value="200"/>	<input style="width: 95%;" type="text" value="∞"/>	%

Response method:

Log

Low Slightly high Moderately high Severely high

Submit

The flow anomaly analysis method includes Comparison based on data in the same period and threshold comparison.

Comparison based on data in the same period:

When the default configuration is used, this mode is used by default. The system compares the flow (bps) of the engine at the current 10-minute time point with the configured automatic analysis coefficient and triggers an alarm if any exception is found. When the custom config is used, the system compares the number of flow packets (pps) of the engine at the current 10-minute time point with the configured automatic analysis coefficient and triggers an alarm if any exception is found.

In Comparison based on data in the same period mode, you can modify the flow analysis parameters. The alarm levels are Low, Slightly High, Moderately High, and Severely High.

Alarm parameter Total flow

Configuration type: Default config Custom config

Exception analysis: Comparison based on data in the same period Threshold comparison

Low:	<input type="text" value="0"/>	<input type="text" value="50"/>	%
Slightly high:	<input type="text" value="50"/>	<input type="text" value="150"/>	%
Moderately high:	<input type="text" value="150"/>	<input type="text" value="200"/>	%
Severely high:	<input type="text" value="200"/>	<input type="text" value="∞"/>	%

Response method:

Log

Low Slightly high Moderately high Severely high

Email ?

You can configure the response method as required, including whether to generate the alarm log, whether to trigger an alarm, enable or disable alarms at which level, and whether to send the alarm message through emails.

Response method:

Log

Low Slightly high Moderately high Severely high

Email ?

When no email address is configured at the control center, the message "No email list is available" is displayed. Choose **System management > Response method > Email config** to enable email alarm.

Log

No email list is available. Choose System management > Response method > Email config to enable email alarm.

Email ?

Slightly high Moderately high Severely high

When email addresses are configured at the control center, the recipient list is displayed. You can select a recipient and then the alarm message is sent to the

recipient so that relevant personnel can view the flow in real time.

Email ?

<input type="checkbox"/>	Name	Email
<input type="checkbox"/>	jerry	778541123@facebook...

Threshold comparison:

If threshold comparison is enabled, the system compares the flow of the engine at the current 10-minute time point with the configured threshold and triggers an alarm when any exception is found.

You can click the flow anomaly analysis method switch button to switch to the threshold comparison mode.

Exception analysis:

Comparison based on data in the same period

Threshold comparison

In threshold comparison mode, you can modify the flow analysis parameters. The alarm levels are Low, Slightly High, Moderately High, and Severely High.

Exception analysis:

Comparison based on data in the same period

Threshold comparison

Unit: bps(By bit)

Order of magnitudes: 1

Low: 0 50 bps

Slightly high: 50 150 bps

Moderately high: 150 200 bps

Severely high: 200 ∞ bps

Response method:

Log

Submit

The default flow unit is bps, which can be configured through parameters. You can expand the unit drop-down box, enter the parameter setting page, and select the flow unit. The selected flow unit is used during last login until you modify it.

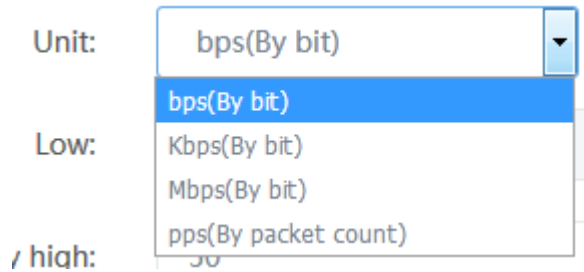
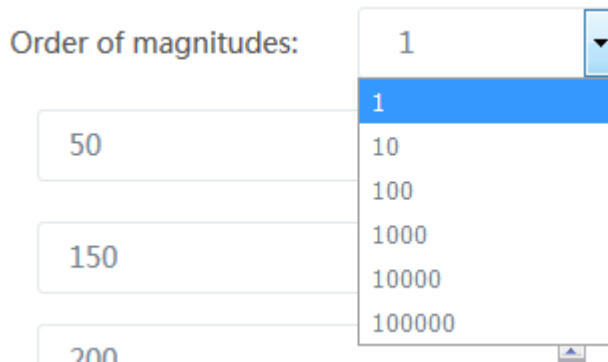


Figure 4-24 Unit parameter setting

You can expand the magnitude order drop-down box to set the magnitude order. After configuration, the range after the corresponding alarm level will be automatically multiplied by the magnitude order.

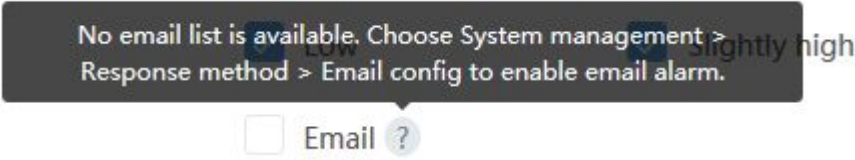


You can configure the response method as required, including whether to generate the alarm log, whether to trigger an alarm, enable or disable alarms at which level, and whether to send the alarm message through emails.

Response method:

- Log
- Low Slightly high Moderately high Severely high
- Email ?

When no email address is configured at the control center, the message "No email list is available" is displayed. Choose **System management > Response method > Email config** to enable email alarm.



When email addresses are configured at the control center, the recipient list is displayed. You can select a recipient and then the alarm message is sent to the recipient so that relevant personnel can analyze the flow in real time.

Email ?

<input type="checkbox"/>	Name	Email
<input type="checkbox"/>	jerry	778541123@facebook...

After custom alarm parameter configurations are stored, the configurations are displayed in the macro flow parameter configuration settings list.

Flow type	Analysis method	Response method	Configuration type	Update time	Operation
Total flow	Comparison of the same period	Log/Alarm	Custom config	2018-12-14 09:47:16	✎
Web flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
Email flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
Database flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
P2P flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎
Other flow	Comparison of the same period	Log/Alarm	Default config	2017-04-10 13:13:02	✎

Showing 1 to 6 of 6 entries Show 10 entries 1

4.2 Micro flow

The micro flow statistics module mainly displays the flow of each engine of the system, including micro flow analysis and micro flow alarm parameter settings. The micro flow analysis function is mainly used to make statistics on the real-time micro flow distribution of P2P, DNS, IP address/port, emphasis protocol, key Operation, and critical web behavior list.

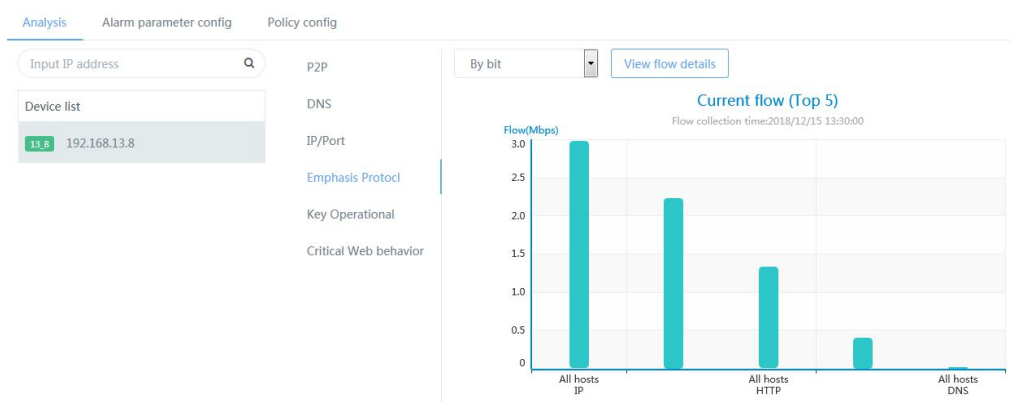
Flow is measured every 10 minutes and the minimum unit of measurement is bps, that is, bits per second. The engine adaptively displays the flow units based on the detected flow. The flow unit can be bps, Kbps, Mbps, or Gbps (by the number of bits) or pps (by the number of packets).

Based on threshold comparison or automatic machine analysis configured, the flow

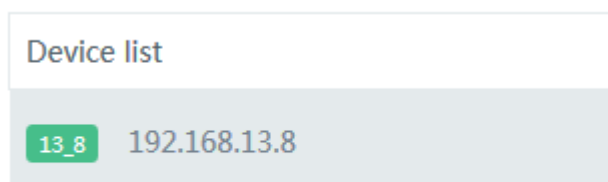
alarm module can judge whether the flow is low, slightly high, moderately high, or severely high based on the analysis results.

4.2.1 Analysis

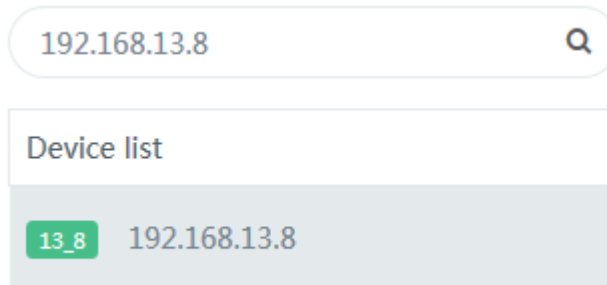
The first micro flow statistics page displays the flow of all engines in the system, including flow of P2P, DNS, IP address/port, key operational, and critical web behaviors (among them, the P2P flow type covers 16 protocols, the emphasis protocol type covers 27 protocols, the key operational type covers three types of packets, and critical web behavior type covers three request modes, as described in the new strategy module).



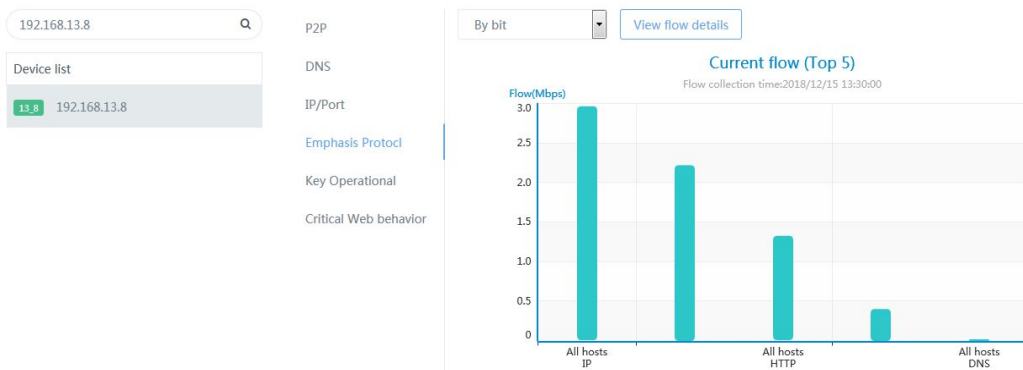
The device list is listed on the left side of the page, mainly the engines mounted under this control center.



You can enter the engine IP address in the query column below the device list to locate the engine.



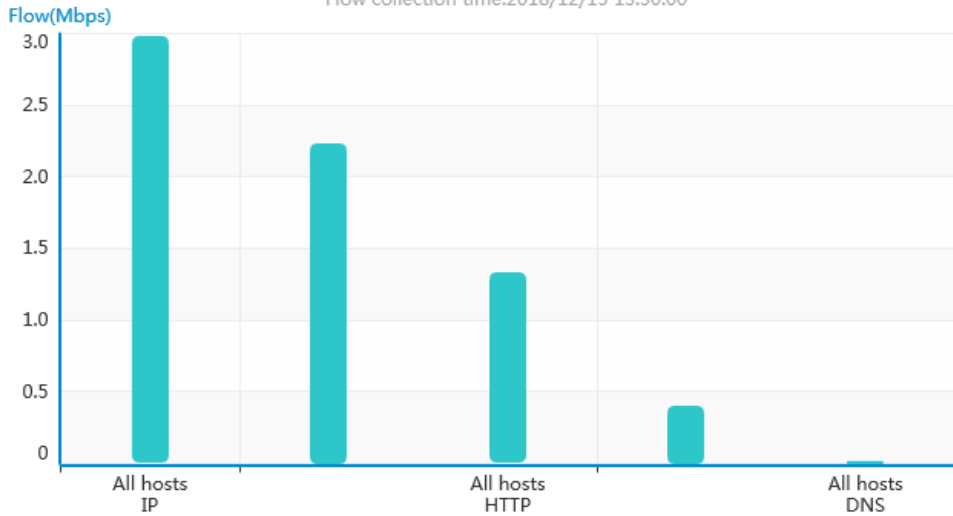
On the right side of the page, the micro flow of the selected engine is displayed in a bar chart (flow change at the current time in a bar chart, and Top 5 flow at every 10-minute time point). Items displayed include P2P, DNS, IP address/port, emphasis protocols, key operational, and critical web behaviors. The current flow value is displayed in bytes (bps).



You can click **[Emphasis protocol]** to view the current Top 5 flow of key protocols in micro flow.

Current flow (Top 5)

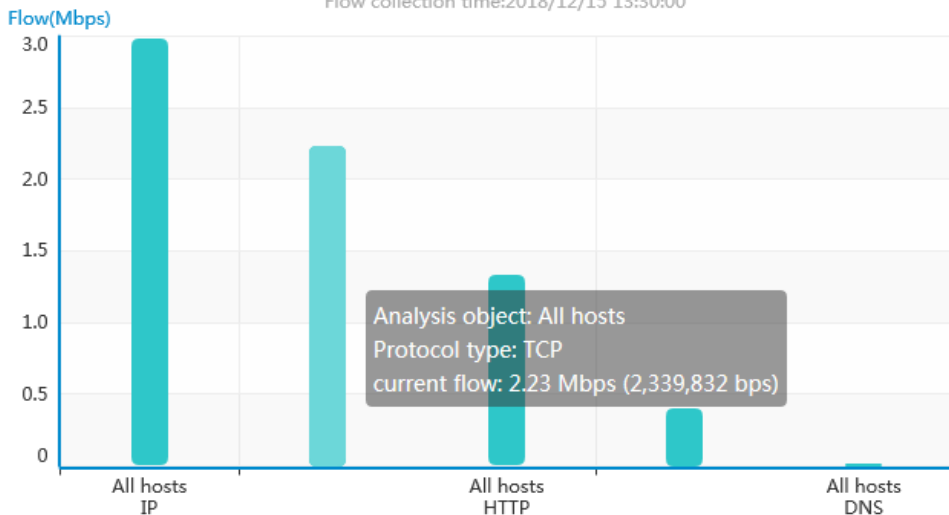
Flow collection time:2018/12/15 13:30:00



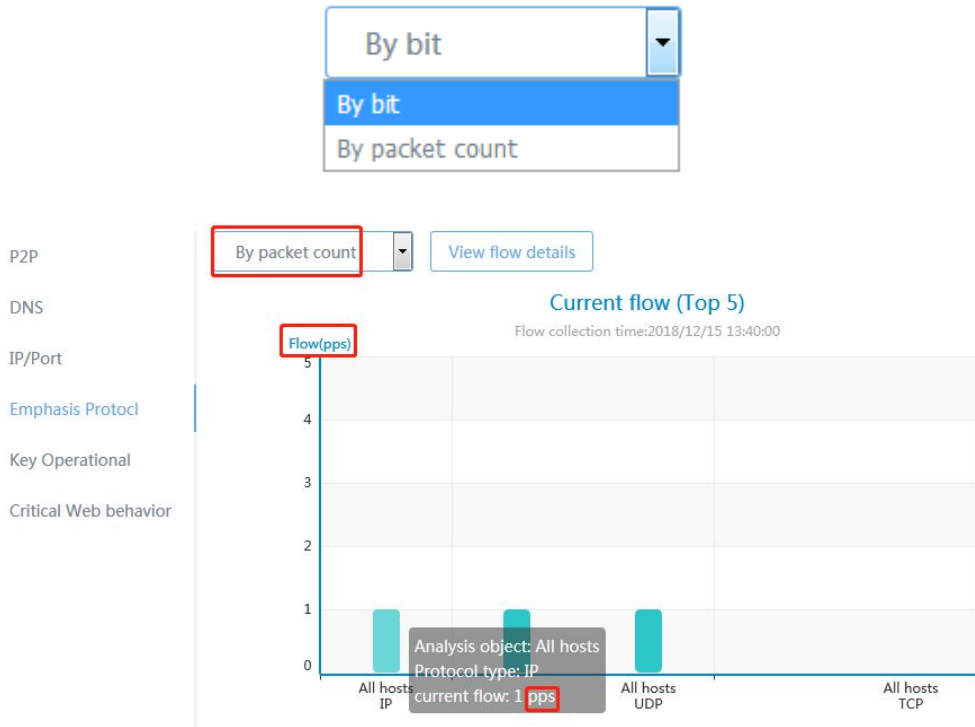
You can hover the mouse over the area map of the corresponding time point in the bar chart to view the flow at that time point.

Current flow (Top 5)

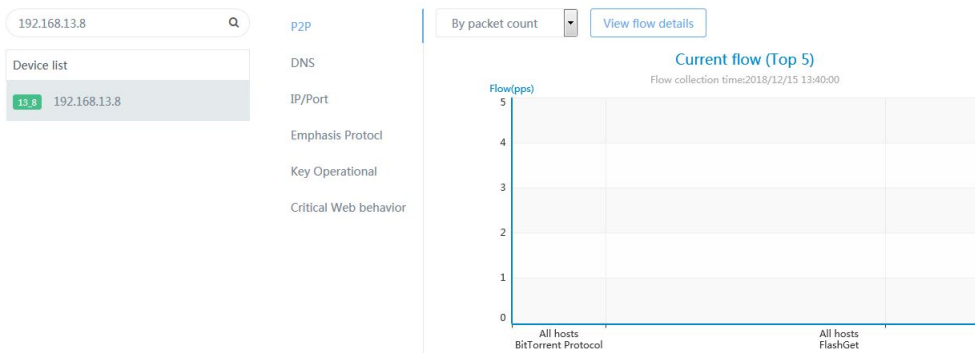
Flow collection time:2018/12/15 13:30:00



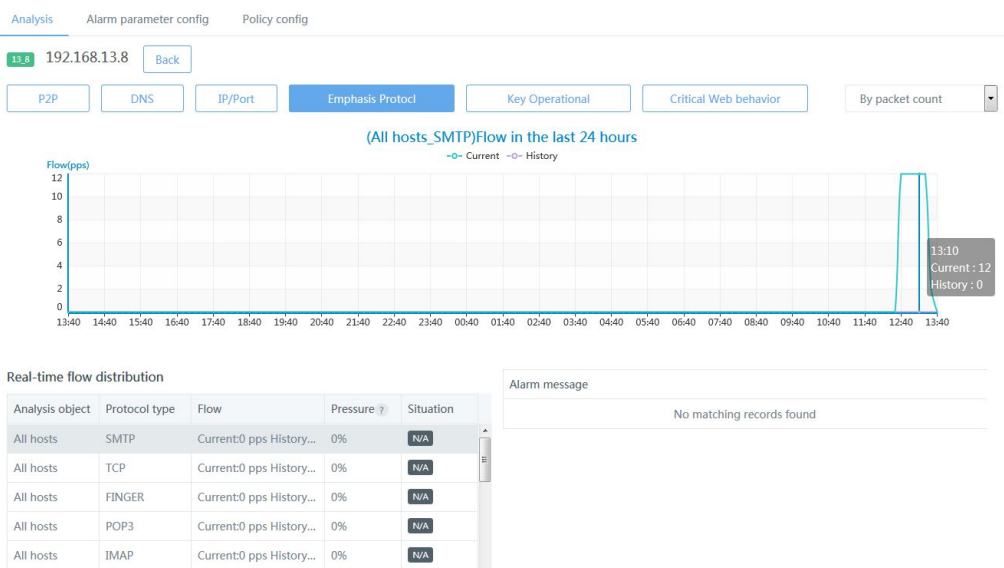
You can click to switch the display mode at the top of the page to select to display the current flow of each device by the number of packets (pps) or by the number of bits (bps).



You can click a device in the device list to display the micro flow of the device on the right of the page. For example, if you want to view the **emphasis protocol information** in micro flow of the engine-IDS, click 192.168.13.8 in the device list.



You can click the **[View flow details]** button at the top of the page to enter the P2P flow detailed analysis tab on the micro flow page.



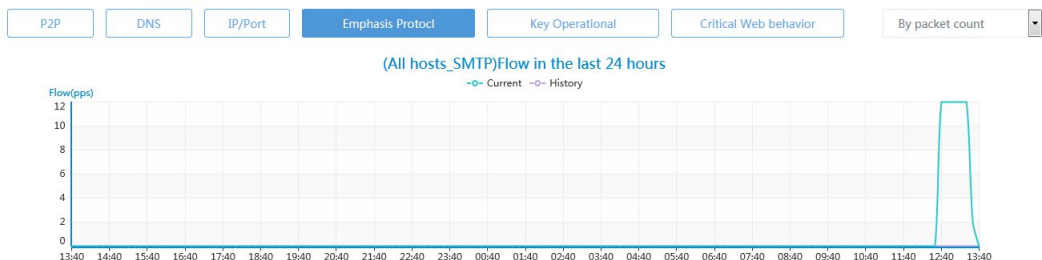
You can click the **[Back]** button on the flow analysis details page to return to the micro flow analysis page.



The micro flow detailed analysis page mainly displays the flow in the last 24 hours, the real-time flow distribution, and alarm message.

Flow in the last 24 hours:

This module displays the micro flow statistics in the last 24 hours every 10 minutes. When the mouse is hovered over the corresponding flow curve at the time point, the corresponding flow is displayed, with the green curve representing the current flow situation and the purple curve representing the historical flow situation.



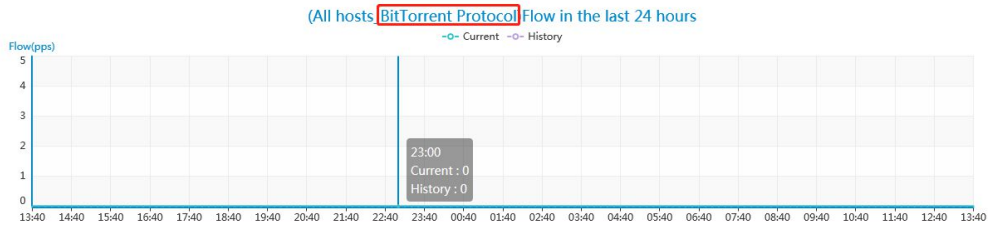
Real-time flow distribution:

The flow distribution list displays the analysis target, protocol type, flow, flow pressure, and running situation. The running situation column displays the current running status. The P2P protocol types include Maze, Thunderbolt flow, Baidu Xiaba flow, POCO flow, Kamun flow, and Cool Dog flow. The protocol types are described in the "micro flow configuration strategy module" later.

Real-time flow distribution

Analysis object	Protocol type	Flow	Pressure ?	Situation
All hosts	SMTP	Current:0 pps History...	0%	N/A
All hosts	TCP	Current:0 pps History...	0%	N/A
All hosts	FINGER	Current:0 pps History...	0%	N/A
All hosts	POP3	Current:0 pps History...	0%	N/A
All hosts	IMAP	Current:0 pps History...	0%	N/A
All hosts	SNMP	Current:0 pps History...	0%	N/A
All hosts	RLOGIN	Current:0 pps History...	0%	N/A
All hosts	METRICS SEN	Current:0 pps History...	0%	N/A

When a flow type is clicked, the specific flow is displayed in other modules. For example, when you click the BitTorrent flow on the real-time flow distribution page, the today's flow and alarm message modules will display the running situation of the BitTorrent flow in the P2P flow.



Real-time flow distribution

Analysis object	Protocol type	Flow	Pressure ?	Situation
All hosts	BitTorrent Pr...	Current0 pps History...	0%	N/A
All hosts	100Bao	Current0 pps History...	0%	N/A
All hosts	x.baidu.com	Current0 pps History...	0%	N/A
All hosts	FlashGet	Current0 pps History...	0%	N/A
All hosts	Bitcomet	Current0 pps History...	0%	N/A
All hosts	eD2k Protocol	Current0 pps History...	0%	N/A
All hosts	KuGoo	Current0 pps History...	0%	N/A
All hosts	emule Protocol	Current0 pps History...	0%	N/A

Alarm message

No matching records found

Alarm message:

This module displays the comparison of various flow at various time points with the set threshold or historical flow in the same period.

4.2.2 Alarm parameter config

You can choose **Flow statistics > Micro flow > Alarm parameter config** to view six types of micro flow analysis parameters. By default, the system displays the comparison result of historical flow in the same period and performs automatic machine analysis. Default system parameters are: low coefficient: 0 to 50; normal coefficient: 50 to 100; slightly high coefficient: 100 to 150; moderately high coefficient: 150 to 200, and severely high coefficient: 200 to ∞.

Flow type	Analysis method	Response method	Configuration type	Update time	Operation
PPS	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
DNIS	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
IP/Port	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
Emphasis Protocol	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
Key Operational	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
Critical Web behavior	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎

You can click the **[Edit]** button after a flow type to display the flow alarm parameters of this type, for example, alarm parameters of the key protocol flow.

Alarm parameter P2P

Configuration type: Default config Custom config

Exception analysis: Comparison based on data in the same period Threshold comparison

Low: %

Slightly high: %

Moderately high: %

Severely high: %

Response method:

Log

Low Slightly high Moderately high Severely high

To use the custom config mode, you can click the configuration type setting switch button to enter the custom config mode.

Configuration type:

Default config

Custom config

Alarm parameter IP/Port

Configuration type: Default config Custom config

Exception analysis: Comparison based on data in the same period Threshold comparison

Low: %

Slightly high: %

Moderately high: %

Severely high: %

Response method:

Log

Low Slightly high Moderately high Severely high

The flow anomaly analysis method includes Comparison based on data in the same period and threshold comparison.

Comparison based on data in the same period:

When the default configuration is used, this mode is used by default. The system compares the flow (bps) of the engine at the current 10-minute time point with the configured automatic analysis coefficient and triggers an alarm if any exception is found. When the custom config is used, the system compares the number of flow packets (pps) of the engine at the current 10-minute time point with the configured automatic analysis coefficient and triggers an alarm if any exception is found.

In Comparison based on data in the same period mode, you can modify the flow analysis parameters. The alarm levels are Low, Slightly High, Moderately High, and Severely High.

Exception analysis: Comparison based on data in the same period Threshold comparison

Low:	<input type="text" value="0"/>	<input type="text" value="50"/>	%
Slightly high:	<input type="text" value="50"/>	<input type="text" value="150"/>	%
Moderately high:	<input type="text" value="150"/>	<input type="text" value="200"/>	%
Severely high:	<input type="text" value="200"/>	<input type="text" value="∞"/>	%

You can configure the response method as required, including whether to generate the alarm log, whether to trigger an alarm, enable or disable alarms at which level, and whether to send the alarm message through emails.

Response method:

- Log
- Low
- Slightly high
- Moderately high
- Severely high
- Email ?

When no email address is configured at the control center, the message "No email list is available" is displayed. Choose **System management > Response method > Email config** to enable email alarm.

No email list is available. Choose System management > Response method > Email config to enable email alarm.

Slightly high Moderately high Severely high

Email ?

When email addresses are configured at the control center, the recipient list is displayed. You can select a recipient and then the alarm message is sent to the recipient so that relevant personnel can analyze the flow in real time.

Email ?

<input type="checkbox"/>	Name	Email
<input type="checkbox"/>	sundy	sdyl@ids.com

Threshold comparison:

If threshold comparison is enabled, the system compares the flow of the engine at the current 10-minute time point with the configured threshold and triggers an alarm when any exception is found.

You can click the flow anomaly analysis method switch button to switch to the threshold comparison mode.

Configuration type:

Exception analysis:

In threshold comparison mode, you can modify the flow analysis parameters. The alarm levels are Low, Slightly High, Moderately High, and Severely High.

Configuration type:

Exception analysis:

Unit: Order of magnitudes:

Low: bps

Slightly high: bps

Moderately high: bps

Severely high: bps

Response method:

Figure 4-53 Threshold comparison parameter display

The default flow unit is bps, which can be configured through parameters. You can expand the unit drop-down box, enter the parameter setting page, and select the flow unit. The selected flow unit is used during last login until you modify it.

Figure 4-54 Unit selection page

You can expand the magnitude order drop-down box to set the magnitude order. After configuration, the range after the corresponding alarm level will be automatically multiplied by the magnitude order.

Exception analysis:	Comparison based on data in the same period		✓ Threshold comparison	
Unit:	bps(By bit)		Order of magnitudes:	10000
Low:	0		500000	bps
Slightly high:	1000000		1500000	bps
Moderately high:	1500000		2000000	bps
Severely high:	2000000		∞	bps

You can configure the response method as required, including whether to generate the alarm log, whether to trigger an alarm, enable or disable alarms at which level, and whether to send the alarm message through emails.

Response method:

Log
 Low Slightly high Moderately high Severely high
 Email ?

When no email address is configured at the control center, the message "No email list is available" is displayed. Choose **System management > Response method > Email config** to enable email alarm.

No email list is available. Choose System management > Response method > Email config to enable email alarm.
 Slightly high Moderately high Severely high
 Email ?

When email addresses are configured at the control center, the recipient list is displayed. You can select a recipient and then the alarm message is sent to the recipient so that relevant personnel can analyze the flow in real time.

Email ?

<input type="checkbox"/>	Name	Email
<input type="checkbox"/>	sundy	sdy1@ids.com

After custom alarm parameter configurations are stored, the configurations are displayed in the micro flow parameter configuration settings list.

Flow type	Analysis method	Response method	Configuration type	Update time	Operation
POP	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
DNS	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
SP/Port	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
Emphasis Protocol	Threshold comparison	Log/Alarm	Custom config	2018-12-15 13:53:37	✎
Key Operational	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎
Critical Web behavior	Comparison of the same period	Log/Alarm	Default config	2017-05-12 16:02:24	✎

Showing 1 to 6 of 6 entries Show 10 entries 1

4.2.3 Policy config

When you choose **Flow statistics > Micro flow > Policy config**, the default policy list page is displayed, as shown in the following figure:

Analysis Alarm parameter config Policy config

Policy list Policy set list New Delete

Type	Policy details	Operation
<input type="checkbox"/> P2P	Analysis object : All hosts.Protocol type:BitTorrent Protocol,100Bao,emule Protocol,Kad Protocol,eD2k Protocol,KuGoo,Kamun,POCO,Kazaa,Maze,T...	
<input type="checkbox"/> DNS	Analysis object : All DNS clients.Protocol type:	
<input type="checkbox"/> IP/Port	Analysis object : Any host:Any port -> Any host:Any port.Protocol type:TCP	
<input type="checkbox"/> Emphasis Protocl	Analysis object : All hosts.Protocol type:ARP,AUTH,CHARGEN,DNS,ECHO,FINGER,FTP,HTTP,IGMP,IMAP,IP,IRC,MSRPC,NETBIOS-SSN,NNTP,POP3,RIP...	
<input type="checkbox"/> Key Operational	Analysis object : All hosts.Protocol type:RST message,SYN message,Retransmit message	
<input type="checkbox"/> Critical Web behavior	Analysis object : All Web clients.Protocol type:GET,POST,HEAD	

Showing 1 to 6 of 6 entries

Policy list:

When you click the **[New]** button in the upper-right corner, the policy creation page is displayed. In the flow type drop-down box, six new protocol types can be created, including P2P, DNS, IP address/port, emphasis protocol, key operational, and Critical Web behavior.

New policy ✕

*Flow type: ▼

*Type:

P2P
 DNS
 IP/Port
 Emphasis Protocl
 Key Operational
 Critical Web behavior

*Statistics/analysis object:

All hosts

IP address of the specified host

Submit

P2P flow type:

New policy ×

*Flow type:

*Type:

<input type="checkbox"/> BitTorrent Protocol	<input type="checkbox"/> 100Bao	<input type="checkbox"/> emule Protocol	<input type="checkbox"/> Kad Protocol
<input type="checkbox"/> eD2k Protocol	<input type="checkbox"/> KuGoo	<input type="checkbox"/> Kamun	<input type="checkbox"/> POCO
<input type="checkbox"/> Kazaa	<input type="checkbox"/> Maze	<input type="checkbox"/> Thunder	<input type="checkbox"/> QQ cyclone
<input type="checkbox"/> Ares	<input type="checkbox"/> x.baidu.com	<input type="checkbox"/> FlashGet	<input type="checkbox"/> Bitcomet

*Statistics/analysis object:

All hosts

IP address of the specified host

DNS flow type:

New policy ×

*Flow type:

*Statistics/analysis object:

All DNS clients

Specified DNS server (IP address)

IP /port flow type:

New policy ×

*Flow type: IP/Port

Host (IP address)-A: Any host

Port-A: Any port

Direction: A->B

Host IP address-B: Any host

Port-B: Any port

Protocol type: TCP

Submit

emphasis protocol flow type:

New policy ×

*Flow type: Emphasis Protocol

*Protocol type:

<input type="checkbox"/> ARP	<input type="checkbox"/> AUTH	<input type="checkbox"/> CHARGEN	<input type="checkbox"/> DNS
<input type="checkbox"/> ECHO	<input type="checkbox"/> FINGER	<input type="checkbox"/> FTP	<input type="checkbox"/> HTTP
<input type="checkbox"/> IGMP	<input type="checkbox"/> IMAP	<input type="checkbox"/> IP	<input type="checkbox"/> IRC
<input type="checkbox"/> MSRPC	<input type="checkbox"/> NETBIOS-SSN	<input type="checkbox"/> NNTP	<input type="checkbox"/> POP3
<input type="checkbox"/> RIP	<input type="checkbox"/> RLOGIN	<input type="checkbox"/> SMTP	<input type="checkbox"/> SNMP
<input type="checkbox"/> SUNRPC	<input type="checkbox"/> TCP	<input type="checkbox"/> TDS	<input type="checkbox"/> TELNET
<input type="checkbox"/> TNS	<input type="checkbox"/> UDP	<input type="checkbox"/> WHOIS	

*Statistics/analysis object:

All hosts

IP address of the specified host

Submit

Key Operational flow type:

New policy ×

*Flow type:

*Packet type: RST message SYN message Retransmit message

*Statistics/analysis object:

All hosts

IP address of the specified host

critical web behavior flow type:

New policy ×

*Flow type:

*Request mode: GET POST HEAD

*Statistics/analysis object:

All Web clients

Specified Web server (IP address)

Assume that the P2P flow type is selected, 16 protocols are configured, and the statistics/analysis target is set to **All hosts**. (16 protocols are available for the P2P flow type. You can select a single protocol or multiple protocols.)

*Flow type:

*Type:

<input type="checkbox"/> BitTorrent Protocol	<input type="checkbox"/> 100Bao	<input type="checkbox"/> emule Protocol	<input type="checkbox"/> Kad Protocol
<input checked="" type="checkbox"/> eD2k Protocol	<input checked="" type="checkbox"/> KuGoo	<input checked="" type="checkbox"/> Kamun	<input type="checkbox"/> POCO
<input type="checkbox"/> Kazaa	<input type="checkbox"/> Maze	<input type="checkbox"/> Thunder	<input type="checkbox"/> QQ cyclone
<input checked="" type="checkbox"/> Ares	<input type="checkbox"/> x.baidu.com	<input type="checkbox"/> FlashGet	<input type="checkbox"/> Bitcomet

When you hover the mouse over a protocol in the P2P flow type, the protocol description is displayed:

*Flow type:

*Type:

BitTorrent Protocol 100Bao emule Protocol Kad Protocol

eD2k Protocol KuGoo Kamun POCO

Kazaa Maza Thunder Cyclone

Ares

Statistics/analysis object:

All hosts

IP address

The eD2k is a completely free distributed file sharing network protocol with open sources, and it is widely used at present.

File sharing based on the eD2k protocol has the difference from traditional file sharing that shared files are not concentrated on one server to be downloaded by users but dispersed on the hard disks of all participants. All participants form a virtual network, every user can download files from any computer in the virtual network, and every one can share his own files with any one simultaneously.

Using the eD2k protocol to download data may occupy a lot of network bandwidth. There are many sharing tools using the protocol at present, mainly including eDonkey2000, emule, etc.

You can set the statistics/analysis target is set to **All hosts** or **IP address of the specified host**. In **All hosts** mode, statistics are made on the flow of all hosts. In **IP address of the specified host** mode, statistics are made on the flow of the host based on the entered IP address, for example, 192.168.1.1.

*Statistics/analysis object:

All hosts

IP address of the specified host

For example : 192.168.1.1

When an incorrect IP address is entered, the following message is displayed at the top of the page:

! IP address of the specified host: The IP address is invalid.

You can save the configured P2P flow type and then close the page. The configured policy is displayed on the policy list page:

Policy list		Policy set list		New	Delete
Type	Policy details			Operation	
<input checked="" type="checkbox"/>	P2P	Analysis object : All hosts, Protocol type: BitTorrent Protocol, 100Bao, emule Protocol, Kad Protocol, eD2k Protocol, KuGoo, Kamun, POCO, Kazaa, Maza, T...			

In the created policy set list, you can click the **[Edit]** button to edit the policy. The policy modification page is displayed. You can modify the policy, submit the modification, and

then close the page.

You can delete a single policy. You can click OK in the displayed page to delete the policy.






Are you sure you want to delete the selected policy?

Cancel

OK

Policy set list:

Click the **[Policy set list]** button to go to the policy list page:

Name	Policy count	Modification time	Description	Operation
sdv	6	2018-12-15 12:28:03	sdv_test	  

To create a policy set, click the **[New]** button in the upper-right corner of the policy set list. The policy set creation page is displayed:

New policy set ×

*Name:

Description:

No policy is selected: Select the policy:

Policy filtering

→ →

Flow type : P2P,Analysis object:All hosts,Protocol type:BitTorrent Pro
Flow type : DNS,Analysis object:All DNS clients,Protocol type:
Flow type : IP/Port,Analysis object:Any host-> Any host:An
Flow type : Emphasis Proctol,Analysis object:All hosts,Protocol type:A
Flow type : Key Operational,Analysis object:All hosts,Protocol type:RS

Policy filtering

← ←

On the policy set creation page, enter a name for the policy set at a length of no more than 50 characters, excluding special characters. The description column can be left blank, or you can enter numbers, letters, and characters at a length of no more than 100 characters.

*Name:

Description:

In the policy set creation dialog box, you can add a policy. You can select a policy in the **No policy is selected** check box (policies here are policies created on the policy list page) on the left and add it to the **Selected the policy** check box on the right. Or, you can click the **→→** button to add all the policies in the check box on the left to the check box on the right. The policy can be delivered to the engine. Besides, you can remove an added policy from the check box on the right or click the **←←** button to remove all the added policies.

Select a policy to be added:

New policy set ×

*Name:

Description:

No policy is selected:

Policy filtering

→ →

Flow type : P2P,Analysis object:All hosts,Protocol type:BitTorrent Pro

Flow type : DNS,Analysis object:All DNS clients,Protocol type:

Flow type : IP/Port,Analysis object:Any host-> Any host:An

Flow type : Emphasis Proctcl,Analysis object:All hosts,Protocol type:A

Flow type : Key Operational,Analysis object:All hosts,Protocol type:RS

Select the policy:

Policy filtering

← ←

Click a single policy and add it:

New policy set

×

*Name: This field cannot be empty. A maximum of 50 characters are allowed.

Description: A maximum of 100 characters are allowed.

No policy is selected:

Select the policy:

Policy filtering

→ →

Flow type : P2P,Analysis object:All hosts,Protocol type:BitTorrent Pro
Flow type : DNS,Analysis object:All DNS clients,Protocol type:
Flow type : Emphasis Protocl,Analysis object:All hosts,Protocol type:A
Flow type : Key Operational,Analysis object:All hosts,Protocol type:RS
Flow type : Critical Web behavior,Analysis object:All Web clients,Prot

Policy filtering

← ←

Flow type : IP/Port,Analysis object:Any host:Any port -> Any host:An

Submit

After all policies are added, no policy is available in the check box on the left.

New policy set

×

*Name: This field cannot be empty. A maximum of 50 characters are allowed.

Description: A maximum of 100 characters are allowed.

No policy is selected:

Select the policy:

Policy filtering

→ →

Policy filtering

← ←

Flow type : P2P,Analysis object:All hosts,Protocol type:BitTorrent Pro
Flow type : DNS,Analysis object:All DNS clients,Protocol type:
Flow type : IP/Port,Analysis object:Any host:Any port -> Any host:An
Flow type : Emphasis Protocl,Analysis object:All hosts,Protocol type:A
Flow type : Key Operational,Analysis object:All hosts,Protocol type:RS

Submit

To filter policies, enter the filtering content (such as the flow type, analysis target, and protocol type) in the **Selected the policy** check box.




Select the policy:

P2P

← ←

Flow type : P2P,Analysis object:All hosts,Protocol type:BitTorrent Pro

Save the added policy and exit the page. The policy set is displayed on the new policy set list page.

Name	Policy count	Modification time	Description	Operation
sdv	6	2018-12-15 12:28:03	sdv_test	  

Showing 1 to 1 of 1 entries

To modify the new policy set list, click the **[Edit]** button in the operation column. The policy set list modification page is displayed.

To delete a policy set, click the **[Delete]** button and then click **[OK]** in the policy set deletion dialog box displayed.



Are you sure you want to delete the selected policy?

Cancel

OK

To deliver a created policy set, click the **[Deliver]** button. The policy distribution page is

displayed:

Deliver policy set sdy ×

No engine list selected: An engine list is selected:

Filter the engine list

→ →

182-192.168.11.182
13_8-192.168.13.8

Filter the engine list

← ←

Submit

In the filter online engine list check box, enter the filter condition. The content retrieved is the engine name and engine IP address.

No engine list selected:

→ →

13_8-192.168.13.8

In the online engine list, select an engine to be delivered. You can also click the → → button to deliver multiple engines. One policy set can be delivered to multiple engines but one engine can accept only one policy set.

Deliver policy set sdy



No engine list selected:

→ →

An engine list is selected:

← ←

13_8-192.168.13.8

Submit

Click the [**Submit**] button. The message " **The policy set is delivered successfully** " is displayed.

... The policy set is delivered successfully.

5 Statistical analysis

The statistical report module is the main module for statistical analysis.

The statistical report module consists of the task list and execution result sub-modules. The task list page displays the basic report information, including the report name, submitter, submitting organization, and description. The report creation button allows you to select the report types suitable for your environment, including the analysis report, basic statistical report, advanced statistical report, and event details report, and set the report query time range and tasks for report cycle execution or manual execution according to your needs, as shown in the following figure.

Task list Execution result

New Query Import Export Delete

<input type="checkbox"/>	SN	List name	Execution method	Submitted by	Submitting ORG	Description	Submission time	Related report	Operation
<input type="checkbox"/>	1	Event details report	Manual				2018-12-12 18:39:51	Related report	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	2	Advanced statistical...	Manual				2018-12-12 18:39:36	Related report	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	3	Analysis report	Manual				2018-12-12 18:39:20	Related report	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	4	Basic statistical re...	Manual				2018-12-12 18:39:05	Related report	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Showing 1 to 4 of 4 entries Show entries

The report execution result page displays executed report tasks, as shown in the following figure.

Task list Execution result

Report name : Start : End :

SN	Report name	Execution time	Execution result	Operation
1	Basic statistical report	2018-12-12 18:44:42	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	Analysis report	2018-12-12 18:44:41	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	Advanced statistical report	2018-12-12 18:44:41	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4	Event details report	2018-12-12 18:44:40	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5	Basic statistical report	2018-12-12 18:42:42	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6	Analysis report	2018-12-12 18:42:41	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7	Advanced statistical report	2018-12-12 18:42:41	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
8	Event details report	2018-12-12 18:42:40	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
9	Basic statistical report	2018-12-12 18:42:39	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
10	Analysis report	2018-12-12 18:42:39	Successful execution of reports	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Showing 1 to 10 of 12 entries Show entries

5.1 Report task configuration

5.1.1 New report task

New analysis report:

Click the [New] button in the task list to add a new report task. The configuration report page is displayed, as shown in the following figure:

The screenshot shows the 'Configure report task' page. The 'Basic report configuration' section contains four input fields: 'Report name', 'Submitted by', 'Submitting ORG', and 'Description'. The 'Report type' section has four radio button options: 'Analysis report', 'Basic statistical report', 'Advanced statistical report', and 'Event details report'. The 'Analysis report' option is selected. Below the 'Report type' section, there is a 'SetTopN=' field with a value of 5 and a range '(5 ≤ N ≤ 100)'. At the bottom right, there are 'Next step' and 'Cancel' buttons.

When creating a new report task, you must fill in the report name, submitter and submitting organization. The description can be filled in according to the actual needs, and the report name cannot be duplicated. Enter relevant information, as shown in the following figure:

This screenshot is identical to the previous one, but the 'Report name', 'Submitted by', and 'Submitting ORG' fields are now filled with the text 'jerry'. The 'Description' field remains empty. The 'Analysis report' radio button is still selected, and the 'SetTopN=' field shows a value of 5. The 'Next step' and 'Cancel' buttons are visible at the bottom right.

Click the [Next step] button. The selecting analysis report template page is displayed, as shown in the following figure:

Configure report te...

Select an analysis report template

Analysis type

- Event occurrence analysis
- Event level analysis
- Security type analysis
- Attacker hazard degree evaluation
- Affected system analysis
- Analysis on IP address with high event occurrence
- Analysis on frequent events in the current period
- Attack type evaluation

Basic time period

Today Last 3 days Last 7 days Last 10 days Last 15 days

Previous step Next step Cancel

You can select required analysis types from eight options in the analysis report template. The time period is divided into the basic time period and the advanced time period. Select an event occurrence period for the Basic time period to generate the analysis report. When Advanced time period is selected, the drop-down menu appears, as shown in the following figure:

Configure report te...

Select an analysis report template

Fixed time period

Start time:

End time:

Non-fixed time period

*Cycle length hours

*Start days And, hours ago

Add Remove Move up Move down

Previous step Next step Cancel

When Fixed time period is selected in Advanced time period mode, you can select the start time and end time to generate the analysis report as required. When Non-fixed time period is selected, add a time period "starting from the 3rd hour of the last day, with

every 5 hours as a cycle" and take today 2012-07-18 as the benchmark. Then, events occurred during 03:00-08:00 of 2012-07-17 are recorded in the log report.

Select a report template and click the [Next step] button to enter the query condition configuration page. After configuring the query condition, click the [Next step] button to enter the task execution cycle configuration page, as shown in the following figure:

Configure report te...

⚙️ Configure task execution period

Execution period

Manually execute

Every day

Every week

Every month

Execution time For example 13:22:01

Tasks can be executed manually or automatically. When Manual execution is selected, you must click the [Execute] button to generate the report. In automatic execution mode, the task can be automatically executed on a regular basis according to the hours, minutes and seconds of each day, week, and month.

After configuring the task execution cycle, click the [Next step] button to enter the report task output format configuration page. On this page, you can select the format of the generated report file and define the custom email group. Output format options are HTML, PDF, EXCEL, and WORD, as shown in the following figure:

⚙️ Configure report task output format

File format

HTML PDF EXCEL WORD

Use the custom email group

RECIPIENT NAME	EMAIL	AVAILABILITY
----------------	-------	--------------

When Use custom email group is checked, the drop-down box is expanded, as shown in the following figure:

See 7.1.3 Email configuration for details about how to configure the custom email group.

⚙️ Configure report task output format

File format

HTML PDF EXCEL WORD

Use the custom email group

RECIPIENT NAME	EMAIL	AVAILABILITY
jerry	778541. [REDACTED]	<input type="checkbox"/>

Previous step Submit Cancel

After configuration, the generated report can be directly forwarded to the user email box.

After configuration, click the [Submit] button. The analysis report generated based on the configuration is displayed in the report task list.

New basic statistical report

To add a new report task, click the [New] button. The report configuration page is displayed, as shown in the following figure:

⚙️ Basic report configuration

Basic report configuration

*Report name:

*Submitted by:

*Submitting ORG:

Description:

Report type

Analysis report
Reports of this type contain a large amount of contrast data and can be used for security analysis and decision-making

Basic statistical report
Reports of this type contain a large amount of basic statistics on occurred events and can be used by O&M personnel for preliminary statistics and analysis on events

Advanced statistical report
Reports of this type contain a large amount of multi-dimensional statistics on occurred events and can be used by O&M personnel for detailed statistics and analysis on events

Event details report
Reports of this type contain details of occurred events and can be used by O&M personnel for event query and analysis. Reports of latest 3000 events are supported

SetTopN= (5≤N≤100) Next step Cancel

When creating a new report task, select "Basic statistics report" for Report type, and enter the report name, submitter, and submitting organization. The report name cannot be duplicated. When generating a basic statistical report, you can set a Top N value, where N ranges from 5 to 100 and indicates the maximum number of statistical events for each type of report. Click the [Next step] button to enter the basic statistical report template selection page, as shown in the following figure:

⚙️ Select a basic statistical report template

Event basis statistics

- Event statistics by source IP address
- Event statistics by destination IP address
- Event statistics by level
- Event statistics by name
- Event statistics by affected system
- Event statistics by affected device
- Event statistics by popularity
- Event statistics by security type
- Traffic statistics by time

Summary

- Database statistics

Previous step
Next step
Cancel

Based on your demand, select the basic event statistics type and the abstract. Then, click the [Next step] button to enter the query condition configuration page, as shown in the following figure:

⚙️ Set search conditions

[← Occurrence time](#)
[Event name](#)
[Report engine](#)
[Security type](#)
[Event level](#)
[Affected device](#)
[Affected system](#)
[Prevalence](#)
[Communication](#)
[IP address](#)

Set time range

Today
 Start time: 2018-12-05 18:53:50
 End time: 2018-12-12 18:53:50

[Previous step](#)
[Next step](#)
[Cancel](#)

After the query condition is configured, configure the task execution cycle and report task output format. For details about the configuration method, see New analysis report above.

New advanced statistical report:

To add a new report task, click the [New] button. The report configuration page is displayed, as shown in the following figure:

⚙️ Basic report configuration

<p>Basic report configuration</p> <p>*Report name: <input type="text" value="jerry"/></p> <p>*Submitted by: <input type="text" value="jerry"/></p> <p>*Submitting ORG: <input type="text" value="jerry"/></p> <p>Description: <input type="text"/></p>	<p>Report type</p> <p><input type="radio"/> Analysis report Reports of this type contain a large amount of contrast data and can be used for security analysis and decision-making</p> <p><input type="radio"/> Basic statistical report Reports of this type contain a large amount of basic statistics on occurred events and can be used by O&M personnel for preliminary statistics and analysis on events</p> <p><input checked="" type="radio"/> Advanced statistical report Reports of this type contain a large amount of multi-dimensional statistics on occurred events and can be used by O&M personnel for detailed statistics and analysis on events</p> <p><input type="radio"/> Event details report Reports of this type contain details of occurred events and can be used by O&M personnel for event query and analysis. Reports of latest 3000 events are supported</p>
---	---

SetTopN= (5 ≤ N ≤ 100) [Next step](#) [Cancel](#)

When creating a new report task, select "Advanced statistics report" for Report type,

and enter the report name, submitter, and submitting organization. The report name cannot be duplicated. When generating an advanced statistical report, you can set a Top N value, where N ranges from 5 to 100 and indicates the maximum number of statistical events for each type of report. Click the [Next step] button to enter the advanced statistical report template selection page, as shown in the following figure:

⚙️ Select an advanced statistical report template

- Event name**
 - <Event name + source IP address> cross statistics
 - <Event name + destination IP address> cross statistics
 - <Event name + destination IP address + source IP address> cross statistics
 - <Event name + source IP address + destination IP address> cross statistics
- Event level**
 - <Event level + source IP address> cross statistics
 - <Event level + destination IP address> cross statistics
- Source IP address**
 - <Source IP address + event name> cross statistics
 - <Source IP address + event level> cross statistics

Previous step Next step Cancel

Based on your demand, configure the engine, event name, event level, source IP address, destination IP address, processing status, affected system, affected device, and covert channel. Then, configure the query condition, task execution cycle and report task output format. For details about the configuration method, see New analysis report above.

New event details report:

To add a new report task, click the [New] button. The report configuration page is displayed, as shown in the following figure:

⚙️ Basic report configuration

Basic report configuration	Report type
<p>*Report name: <input type="text" value="jerry"/></p> <p>*Submitted by: <input type="text" value="jerry"/></p> <p>*Submitting ORG: <input type="text" value="jerry"/></p> <p>Description: <input type="text"/></p>	<p><input type="radio"/> Analysis report Reports of this type contain a large amount of contrast data and can be used for security analysis and decision-making</p> <p><input type="radio"/> Basic statistical report Reports of this type contain a large amount of basic statistics on occurred events and can be used by O&M personnel for preliminary statistics and analysis on events</p> <p><input type="radio"/> Advanced statistical report Reports of this type contain a large amount of multi-dimensional statistics on occurred events and can be used by O&M personnel for detailed statistics and analysis on events</p> <p><input checked="" type="radio"/> Event details report Reports of this type contain details of occurred events and can be used by O&M personnel for event query and analysis. Reports of latest 3000 events are supported</p>
<p>SetTopN= <input type="text" value="5"/> (5 ≤ N ≤ 100) <input type="button" value="Next step"/> <input type="button" value="Cancel"/></p>	

When creating a new report task, select Event details report for Report type. You must fill in the report name, submitter and submitting organization. The description can be filled in according to the actual needs, and the report name cannot be duplicated. Click the [Next step] button, and configure the query condition, task execution cycle and report task output format. For details about the configuration method, see New analysis report above.

5.1.2 Import a report task

To import a report task, click the [Import] button. In the import report task dialog box displayed, browse and select the location of the file, as shown in the following figure:

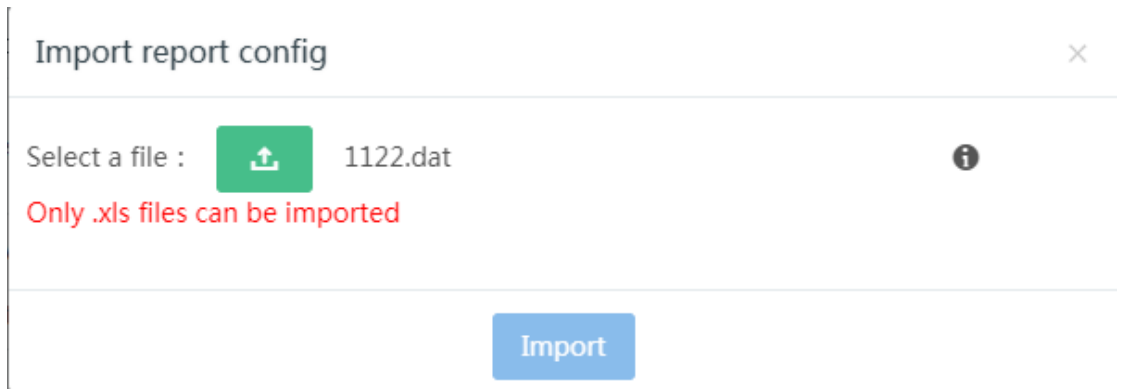
Import report config ×

Select a file : No file is selected ℹ️

Click the [Submit] button. The following information is displayed for successful import.



When a file with an incorrect extension is imported, the following error message is returned:



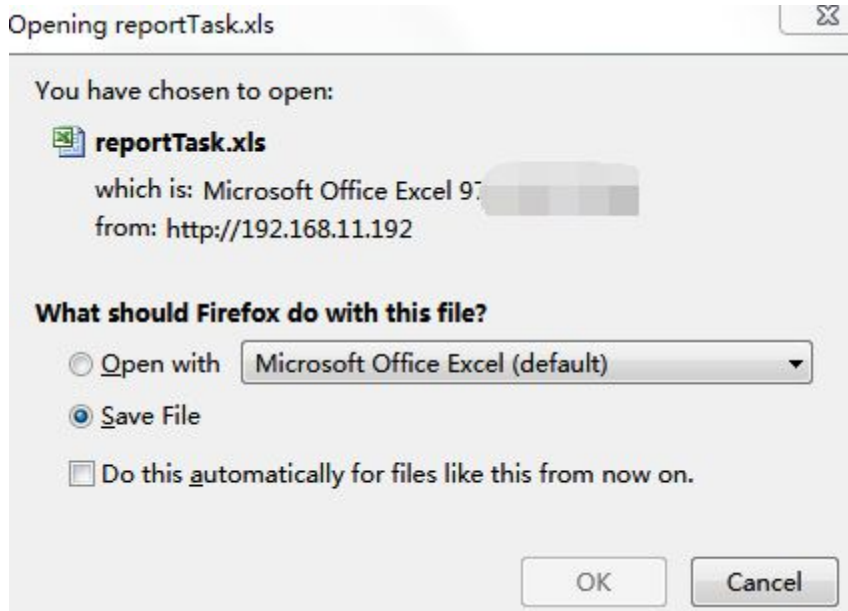
When a file with incorrect data is imported, the following error message is returned:



5.1.3 Export a report task

You can export a single report task or export report tasks in batches.

To export report tasks in batches, click the [Export] button. The export report tasks dialog box is displayed, as shown in the following figure. The report list can be exported to an .xls file, which can be opened by Excel, as shown in the following figure:



To export a single report task, click the [Export] button. The export report tasks dialog box is displayed. The report list can be exported to an .xls file, which can be opened by Excel.



When the report list is exported to an .xls file, the confirmation dialog box may not be displayed due to the machine environment. Instead, IE directly calls the installed Excel software to open the file to be downloaded. In this case, you can only return to the report file list page through IE's back function.

5.1.4 Edit a task report

Click the [Edit] button in the report task list to modify the report task, as shown in the following figure:

⚙️ Basic report configuration

Basic report configuration	Report type
<p>*Report name: <input type="text" value="Analysis report"/></p> <p>*Submitted by: <input type="text" value="abc"/></p> <p>*Submitting ORG: <input type="text" value="abq"/></p> <p>Description: <input type="text"/></p>	<p><input checked="" type="radio"/> Analysis report Reports of this type contain a large amount of contrast data and can be used for security analysis and decision-making</p> <p><input type="radio"/> Basic statistical report Reports of this type contain a large amount of basic statistics on occurred events and can be used by O&M personnel for preliminary statistics and analysis on events</p> <p><input type="radio"/> Advanced statistical report Reports of this type contain a large amount of multi-dimensional statistics on occurred events and can be used by O&M personnel for detailed statistics and analysis on events</p> <p><input type="radio"/> Event details report Reports of this type contain details of occurred events and can be used by O&M personnel for event query and analysis. Reports of latest 3000 events are supported.</p>
<p>SetTopN= <input type="text"/> (5≤N≤100)</p> <p><input type="button" value="Next step"/> <input type="button" value="Cancel"/></p>	

Note that the report name and report type of the four types of log reports cannot be modified. Other configuration items can be modified. For details about the configuration method, see New analysis task above.

5.1.5 Delete a report task

Click the [Delete] icon in the line where the report task is located, and a query dialog box is displayed, as shown in the following figure:



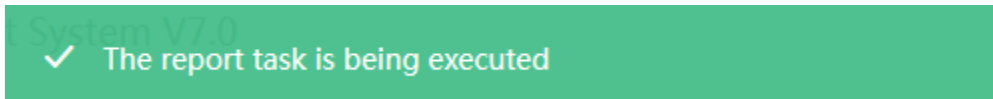
Are you sure you want to execute this task?

Click the [Confirm] button and the specified report is deleted.

You can delete report tasks in batches.

5.1.6 Manually execute a report task

Only one-time report tasks can be executed manually, and periodical tasks cannot be executed manually. Click the [Execute] icon in the line where the report task is located. The report task is executed manually, as shown in the following figure.








5.1.7 Related report file

Click the link of [Related report file] in the line where the report task is located to enter the report list page related to the report, as shown in the following figure. The selected report name is used as the query condition in the drop-down filter box, as shown in the following figure:

Task list Execution result

Report name : Analysis report Start : End : Query

SN	Report name	Execution time	Execution result	Operation
1	Analysis report	2018-12-13 19:45:12	Successful execution of reports	   
2	Analysis report	2018-12-13 19:45:05	Successful execution of reports	   

Showing 1 to 2 of 2 entries Show 10 entries 1

5.1.8 Send reports by email

After a new report is created and the report task output format template is configured, you can configure a custom email group to send the report, as shown in the following figure: (See 7.1.3 Email configuration for the custom email group configuration):

⚙️ Configure report task output format

File format

HTML PDF EXCEL WORD

Use the custom email group

RECIPIENT NAME	EMAIL	AVAILABILITY
jerry	778541123@f. [REDACTED]	<input type="checkbox"/>

[Previous step](#) [Submit](#) [Cancel](#)

Select Use custom email group, and select a recipient in the drop-down list, as shown in the following figure:

RECIPIENT NAME	EMAIL	AVAILABILITY
jerry	77854 [REDACTED]	<input checked="" type="checkbox"/>

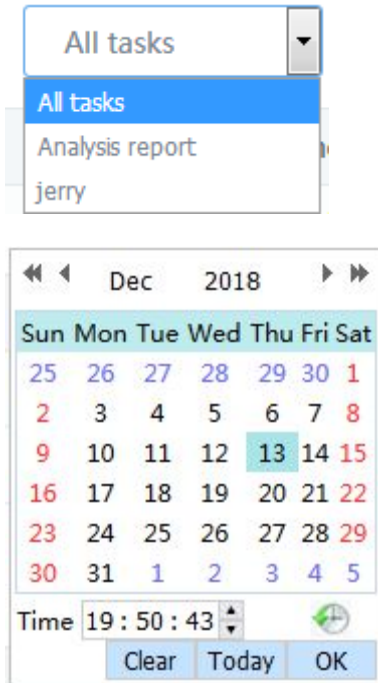
Select a custom recipient, select the "Enable or not" option box in the recipient column (this option is not selected by default), and click the [Submit] button after configuring the recipient. Then a new report task is created.

5.2 Report execution result

You can query, delete, view, and download log reports according to the report name and the report generation time range.

5.2.1 Query the report result

Select the report name, start date, and end date to query the report result file list. The query conditions are as follows:



If the report results are queried by time, both the start time and the end time must be set. When only one of them is set, query fails. Besides, the end time must be later than the start time.

The system performs query according to the configured query conditions. The query results are as follows:

Task list Execution result

Report name : Start : End :

SN	Report name	Execution time	Execution result	Operation
No data available in table				

Show entries

5.2.2 Delete a report directory

Click the [Delete] button in the line where the report file list is located, and the confirmation window is displayed.



Are you sure you want to execute this task?

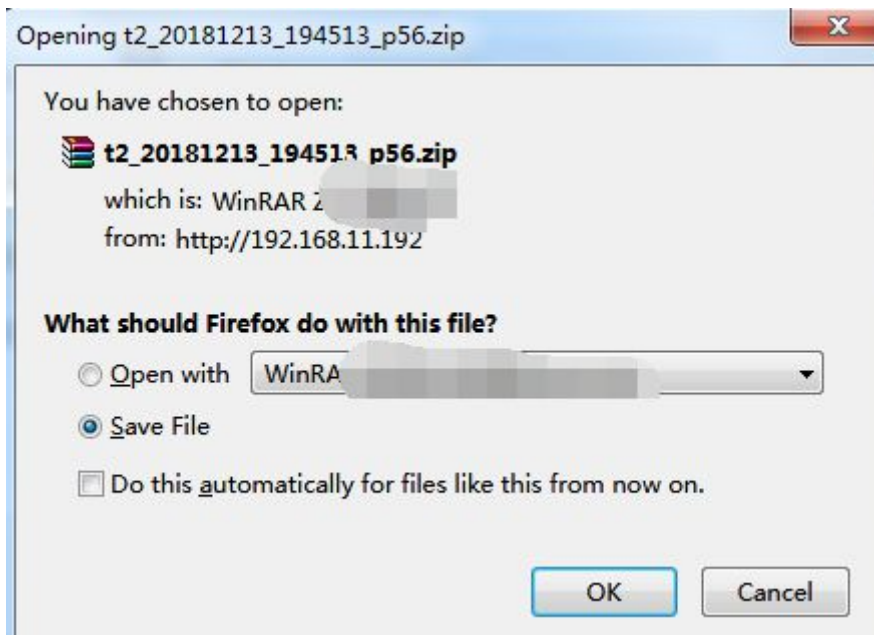
Cancel

Confirm

Click the [Confirm] button and the report file and its directory are deleted.

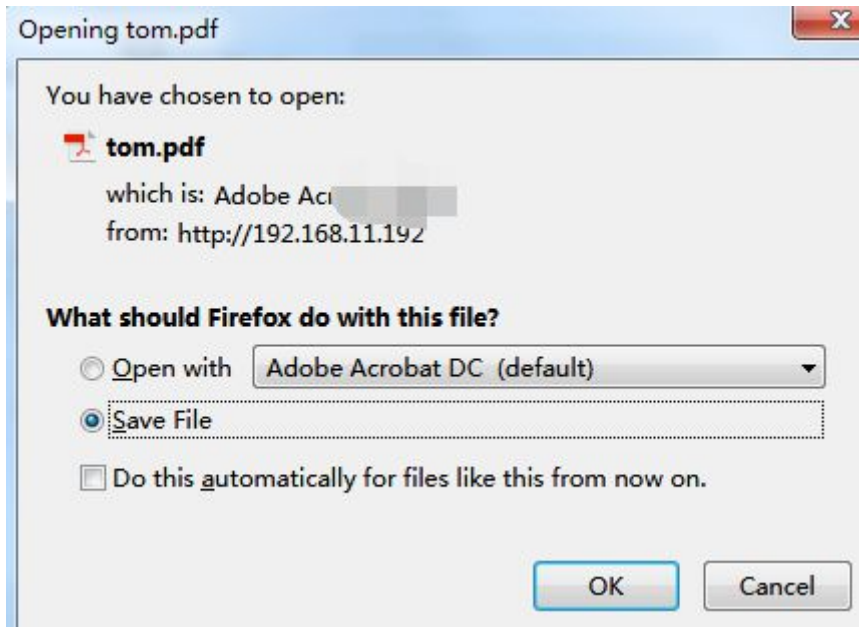
5.2.3 View the HTML file

The HTML file can be opened by clicking the report file hyperlink in the line where the report file list is located, as shown in the following figure:



5.2.4 Download a PDF file

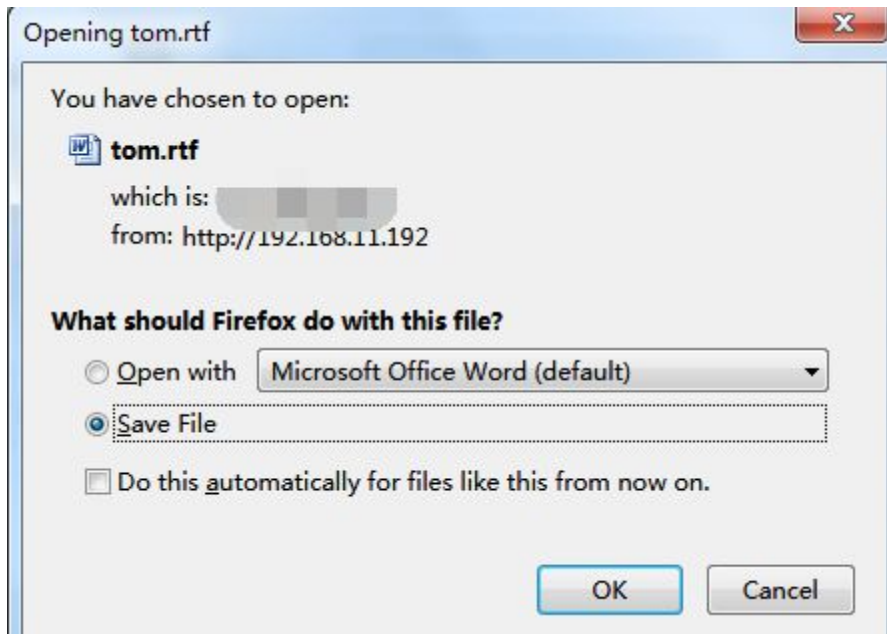
Click the [Download PDF] icon in the line where the report file list is located. The download confirmation dialog box is displayed. After you click the [Save] button, the PDF file is downloaded to your computer, as shown in the following figure:



When the report list is exported to a PDF file, the confirmation dialog box may not be displayed due to the machine environment. Instead, IE directly calls the installed PDF reader software to open the file to be downloaded. In this case, you can only return to the report file list page through IE's back function.

5.2.5 Download a WORD file

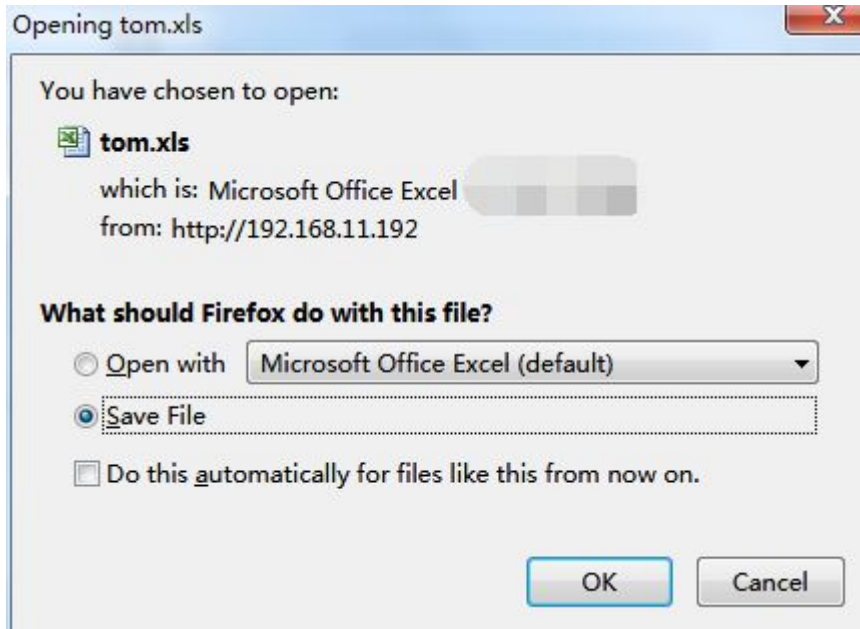
Click the [Download WORD] icon in the line where the report file list is located. The download confirmation dialog box is displayed. After you click the [Save] button, the WORD file is downloaded to your computer.



When the report list is exported to a WORD file, the confirmation dialog box may not be displayed due to the machine environment. Instead, IE directly calls the installed WORD software to open the file to be downloaded. In this case, you can only return to the report file list page through IE's back function.

5.2.6 Download an EXCEL file

Click the [Download EXCEL] icon in the line where the report file list is located. The download confirmation dialog box is displayed. After you click the [Save] button, the EXCEL file is downloaded to your computer, as shown in the following figure:



When the report list is exported to an EXCEL file, the confirmation dialog box may not be displayed due to the machine environment. Instead, IE directly calls the installed EXCEL software to open the file to be downloaded. In this case, you can only return to the report file list page through IE's back function.

5.2.7 Change IE's settings for opening the downloaded files directly

To open the downloaded files directly through IE, choose My computer > Menu > Tools > Folder options, click File type, select the file type that needs to be changed from the registered file types, such as XLS, click Advanced, and select Open it after download without selecting Browse in the same window, and click OK. Restart IE to check whether a confirmation dialog box is displayed.

6 Detection configuration

The detection configuration module is used by the administrator to configure the feature detection, asset, component, file detection, virus detection, URL detection, and covert channel detection modules based on customer demands.

The feature detection configuration module includes the policy set, policy template, feature event, secondary event and DoS, scanning class, weak password configuration, and event merging modules.

The asset configuration module is used to configure the key web server and IP-MAC binding.

The device management module is used to configure the component management, engine configuration, and superior status.

The file detection configuration module is used to configure the blacklist and whitelist.

The virus detection configuration module is used to configure the virus detection configuration.

The URL credibility library module is used to configure the blacklist and whitelist.

The covert channel library module is used to configure the covert channel library.

6.1 Feature detection configuration

























6.1.1 Overview

You can create and manage the policy set on the system Web side. The system default policy set allows viewing, deriving and exporting policy sets but does not allow deleting policy sets. You can create, edit, set effectiveness for, apply a template for, and delete a policy set. You can also merge, import, export, and derive policy sets.

6.1.2 Policy set operation

The policy set editing page consists of command buttons and a list, as shown in the

following figure:

TYPE	NAME	DESCRIPTION	CREATION TIME	OPERATION
system	Hot Event Set	Contains only the latest and most popular attack even	2017-02-02 00:00:00	     
system	Intranet Event Set	All events other than online entertainment	2017-02-02 00:00:00	     
system	Medium and High Level Event Set	Contains only medium and high level events	2017-02-02 00:00:00	     
user	all	all events	2018-11-28 09:21:08	     

Command button:

Command buttons are used to create, merge, import, and refresh policy sets.























New: Create a new policy set.

Merge: Merge multiple policy sets into a new policy set.

Import: Import exported policy sets.

Refresh: Refresh the policy set list.







The list is as follows:

TYPE	NAME	DESCRIPTION	CREATION TIME	OPERATION
system	Hot Event Set	Contains only the latest and most popular attack even	2017-02-02 00:00:00	     
system	Intranet Event Set	All events other than online entertainment	2017-02-02 00:00:00	     
system	Medium and High Level Event Set	Contains only medium and high level events	2017-02-02 00:00:00	     
user	all	all events	2018-11-28 09:21:08	     

The entries in the list are display item information. The rightmost column in a list is generally the operation column, and operations can be performed on the entry.

Icon:

The icons on web pages help you with configuration and management. When you move the cursor over an icon, a message appears to show the meaning of the icon. The following table describes the icons.

Icon	Name	Description
	View	Open the default policy set.
	Deliver policy	Deliver the current policy set to the engine.
	Edit	Edit a custom policy set.
	Derive	Derive a new policy set from the current policy set.
	Export	Export the current policy set to a local specified
	Delete	Delete a custom policy set.

6.1.3 New policy set

Function: Create a new policy set.

Procedure:

Go to the policy set list page:

Click the **[New]** button in the top right list. A dialog box is displayed, as shown in the following figure:

The image shows a dialog box titled "New policy set" with a close button (X) in the top right corner. The dialog contains two input fields: a text box for "Name" (marked with a red asterisk) and a text area for "Description". Below the "Name" field is a validation message: "Can not be empty and can not exceed 50." Below the "Description" field is a validation message: "Bytes must not exceed 120." At the bottom center of the dialog is a blue button labeled "Next step".

Enter a name and description in the dialog box and click **[Next step]**. The event selection dialog box is displayed, as shown in the following figure:

Select an event. ×

Merge method: Protocol type Content: Query Total 6280 Entries

<input type="checkbox"/>	Event name
<input type="checkbox"/>	▶ ARP(2)
<input type="checkbox"/>	▶ AUTH(2)
<input type="checkbox"/>	▶ DNS(49)
<input type="checkbox"/>	▶ FINGER(21)
<input type="checkbox"/>	▶ FTP(85)
<input type="checkbox"/>	▶ HTTP(3896)
<input type="checkbox"/>	▶ ICMP(31)
<input type="checkbox"/>	▶ IGMP(1)

Previous step
Submit

Select the event to be added or find the target event through fuzzy query, and then click the **[Submit]** button to submit and add it. Click **[Previous step]** to return to the previous operation, and click the **X** button to cancel the operation.



The name and description of the policy set cannot be empty. The name and description of the policy set cannot contain special characters (for example, ~, !, @, #, \$, %, &, and *).

6.1.4 Import a policy set

Function: Import an exported policy set file to the policy set list of the current system.

Procedure:

Go to the policy set list page:

Click the **[Import]** button in the top right list. A dialog box is displayed, as shown in the following figure:

Import policy set ✕

Policy file: No file selected.

It takes a long time to import a policy set containing multiple policies..

Select a policy set file suffixed by .policy to be imported.

Click **[Submit]** for submission or click **X** to cancel the operation.

After submission, return to the policy set list page and refresh the page to check whether the policy set is imported.



If the file is invalid, an error message is returned.

6.1.5 Open a policy set

Function: Open the default policy set and view policy items.

Procedure:

Go to the policy set list page:

Click **View** in the list (click **[Edit]** in a custom policy set) to go to the policy item list page.

Note: The default policy set can only be viewed and cannot be edited as shown in the following figure:

Grouping method: Protocol type Content: Query Total 6278 Entries

Event description	Event alias	State	Effectiveness	Event level	Response method	Merge method	Operation
AUTH(2)							
DNS(49)							
FINGER(21)							
FINGER_User_Name_Enumerate_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_bomb_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_Cybercop_Scan		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_Cybercop_Redirection		Report	✓	Middlelevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_freebsd-4.1.1_Attempt		Report	✓	Middlelevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_NULL_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_Redirection_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_root_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_search_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_version_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_W_Pipe_Attempt		Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
FINGER_Point User Attempt		Report	✓	Middlelevel	Alarm+Local storage	Merge by source...	✎ 🗑

6.1.6 Edit a policy set

Function: Open a custom policy set and edit the policy items.

Procedure:

Go to the policy set list page:

Click **Edit** in the list to go to the policy item list page.



The modified policy set takes effect only when it is delivered to the engine.

The policy item list is as follows:

Apply template Set effectiveness Add Delete

Grouping method: Protocol type Content: Query Total 6269 Entries

Event description	Event alias	State	Effectiveness	Event level	Response method	Merge method	Operation
FTP(85)							
HTTP(3689)							
HTTP_Bboard_Access	Detected CGI program access	Report	✗	Non-attack	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_bb-rep.sh_Access	Detected CGI program access	Report	✗	Non-attack	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_bb-replog.sh_Access	Detected CGI program access	Report	✗	Non-attack	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_BigBrother_Access	Detected CGI program access	Report	✗	Non-attack	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_bigconf.rgl_Access	Detected CGI program access	Report	✗	Non-attack	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_BitKeeper_Arbitrary_Command_Execution_Attempt	Detected attacks on CGI program	Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_BitKeeper_Arbitrary_Command_Execution	Detected attacks on CGI program	Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_bizdbsearch_Attempt	Detected attacks on CGI program	Report	✓	Lowlevel	Alarm+Local storage	Merge by source...	✎ 🗑
HTTP_Blahz-DNS_dstuff.oho_Access	Detected CGI program access	Report	✗	Non-attack	Alarm+Local storage	Merge by source...	✎ 🗑

Note: Only custom policy sets can be added, deleted, modified, and batch deleted, and

you can only apply a template and set effectiveness for custom policy sets.

Grouping method:

Click the grouping method list in the policy list toolbar to display policies according to the protocol type, attack type, security type, popularity, event level, affected device, and affected system.

Query:

Enter a keyword in the name input box and click **[Query]** or press **Enter** to query policies in fuzzy query mode. For example, if an "IP address" is entered, all the policies of which names contain the keyword IP address are displayed. The name is not case-sensitive.

The screenshot shows the top navigation bar with buttons for 'Apply template', 'Set effectiveness', 'Add', and 'Delete'. Below it, the 'Grouping method' is set to 'Protocol type' and the 'Content' field is empty. A 'Query' button is visible next to the 'Total 6269 Entries' label. The main table has the following columns: Event description, Event alias, State, Effectiveness, Event level, Response method, Merge method, and Operation. The table lists several policy items, including ARP(2), AUTH(2), AUTH_ident_Version_Exploration, AUTH_Illegal_Data, DNS(49), FINGER(21), FTP(85), HTTP(3889), ICMP(31), IGMP(1), and IMAP(30). The 'AUTH_ident_Version_Exploration' and 'AUTH_Illegal_Data' items are expanded, showing their respective states (Report), effectiveness (green checkmarks), event levels (Misbehavior and Lowlevel), response methods (Alarm+Local storage), and merge methods (Merge by source...). Each item also has a small icon for operations.

New policy item:

To add a new policy item to the policy set, click **[Add]** to open the new policy item dialog box, as shown in the following figure:

This screenshot is similar to the previous one, but the 'Add' button in the top navigation bar is highlighted with a red box. The 'Grouping method' is still 'Protocol type' and the 'Content' field is empty. The 'Query' button is also visible. The table below shows a different set of policy items: ARP(2), AUTH(2), DNS(49), FINGER(21), FTP(85), HTTP(3889), ICMP(31), IGMP(1), IMAP(30), IP(4), and IRC(1). The 'IP(4)' and 'IRC(1)' items are expanded, showing their respective states (Report), effectiveness (green checkmarks), event levels (Lowlevel and Lowlevel), response methods (Alarm+Local storage), and merge methods (Merge by source...).

Policies can be grouped by the protocol type, security type, popularity, event level, affected device, and affected system. Select the default grouping method (protocol type) and click **[Event name]**. The event details page is displayed, as shown in the following figure: Enter a keyword in the input box below the event name in the header and click **[Query]** to retrieve events by event name.

The screenshot shows a dialog box titled "Event details" with a close button (X) in the top right corner. Below the title is a table with the following data:

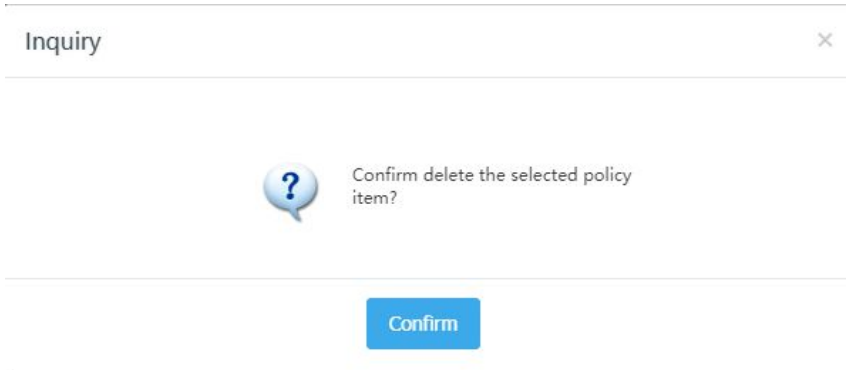
Event name	AUTH_ident_Version_Exploration
Event alias	
Event description	This alert indicates that a remote user may have used the "ldistfp" tool to attempt to detect the ident server. If detecting successfully, this remote user can determine the version of the ident server and the operating system of the destination host.
Event level	Medium risk
Event type	Security scan
Process degree	Not popular
Vulnerability discovery time	
Affected system	Non-critical system
Affected device	Multiple operating system
Event processing method	We suggest that users close the Ident service
Affected software	

At the bottom center of the dialog box is a blue button labeled "Close".

Click the check button before the event list to select the event to be added. You can select and de-select multiple events in multiple event groups. Click **[Submit]** after selecting the event, add the selected event to the policy, return to the policy item list, and refresh the page.

Delete in batches:

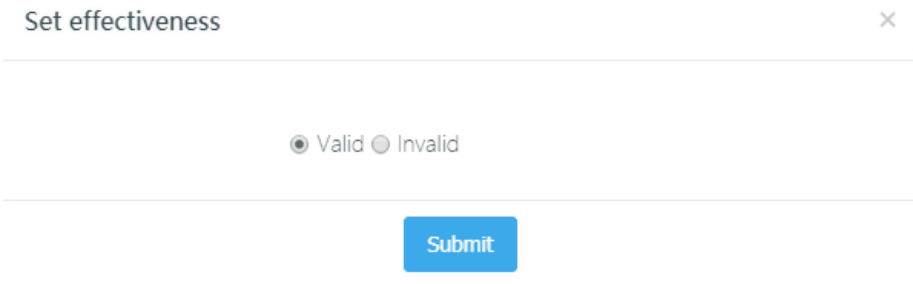
Select the policy items to be deleted and click **[Delete]**. The confirmation dialog box is displayed. If no policy item is selected, the message "Please select a policy item" is displayed. The confirmation dialog box is as follows:



Click **[Confirm]**. All the selected policy items are deleted. Return to the policy item list and refresh the page.

Set effectiveness in batches:

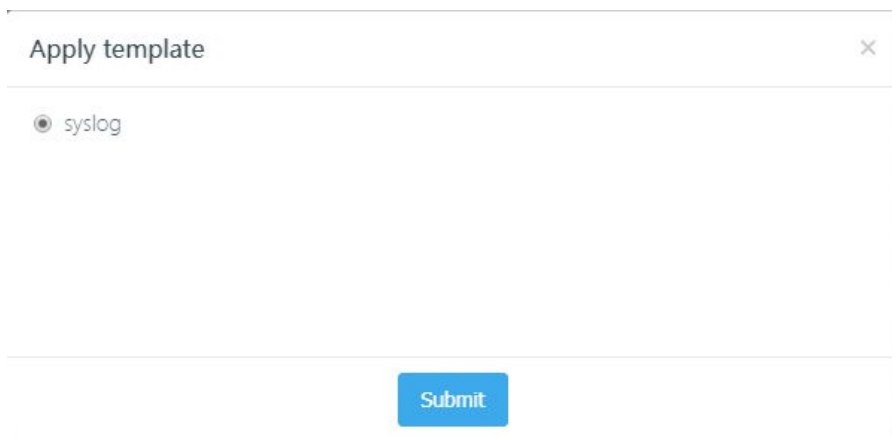
Select the policy items to be set and click **[Set effectiveness]**. The set effectiveness dialog box is displayed. If no policy item is selected, the message "Please select a policy item" is displayed. The set effectiveness dialog box is as follows:



Select **Valid** or **Invalid** and click **[Submit]**. Return to the policy item list and refresh the page.

Apply template:

Select a policy item to which the template is applied and click **[Apply template]**. The template application dialog box is displayed. If no policy item is selected, the message "Please select a policy item" is displayed. The template application dialog box is as follows:

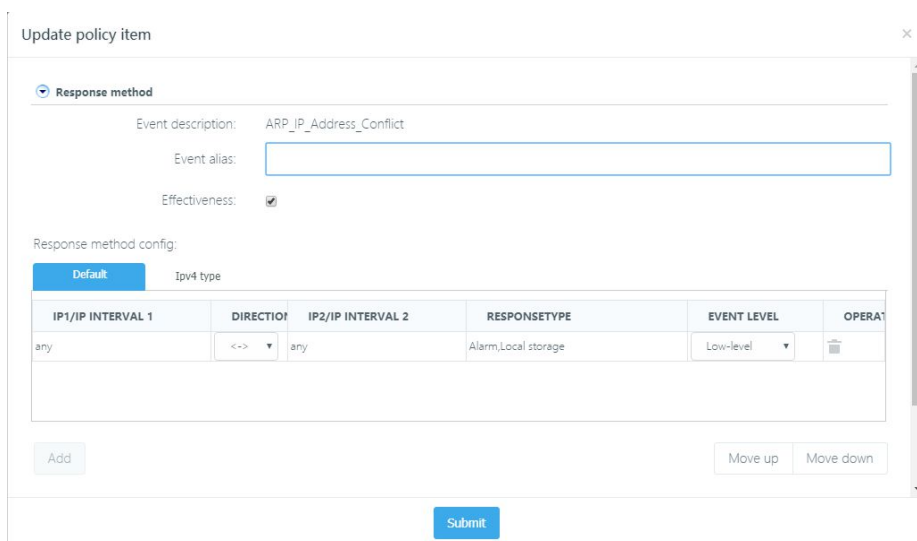


Select the template to be applied and click **[Submit]**. Return to the policy item list and refresh the page.

Note: If no policy template is selected, the message "No policy template. Please add a template" is displayed.

Edit a policy item:

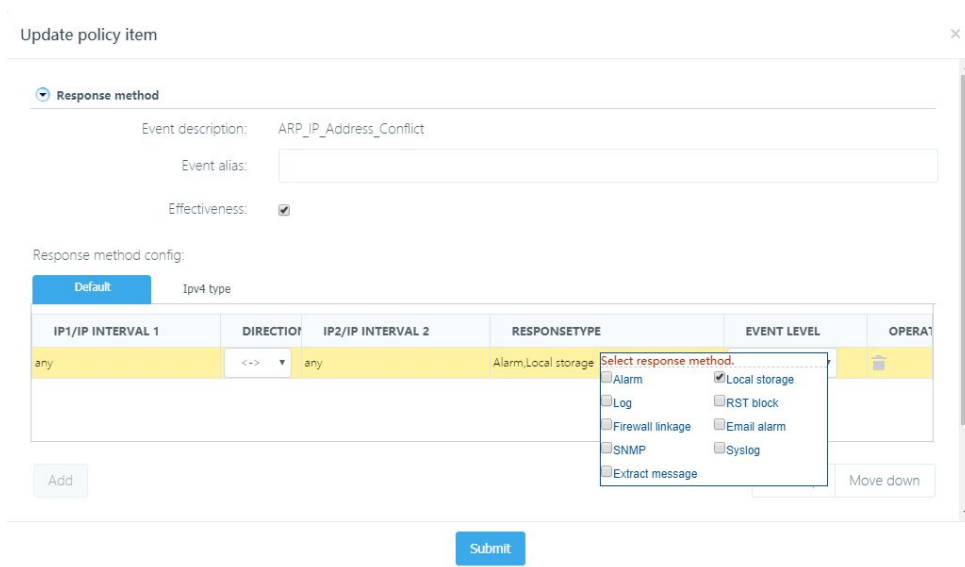
Click **[Edit]**. The policy item editing dialog box is displayed, as shown in the following figure:



Response method:

Options include: event effectiveness, event level, and response method sub-item. The response method sub-items include Log, Alarm, Local storage, RST block, Firewall linkage, Syslog, SNMP, Email alarm, and extracting the original packet. When the

stand-alone response method is selected, the response method option list is opened, as shown in the following figure. By default, in the response method, the IP address/IP address range is any, the direction is <->, and the event level is the default level, which indicates that the event's response method and event level are applied to any source and destination IP addresses. The default IP address/IP address range in the response method cannot be modified or deleted. The response method and event level can be modified, as shown in the following figure:



As for IPv4-based IP address, click **[Add]** below the response method to add the IP address/IP address range response method, as shown in the following figure.

Update policy item

Response method

Event description: ARP_IP_Address_Conflict

Event alias:

Effectiveness:

Response method config:

Default **Ipv4 type**

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERATION
1.1.1.1	->	1.1.1.254	alarm,log	Non-attack	

Add Move up Move down

Submit

As for IPv4-based IP address, click the IP address/IP address range to enter the edit mode. Enter an IP address/IP address range. Separate the IP address ranges by "-". "->" indicates that the IP1/IP1 range is the source IP address/IP address range while the IP2/IP2 range is the destination IP address/IP address range. "<-" indicates that the IP2/IP2 range is the source IP address/IP address range while the IP1/IP1 range is the destination IP address/IP address range. "<->" indicates both the IP1/IP1 range and IP2/IP2 range can be source or destination IP address/IP address range, as shown in the following figure:

Update policy item

Response method

Event description: ARP_IP_Address_Conflict

Event alias:

Effectiveness:

Response method config:

Default **Ipv4 type**

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERATION
IP section use-Number segmentation	-->	IP section use-Number segmentation		Non-attack	
1.1.1.1	-->	1.1.1.254	alarm,log	High-level	

Add Move up Move down

Submit

Click **[Response method]** to select the enabled response method meeting this IP address configuration. You can select the event level from the event level drop-down list, as shown in the following figure:

Update policy item

Response method

Event description: ARP_IP_Address_Conflict

Event alias:

Effectiveness:

Response method config:

Default **Ipv4 type**

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERATION
IP section use-Number segmentation	-->	IP section use-Number segmentation		Non-attack	
1.1.1.1	-->	1.1.1.254	alarm,log	Low-level	

Add Move down

Submit

Click **[Delete]** in the operation column to delete the specified configuration.

You can configure the IP address/IP address range response according to above steps. The configuration in the following figure indicates that the source IP address of the "ARP_IP address conflict" event is 1.1.1.1 and the destination IP address belongs to the

range of 10.0.0.1-20.0.0.1. Logs and alarms are enabled in the response method. The event level is Medium. If the event IP address does not meet the first configuration, the any<->any response method is enabled: logs and alarms. The event level is Low-risk, as shown in the following figure:

Update policy item

Response method

Event description: ARP_IP_Address_Conflict

Event alias:

Effectiveness:

Response method config:

Default **ipv4 type**

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERATION
1.1.1.1	<->	10.0.0.1-20.0.0.1	alarm,log	High-level	

This function supports ranking by IP address and configurations with IP addresses ranked top prevail. Besides, we can move up or down all the entries to adjust the matching sequence. Select an entry, click **[Move up]** or **[Move down]** to increase the priority of the entry.

Merge method:

Click the merge method header to expand the page shown in the following figure:

Merge methods include: By IP address and by IP address and port. If you select to merge by network segment, enter a network segment in the corresponding field. The default network segment is 255.255.255.255.

Filter condition:

Click the filter condition header to expand the page shown in the following figure:

Filter conditions include: IP address, MAC address, and their relationship. The logic options for filter by IP address or MAC address is AND and OR.

To filter by MAC address, click **[Add]**. The MAC address adding dialog box is displayed, as shown in the following figure:

Enter an MAC address in the format of XX:XX:XX:XX:XX:XX. If the address format is incorrect, the message "Incorrect MAC address" is displayed. Click **[OK]** to add the MAC address and return to the policy set modification dialog box.

To filter by IP address, click **[Add]**. The IP address adding dialog box is displayed, as shown in the following figure:

The image shows a dialog box titled "AddIP" with a close button in the top right corner. The main content area contains the following text: "IP format: xxx.xxx.xxx.xxx" followed by "or xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy". Below this is a label "IP address :" followed by a rectangular text input field. At the bottom of the dialog, there are two blue buttons labeled "OK" and "Cancel".

You can add a single IP address or an IP address segment. Enter the IP address or IP address segment correctly. If the address format is incorrect, the message "Incorrect IP address" is displayed. Click **[OK]** to add the IP address and return to the policy set modification dialog box.

After modifying the policy item, click **[Submit]**. Return to the policy item list and refresh the page.

View event details:

Click **Event name** in the policy item list. The details of the current event are displayed. For example, when "DNS_Authors detection" is clicked, the details are displayed as follows.

Event details	
Event name	DNS_Authors_Exploration
Event alias	
Event description	Remote intruders try to explore the version of BIND running on the domain name server by querying authors.bind. The authors.bind is used to provide a method which runs the Named server information it may cause the leakage of BIND version, so remote i
Event level	Medium risk
Event type	Security scan
Process degree	Not popular
Vulnerability discovery time	
Affected system	Non-critical system
Affected device	Multiple operating system
Event processing method	We suggest that users pay close attention to the following actions of the source IP address.
Affected software	Other Application

[Close](#)

Details include the event name, event alias, event description, risk level, event type, popularity, vulnerability discovery time, affected system, affected device, event processing method, and affected software version. Click [**Close**] to close the event details dialog box.

6.1.7 Derive a policy set

Function: Derive a new policy set from existing policy sets.

Procedure:

Go to the policy set list page:

Click [**Derive**] in the list. A dialog box is displayed, as shown in the following figure:

Derive Policy set

Name *

Can not be empty and can not exceed 50.

Description

Bytes must not exceed 120.

Submit Close

In the dialog box, enter the name and description:

Click **Submit** to derive the policy set. After a policy set is derived, return to the policy set list page or click **Close** to cancel the operation.



The policy set name cannot be empty or contain more than 50 characters. The description can be empty but cannot contain more than 120 characters. The policy set name cannot contain special characters, such as ~!@#\$\$%^&*+\\;'V{}|.\ "<>?.

6.1.8 Export a policy set

Function: Export the current policy set to a local specified position.

Procedure:

Go to the policy set list page:

Click **Export** in the list. A dialog box is displayed, as shown in the following figure:

Select a local path to save the policy set.

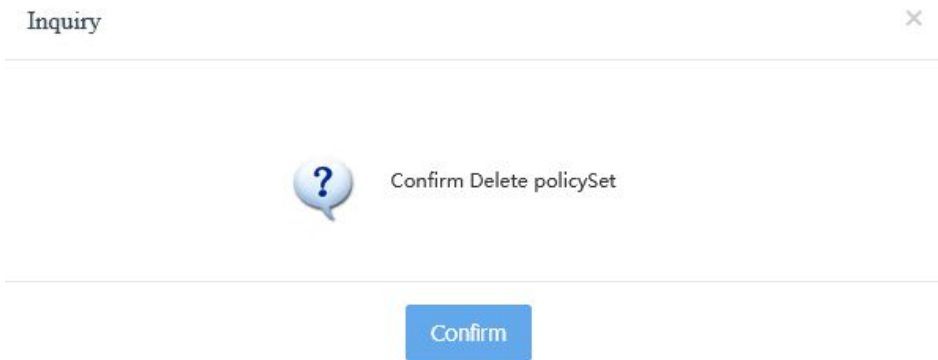
6.1.9 Delete a policy set

Function: Delete the current policy set.

Procedure:

Go to the policy set list page:

Click **[Delete]** in the list. A dialog box is displayed, as shown in the following figure:





Click **[OK]** to delete the policy set and return to the policy set list.

Note: The system policy set cannot be deleted.

6.1.10 Policy template

The policy template allows you to customize the event processing method and response method and modify the default processing method and response method of the policy set. The policy template list is as follows:

SN	NAME	DESCRIPTION	LAST UPDATE TIME	OPERATION
1	syslog		2017-11-02 16:18:24	 
2	SNMP		2017-11-02 16:20:49	 
3	Email		2017-11-02 16:21:16	 

New policy template:

To create a new policy response template, click **[New]**. The new template dialog box is displayed, as shown in the following figure:

Create template
✕

***Name:**

Can not be empty and can not exceed 50.

Description:

Bytes must not exceed 120.

Next step

In the dialog box, enter the name and description and click **[Next step]**. The template content dialog box is displayed, as shown in the following figure:

Create template
✕

Apply scope:

Set response method
 Set merge method
 Set filtering condition

Response method

Response method:

Default

Ipv4 type

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERAT
any	<->	any	Alarm,Local storage	Keep Value	✕

Add

Move up

Move down

Previous step

Submit

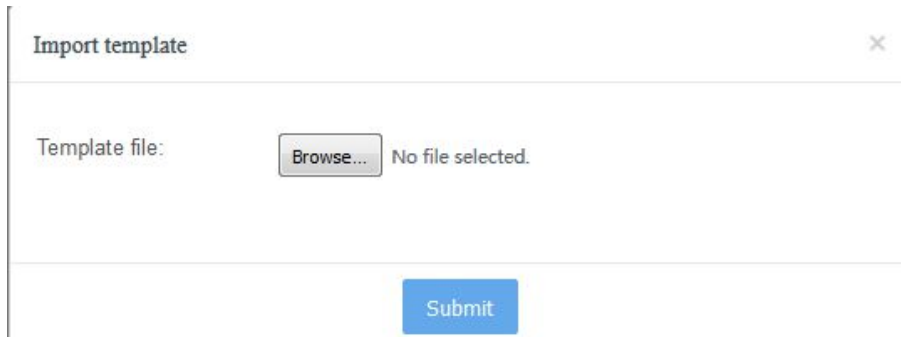
Edit the template content and click **[Submit]** to add the policy template. Then, return to the policy template list page.

Import a policy template:

You can import a backed up policy template to the current system.

Click **[Import]**. The policy template import dialog box is displayed, as shown in the

following figure:



Select the file to be imported and click **[Submit]**. After the file is imported, the page is redirected to the policy template list page.

Export a policy template:

You can export all the current policy templates to a local specified position.

Click **[Export]** in the list. A file download dialog box is displayed.

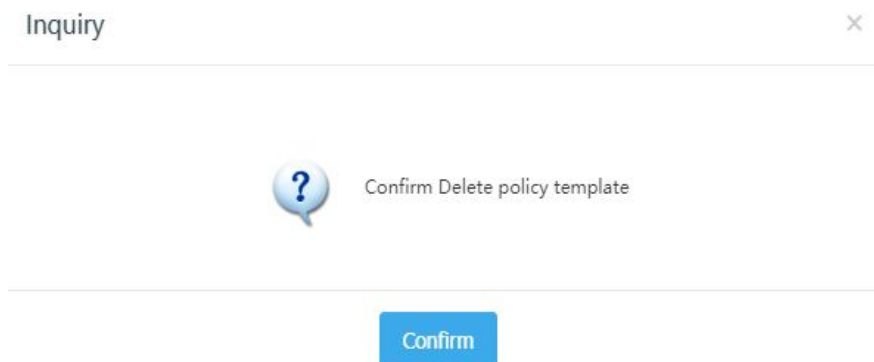
Select a local path to save the file.

Delete a policy template:

You can delete an existing policy template.

Open the policy template list.

Click **[Delete]**. A dialog box is displayed, as shown in the following figure:



Click **[Confirm]** to delete the selected policy template and return to the policy set list. Or,

you can click **x** to cancel the operation.

Edit a policy template:

After creating a policy template, you need to modify its configuration.

Open the policy template list.

Click **[Edit]**. The template modification dialog box is displayed, as shown in the following figure:

Modify template

Name:

Apply scope:

Set response method Set merge method Set filtering condition

Response method

Response method:

Default Ipv4 type

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERAT
any	<->	any	Syslog, Local storage	Keep Value	

On the policy template, you can set the application scope, response method, merge method, and filter condition. When you select an application scope, the corresponding settings are displayed.

Response method:

In the IP address/IP address range response method, options are log, alarm, stand-alone storage, Syslog, SNMP, and email alarm.

Merge method:

Select **Set merge method** under **Application scope** to expand the page shown in the following figure:

Modify template

Merge method

Merge by IP address:

Merge <source IP address> <destination IP address>

<source and destination IP address> <source IP segment and destination IP > <destination IP segment and source IP >

IP and port:

<source IP and source port> <source IP and destination port> <destination IP and source port>

<destination IP and destination port> <source IP segment and destination port> <source IP segment and source port>

<destination IP segment and source port> <destination IP segment and destination port>

Segment config:

Source IP address segment

Destination IP address segment

Submit

Merge methods include: By IP address and by IP address and port. If you select to merge by network segment, enter a network segment in the corresponding field. The default network segment is 255.255.255.255.

Filter condition:

Select **Set filter condition** under **Application scope** to expand the page shown in the following figure:

Modify template

Filtering conditions

MAC and IP address filtering relationship and or

Differentiate source and destination MAC addresses

Reverse overlook

Source MAC address (a maximum of 200 characters)	Operation
<input type="button" value="Add"/>	

Reverse overlook

Destination MAC address (a maximum of 200 characters)	Operation
<input type="button" value="Add"/>	

Differentiate source and destination IP addresses

Submit

Filter conditions include: IP address, MAC address, and their relationship. The logic options for filter by IP address or MAC address is AND and OR.

To filter by MAC address, click **[Add]**. The MAC address adding dialog box is displayed,

as shown in the following figure:

Add MAC address x

MAC address format: XX:XX:XX:XX:XX:XX

MAC address:

OK

Enter an MAC address in the format of XX:XX:XX:XX:XX:XX. If the address format is incorrect, the message "Incorrect MAC address" is displayed. Click **[OK]** to add the MAC address and return to the policy set modification dialog box.

To filter by IP address, click **[Add]**. The IP address adding dialog box is displayed, as shown in the following figure:

Add IP x

IP format: xxx.xxx.xxx.xxx
ORxxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy

IP address:

OK

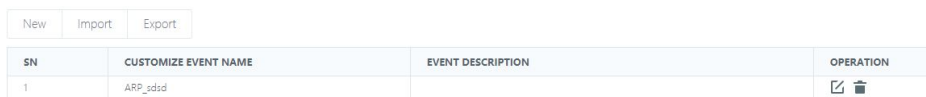
You can add a single IP address or an IP address segment. Enter the IP address or IP address segment correctly. If the address format is incorrect, the message "Incorrect IP address" is displayed. Click **[OK]** to add the IP address and return to the policy set modification dialog box.



After modifying the policy template, click **[Submit]** and return to the policy template list.

6.1.11 Customize the feature event

This module allows you to customize an event. Feature events are events that have matching rules in network flow. By matching these features, we can analyze the behavior with some attacks. Feature event is a mature pattern matching technology used in mainstream intrusion detection today. This detection technology takes protocol analysis as its core and uses the pattern matching method to filter network flow based on protocol analysis.

Choose **Detection configuration > Feature detection configuration > Feature event** to go to the custom feature event page, as shown in the following figure:



New	Import	Export	
SN	CUSTOMIZE EVENT NAME	EVENT DESCRIPTION	OPERATION
1	ARP_sdid		 

New basic feature event:

Click **[New]** to add a feature event in the new event window displayed, as shown in the following figure:

Configuration procedure:

New feature event
✕

*Event name: <input style="width: 90%;" type="text" value="ARP"/>	Event alias: <input style="width: 90%;" type="text"/>
Event description: <input style="width: 90%;" type="text"/>	Event level: <input style="width: 90%;" type="text" value="Non attack"/>
Protocol type: <input style="width: 90%;" type="text" value="ARP"/>	Security type: <input style="width: 90%;" type="text" value="Buffer overflow"/>
Affected system: <input style="width: 90%;" type="text" value="Non-critical system"/>	Affected device: <input style="width: 90%;" type="text" value="Non-critical equipment"/>
Prevalence: <input style="width: 90%;" type="text" value="No threat"/>	Src/Dest IP reversion: <input style="width: 90%;" type="text" value="No"/>

Base Feature

Feature definition: [Definition wizard](#) Syntax check

Response parameter definition: [Parameter wizard](#) Syntax check

[Customize policy set](#)

Submit

Parameter description:

Event name: Enter an event name. The name must be started with the event protocol. This field is mandatory.

Event alias: Enter an event alias for convenient memory.

Event description: Describe the event. The description cannot exceed 120 characters. This field is optional.

Risk level: Select the event level. Options are non-attack events, low-risk events, medium-risk events, and high-risk events. The default level is non-attack events.

Protocol type: Select the protocol type of the event.

Security type: Select the security type of the event.

Affected system: Select the key system affected by the event.

Affected device: Select the key device affected by the event.

Prevalence: Select the event popularity.

Src/Dest IP reversion: Select whether to switch between the source IP address and destination IP address of the event.

Feature definition: Enter the event's feature definition string. You are recommended to define the event by following the **Feature definition wizard** and click **Syntax check** to check the definition syntax. This field is mandatory.

Response parameter definition: Enter the event's return parameter definition string. You are recommended to define the return parameter by following the **Return parameter help** and click **Syntax check** to check the definition syntax. The return parameter string cannot exceed 128 characters. This field is optional.

Customize policy set: Select a response method for the feature event and add the response method to the custom policy set. When creating a new feature event, you can specify no policy set for the event and then add a policy set by choosing **Feature detection configuration > Policy set**.

Configuration case

We want to monitor all users who visit the www.sina.com.cn website in the network segment, and to monitor whether the users have visited the file named index.php.

Click **[New]** to add a feature event in the new event window displayed.

Enter the event name. The name should clearly indicate the event definition for easy understanding and management. "HTTP_selfdefine_001" is used in this example.

Enter the event alias. For future query convenience, "Sina access monitoring" is used in this example.

Enter the event description as required. "Feature event definition demonstration" is used in this example.

Select the event level as required. "High-risk event" is used in this example.

Select the event protocol type. Because we want to monitor all users who visit the www.sina.com.cn website in the network segment, "HTTP" is selected for the protocol type.

Select the event security type. Because we want to monitor and audit the flow in the network segment, "Security audit" is selected for the security type.

Select the affected system as required. "MySQL" is used in this example.

Select the affected device as required. "Multiple network devices" is used in this example.

Select the popularity as required. "Popular" is used in this example.

Set **Src/Dest IP address reversion** to **No**.

New feature event ×

*Event name:	<input type="text" value="HTTP_001"/>	Event alias:	<input type="text" value="sina access control"/>
Event description:	<input type="text" value="just for teset"/>	Event level:	<input type="text" value="Highlevel"/>
Protocol type:	<input type="text" value="HTTP"/>	Security type:	<input type="text" value="Security scan"/>
Affected system:	<input type="text" value="Non-critical system"/>	Affected device:	<input type="text" value="Non-critical equipment"/>
Prevalence:	<input type="text" value="Popular"/>	Src/Dest IP reversion:	<input type="text" value="No"/>

Base Feature

Feature definition: [Definition wizard](#)

Response parameter definition: [Parameter wizard](#)

[Customize policy set](#)

Define the event feature by following the **Feature definition wizard**. Click the link of **[Definition wizard]**. The feature definition wizard window is displayed, as shown in the following figure:

Definition wizard



Protocol variable:



Details:

Variable name:

Description:

Operator:

Data value:

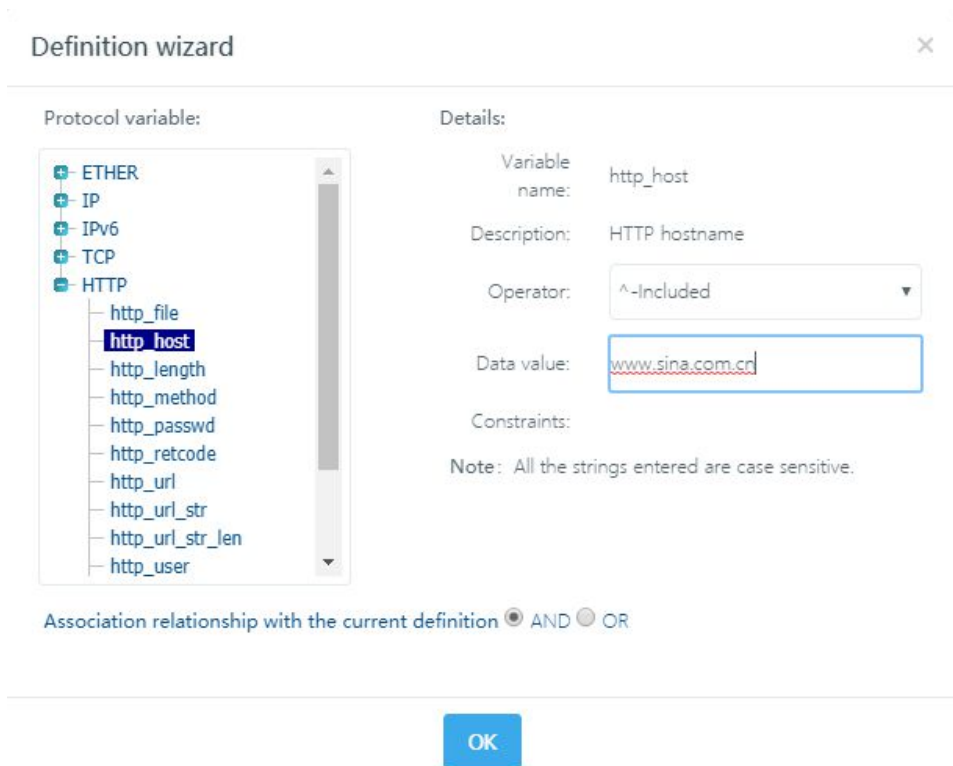
Constraints:

Note: All the strings entered are case sensitive.

Association relationship with the current definition AND OR

OK

Because we want to monitor the website `www.sina.com.cn`, select "http_host" from the protocol variable directory tree on the left and select the operator "`^ - included`" in the **Details** column on the right, and enter "`www.sina.com.cn`" in the **Data value** field, as shown in the following figure:



Then, click **[OK]**. The feature definition string "http_host^www.sina.com.cn" is generated in the feature definition input box, as shown in the following figure:

New feature event



*Event name:	<input type="text" value="HTTP_001"/>	Event alias:	<input type="text" value="sina access control"/>
Event description:	<input type="text" value="just for teset"/>	Event level:	<input type="text" value="Highlevel"/>
Protocol type:	<input type="text" value="HTTP"/>	Security type:	<input type="text" value="Security scan"/>
Affected system:	<input type="text" value="Non-critical system"/>	Affected device:	<input type="text" value="Non-critical equipment"/>
Prevalence:	<input type="text" value="Popular"/>	Src/Dest IP reversion:	<input type="text" value="No"/>

Base Feature

Feature definition: [Definition wizard](#)

Response parameter definition: [Parameter wizard](#)

[Customize policy set](#)

Click the link of [**Definition wizard**] and select another feature definition. Because the name of the monitored file is index.php, select "http_url" from the protocol variable directory tree on the left and select the operator "^ - included" in the **Details** column on the right, and enter "index.php" in the **Data value** field, Confirm the join relationship between the two feature definitions before clicking [**OK**]. "AND" is used in this example, as shown in the following figure:

Definition wizard



Protocol variable:

- [-] ETHER
- [-] IP
- [-] IPv6
- [-] TCP
- [-] HTTP
 - [-] http_file
 - [-] http_host
 - [-] http_length
 - [-] http_method
 - [-] http_passwd
 - [-] http_retcode
 - [-] http_url**
 - [-] http_url_str
 - [-] http_url_str_len
 - [-] http_user

Details:

Variable name: http_url

Description: Decoded URL

Operator: ^-Included

Data value: index.php

Constraints:

Note: All the strings entered are case sensitive.

Association relationship with the current definition AND OR

OK

Then, click **[OK]**. The feature definition string "http_host^www.sina.com.cn&http_url^index.php" is generated in the feature definition input box, as shown in the following figure:

New feature event



*Event name:	<input type="text" value="HTTP_001"/>	Event alias:	<input type="text" value="sina access control"/>
Event description:	<input type="text" value="just for treset"/>	Event level:	<input type="text" value="Highlevel"/>
Protocol type:	<input type="text" value="HTTP"/>	Security type:	<input type="text" value="Security scan"/>
Affected system:	<input type="text" value="Non-critical system"/>	Affected device:	<input type="text" value="Non-critical equipment"/>
Prevalence:	<input type="text" value="Popular"/>	Src/Dest IP reversion:	<input type="text" value="No"/>

Base Feature

Feature definition: [Definition wizard](#)

```
http_host^www.sina.com.cn&http_url^index.php
```

Response parameter definition: [Parameter wizard](#)

[Customize policy set](#)

Submit

You can click **Syntax check** to check whether the feature definition string is correct. Click **[Syntax check]**. The check result window is displayed.

If the feature definition string passes the check, the following message is displayed:

Information



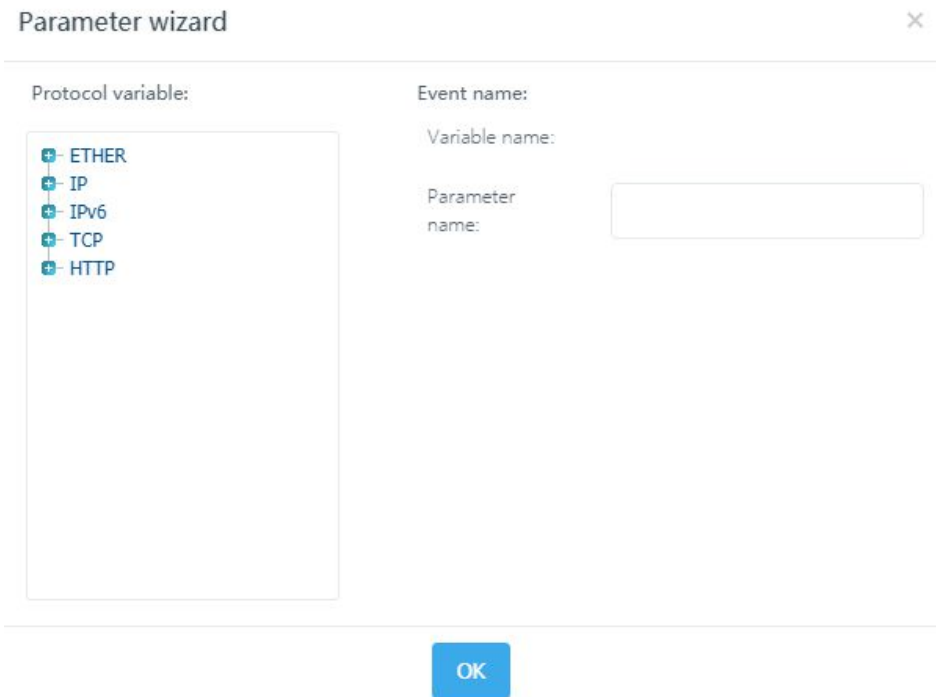
Correct syntax.

Close

If the feature definition string fails the check, the corresponding error message is

returned.

You are recommended to define the return parameter by following the **Response parameter wizard**. Click the link of [**Parameter wizard**]. The response parameter wizard window is displayed, as shown in the following figure:



Because the detected `http_url` is used as the return variable, select "http_url" from the protocol variable directory tree on the left and enter "URL" as the return prompt in the Details column on the right, as shown in the following figure:

Parameter wizard



Protocol variable:

- ETHER
- IP
- IPv6
- TCP
- HTTP
 - http_file
 - http_host
 - http_length
 - http_method
 - http_passwd
 - http_retcode
 - http_url**
 - http_url_str
 - http_url_str_len
 - http_user
 - http_msgbody

Event name:

Variable name: http_url

Parameter name:

OK

Click **[OK]**. The return parameter string "URL=http_url" is generated in the return parameter input box, as shown in the following figure:

New feature event



*Event name:	<input type="text" value="HTTP_001"/>	Event alias:	<input type="text" value="sina access control"/>
Event description:	<input type="text" value="just for teset"/>	Event level:	<input type="text" value="Highlevel"/>
Protocol type:	<input type="text" value="HTTP"/>	Security type:	<input type="text" value="Security scan"/>
Affected system:	<input type="text" value="Non-critical system"/>	Affected device:	<input type="text" value="Non-critical equipment"/>
Prevalence:	<input type="text" value="Popular"/>	Src/Dest IP reversion:	<input type="text" value="No"/>

Base Feature

Feature definition: [Definition wizard](#)

Response parameter definition: [Parameter wizard](#)

[Customize policy set](#)

Submit

You can click **Syntax check** to check whether the return parameter definition string is correct. Click **[Syntax check]**. The check result window is displayed.

If the return parameter definition string passes the check, the following message is displayed:

Information





Correct syntax.

Close

If the return parameter definition string fails the check, the corresponding error message is returned.

Select a policy set. Click the link of **[Customize policy set]**. In the dialog box displayed, select the response method and custom policy set for the feature event, as shown in the following figure:

After entering relevant information for the feature event as required, click **[Submit]**. If the entered information is correct and meets the requirements, the added event is displayed in the event list, as shown in the following figure:

SN	CUSTOMIZE EVENT NAME	EVENT DESCRIPTION	OPERATION
1	HTTP_001	just for test	 

Otherwise, an error message is returned, and the event is not added to the event list until you enter relevant information as required.

Edit the feature event definition:

Click **[Edit]**. In the event editing window displayed, edit an existing feature event, as shown in the following figure:

Configuration procedure:

Edit feature event✕

Event name <input style="border: 1px solid #add8e6; border-bottom: 2px solid #add8e6;" type="text" value="HTTP_001"/> *	Event alias <input style="width: 90%;" type="text" value="sina access control"/>
Event description: <input style="width: 90%;" type="text" value="just for treset"/>	Event level <input style="width: 90%;" type="text" value="Highlevel"/>
Protocol type <input style="width: 90%;" type="text" value="HTTP"/>	Security type <input style="width: 90%;" type="text" value="Security scan"/>
Affected system <input style="width: 90%;" type="text" value="Non-critical system"/>	Affected device <input style="width: 90%;" type="text" value="Non-critical equipment"/>
Prevalence <input style="width: 90%;" type="text" value="Popular"/>	Src/Dest IP reversion <input style="width: 90%;" type="text" value="No"/>

Feature definition [Definition wizard](#)

http_host^www.sina.com.cn&http_url^index.php

Response parameter definition [Parameter wizard](#)

URL=http_url

[Customize policy set](#)

Parameter description:

Event name: Enter an event name. The name must be started with the event protocol. This field is mandatory.

Event alias: Enter an event alias for convenient memory.

Event description: Describe the event. The description cannot exceed 120 characters. This field is optional.

Risk level: Select the event level. Options are connection events, low-risk events, medium-risk events, and high-risk events. The default level is connection events.

Protocol type: Select the protocol type of the event.

Security type: Select the security type of the event.

Affected system: Select the key system affected by the event.

Affected device: Select the key device affected by the event.

Prevalence: Select the event popularity.

Src/Dest IP reversion: Select whether to switch between the source IP address and destination IP address of the event.

Feature definition: Enter the event's feature definition string. You are recommended to define the event by following the **Feature definition wizard** and click **Syntax check** to check the definition syntax. This field is mandatory.

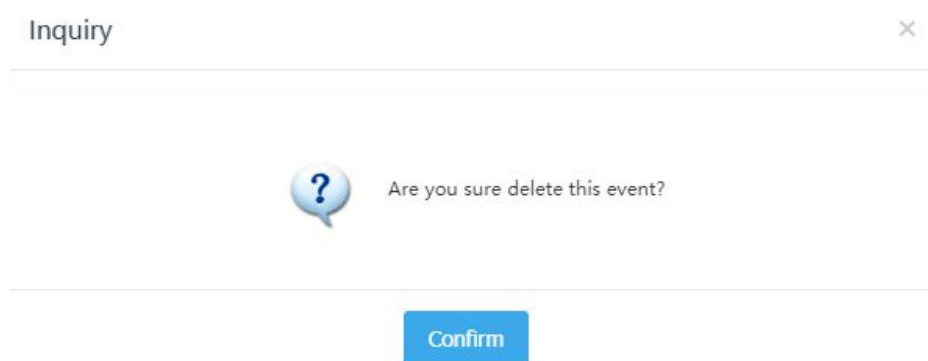
Response parameter definition: Enter the event's return parameter definition string. You are recommended to define the return parameter by following the **Parameter wizard** and click **Syntax check** to check the definition syntax. The return parameter string cannot exceed 128 characters. This field is optional.

Customize policy set: Select a response method for the feature event and add the response method to the custom policy set. When creating a new feature event, you can specify no policy set for the event and then add a policy set by choosing **Feature detection configuration > Policy set**.

Edit the feature event definition:

Click **[Delete]**. A window is displayed, asking you whether to delete the current custom event, as shown in the following figure:

Configuration procedure:



Export the event definition file:

Click **[Export]**. A new window is displayed, asking you whether to open or save the event definition file.

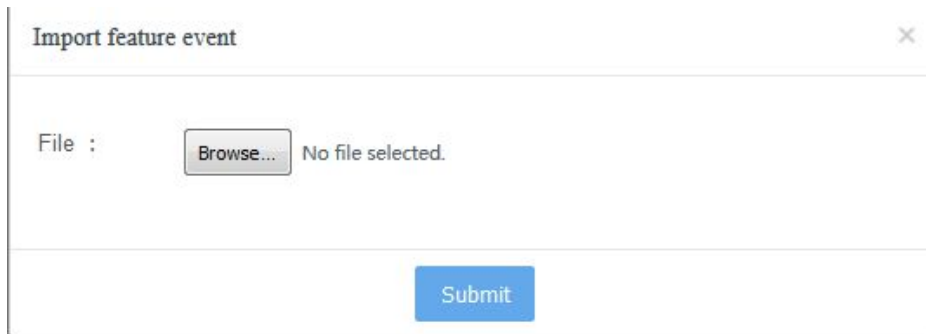
Configuration procedure:

Select a local directory and save the file.

Import the event definition file:

Configuration procedure:

Click **[Import]**. The event definition file import window is displayed, as shown in the following figure:

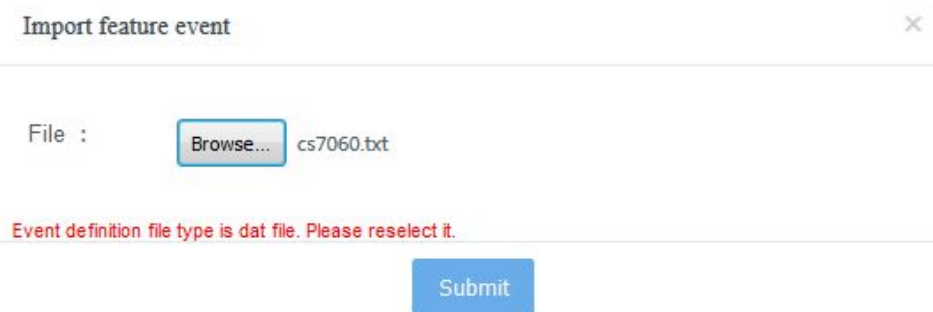


Import feature event

File : No file selected.

Click **[Select file]**. In the window displayed, select the event definition file to be imported and click **[Submit]**.

If the selected event definition file is not a DAT file, the following message is displayed:





Import feature event

File : cs7060.txt

Event definition file type is dat file. Please reselect it.

After the file is imported, the imported feature event definition is displayed in the event list, as shown in the following figure:

SN	CUSTOMIZE EVENT NAME	EVENT DESCRIPTION	OPERATION
1	HTTP_001	just for test	 

6.1.12 Customize a secondary event

Different from feature events, secondary events are not detected by event occurrence

statistics instead of feature matching. Because there are many attacks and detection behaviors in the network that are difficult to find their features, it is almost impossible to carry out intrusion prevention without extracting features in a misuse-based intrusion detection system. In a word, the secondary event is a mechanism to judge whether to make response within a specified period of time by introducing the statistical function num() on the basis of the feature event. Similar to feature events, secondary events can also be customized by the user, as shown in the following figure:

SN	CUSTOMIZE EVENT NAME	EVENT DESCRIPTION	OPERATION
1	ICMP_001	test for secondary event	 

New secondary event definition:

Click **[New]** to add a secondary event in the new secondary event window displayed, as shown in the following figure:

Configuration procedure:

Create secondary event
×

*Event name:

Event description:

Protocol type:

Affected system:

Prevalence:

Event definition: [Definition wizard](#)

Merging period: (1-120)Second

[Customize policy set](#)

Event alias:

Event level:

Security type:

Affected device:

Parameter description:

Event name: Enter an event name. The name must be started with the event protocol. This field is mandatory.

Event alias: Enter an event alias for convenient memory.

Event description: Describe the event. The description cannot exceed 120 characters. This field is optional.

Event level: Select the event level. Options are non-attack events, low-risk events, medium-risk events, and high-risk events. The default level is non-attack events.

Protocol type: Select the protocol type of the event.

Security type: Select the security type of the event.

Affected system: Select the key system affected by the event.

Affected device: Select the key device affected by the event.

Prevalence: Select the event popularity.

Event definition: Enter the event definition string. You are recommended to define the event by following the **Event definition wizard** and click **Syntax check** to check the definition syntax. This field is mandatory.

Merging period: Define the merging period threshold for the secondary event.

Customize policy set: Select a response method for the secondary event and add the response method to the custom policy set. When creating a new secondary event, you can specify no policy set for the event and then add a policy set by choosing **Feature detection configuration > Policy set**.

Configuration case:

We want to monitor the cumulative number of the "ICMP_PING_events" of all the visible hosts in the network occurred to the protected destination host 192.168.1.187 within the specified period of time. The threshold is set to 10 in this example.

Click [**New**]. The new secondary event window is displayed.

Enter the event name. The name should clearly indicate the event definition for easy understanding and management. "ICMP_selfdefine_001" is used in this example.

Enter the event alias. For future query convenient, "ICMP_PING_event monitoring" is used in this example.

Enter the event description as required. "Secondary event definition demonstration" is used in this example.

Select the event level as required. "Medium-risk event" is used in this example.

Select the event protocol type. Because the based feature event to be monitored is the "ICMP_PING_event", "ICMP" is selected for the protocol type.

Select the event security type. Because frequent "ICMP_PING_events" in the network result in the DDoS Ping attacks, "Distributed DoS" is selected for the security type.

Select the affected system as required. "Web server" is used in this example.

Select the affected device as required. "UNIX OS" is used in this example.

Select the popularity as required. "Popular" is used in this example.

Set the merging period threshold to 60s,
as shown in the following figure:

Create secondary event ×

*Event name:	<input type="text" value="ICMP_001"/>	Event alias:	<input type="text" value="ICMP_PING_event"/>
Event description:	<input type="text" value="test for secondary event"/>	Event level:	<input type="text" value="Middlelevel"/>
Protocol type:	<input type="text" value="ICMP"/>	Security type:	<input type="text" value="DDoS"/>
Affected system:	<input type="text" value="Web server"/>	Affected device:	<input type="text" value="UNIX OS"/>
Prevalence:	<input type="text" value="Popular"/>		
Event definition:	Definition wizard <input type="button" value="Syntax check"/>		
	<input type="text"/>		
Merging period:	<input type="text" value="60"/>	(1-120)Second	

[Customize policy set](#)

Define the event by following the **Event definition wizard**. Click the link of [**Definition wizard**]. The event definition wizard window is displayed, as shown in the following figure:

Function name: num

Detection event: Select events by class

IP address type: IPv4

Source IP address: This item is not considered. 0.0.0.0

Destination IP address: This item is not considered. 0.0.0.0

Source port: This item is not considered.

Destination port: This item is not considered.

Operator: >

Cumulative number:

Association relationship (the association relationship in the definition string must be unique) and or

OK

Parameter description:

Detection event: This secondary event is based on feature event. Therefore, the event must be selected by clicking **Select events by class**. You cannot enter the event name manually.

IP address type: Select IPv4 or IPv6 based on your demand or event occurrence scenario.

Source IP address: Select the IP address of the source host to be monitored. Options in the drop-down list are: **Specified IP address**, **Same each time**, **Different each time**, and **This item is not considered**. **This item is not considered** is used by default.

When **Specified IP address** is selected, enter the specified IP address in the input box.

Destination IP address: Select the IP address of the destination host to be monitored. Options in the drop-down list are: **Specified IP address**, **Same each time**, **Different each time**, and **This item is not considered**. **This item is not considered** is used by default. When **Specified IP address** is selected, enter the specified IP address in the input box.

Source port: Enter the port number of the source host to be monitored. Options in the drop-down list are **Same each time**, **Different each time**, and **Ignore**. **Ignore** is used by default.

Destination port: Enter the port number of the destination host to be monitored. Options in the drop-down list are **Same each time**, **Different each time**, and **This item is not considered**. **This item is not considered** is used by default.

Operator: Define the comparison relationship between the event statistics count and cumulative number. The default value is "> - greater than", which cannot be modified.

Cumulative number: Define the statistics count of the feature event based on which the secondary event is monitored in the event merging period. This threshold is the most important parameter of the secondary event. You can set the threshold as required.

Select the feature event based on which the secondary event is monitored, and click **Select events by class**. The event selection window is displayed. On the top of the window, the drop-down list of the protocol types is displayed. The event name list displays all the feature events of the corresponding protocol type. Because we want to select the feature event "ICMP_PING_event", select "ICMP" from the protocol type drop-down list and "ICMP_PING_event" in the list on the right, as shown in the following figure:

Event selection ×

Protocol type: Content:

	Event name
<input checked="" type="radio"/>	ICMP_TCP/IP_Stack_Vulnerability_Denial_of_Service
<input type="radio"/>	ICMP_Backdoor_Gimmiv_Connection
<input type="radio"/>	ICMP_Ssping_Fragment_DoS
<input type="radio"/>	SCAN_ICMP_Scanning_Exploration
<input type="radio"/>	DOS_ICMP_FLOOD_Denial_of_Service
<input type="radio"/>	ICMP_Damaged_IP_Header
<input type="radio"/>	ICMP_Backdoor_NTROOTKIT_Connection
<input type="radio"/>	ICMP_DDoS_TFN_Exploration
<input type="radio"/>	ICMP_DDoS_TFN_Server_Response
<input type="radio"/>	ICMP_TraceRoute

Click **[OK]**. The "ICMP_PING_event" is displayed in the event check input box in the event definition wizard, as shown in the following figure:

Event definition wizard



Function name: num

Detection event:

IP address type: IPv4

Source IP address:

Destination IP address:

Source port:

Destination port:

Operator:

Cumulative number:

Association relationship (the association relationship in the definition string must be unique) and or

OK

Configure other parameters in the event definition help window.

Select **This item is not considered** (default) for **Source IP address**.

Because the destination protocol to be protected is 192.168.1.187, select **Specified IP address** for **Destination IP address**, and enter "192.168.1.187" in the input box.

Select **This item is not considered** (default) for **Source port**.

Select **This item is not considered** (default) for **Destination port**.

Use the default operator "> - greater than".

You can set the cumulative number as required. 10 is used in this example, which can be adjusted based on actual use effect.

If other event definition units are defined, you need to set the join relationship between the current definition and previous definitions. Options are AND and OR, as shown in the following figure:

Event definition wizard



Function name: num

Detection event:

IP address type: IPv4

Source IP address:

Destination IP address:

Source port:

Destination port:

Operator:

Cumulative number:

Association relationship (the association relationship in the definition string must be unique) and or

OK

After configuring the parameters on the event definition wizard, click **[OK]**. The event definition string "num(event=ICMP_PING_event,dip=192.168.1.187)>10" is generated in the event definition input box, as shown in the following figure:

Create secondary event



*Event name:	<input type="text" value="ICMP_001"/>	Event alias:	<input type="text" value="ICMP_PING_event"/>
Event description:	<input type="text" value="test for secondary event"/>	Event level:	<input type="text" value="Middlelevel"/>
Protocol type:	<input type="text" value="ICMP"/>	Security type:	<input type="text" value="DDoS"/>
Affected system:	<input type="text" value="Web server"/>	Affected device:	<input type="text" value="UNIX OS"/>
Prevalence:	<input type="text" value="Popular"/>		
Event definition:	Definition wizard <input type="button" value="Syntax check"/>		
	<input type="text" value="yum(event=ICMP_PING_Event,dip=192.168.1.187)>10"/>		
Merging period:	<input type="text" value="60"/>		(1-120)Second

[Customize policy set](#)

Submit

You can click **Syntax check** to check whether the event definition string is correct. Click **[Syntax check]**. The check result window is displayed.

If the event definition string passes the check, the following message is displayed:

Information



Correct syntax.

Close

If the event definition string fails the check, the corresponding error message is returned.

When the cumulative occurrence count exceeds the preset threshold within the specified merging period, this secondary event is reported once. The threshold ranges from 1s to 120s.

Select a policy set. Click the link of **[Customize policy set]**. In the dialog box displayed, select the response method and custom policy set for the secondary event, as shown in

the following figure:

Selection policy set. ×

Response method:

Alarm Local storage RST block Firewall linkage Log


Email alarm SNMP Syslog Extract packet

Policy name:

all

After entering relevant information for the secondary event as required, click **[Submit]**.

If the entered information is correct and meets the requirements, the added event is displayed in the event list, as shown in the following figure:

SN	CUSTOMIZE EVENT NAME	EVENT DESCRIPTION	OPERATION
1	ICMP_001	test for secondary event	 

Otherwise, an error message is returned, and the event is not added to the event list until you enter relevant information as required.

Edit secondary event definition:

Click **[Edit]**. In the event editing window displayed, edit an existing secondary event, as shown in the following figure:

Configuration procedure:

*Event name	<input type="text" value="ICMP_001"/>	Event alias	<input type="text" value="ICMP_PING_event"/>
Event description	<input type="text" value="test for secondary event"/>	Event level	<input type="text" value="Middlelevel"/>
Protocol type	<input type="text" value="ICMP"/>	Security type	<input type="text" value="DDoS"/>
Affected system	<input type="text" value="Web server"/>	Affected device	<input type="text" value="UNIX OS"/>
Prevalence	<input type="text" value="Popular"/>		
Event definition	Definition wizard <input type="button" value="Syntax check"/>		
	<input type="text" value="num(event=ICMP_PING_Event,dip=192.168.1.187)>10"/>		
Merging period	<input type="text" value="60"/>	(1-120)Second	
Customize policy set			

Parameter description:

Event name: Enter an event name. The name must be started with the event protocol. This field is mandatory.

Event alias: Enter an event alias for convenient memory.

Event description: Describe the event. The description cannot exceed 120 characters. This field is optional.

Event level: Select the event level. Options are non-attack events, low-risk events, medium-risk events, and high-risk events. The default level is non-attack events.

Protocol type: Select the protocol type of the event.

Security type: Select the security type of the event.

Affected system: Select the key system affected by the event.

Affected device: Select the key device affected by the event.

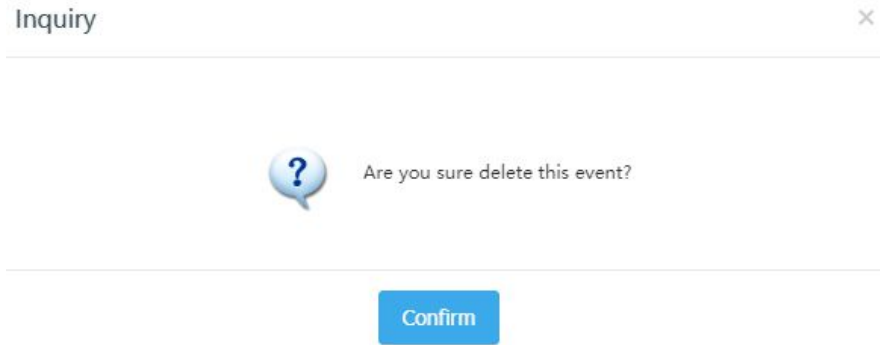
Prevalence: Select the event popularity.

Event definition: Enter the event definition string. You are recommended to define the event by following the **Event definition wizard** and click **Syntax check** to check the definition syntax. This field is mandatory.

Delete secondary event definition:

Click **[Delete]**. A window is displayed, asking you whether to delete the current secondary event, as shown in the following figure:

Configuration procedure:



Export the event definition file:

Click **[Export]**. A new window is displayed, asking you whether to open or save the event definition file.

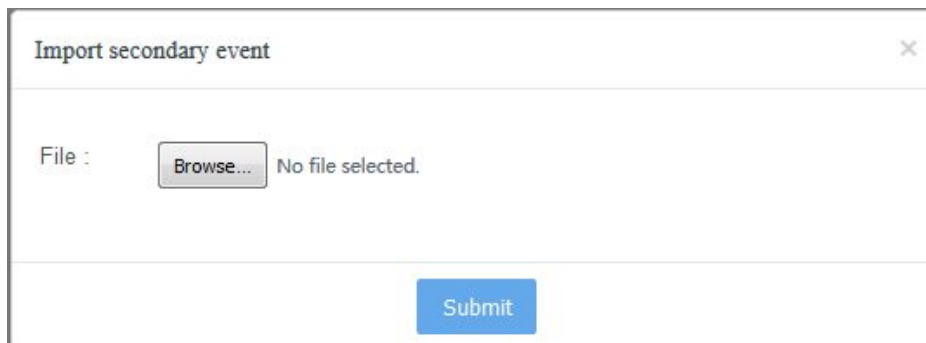
Configuration procedure:

Select a local directory and save the file.

Import the event definition file:

Configuration procedure:

Click **[Import]**. The event definition file import window is displayed, as shown in the following figure:



Click **[Select file]**. In the window displayed, select the event definition file to be imported and click **[Submit]**.

If the selected file is not an event definition file, the following message is displayed:

Import secondary event ✕

File : cs7060.txt

The specified event definition file is a DAT file. Please select a file of another type.

After the file is imported, the imported feature event definition is displayed in the event list.



After the secondary event is added, it is automatically distributed to the type of "**Needing attention**" in the key attention module.

6.1.13 DoS and scanning events

A threshold must be set for DoS and scanning events to reduce false report due to their mass nature. Choose **Feature detection configuration > DoS and scanning events**. The DoS and scanning event threshold setting page is displayed, as shown in the following figure:

Policy set Policy template Feature event Secondary event DoS and scan type Weak password config Event merging

Event name	Event type	Event (s)	Quantity	Operation
SCAN_ICMP_Scanning_Exploration	scan	1	10	
SCAN_UDP_Port_Scanning	scan	1	20	
SCAN_SYNONLY_TCP_Port_Scanning	scan	1	10	
DOS_TCP_FLOOD_Denial_of_Service[STREAM]	flood	1	2048	
DOS_TCP_FLOOD_Denial_of_Service[HALFSESSION]	flood	1	4096	
DOS_TCP_FLOOD_Denial_of_Service[SYNRST]	flood	1	4096	
DOS_SYN_FLOOD_Denial_of_Service[SYNONLY]	flood	1	4096	
DOS_UDP_FLOOD_Denial_of_Service	flood	1	4096	
DOS_ICMP_FLOOD_Denial_of_Service	flood	1	4096	

(filtered from 9 total entries)

This module is related to the event library. If the event library has no DoS and scanning event, no event is displayed in this module.

You can only perform the edit operation in this module. Click **[Edit]** after an event to enter the event threshold edit page. Taking the SCAN_SYNONLY_TCP port scanning event as an example, the event threshold edit page is as follows:

Enter the time and threshold value, select a time unit, and click **[OK]**, as shown in the following figure:

Event name	Event type	Event (s)	Quantity	Operation
SCAN_ICMP_Scanning_Exploration	scan	1	10	
SCAN_UDP_Port_Scanning	scan	1	20	
SCAN_SYNONLY_TCP_Port_Scanning	scan	1	10	
DOS_TCP_FLOOD_Denial_of_Service[STREAM]	flood	1	2048	
DOS_TCP_FLOOD_Denial_of_Service[HALFSESSION]	flood	1	4096	
DOS_TCP_FLOOD_Denial_of_Service[SYNRST]	flood	1	4096	
DOS_SYN_FLOOD_Denial_of_Service[SYNONLY]	flood	1	4096	
DOS_UDP_FLOOD_Denial_of_Service	flood	1	4096	
DOS_ICMP_FLOOD_Denial_of_Service	flood	1	4096	

(filtered from 9 total entries)

Each event has default configurations. The time and threshold fields can be edited. The time unit options are second, minute, hour, and day. You can select one as required. In the following figure, the time unit is minute and the threshold value is 100, as shown in the following figure:

Edit Event threshold



Event name

Time

Quantity

After the configuration is submitted, the time value is converted to a value in the unit of second, as shown in the following figure:

Event name	Event type	Event (s)	Quantity	Operation
SCAN_ICMP_Scanning_Exploration	scan	1	60	
SCAN_UDP_Port_Scanning	scan	1	20	
SCAN_SYNONLY_TCP_Port_Scanning	scan	1	10	
DOS_TCP_FLOOD_Denial_of_Service[STREAM]	flood	1	2048	
DOS_TCP_FLOOD_Denial_of_Service[HALFSESSION]	flood	1	4096	
DOS_TCP_FLOOD_Denial_of_Service[SYNRST]	flood	1	4096	
DOS_SYN_FLOOD_Denial_of_Service[SYNONLY]	flood	1	4096	
DOS_UDP_FLOOD_Denial_of_Service	flood	1	4096	
DOS_ICMP_FLOOD_Denial_of_Service	flood	1	4096	

(filtered from 9 total entries)

Click **[Edit]**. The time value on the page is converted to a value in the unit of second:

Edit Event threshold



Event name

Time

Quantity

After the configuration is submitted, the time value is converted to a value in the unit of second when the time unit is set to hour or day after you click [**Edit**].

Note: The event count in this module is related to that in the event library. If a DoS and scanning event is deleted from the event library, that event is also deleted from this module.

6.1.14 Weak password configuration

This module is used to configure passwords consisting of letters and numbers, for example, "123" and "abc". The password is detected when you access the server and the detection result is reported.

Go to the weak password configuration page and configure the items as required, as shown in the following figure:

Start weak password detection

Config item

The password and user name cannot be inclusive with each other.

The password must contain more than eight characters.

The password cannot contain only digits.

The password cannot contain only letters.

The password must contain characters other than digits and letters.

The password cannot contain only uppercase or lowercase letters.

The password cannot contain only incremental, decremental, or duplicate letters or digits.

Advanced config

Do not display the user password

Click [**Submit**]. In the engine selection page displayed, select the engine to which the configuration is delivered, as shown in the following figure:

Select an engine.



<input type="checkbox"/>	IP address	Engine name
<input checked="" type="checkbox"/>	192.168.58.142	142

OK

Click **[OK]**. The message "Weak password configured successfully" is displayed.

✓ Configured successfully.



The weak password configuration is delivered to different engines through the web page. The configuration status is not displayed on the page. The default page display is as follows:

Start weak password detection

Config item

- The password and user name cannot be inclusive with each other.
- The password must contain more than eight characters.
- The password cannot contain only digits.
- The password cannot contain only letters.
- The password must contain characters other than digits and letters.
- The password cannot contain only uppercase or lowercase letters.
- The password cannot contain only incremental, decremental, or duplicate letters or digits.

Advanced config

Do not display the user password

Submit

6.1.15 Event merging

The event merging module can be used to configure the merging period and the maximum number of merges for an engine event.

Choose **Feature detection > Event merging**, as shown in the following figure:



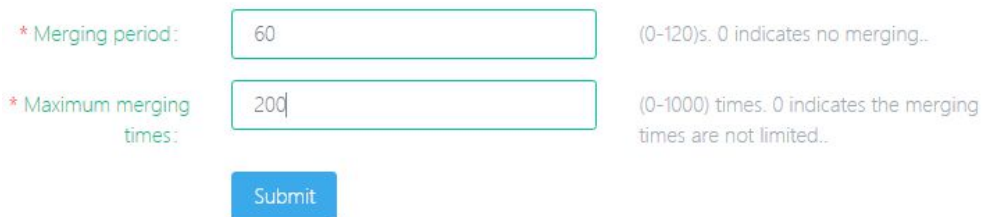
* Merging period: (0-120)s. 0 indicates no merging..

* Maximum merging times: (0-1000) times. 0 indicates the merging times are not limited..

Merging period: Configure the merging period of the events, in the unit of seconds. The range is 0s to 120s. 0 indicates not merging. The default merging period is 60s.

Maximum merging times: Configure the maximum number of times that events can be merged. The range is 0 to 1000. 0 indicates no limit on the maximum number of merges. The default maximum number of merges is 255.

The merging period and maximum number of merges can be configured. Enter a correct merging period and maximum number of merges and click [**Submit**], as shown in the following figure:



* Merging period: (0-120)s. 0 indicates no merging..

* Maximum merging times: (0-1000) times. 0 indicates the merging times are not limited..

Click [**Submit**]. In the engine selection page displayed, select the engine to which the configuration is delivered, as shown in the following figure:

Select an engine. ×

<input type="checkbox"/>	IP address	Engine name
<input checked="" type="checkbox"/>	192.168.58.142	142

OK

Click **[OK]**. The message "Configuration saved successfully" is displayed:

✓ Configured successfully.



The event merging configuration is delivered to different engines through the web page. The configuration status is not displayed on the page. The default page display is as follows:

* Merging period:

(0-120)s. 0 indicates no merging..

* Maximum merging times:

(0-1000) times. 0 indicates the merging times are not limited..

Submit

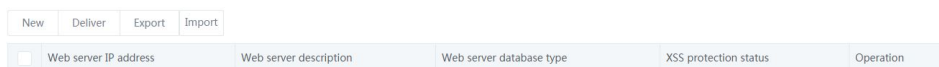
6.2 Asset config

6.2.1 Key Web server

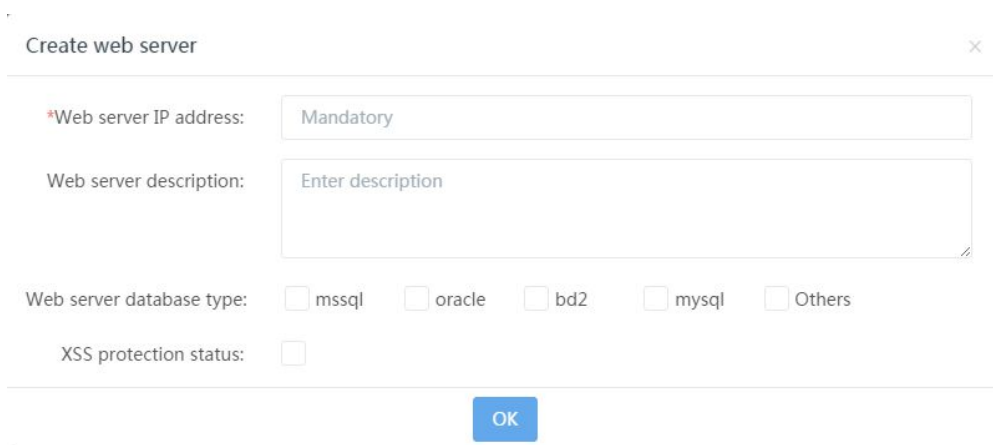
SQL injection is performed through a normal HTTP service port. Seemingly, it is not different from normal Web access, and thus is hard to detect. XSS is a passive attack. The attacker first constructs a cross-site page and compiles a script or by other means to trigger an HTTP request to the attacked site when users browse the page, causing

great harm to users. This version has added a key Web server module, which can accurately and time detect and report this kind of events.

Go to the key Web server level-3 menu under **Asset configuration**, as shown in the following figure:



Click **[New]**. The new key Web server page is displayed, as shown in the following figure.

A screenshot of a 'Create web server' form. The form has a title bar with 'Create web server' and a close button. It contains four main sections: 1. 'Web server IP address:' with a text input field containing 'Mandatory' and a red asterisk indicating it is mandatory. 2. 'Web server description:' with a larger text input field containing 'Enter description'. 3. 'Web server database type:' with five radio button options: 'mssql', 'oracle', 'bd2', 'mysql', and 'Others'. 4. 'XSS protection status:' with a single checkbox. At the bottom center of the form is a blue 'OK' button.

Parameter description:

Web Server IP address: Enter the IP address of the key server to be protected.

Web Server description: Describe the key server to be protected.

Web Server database type: Select one or more databases based on the HTTP_SQL injection attack.

XSS protection status: Select whether to enable the XSS protection function.

Fill in relevant fields as required, as shown in the following figure.

Web server IP address: 192.168.10.10

Web server description: Enter description

Web server database type: mssql oracle bd2 mysql Others

XSS protection status:

OK

This configuration means that the MSSQL and Oracle on the server with the IP address of 192.168.10.30 are protected against HTTP_SQL injection attacks and XSS protection is enabled for the IP address.

Click **[OK]**. The configuration is displayed in the key Web server list, as shown in the following figure.

Web server IP address	Web server description	Web server database type	XSS protection status	Operation
<input type="checkbox"/> 192.168.10.10	N/A	[mssql] [oracle]	Enable	

Then, select the server to be protected and click **[Deliver]**. In the engine selection page displayed, select the engine to which the configuration is delivered, as shown in the following figure:

<input type="checkbox"/>	Engine name	IP address
<input checked="" type="checkbox"/>	188	192.168.58.188

OK

Click **[OK]**. The configuration is delivered to the engine and the message "Delivered successfully" is displayed (the response is slow), as shown in the following figure:



Click **[Edit]** to modify the Web server configuration. The server IP address cannot be modified, as shown in the following figure:

Modify the key web server ✕

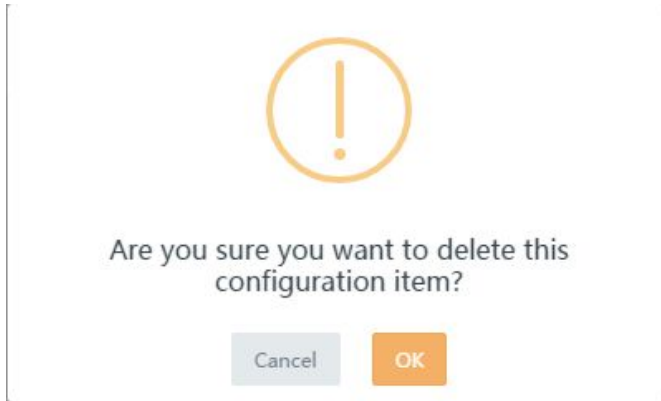
*Web server IP address:

Web server description:

Web server database type: mssql oracle bd2 mysql Others

XSS protection status:

Click **[Delete]** to delete a configuration item. The confirmation dialog box is displayed, as shown in the following figure:



Click **[OK]**. The Web server of the specified IP address is deleted.

When using this module, note that:

If you click **[Deliver]** without making any configuration, all the IP addresses are protected against the HTTP_SQL injection attack, HTTP_XSS protection, and HTTP_XSS script injection. These events occurring on any IP address will be detected and reported.

Add the following two configuration items and deliver them to the engine, as shown in the following figure:

New Deliver Export Import					
<input checked="" type="checkbox"/>	Web server IP address	Web server description	Web server database type	XSS protection status	Operation
<input checked="" type="checkbox"/>	10.10.10.10	N/A	[mssql] [oracle]	Enable	
<input checked="" type="checkbox"/>	20.20.20.20	N/A	unEnabled	Not enabled	

In this case, only the MSSQL database on the server with the IP address of 192.168.10.30 is protected against the Oracle injection attack, and the server with the IP address of 192.168.10.50 is protected against the HTTP_XSS protection and HTTP_XSS script injection. Only these three types of events occurring on the two servers are detected and reported. Servers of other IP addresses are not protected against these events and events occurring on them are not reported.

Add the following two configuration items and deliver them to the engine, as shown in the following figure:

New Deliver Export Import					
<input checked="" type="checkbox"/>	Web server IP address	Web server description	Web server database type	XSS protection status	Operation
<input checked="" type="checkbox"/>	10.10.10.10	N/A	unEnabled	Not enabled	
<input checked="" type="checkbox"/>	20.20.20.20	N/A	unEnabled	Enable	

In this case, only the server with the IP address of 192.168.10.50 is protected against the HTTP_XSS protection and HTTP_XSS script injection. Only the HTTP_XSS protection and HTTP_XSS script injection events occurring on this server are detected and reported. Servers of other IP addresses are not protected against these events and events occurring on them are not reported. However, the HTTP_SQL injection attack occurring on a server of any IP address are defended and reported.

Add the following two configuration items and deliver them to the engine, as shown in the following figure:

New Deliver Export Import					
<input checked="" type="checkbox"/>	Web server IP address	Web server description	Web server database type	XSS protection status	Operation
<input checked="" type="checkbox"/>	10.10.10.10	N/A	[mssql] [oracle]	Not enabled	
<input checked="" type="checkbox"/>	20.20.20.20	N/A	unEnabled	Not enabled	

In this case, only the server with the IP address of 192.168.10.30 is protected against the MSSQL or MSSQL HTTP_SQL injection. Only the HTTP_SQL injection events occurring on this server are detected and reported. Servers of other IP addresses are not protected against the HTTP_SQL events and HTTP_SQL events occurring on them are not reported. However, the HTTP_XSS protection and HTTP_SQL injection attack occurring on a server of any IP address are defended and reported.

Add the following two configuration items and deliver them to the engine, as shown in the following figure:

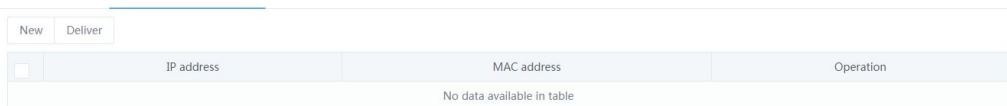
New Deliver Export Import					
<input checked="" type="checkbox"/>	Web server IP address	Web server description	Web server database type	XSS protection status	Operation
<input checked="" type="checkbox"/>	10.10.10.10	N/A	unEnabled	Not enabled	
<input checked="" type="checkbox"/>	20.20.20.20	N/A	unEnabled	Not enabled	

The effect of this configuration is same to that when you click **[Deliver]** without making any configuration. Servers of all IP addresses are protected against the HTTP_SQL injection attack, HTTP_XSS protection, and HTTP_XSS script injection and such events occurring on servers of any IP address are detected and reported.

6.2.2 IP-MAC address binding

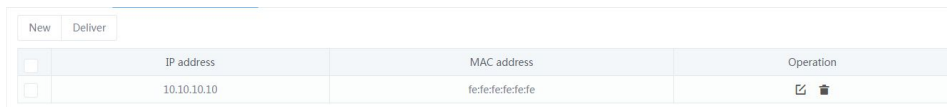
IP-MAC address binding means binding an IP address to a MAC address. It can be used to detect the ARP address spoofing and ARP address conflict events in the packets, and distinguish DHCP dynamic IP addresses from static IP addresses.



Choose **Asset config > IP-MAC address binding**, as shown in the following figure:



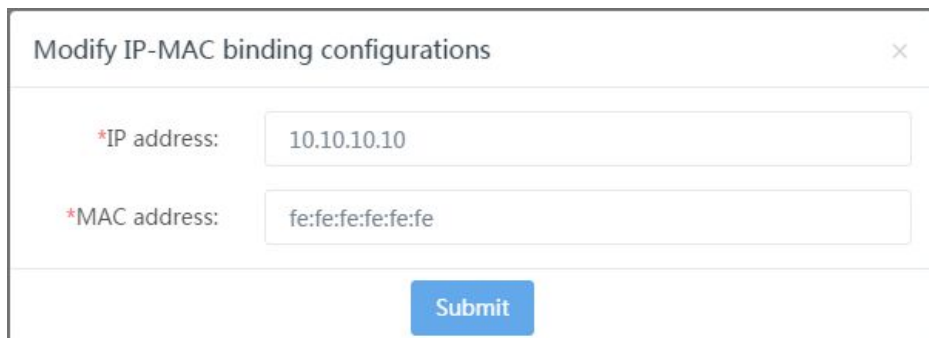
	IP address	MAC address	Operation
No data available in table			

Enter an IP address in the IP address column and a MAC address to be bound in the MAC address column, and click **[New]**. A new IP-MAC address binding message is generated (a maximum of five IP-MAC binding messages can be delivered), as shown in the following figure:



	IP address	MAC address	Operation
<input type="checkbox"/>	10.10.10.10	fe:fe:fe:fe:fe:fe	 

Click **[Edit]** in the operation area to modify the bound IP address or MAC address, as shown in the following figure:

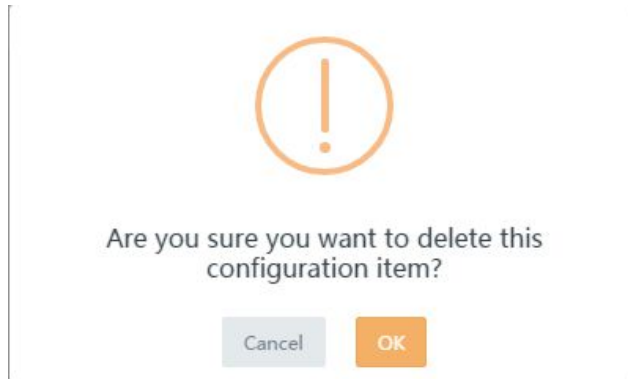


Modify IP-MAC binding configurations

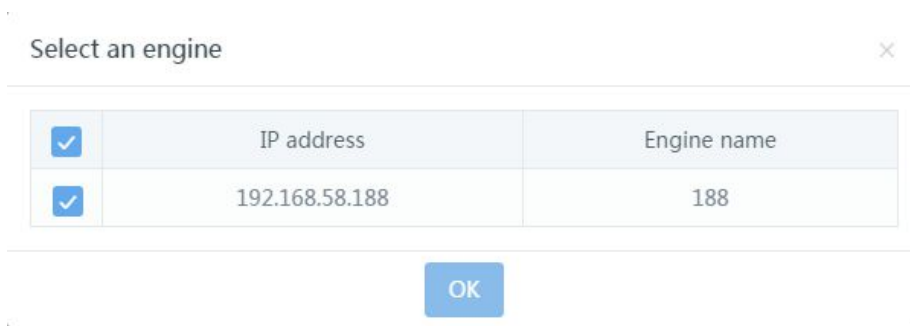
*IP address:

*MAC address:

Click **[Delete]** to delete an IP-MAC address binding message, as shown in the following figure:








Select a configuration and click **[Deliver]**. In the engine selection page displayed, select the engine to which the configuration is delivered, as shown in the following figure:



Click **[OK]**. The IP-MAC address binding message is delivered to the engine.

6.3 Device management

The module is used for device management, including editing, deleting, connecting, or disconnecting a device, creating a cascading device or a multi-host engine, and configuring authorization, engine details, dynamic detection engine, and superior status. The device management list is as follows.

Name	IP address	Description	Creation time	Policy set	Operation
Local Control Center	192.168.58.142	N/A	2018-12-12 17:49:10	N/A	N/A
188	192.168.58.188	N/A	2018-12-13 18:45:56	all(2018-12-11 14:44:22)	    

6.3.1 New device

The new device function is used for multi-host and multi-level management of engines and cascading management of the engine type management engine and control center.

New device
✕

Device type:

*Name:

*IP address:

Description:

6.3.2 Authorization configuration

This module is used to import and activate the authorization code and display the authorization status.

Click [Authorization information] to go to the authorization configuration page.

Name	IP address	Description	Creation time	Policy set	Operation
Local Control Center	192.168.58.142	N/A	2018-12-12 17:49:10	N/A	N/A
188	192.168.58.188	N/A	2018-12-13 18:45:56	all(2018-12-11 14:44:22)	<input type="button" value="✎"/> <input type="button" value="✖"/> <input type="button" value="🔄"/> <input style="border: 2px solid red;" type="button" value="🔍"/> <input type="button" value="🗑️"/>

(filtered from 2 total entries)

(1) Activate the trial authorization for first login

Authorization configuration

Import authorization file :

Engine SN :

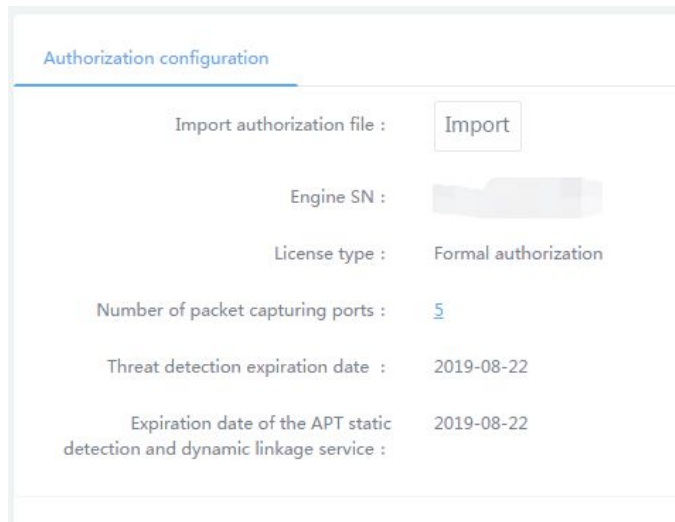
License type : Unauthorized

Number of packet capturing ports :

Threat detection expiration date : Unauthorized

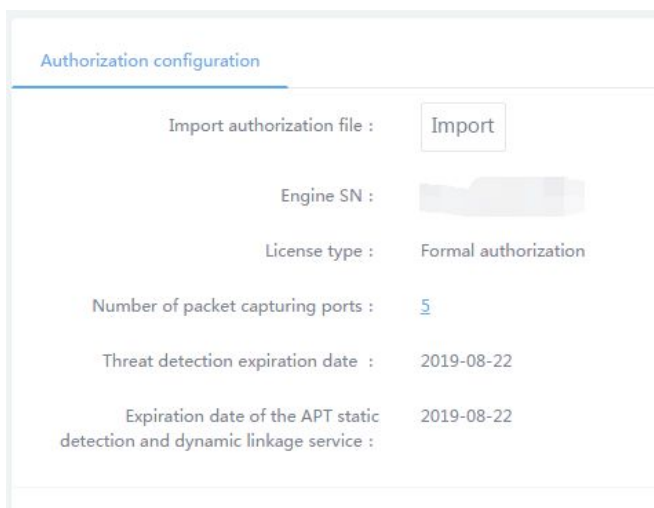
Expiration date of the APT static detection and dynamic linkage service : Unauthorized

Click [**Trial activation**]. After the authorization is successful, each module automatically updates the authorization information.



(2) Import the authorization file

Click **[Import]** and select the authorization file to be imported. After the authorization is successful, each module automatically updates the authorization information based on the authorization code, as shown in the following figure:



Import authorization file: Click **[Import]**, find the authorization file provided by Hirschmann IT, and click **[OK]**. After the authorization is successful, the authorization information of this engine is updated on the page.

Engine SN: The unique ID of the product. For more authorization, provide the engine SN to Hirschmann IT. Hirschmann IT will provide you with an authorization file. You can

use the authorization file to authorize the engine.

License type: Display the engine authorization status, including **Formal**, **Trial**, and **Unauthorized**.

Number of packet capturing ports: Display the number of packet capturing ports.

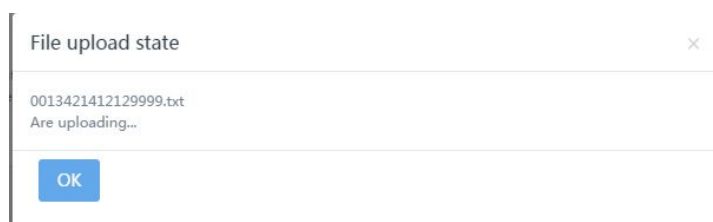
Event library expiration: Display the upgrade expiration date of the event library.

Upgrade expiration date of the AV virus library: Display the upgrade expiration date of the AV virus library.

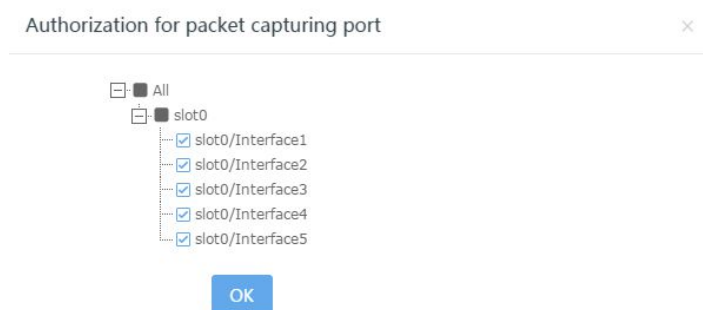
Static detection expiration date: Display the static detection expiration date.

Dynamic detection expiration date: Display the dynamic detection expiration date.

Attack detection module of the Web server : Display whether to authorize the Web server attack detection module.



Click **[Number of packet capturing ports]**. On the packet capturing port authorization page displayed, select the packet capturing port and then click **[OK]**, as shown in the following figure:



6.3.3 Device status

Click **[Details]** in the operation column to display the device status. The device status

page displays the basic device information, engine status, and configuration details.

Basic information:

Record the general device information and session statistics.

Engine version: Display the version of the feature detection module.

Engine policy name: Display the policy set applied to the current engine.

Number of engine TCP sessions: Display the cumulative statistics on the number of TCP sessions of the engine.

Number of engine HTTP sessions: Display the cumulative statistics on the number of HTTP sessions of the engine.

Device state

Basic information

Engine state

Configuration details

General information

Engine version : 0700R0600820171127140643
Engine policy name : all(2018-12-11 14:44:22)
Number of engine TCP sessions : 0
Number of engine HTTP sessions : 0

Engine state:

Record the running status of the feature detection module, including the system information and NIC status.

System information: Display the kernel information of the feature detection module.

NIC state: Record the current duplex mode, rate, usage, current number of packets, and current number of bits of each NIC.

Device state

Basic information

Engine state

Configuration details

System information

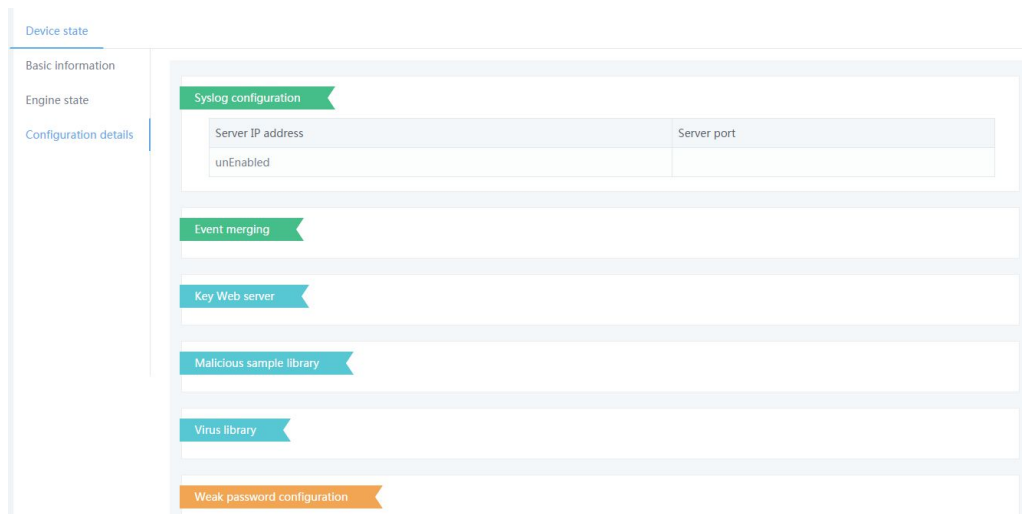
Kernel 3.1644

NIC state

NIC (name)	Duplex mode	Rate (Mbps)	Use	Number of current packets	Number of current bits
slot0/Interface1	Half duplex	10	Packet capturing port	242	218,480
slot0/Interface2	Unknown	Unknown	Packet capturing port	0	0
slot0/Interface3	Unknown	Unknown	Packet capturing port	0	0
slot0/Interface4	Unknown	Unknown	Unknown	0	0
slot0/Interface5	Unknown	Unknown	Unknown	0	0
slot0/eth0	Full duplex	100	Communication port	24	48,944

Configuration details:

Display the configuration of Syslog, event merging, key Web server, malicious sample library, virus library, weak password, IP-MAC address binding, and evasion detection, as shown in the following figure:





6.3.4 Dynamic engine configuration

Click **[New]**. In the page displayed, add a dynamic engine. Parameters include the engine name, engine IP address, engine description, engine port, user name, and password, as shown in the following figure:

The 'Add APT engine' dialog box contains the following fields and controls:

- *Engine name:
- *Engine IP address:
- Engine description:
- *Engine port :
- *User name:
- *Password:
- Connectivity test button
- OK button

After the engine is added, the following page is displayed:

IP address	Engine name	Engine description	Connection state	Operation
192.168.58.143	IDS		Not connected	 

Click **[Edit]** in the operation column to modify the engine configuration, as shown in the following figure:

Add APT engine ×

*Engine name:

*Engine IP address:

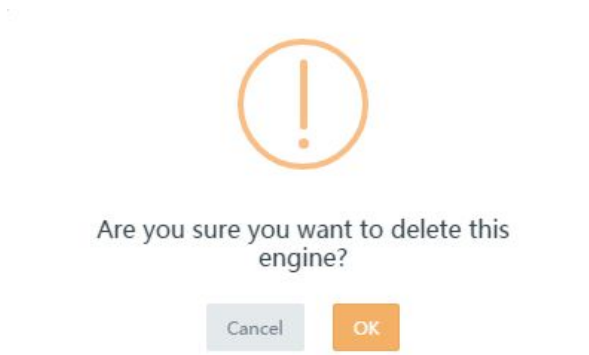
Engine description:

*Engine port :

*User name:

*Password:

Click **[Delete]** in the operation column to delete the engine configuration, as shown in the following figure:

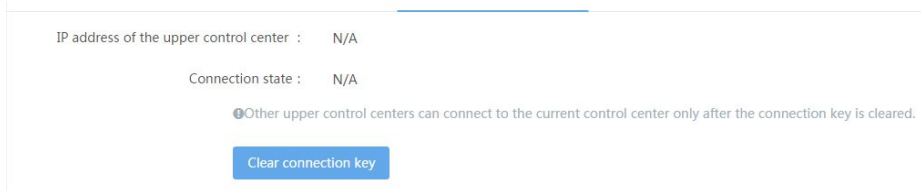


6.3.5 Superior status

The upper-level control center IP address field displays the IP address of the upper-level engine that manages the current engine.

The connection status field displays the connection status (Connected/Disconnected) between the current engine and its upper-level engine.

Click **[Clear connection key]** to clear the connection key between the current engine control center and its upper-level engine control center. Only when the connection key is cleared can other upper-level engine control centers be connected to the current engine control center, as shown in the following figure:



6.4 File detection configuration

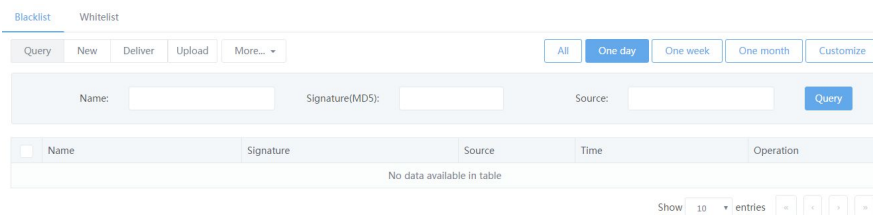
6.4.1 Blacklist

In addition to custom blacklists, the blacklist sample files added in the sample logs are also recorded to this module.

Operation buttons from left to right are: **Query, New, Deliver, Upload (sample) file,** and **More** (batch import and batch export).

Query:

You can screen the list records by configuring a query condition. Query conditions include name, signature (MD5 value), and source, as shown in the following figure:



New:

You can add a signature (MD5 value) to create a blacklist, as shown in the following figure:

Signature
×

*Name:

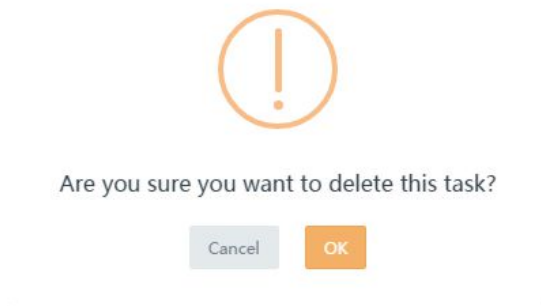
*Signature:

Click **[Submit]**. Then, the blacklist signature is displayed in the configuration list. The name, signature, source, time, and operation are displayed, as shown in the following figure:

<input type="checkbox"/>	Name	Signature	Source	Time	Operation
<input type="checkbox"/>	test	11223344556677881122334455667788	adm	2018-12-13 19:13:19	

The source indicates by whom the blacklist is created. You can enter the user name here.

In the operation column, you can delete a blacklist configuration, as shown in the following figure:



Deliver:

Select an item in the blacklist and click **[Deliver]**. In the engine selection page displayed, select the engine to which the configuration is delivered, as shown in the following figure:

Select an engine. ×

<input type="checkbox"/>	IP address	Engine name
<input checked="" type="checkbox"/>	192.168.58.188	188

Click **[OK]**. The message "Delivered successfully" is displayed:



Upload file:

You can manually upload a sample file to configure the blacklist. The maximum file size is 10 MB. A maximum of 300 files can be uploaded at a time, as shown in the following figure:

Blacklist Whitelist

Query New Deliver Upload More... All One day One week One month Customize

Name: MD5: Source:

Name	Source	Time	Operation
<input type="checkbox"/> test	2334455667788	adm 2018-12-13 19:13:19	<input type="button" value="↓"/> <input type="button" value="🗑"/>

Showing 1 to 1 of 1 entries Show 10 entries 1

Only files of no more than 10 MB are supported

A maximum of 300 files can be uploaded at a time

More:

Import: Make configuration for batch blacklist import. The file must be an .xls file, as shown in the following figure:

Import blacklist ×

Please select:: ?

Export: Make configuration for batch blacklist export, and select a path to save the configuration.

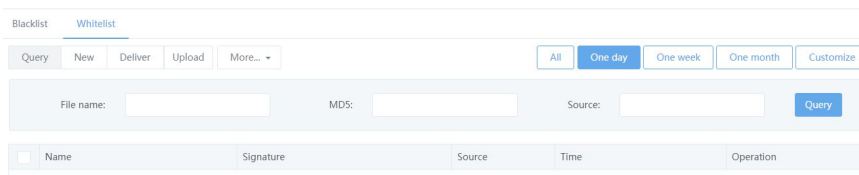
6.4.2 Whitelist

In addition to custom whitelists, the whitelist sample files added in the sample logs are also recorded to this module.

Operation buttons from left to right are: **Query**, **New**, **Deliver**, **Upload (sample) file**, and **More** (batch import and batch export).

Query:

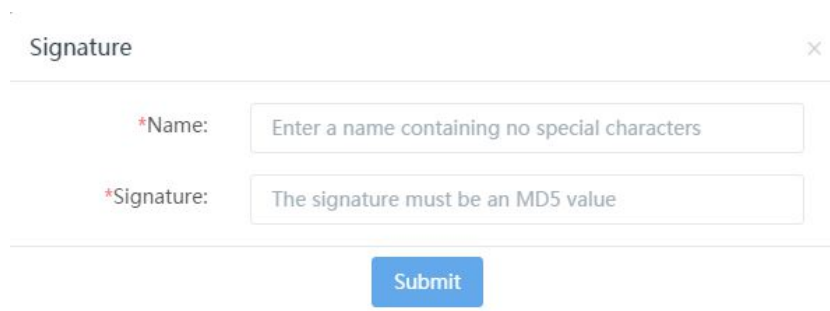
You can screen the list records by configuring a query condition. Query conditions include name, signature (MD5 value), and source, as shown in the following figure:



The screenshot shows the 'Whitelist' section of a web interface. At the top, there are tabs for 'Blacklist' and 'Whitelist'. Below the tabs is a navigation bar with buttons for 'Query', 'New', 'Deliver', 'Upload', and 'More...'. To the right of these buttons are filters for 'All', 'One day', 'One week', 'One month', and 'Customize'. Below the navigation bar is a search form with three input fields: 'File name:', 'MD5:', and 'Source:'. A blue 'Query' button is located to the right of the 'Source' field. Below the search form is a table with columns for 'Name', 'Signature', 'Source', 'Time', and 'Operation'. The table is currently empty.

New:

You can add a signature (MD5 value) to create a whitelist, as shown in the following figure:



The screenshot shows a 'New' form for creating a whitelist. The form has a title 'Signature' and a close button 'X'. It contains two required fields: '*Name:' with a placeholder 'Enter a name containing no special characters' and '*Signature:' with a placeholder 'The signature must be an MD5 value'. A blue 'Submit' button is located at the bottom of the form.

Deliver:

Select an item in the whitelist and click **[Deliver]**. In the engine selection page displayed, select the engine to which the configuration is delivered, as shown in the following figure:

<input type="checkbox"/>	IP address	Engine name
<input checked="" type="checkbox"/>	192.168.58.188	188

OK

Click **[OK]**. The message "Delivered successfully" is displayed:



Upload file:

You can manually upload a sample file to configure the whitelist. The maximum file size is 10 MB. A maximum of 300 files can be uploaded at a time. (See Figure 6-131)

More:

Import: Make configuration for batch whitelist import. The file must be an .xls file, as shown in the following figure:

Export: Make configuration for batch whitelist export, and select a path to save the configuration.

6.5 Virus detection configuration

With the rapid development of the Internet, computer viruses pose an increasing threat to information security. Especially in the network environment, the diversification of propagation path and application environment makes the occurrence frequency of network computer virus higher, more latent, more influential, and more destructive than ordinary computer virus. The prevention and control of network viruses and information security have become the key research objects in the computer field.

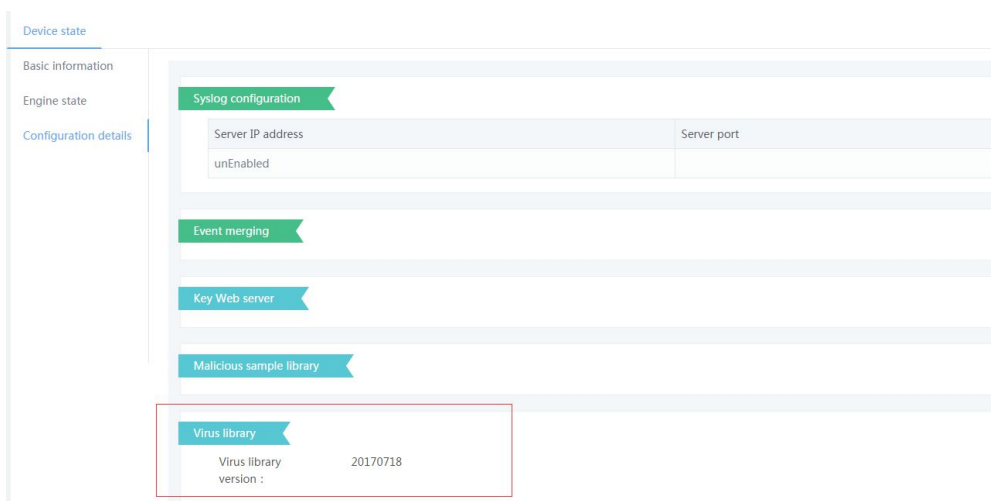
In the Internet environment, security threats mainly come from four sources: file downloaded, emails, chat tools, and download tools. Files browsed on or downloaded from the Internet may carry viruses. Most Internet email systems allow you to transmit emails with formatted documents between networks. Some chat tools provide online file transfer functions, such as MSN and QQ. Download tools include P2P, BT, and eDonkey.

IDS anti-virus detection function is mainly based on protocols of HTTP, FTP, POP3, IMAP and SMTP. You can enable scanning detection for files transmitted between networks based on the file type and enable to report the scanning and detection results.

Before you configure the virus detection, the following two conditions must be met:

First, the engine has been connected.

Second, the engine virus library has been upgraded to the required version. You can view the last version update time of the current virus library in the engine details on the device management page, as shown in the following figure.

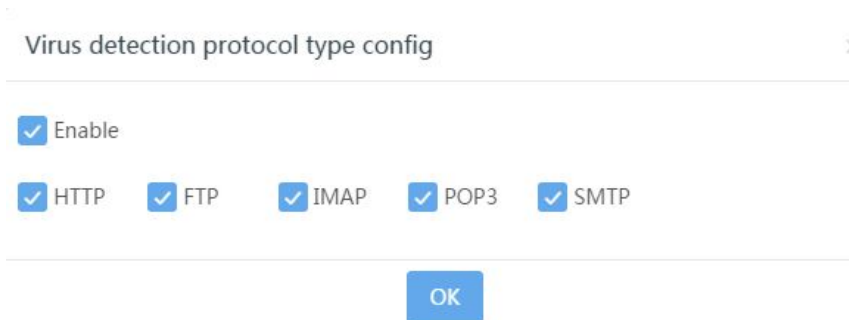


Virus detection config

Go to the **Virus detection config** page, click [**Virus detection protocol type config**] in the engine operation column. The configuration page is displayed, as shown in the following figure.



By default, five protocols are all not enabled. To enable a protocol, tick **Enable**, select the required protocol, and click **[OK]**. Then, the following dialog box is displayed.



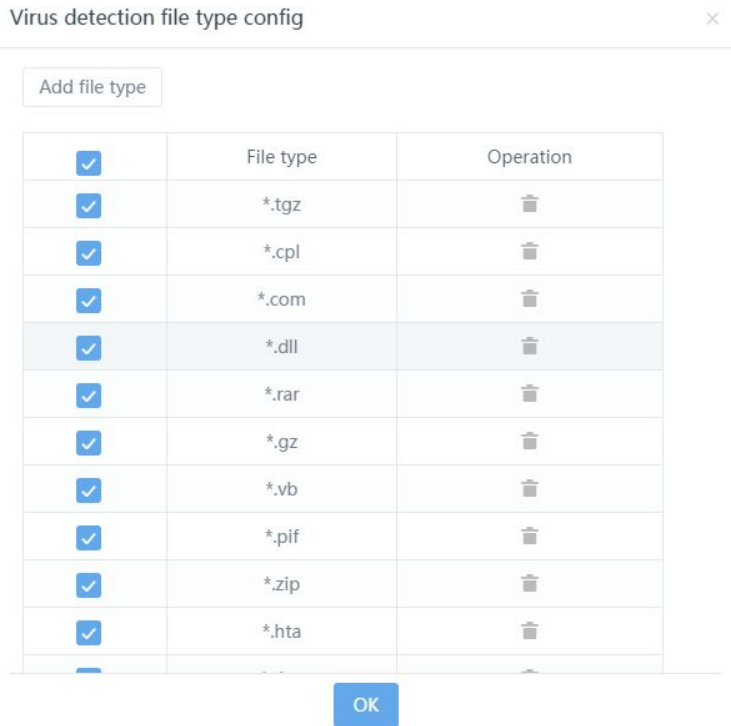
Click **[OK]**. The message "Protocol configured successfully" is displayed, as shown in the following figure:



If you do not want to submit the current protocol type configuration, click **X**. The page is redirected to the **Virus detection config** page.

Virus detection file type config

Go to the **Virus detection config** page, click **[Virus detection file type config]** in the engine operation column. The configuration page is displayed, as shown in the following figure.



By default, 17 file types are all enabled. To disable some file types, de-select the file types, and click **[OK]**, as shown in the following figure. Note that the default 17 file types cannot be deleted.

You can also customize the virus detection file type. To add a custom file type, click **[Add file type]** and select the file type to be added. Note that the new file type must be started by "*."; it can contain letters and numbers that do not exceed 10 characters, for example, "*.7z". Click **[Add]**. The new file type is added to the file type list. Then, click **[OK]**, as shown in the following figure.

Virus detection file type config

×

Add file type

File type:

<input checked="" type="checkbox"/>	File type	Operation
<input checked="" type="checkbox"/>	*.tgz	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.cpl	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.com	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.dll	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.rar	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.gz	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.vb	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.pif	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.zip	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	*.hta	<input type="button" value="Delete"/>
<input type="checkbox"/>		<input type="button" value="Delete"/>

To delete a custom detection file type, click **[Delete]** in the operation column and then click **[OK]**.

7 System management

The system management module consists of the response method, system maintenance, general configuration, and running log modules.

The response method module consists of the Syslog configuration, SNMP configuration, email configuration, and firewall configuration modules.

The system maintenance module consists of the upgrade management, system upgrade, and storage maintenance modules.

The general configuration module consists of the time configuration, proxy configuration, and attention degree configuration modules.

The running log module consists of the system running log and diagnosis log modules.

7.1 Response method

7.1.1 Syslog configuration

The Syslog configuration module can send detection events (including feature events, convert channel events, URL credibility detection events, virus detection events, and file detection events) and resource alarm messages to the specified Syslog server.

Choose **System management > Response method > Syslog config** to make the Syslog response configuration.

Syslog config SNMP config Email config Firewall linkage

Detection event
Resource alarm

Server IP1:

Server IP2:

Server port:

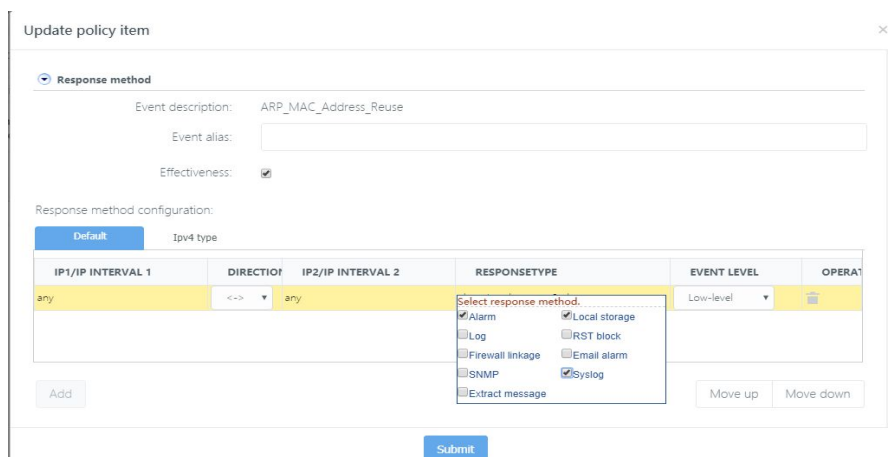
i Enable feature detection response in the response method of the policy set to make it take effect.

i Detection events include feature events , file detection

Submit

Choose **Detection config > Feature detection > Policy set** to select the Syslog

response method for the specified event. To configure the Syslog response method for multiple events, add a Syslog response method policy template and apply the template to multiple events.

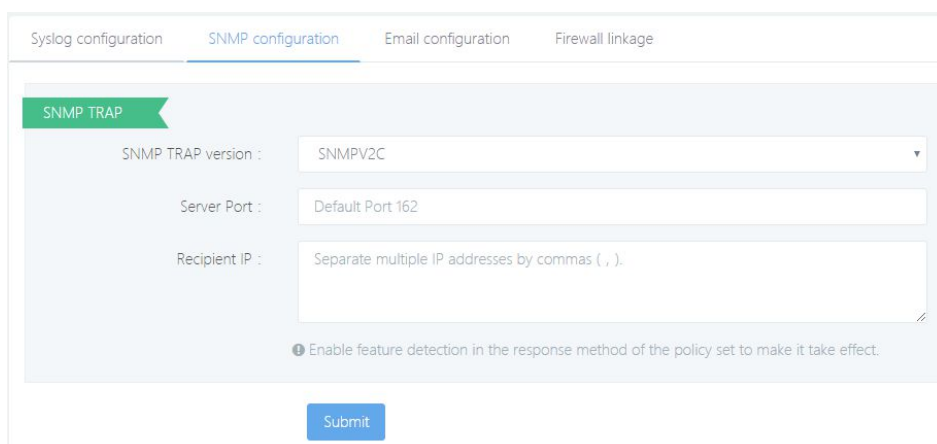


7.1.2 SNMP configuration

The feature detection log can be sent to the specified SNMP server.

Choose **System management > Response method > SNMP config** to make the SNMP response configuration.

Configure the SNMP TRAP version, server port, and the receiver IP address.



Choose **Detection config > Feature detection > Policy set** to select the SNMP response method for the specified event. To configure the SNMP response method for multiple events, add an SNMP response method policy template and apply the template to multiple events.

Update policy item

Response method

Event description: ARP_MAC_Address_Reuse

Event alias:

Effectiveness:

Response method configuration:

Default Ipv4 type

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERATION
any	<->	any	alarm,Local storage,SNMP	Warning level	

Select response method.

Alarm Local storage

Log RST block

Firewall linkage Email alarm

SNMP Syslog

Extract message

7.1.3 Email configuration

The feature detection log can be sent to the specified recipient by email.

Sender config:

Choose **System management > Response method > Email config** to make the sender configuration.

Configure the email sender server address, port, SMTP server identity authentication, and sending interval.

Parameter description:

Name: Enter the sender name.

Email: Enter the sender email address.

Server IP (IP address or domain name): Enter the IP address or domain name of the email server.

Port: Port 25 is used by default, which can be modified.

Account: Enter the sender email address.

Password: Enter the sender email password.

Proxy server: A proxy server can be configured.

Send interval: The alarm email sending interval is valid only when the email alarm function is enabled. This setting is invalid for the log report sending function.



The item "SSL required for this server" is selected by default. Do not select this item when a 163.com or 263.com email boxes are used because they do not support SSL.

After configuring the recipient information, click **[Test]**. When a recipient exists, the email is sent.

Then, a test email is displayed in the recipient email box.

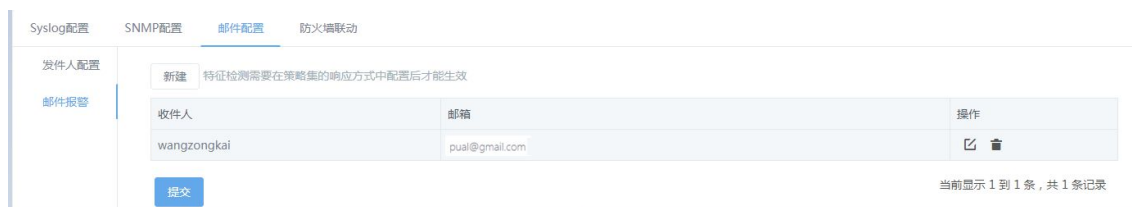
If the recipient information is incorrect or no recipient is configured, the system fails to send the email after you click **[Test]**.

After configuring the recipient information, click **[Submit]**.

Feature detection email response:

Choose **System management > Response method > Email config > Email alarm** to make the email response configuration.

Click **[New]** to add a recipient and email address.

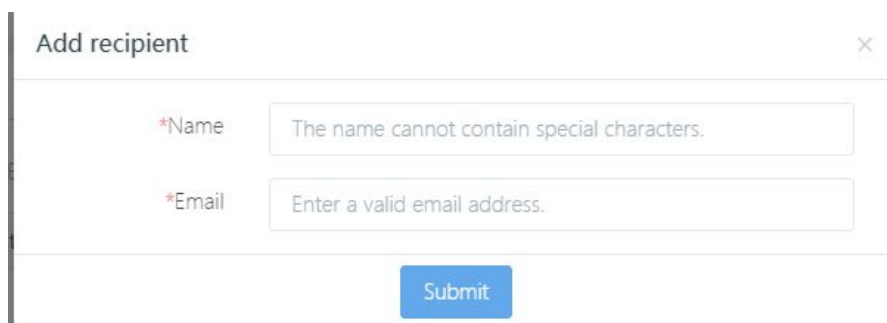


The screenshot shows a web interface with a navigation bar at the top containing 'Syslog配置', 'SNMP配置', '邮件配置', and '防火墙联动'. The '邮件配置' (Email Config) section is active. On the left, there are two sub-sections: '发件人配置' (Sender Config) and '邮件报警' (Email Alarm). Under '邮件报警', there is a '新建' (New) button with a tooltip that says '特征检测需要在策略集的响应方式中配置后才能生效'. Below this is a table with the following data:

收件人	邮箱	操作
wangzongkai	pual@gmail.com	✎ 查

At the bottom left of the table area is a '提交' (Submit) button. At the bottom right, it says '当前显示 1 到 1 条, 共 1 条记录' (Currently displaying 1 to 1 records, total 1 records).

Click **[New]** to edit the recipient information.



The screenshot shows a dialog box titled 'Add recipient' with a close button (X) in the top right corner. It contains two input fields:

- *Name: The name cannot contain special characters.
- *Email: Enter a valid email address.

At the bottom center of the dialog is a blue 'Submit' button.

Click **[Delete]** in the operation column to delete a recipient.



Are you sure you want to delete the config



Two buttons are shown: a grey 'Cancel' button and an orange 'Confirm' button.

Choose **Detection config > Feature detection > Policy set** to select the email alarm function for the specified event. To enable the email alarm function for multiple events, add an email alarm response method policy template and apply the template to multiple

events.

Update policy item

Response method

Event description: ARP_MAC_Address_Reuse

Event alias:

Effectiveness:

Response method configuration:

Default Ipv4 type

IP1/IP INTERVAL 1	DIRECTION	IP2/IP INTERVAL 2	RESPONSETYPE	EVENT LEVEL	OPERATION
any	<->	any	alarm,Local	level	

Select response method.

- Alarm
- Local storage
- Log
- RST block
- Firewall linkage
- Email alarm
- SNMP
- Syslog
- Extract message

Add

Submit

7.1.4 Firewall linkage

The RAVEN Intrusion Detection and Management System can work with some firewalls to defend network attacks. To trigger firewall linkage, you need to configure a linkage firewall for the engine and configure the firewall linkage response method for the followed event and deliver the event together with the policy to the engine.

SysLog config SNMP config Email config Firewall linkage

	Device name	IP address	Port	Key	Operation
▼	13_8	192.168.13.8			

Add a firewall:

Click **[Add]** in the engine operation column to add a firewall. Currently, the System supports four firewall types: vip_fw, opsec, netscreen, and topsec.

Add firewall
×

Engine IP address: 192.168.58.188

* Firewall type :

* Firewall IP address :

* Firewall port :

Firewall key

Upload key file

User name and password

User name :

Password :

Parameter description:

Firewall type: Select the firewall type to be added.

Firewall IP address: Enter the IP address of the firewall device. This field is mandatory.

Firewall port: Enter the port in linkage with the firewall.

Firewall key: Enable **Firewall key** and add the key if a key is required for firewall linkage.

Upload key file: Upload the file-type key here.

User name and password: Enter the user name and password of the key here.

Note: A maximum of 20 firewalls can be added.

Delete a firewall:

Click **[Delete]** next to the firewall list. The confirmation dialog box is displayed.



Are you sure you want to delete the configuration?

Cancelre

OK

Click **[OK]**.

7.2 System maintenance

7.2.1 Upgrade management

The upgrade management module mainly consists of six modules: event library upgrade, malicious sample library upgrade, URL credibility library upgrade, threat intelligence library upgrade, feature detection module upgrade, and virus library upgrade.

Event library upgrade: Manually upgrade the event library.

Malicious sample library upgrade: Manually upgrade the malicious sample library.

URL credibility library upgrade: Manually upgrade the URL credibility library.

Threat intelligence library upgrade: Manually upgrade the threat intelligence library.

Feature detection module upgrade: Manually upgrade the feature detection module.

Virus library upgrade: Manually upgrade the virus library.

The list display column consists of upgrade module, current version, latest version, upgrade status, and operation.

Upgrade module: Display the function module list.

Current version: Display the current version of the module.

Latest version: Display the version of the import upgrade package which can be used for upgrade.

Upgrade status: Options are **Upgraded successfully**, **Failed to upgrade**, and **Not upgraded**.

Operation: Options are **Upgrade** and **Delete**.

Note: This version cannot be upgraded.

Upgrade management System upgrade Storage and maintenance

Import

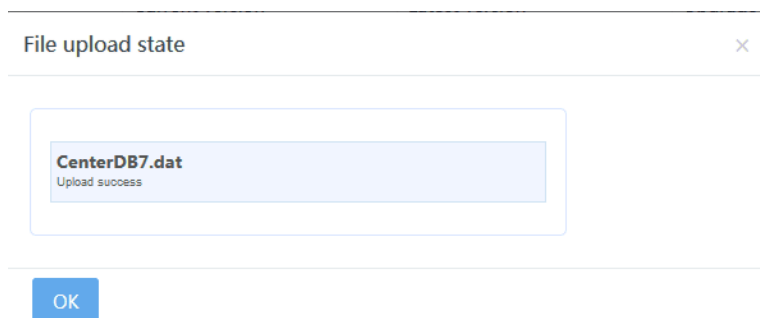
Upgrade module	Current version	Latest version	Upgrade state	Operation
Event library	2018-12-04	No available version	Not upgraded	⌵ 🗑
Feature detection module	N/A	No available version	Not upgraded	⌵ 🗑
AV library	N/A	No available version	Not upgraded	⌵ 🗑

Showing 1 to 3 of 3 entries



The version of each module of different engines may be different, so the current version (N/A) of the malicious sample library, URL credibility library, threat intelligence library, feature detection module, and virus library is not displayed on the upgrade management page. Only the current version of the event library and control center of this engine is displayed.

Click **[Import]** to import the upgrade file.



After the upgrade package is imported, the **[Upgrade]** button in the operation column is highlighted and you can click it for upgrade.



This version is earlier than or equal to the current version. continue?

Cancel OK

You can click **[Delete]** in the operation column to delete the imported upgrade package.



Are you sure you want to delete the latest version?



Cancel

OK



To upgrade other modules, you need to select the corresponding engine and upgrade these modules after the upgrade package is imported.

Select an engine. ×

<input type="checkbox"/>	Engine name	IP address
<input type="checkbox"/>	 Local Control Center	192.168.11.179
<input type="checkbox"/>	 13_8	192.168.13.8

OK

7.2.2 System upgrade

The system upgrade module is used to upgrade the whole system. After you choose **System management > System maintenance > System upgrade**, the current system version is displayed in the version number field.

*FTP server IP :

*FTP server port :

*User name :

*Password :

*Upgrade package path :

Version number:0700R0402B20180129

Parameter description:

FTP server IP: Enter the IP address of the FTP server where the upgrade package is stored.

FTP server port: Enter the FTP server port number.

User name: Enter the user name of the FTP server having the right to download the upgrade package.

Password: Enter the password corresponding to the user name.

Upgrade package path: Enter the storage path of the upgrade package on the FTP server.

After building the FTP server, placing the system upgrade file in the specified path, and filling in the above information correctly, click [**Submit**]. It takes a certain period of time to upgrade the system. After the system is upgraded, the system can be logged in at the Web side.

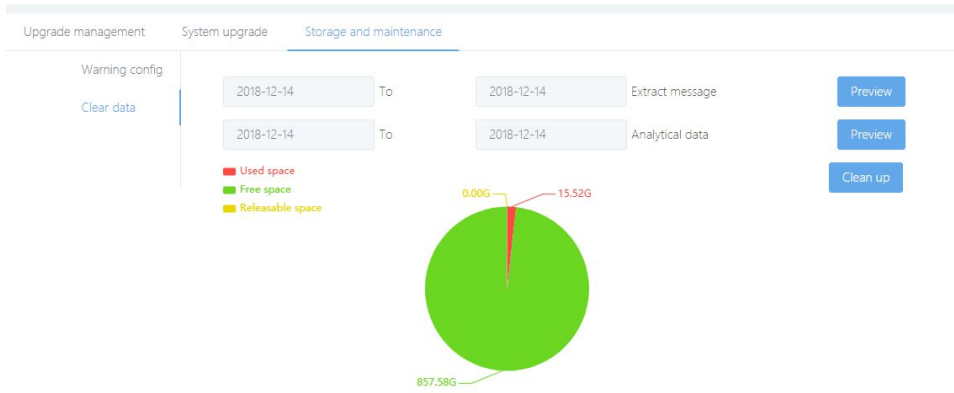
7.2.3 Storage and maintenance

The storage and maintenance graph displays the current hard disk usage. You can set an alarm threshold. When this threshold is exceeded, an alarm is triggered for you to timely know the disk usage, clear the alarm conditions, and ensure normal use of the system.

Data clearing preview:

The pie chart displays the disk usage visually. The clearing module can be used to clear the original packets or the analysis data.

Choose **System management > System maintenance > Storage and maintenance**. By default, the disk space occupied by original packets and analysis data that can be cleared is displayed. Click the time control, select the start time, and click **[Preview]** to view the data that can be cleared in the specified time scope.



Click **[Clear]** and then click **[OK]** on the page displayed. You can clear the original packets and analysis data generated in the specified period of time.



Are you sure you want to clean up the disk now?

Cancel

OK



By default, the current day is used. Pay attention to the time scope when clearing the data. Do not delete recent data.

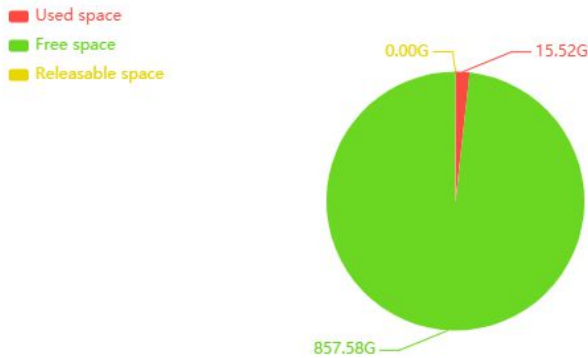
Before deleting logs, you need to back up relevant data, for example, logs and the data execution reports generated during the export period.

After **[Clear]** is clicked, both the original packets and the analysis data in the specified period of time are deleted. Confirm the time

scope entered before clicking **[Clear]**.

Disk usage:

The disk usage pie chart displays the system's current disk storage information, including three modules: used space, free space, and releasable space.



Warning config: Three alarm modes can be configured for the alarm module. When any of the free disk space, memory usage, and CPU usage exceeds the threshold, an alarm is triggered for you to timely know the disk and system usage and clear the alarm conditions.

<input checked="" type="checkbox"/> Local warning	<input type="checkbox"/> Email warning	<input type="checkbox"/> Syslog warning
Remaining free space:	<input type="text" value="860"/>	G Start warning
Memory usage exceeds:	<input type="text" value="75"/>	% Start warning
CPU usage exceeds:	<input type="text" value="75"/>	% Start warning

Local warning: The alarm message is pushed on the Web page and can be viewed in the important messages. The alarm interval is 5 minutes.

Email warning: The alarm message is sent by email. Make sure that the email configuration is correct. The free disk space alarm interval is 12 hours, while the memory and CPU usage alarm interval is 5 minutes.

Syslog warning: The alarm message is generated as a Syslog log. Make sure that the Syslog configuration is correct. The free disk space alarm interval is 12 hours, while the memory and CPU usage alarm interval is 5 minutes.

7.3 General config

7.3.1 Time config

Time synchronization:

The time configuration module is mainly used to configure the system time, as shown in the following figure:

Time config Proxy config Attention degree config

Time synchronization

Timeout

System time: Thursday 2018-12-27 19:54:03 Refresh

Time config:

NTP server synchronize

Server: pool.ntp.org(85.199.214.100) Add

Synchronize

You can use this module to manually set the system time. Click the display box next to **Time config**. The manual time setting window is displayed. You can also synchronize the system time with that of the NTP server. Select **NTP server** synchronize to perform network timing. Select any server from the server drop-down menu and click **[Synchronize]**. The time configuration is made successfully.

Time config Proxy config Attention degree config

Time synchronization

Timeout

System time: Thursday 2018-12-27 19:54:41 Refresh

Time config:

NTP server synchronize

Server: pool.ntp.org(85.199.214.100) Add

Synchronize

Click **[Submit]**. The added server address and name are displayed in the list.

Click **[Back]** at the upper-right corner of the page to return to the time synchronization

page. After **NTP server synchronize** is selected, the custom NTP server is displayed in the server drop-down list. You can select to synchronize the system time with that of the NTP server.

The screenshot shows the 'Time config' section of a web interface. It has three tabs: 'Time config', 'Proxy config', and 'Attention degree config'. Under 'Time config', there are two sub-sections: 'Time synchronization' and 'Timeout'. In the 'Time synchronization' section, there are three radio buttons: 'System time' (selected), 'Time config', and 'NTP server synchronize'. The 'System time' field shows 'Thursday 2018-12-27 19:55:07' with a 'Refresh' button. The 'NTP server synchronize' section has a 'Server:' label and a dropdown menu. The dropdown menu is open, showing a list of servers: 'pool.ntp.org(85.199.214.100)' (highlighted), 'time.nuri.net(211.115.194.21)', and 'clock.via.net(209.81.9.7)'. There is an 'Add' button next to the dropdown.

Timeout:

This module is used to set the page timeout period. The default timeout period is 30 minutes. When no operation is performed within this period, the system is automatically exited.

The screenshot shows the 'Timeout' configuration page. It has two sub-sections: 'Time synchronization' and 'Timeout'. The 'Timeout' section has a 'Page timeout period:' label and a text input field containing '30'. To the right of the input field is the label 'Minute'. Below the input field is a note: 'Note: The timeout period must be less than 999999. 0 indicates that it never times out.' There is a 'Submit' button below the note.

The timeout period must be less than 999999 minutes. 0 indicates that it never times out.

7.3.2 Proxy config

The proxy server is mainly used to send emails. On the proxy configuration page, a list of built proxy servers is displayed and information of each proxy server is displayed, for example, the proxy name, proxy type, server address and port, and operation.

On the proxy configuration page, click **[New]** to go to the new proxy server configuration page.

Add proxy configuration×

*Proxy name :

*Proxy type :

*Server IP :

*Port :

User name :

Password :

Parameter description:

Proxy name: Enter the name of the proxy server to be added.

Proxy type: Socks.

Server IP: Enter the IP address of the proxy server to be added.

Port: Enter the corresponding port number.

User name: Enter the user name of the proxy server.

Password: Enter the password of the server.

After filling in above information, click [**Submit**]. A new proxy server is created. Click [**X**] to cancel creating the proxy server.

You can also click [**Configure**] on the email configuration page to enter the proxy configuration page and configure the proxy server.



Only Socks-type proxy server can be configured on the email configuration page.

7.3.3 Attention degree config

This module is used to configure events needing attention, mainly Top 5 security events

of the home.

It can configure and display statistics on smart analysis, events needing attention, and events not needing attention, and statistics on Top 5 security events. The following is an attention degree configuration page:


Time config Proxy config Attention degree config

Attention type	Event count	Edit
Intelligent analysis	5416	
No attention	0	
Attention	853	

[Submit](#)

After editing the configuration, click **[Submit]** to make the configuration take effect.

Information ×

 Configured successfully.

[Close](#)

Edit Intelligent analysis:

Click **[Edit]** in the line of **Intelligent analysis** below **Attention type** to go to the followed event editing page. If a great number of events are followed, a waiting page is displayed.

Open the followed event editing page.

Grouping method Protocol type Name [Query](#) Total 5416 Entries

Event name	<input type="radio"/> Attention	<input type="radio"/> Not attention	<input checked="" type="radio"/> Smart analysis
▶ ARP(2)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ AUTH(2)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ DNS(33)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ FINGER(2)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ FTP(74)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ HTTP(3366)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ ICMP(3)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ IGMP(1)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ IMAP(9)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ IP(4)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ IRC(1)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ MSRPC(5)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ NETBIOS-SSN(24)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ NNTP(5)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
▶ POP3(2)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

[Submit](#)

Edit the attention type of each event and click [**Submit**]. After the configuration is saved, the page returns to the attention degree configuration page:

Edit events not attention:

Click [**Edit**] in the line of an event not needing attention to go to the event not needing attention editing page. If a great number of events are followed, a waiting page is displayed.

The screenshot shows a web interface with a search bar and a table of network events. The table has columns for 'Event name', 'Attention', 'Not attention', and 'Smart analysis'. The 'Attention' column has radio buttons, and the 'Not attention' column has radio buttons. The 'Smart analysis' column has radio buttons. The table lists various protocols and their counts, such as ARP(2), AUTH(2), DNS(33), FINGER(21), FTP(74), HTTP(3366), ICMP(31), IGMP(1), IMAP(9), IP(4), IRC(1), MSRPC(5), NETBIOS-SSN(24), NNTP(5), and PMAP(2). A 'Submit' button is visible at the bottom right of the table.

Event name	Attention	Not attention	Smart analysis
▶ ARP(2)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ AUTH(2)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ DNS(33)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ FINGER(21)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ FTP(74)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ HTTP(3366)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ ICMP(31)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ IGMP(1)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ IMAP(9)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ IP(4)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ IRC(1)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ MSRPC(5)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ NETBIOS-SSN(24)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ NNTP(5)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ PMAP(2)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Edit the attention type of each event and click [**Submit**]. After the configuration is saved, the page returns to the attention degree configuration page:

Edit events attention:

Click [**Edit**] in the line of an event needing attention to go to the event not needing attention editing page. If a great number of events are followed, a waiting page is displayed.

The screenshot shows a web interface with a search bar and a table of network events. The table has columns for 'Event name', 'Attention', 'Not attention', and 'Smart analysis'. The 'Attention' column has radio buttons, and the 'Not attention' column has radio buttons. The 'Smart analysis' column has radio buttons. The table lists various protocols and their counts, such as ARP(2), AUTH(2), DNS(33), FINGER(21), FTP(74), HTTP(3366), ICMP(31), IGMP(1), IMAP(9), IP(4), IRC(1), MSRPC(5), NETBIOS-SSN(24), NNTP(5), and PMAP(2). A 'Submit' button is visible at the bottom right of the table.

Event name	Attention	Not attention	Smart analysis
▶ ARP(2)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ AUTH(2)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ DNS(33)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ FINGER(21)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ FTP(74)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ HTTP(3366)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ ICMP(31)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ IGMP(1)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ IMAP(9)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ IP(4)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ IRC(1)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ MSRPC(5)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ NETBIOS-SSN(24)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ NNTP(5)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ PMAP(2)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Edit the attention type of each event and click [**Submit**]. After the configuration is saved, the page returns to the attention degree configuration page:

7.4 Running log

7.4.1 Running log

This module records the system running log and displays the SN, time, and content.

SN	Time	Content
1	2018-12-13 19:55:19	Connect to 188(192.168.58.142) failed, because it has been occupied.
2	2018-12-13 19:54:44	Establish connection with 1881(192.168.58.188).
3	2018-12-13 19:54:37	Connect to 188(192.168.58.142) failed, because it has been occupied.
4	2018-12-13 19:52:01	Connect to 188(192.168.58.142) failed, because it has been occupied.
5	2018-12-13 19:50:38	Establish connection with 1881(192.168.58.188).
6	2018-12-13 19:50:37	Add 1881(192.168.58.188) successfully.
7	2018-12-13 19:50:11	Connect to 188(192.168.58.142) failed, because it has been occupied.
8	2018-12-13 19:49:43	Connect to 188(192.168.58.142) failed, because it has been occupied.
9	2018-12-13 19:49:05	Connect to 188(192.168.58.142) failed, because it has been occupied.
10	2018-12-13 19:48:43	Connect to 188(192.168.58.142) failed, because it has been occupied.

Showing 1 to 10 of 25 entries Show 10 entries

You can query the running logs by content, start time or end time.

Content:	<input type="text"/>	Start time:	<input type="text"/>	End time:	<input type="text"/>	<input type="button" value="Query"/>
----------	----------------------	-------------	----------------------	-----------	----------------------	--------------------------------------

You can export the running logs to an Excel file for view and saving.



When the report list is exported to an .xls file, the confirmation dialog box may not be displayed due to the machine environment. Instead, IE directly calls the installed Excel software to open the file to be downloaded. In this case, you can only return to the report file list page through IE's back function.

8 User management

The system divides users accessing the system through the browser into user administrator, configuration administrator, and auditor based on their roles.

The user administrator and auditor are inherent system roles. Each role has a preset user and cannot be deleted or modified except the password. The configuration administrator role can have multiple users. The user administrator can add, delete, and modify the configuration administrator information or lock/unlock other users.

The user administrator is an inherent system user. The default user name is **admin**, which cannot be modified. The initial password is **Raven.private**. The user administrator can change its password by using the change password function on the toolbar.

After logging in to the system, the user administrator can view the user management page and add, delete, modify, or lock the information of the configuration administrator, set the consecutive login time and times, and lock and unlock the IP address.

The auditor is an inherent system user. The default user name is **audit**, which cannot be modified. The initial password is **Raven.audit**. The auditor can change its password by using the change password function on the toolbar.

After logging in to the system, the auditor can view the audit log page. The audit log records operation logs of all users after they log in to the system. The auditor can query, delete, import, and export these operation logs.

The configuration administrator is a role for executing main system services. All system services except user management and audit logs are completed by the configuration administrator. The configuration administrator is added by the user administrator, and its initial password is set by the user administrator. After logging in to the system, the configuration administrator can change its password by using the change password function on the toolbar.

8.1 User list

The user administrator can log in to the system as an **admin** user. After login, the user

administrator can view the configuration administrator user list. The system presets a configuration administrator user named **adm** and the password is **Raven.public**. The user administrator can create, edit, delete, and lock the configuration administrator.

User list Security config Unlock IP address Unlock user

[+ New user](#)

Online state	Login ID	Locking state	Role	Update time	User type	Operation
	admin		User Administrator	2013-06-03 14:13:35	Local user	
	audit		Audit Administrator	2013-06-03 15:08:08	Local user	
	adm		Configuration Administrator	2013-10-10 17:01:40	Local user	
	lzn		Configuration Administrator	2018-12-14 09:37:16	Local user	

Showing 1 to 5 of 5 entries Show entries

8.1.1 New user

Click **[New user]** to create a local user. When you create a new user, the **Login ID**, **Password**, and **Enter the password again** fields must be filled in. The user name consists of letters or numbers, not exceeding 20 characters. The password must be set according to the strength prompt.

The local user creation page is as follows. The **Login ID**, **Password**, and **Enter the password again**, and **Allowed IP address** fields must be filled in. Other items are optional. The user type is local user.

New user
✕

*Login ID:

*Password:

*Enter the password again:

Role:

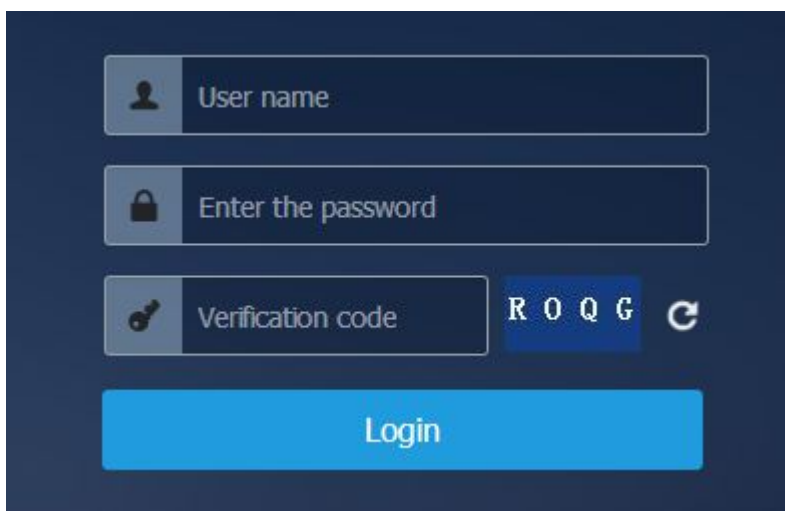
Allowed IP address:

Tel:

E-MAIL:

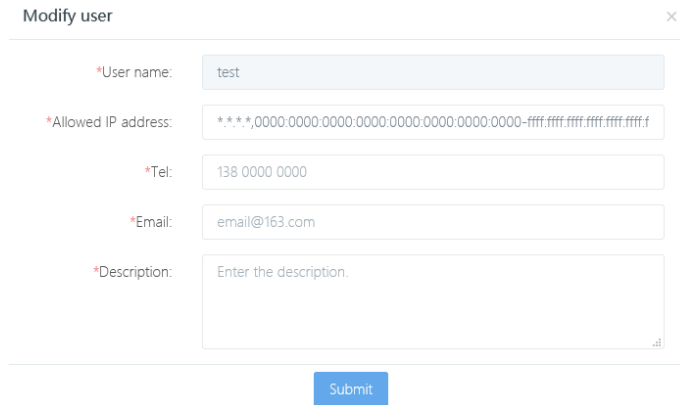
Remarks:

By default, all the IP addresses can access the system through the Web page, that is, "*.*.*,0000:0000:0000:0000:0000:0000:0000:0000-ffff.ffff.ffff.ffff.ffff.ffff". If the IP address "192.168.13.27" is entered, only this IP address can access the control center. When other IP addresses are used, the message "The login IP address is now within the allowed login IP address range. Please contact the administrator" is displayed.



8.1.2 Edit a user

Click **[Edit]** in the line of a user to modify the user configuration. Same to the user creation page, on the user modification page, the login ID cannot be modified. The user password can be reset by the password reset function. Only the contact phone number, email address, description, and other basic information can be modified.



8.1.3 Delete a user

Click **[Delete]** in the line of a user and then click **[OK]**. The user is deleted.

Are you sure you want to delete this user?

Cancel

OK



The user administrator and audit administrator cannot be deleted.

8.1.4 Lock and unlock a user

Click **[Lock]** in the line of a user and then click **[OK]**. After the user is locked, when the user's login ID is used for login, the following error message is displayed.

The image shows a login interface on a dark blue background. It contains three input fields: 'User name' with a person icon, 'Enter the password' with a lock icon, and 'Verification code' with a key icon. The verification code field contains the text 'R O Q G' and a refresh icon. Below these fields is a large blue button labeled 'Login'.

Click [**Unlock**] in the line of a user and then click [**OK**]. The user is unlocked.

Are you sure you want to unlock this user?

A confirmation dialog box with two buttons: a red 'Cancel' button and a green 'OK' button.

8.1.5 Authorization

Click [**Authorization**] in the line of a user. On the user authorization page displayed, authorize a role for the user.

The image shows a 'User authorization' dialog box with a close button (X) in the top right corner. It contains two fields: '*User name:' with the value 'lzn' and '*Role:' with a dropdown menu showing 'Configuration Administrator'. A blue 'Submit' button is located at the bottom center.

8.1.6 Security configuration

This module is mainly used to configure the maximum number of online users, password strength, password security, and login attempt.

The maximum number of online users ranges from 20 to 100. The default value is 20. When the number of online users exceeds 20, login is refused.

By default, the password consists of letters and numbers, with a length of 6 to 20 characters. Assume that the password is changed as follows:

Password strength

- Letters (A-Z or a-z) included
- The password can contain uppercase and lowercase letters (A-Z and a-z)
- Digits (0-9) included
- Special characters (such as !, \$, # and %) included

Password length: ~

In this case, the password strength does not meet the requirement of the user login control center and a password modification page is displayed. The title of the page indicates the current password strength requirement. You are asked to set a new password according to the password strength requirement. After a new password is set, the system is automatically accessed.

Change password

The current password does not conform to the password strength requirement and needs to be reamended. Automatically jump to the front page after the modification is successful.
Current password strength requirement :

required Password,length 6-20 place,need containUppercase letters, Lowercase letters, Numbers

*Login ID :

*Initial password :

*New password :

*Enter the password again. :

If **Enable password change upon initial login** is selected, when you log in to the system for the first time, the login password modification dialog box is displayed, asking you to modify the password to ensure your password security.

Password security

Enable password change upon initial login

Enable password expiration prompt

Password expiration date: (1-180Day)

Solution for password expiration : Warning Force to modify the password

Change password

The current password does not conform to the password strength requirement and needs to be reamended. Automatically jump to the front page after the modification is successful.
Current password strength requirement :

required Password,length 6-20 place,need containUppercase letters, Lowercase letters, Numbers

* Login ID :

* Initial password :

* New password :

* Enter the password again. :

When your password expires, an alarm is triggered or you are forced to modify the password.

8.1.7 Lock and unlock configuration

The user administrator "**admin**" can set the IP address locking time, the number of consecutive login attempts of the same IP address, user locking time, and the number of consecutive login attempts of the same user, and can unlock the locked IP address or user.

The user administrator can set the number of consecutive login attempts of the same user to an integer from 2 to 5 and set the user locking time to an integer from 1 to 30 and then click [**Submit**]. The locking time and times are set.

Try login

Number of login attempts with the same IP address: (2-5)

IP address lock time: (1-30Minute)

Number of login attempts with the same account: (2-5)

Account lock time: (1-30Minute)

The user can set the number of consecutive login attempts of the same user to an integer from 2 to 5 and set the user locking time to an integer from 1 to 30 and then click **[Submit]**. The locking time and times are set.

Try login

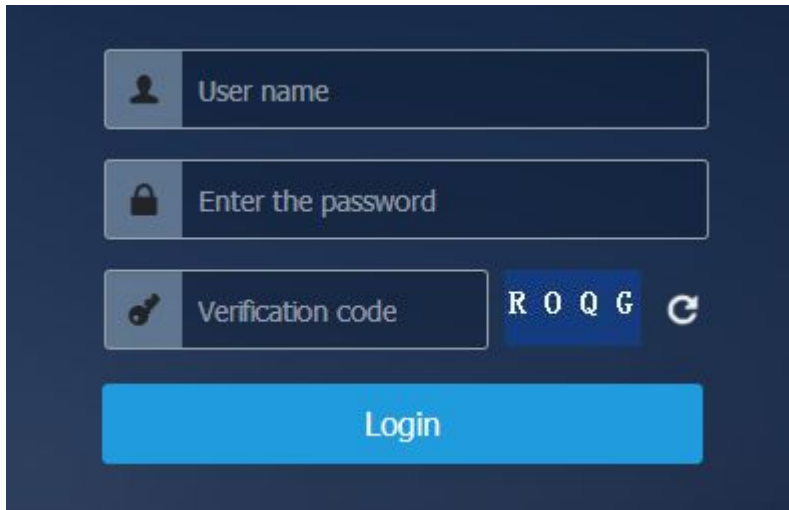
Number of login attempts with the same IP address: (2-5)

IP address lock time: (1-30Minute)

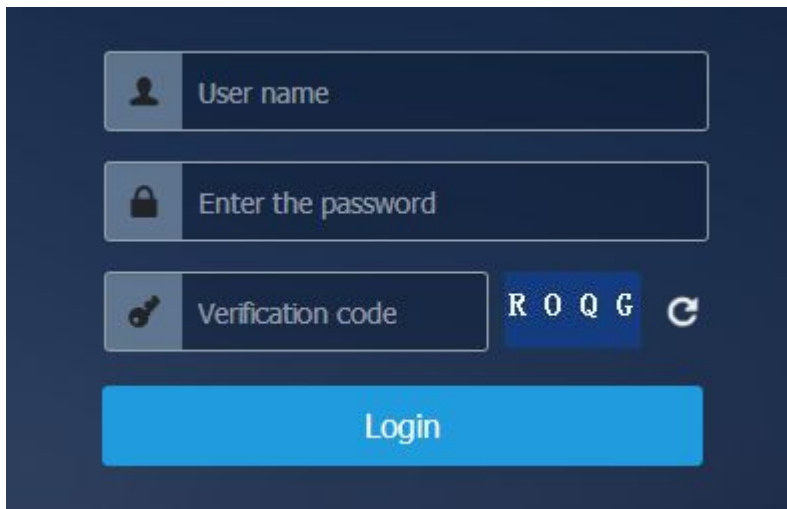
Number of login attempts with the same account: (2-5)


Account lock time: (1-30Minute)


When the number of consecutive login attempts of the same user exceeds the preset value, the following error message is displayed.




When the number of consecutive login attempts of the same IP address exceeds the preset value, the following error message is displayed.



To unlock an IP address, click the  icon in the line of the IP address and click **[OK]**.

SN	IP address	Lock time	Operation
1	192.168.58.135	2018-12-14 10:30:45	

Showing 1 to 1 of 1 entries

To unlock a user, click the  icon in the line of the IP address and click **[OK]**.

SN	User name	Lock time	Operation
1	lzn	2018-12-14 10:33:55	

Showing 1 to 1 of 1 entries



When the number of locking times of the same user is same to that of the same IP address, the user is locked.

8.2 Role list

The user administrator "**admin**" can create, edit, delete, and authorize a role.

Role list

[+ Add role](#)

Online state	Role name	User count	Creation time	Update time	Operation
	User Administrator	1			
	Audit Administrator	1			
	Configuration Administrator	4			

Showing 1 to 3 of 3 entries Show entries

8.2.1 New role

Click **[Add role]** to add a role.

Add role
✕

*Role name:

Description :

8.2.2 Edit a role

Click **[Edit]** to modify the role information.

Modify role ×

*Role name:

Description:

8.2.3 Delete a role

Click **[Delete]** to delete a role. The default user administrator and audit administrator roles cannot be deleted.

Are you sure you want to delete this role?



8.2.4 Authorization

Click **[Authorization]** to authorize a role. As shown in the following figure, only the function modules authorized to a role are displayed in the user login control center of this role. Other modules are shielded.

Role list

Role name	Operation
User Administrator	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Audit Administrator	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Configuration Administrator	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
free	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Showing 1 to 4 of 4 entries Show entries

ROLE AUTHORIZATION

- Home
- Known detection
 - Feature detection
 - File detection
- Flow statistics
 - Macro flow
 - Micro flow
- Statistical analysis
 - Statistical report
- Detection config
 - Feature detection
 - Asset config
 - Device management
 - File detection config
 - Virus detection config
- System management
 - Response method
 - System maintenance
 - General config
 - Running log

8.3 Audit log

The audit log records the user's key operations, and only the auditor role can view the audit log.

SN	Operation time	Operator	Operation	Content	UserIP	Result
1	2018-12-14 10:39:38	audit	User system login	User system login success	192.168.58.135	Success
2	2018-12-14 10:39:30	admin	User logout out	User logout out success	192.168.58.135	Success
3	2018-12-14 10:38:21	admin	Role Management	User admin add role fre...	192.168.58.135	Success
4	2018-12-14 10:38:12	admin	User system login	User system login success	192.168.58.135	Success
5	2018-12-14 10:33:28	admin	Update security configu...	Update security configu...	192.168.58.135	Success
6	2018-12-14 10:31:12	admin	Update security configu...	Update security configu...	192.168.58.135	Success
7	2018-12-14 10:30:30	admin	Update security configu...	Update security configu...	192.168.58.135	Success
8	2018-12-14 10:30:24	admin	User system login	User system login success	192.168.58.135	Success
9	2018-12-14 10:26:47	lzn	User logout out	User logout out success	192.168.58.135	Success
10	2018-12-14 10:24:53	admin	Update security configu...	Update security configu...	192.168.58.135	Success

Showing 1 to 10 of 91 entries Show 10 entries

8.3.1 Query the audit log

You can filter and query audit logs by operator, content, user IP address, and logging time (all, one day, one week, one month, and custom).

SN	Operation time	Operator	Operation	Content	UserIP	Result
1	2018-12-14 10:18:23	adm	User logout out	User logout out success	192.168.58.135	Success
2	2018-12-14 10:18:17	adm	User system login	User system login success	192.168.58.135	Success
3	2018-12-14 10:04:21	adm	Export running log	Export running log succ...	192.168.58.135	Success
4	2018-12-14 10:04:14	adm	Export running log	Export running log succ...	192.168.58.135	Success
5	2018-12-14 10:04:02	adm	User system login	User system login success	192.168.58.135	Success
6	2018-12-14 10:01:55	adm	User system login	User system login success	192.168.58.155	Success
7	2018-12-14 09:51:58	adm	User system login	User system login success	192.168.58.162	Success
8	2018-12-14 09:45:08	adm	User system login	User system login success	192.168.58.228	Success
9	2018-12-14 09:30:10	adm	User system login	User system login success	192.168.58.135	Success
10	2018-12-14 09:23:23	adm	Add recipients	Add recipients success	192.168.58.135	Success

Showing 1 to 10 of 48 entries Show 10 entries

8.3.2 Export the audit log

You can click **[Export]** export the audit log to an .xls file to view the log in Excel.



When the report list is exported to an .xls file, the confirmation dialog box may not be displayed due to the machine environment. Instead, IE directly calls the installed Excel software to open the file to be downloaded. In this case, you can only return to the

report file list page through IE's back function.

8.3.3 Clear the audit log

Click **[Clear]**. All the audit logs are deleted.



All the logs found out will be deleted. Are you sure you want to delete them?

Cancel

OK

Click **[OK]**. All the audit logs found are deleted.

8.3.4 Change IE's settings for opening the downloaded files directly

To open the downloaded files directly through IE,

choose **My computer > Menu > Tools > Folder options**, click **File type**, select the file type that needs to be changed from the registered file types, such as XLS, click **Advanced**, and select **Open it after download** without selecting **Browse in the same window**, and click **OK**. Restart IE to check whether a confirmation dialog box is displayed.

8.3.5 Page up and down

By default, 10 logs are displayed on each page. The total number of pages is displayed. You can click the paging button to view logs on each page. You can click the relevant arrow to page up and down or jump to the first or end page.

Showing 1 to 10 of 48 entries Show entries

You can dynamically set the number of records displayed on each page.

Show 10 ▼ entries

- 10
- 25
- 50
- 100

Annex Engine configuration

Connect the device with the PC based on Windows system by a console line, then start the "super terminal" on the PC, and set the baud rate 9600 to enter the serial port of the device.

The engine uses the super terminal to make basic settings. After configuring the super terminal, press **Enter**. The engine startup page is displayed, as shown in the following figure:

Username:

Enter the user name **adm**, press **Enter**, and then enter the correct password (default password: **Raven.public**). The following page is displayed:

```
Username: adm
Password:
IDS> en
```

Basic functions and commands

Configuration options:

[Function 1]: Display the current settings

Display the current configuration, including the product ID, device SN, IP address of the communication network port, subnet mask, routing configuration, and other information. In the IDS> mode, you can run the **enable** command to enter the IDS# mode. In the IDS# mode, you can run the **configure terminal** command to enter the IDS(config)#.

In the IDS=# mode, run the **show config** command.


```
IDS# show config
*****
Current product_info.id is NULL
Current Serial: 0013351412129999

eth0 : Communicate 192.168.11.192/255.255.255.0

SLOT 0
ge0/0: Unused
ge0/1: Unused
ge0/2: Unused
ge0/3: Unused
ge0/4: Unused

Current VCECOMM PORT: 20001
Current Route:
Gateway[1]: <0.0.0.0/0.0.0.0> <192.168.11.1>
allow access: ping telnet ssh
*****
```

[Function 2]: Change the IP address/subnet mask

Change the IP address/subnet mask of the communication network port. Apply the engine IP address/subnet mask from the network administrator.

To change the IP address/subnet mask, run the **ip address** command in the IDS (config)# mode.

For example, to change the IP address to 192.168.11.182 and use a 24-bite mask, run the following command:

```
IDS(config)# ip address 192.168.1.123/24
```

[Function 3]: Reset the engine authentication key

You can reset the authentication keys of the control center and engine. When the engine is connected to another control center other than the original control center, its key must be reset.

In the IDS(config)# mode, run the **reset vcecomm key** command, as shown in the following figure:

```
IDS# configure terminal
IDS(config)# reset vcecomm key
Key will be reset
Agree?
  (1)==yes
  (2)==no
->1
Key has been reset
IDS(config)#
```

[Function 4]: Change the routing configuration

You can add and change the original routing configuration.

In the IDS(config)# mode, run the **route add | del** command.

For example:

To add a route

Enter the IP address of the gateway. The IP address must be in the same network segment of the network port for which the route is to be set.

IDS(config)#route add 0.0.0.0/0 192.168.11.1

```
IDS(config)# route add 0.0.0.0/0 192.168.11.1
```

To delete a route, run: **IDS(config)# route del.**

For example: Delete the route added in the previous step.

```
IDS(config)# route del
*****
Gateway[1]: <0.0.0.0/0.0.0.0> <192.168.11.1>
*****
chose the one you want to delete:
->1
:0.0.0.0/0.0.0.0> <192.168.11.1>
(1)=
(2)=
->1
```

[Function 5]: Change the serial port login password

You can change the network engine password. The network engine password consists of at least six any numbers or characters. If the new password contains less than six characters, the error message "Password of user is too short, should longer than or equal to 6!" is returned.

Note:

(1) The default password for all the new engines is **Raven.public**. You need to change this password later.

(2) The password should not be too simple; otherwise, it is easily stolen.

In the `IDS(config)#` mode, run the **adm-set-new-password** command to set a new password.

For example, to change the password to Raven4000, run the following command:

```
IDS(config)# adm-set-new-password Raven4000
```

[Function 6] Enable and disable SSH login

This function is used to set whether to allow login to this configuration page based on SSH. It is enabled by default.

In the `IDS(config)#` mode, run the **allow access ssh enable / disable** command. Where, **enable** indicates that this function is enabled while **disable** indicates that this function is disabled.

[Function 7] Enable and disable ping

When this function is enabled, the device management port can be pinged.

In the `IDS(config)#` mode, run the **allow access ping enable / disable** command. Where, **enable** indicates that this function is enabled while **disable** indicates that this function is disabled.

[Function 8] Enable and disable Telnet login

This function is used to set whether to allow login to this configuration page based on Telnet. It is enabled by default.

In the `IDS(config)#` mode, run the **allow access telnet enable / disable** command. Where, **enable** indicates that this function is enabled while **disable** indicates that this function is disabled.

[Function 9]: Customize the packet capturing port: Adjust the packet capturing port as required. The management port and backup management port cannot be used as the packet capturing port.

In the IDS(config)# mode, run the **set capcomm** command.

For example, to set the second port of the first board card to the packet capturing port, run the following command:

```
IDS(config)# set capcomm
Input format as:
0:0-0:1-1:0-1:1-2:0
interface 0:0,0:1,1:0,1:1,2:0 will be setted to capture:
->0:1
IDS(config)#
```

[Function 10]: Restart the engine operating system

In the IDS# mode, run the **reboot** command,

as shown in the following figure:

```
IDS# reboot
The system will be rebooted! Please enter "y/n" to confirm: y
```

[Function 11]: Ping test

The ping test is used to test whether the specified IP address has any active host. The prompt is "Connection normal" or "Connection abnormal".

In the IDS# mode, run the **ping A.B.C.D** command. **A.B.C.D** indicates an IP address.

For example, ping 192.168.11.197. When the connection is normal, the following message is displayed:

```
IDS# ping 192.168.11.114
PING 192.168.11.114 (192.168.11.114): 56 data bytes
64 bytes from 192.168.11.114: seq=0 ttl=64 time=1.039 ms
64 bytes from 192.168.11.114: seq=1 ttl=64 time=0.689 ms
64 bytes from 192.168.11.114: seq=2 ttl=64 time=0.748 ms
64 bytes from 192.168.11.114: seq=3 ttl=64 time=0.810 ms

--- 192.168.11.114 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.689/0.821/1.039 ms
```

[Function 12] Exit the serial port configuration program

This function is used to exit the serial port configuration program. If the program is not exited, you can use the serial port to directly operate on the serial port configuration without login.

In the `IDS#` mode, run the **exit** command.

Note: You cannot click the **X** button at the upper-right corner of the page to close the super terminal. When **X** is clicked, only the super terminal page is closed, the communication between the super terminal and the detection engine does not stop. Therefore, you must run the **exit** command to exit the super terminal each time you modify the basic parameters of the detection engine.

[Function 13]: Reset the password when you forget the password of the user **adm**

When you forget the login password of the user **adm**, you can log in to the system as an **admin** user and reset the password. The default user name and password of the user **admin** are **admin** and **Raven.private**.

In the `IDS(config)#` mode, run the **user administrator USER local PASSWORD priv all** command to reset the user password.

For example: Reset the password of the user **adm** to **Raven.public**.

```
|IDS(config)# user administrator adm local venus70 priv all
```

[Function 14]: View the running situation of the network port:

Log in to the system as an **adm** user, and run the **show interface** command in the `IDS#` mode. To view the package received and sent by a specific network port, run the **show interface [INTERFACE_NAME]** command.

For example: View the running situation of the network port `ge1/1`.

```
IDS# show interface ge0/1
ge0/1    Link encap:Ethernet  HWaddr 00:10:F3:6F:CE:34
         UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
         Interrupt:18 Memory: fbb00000-fbb20000
```

[Function 15]: Configure the SNMP community word:

Log in to the system as an **adm** user, and run the **snmp community** command in the IDS(config)# mode.

```
IDS(config)# snmp community public
IDS(config)#
```

Enter the IDS# mode, and run the **show snmp community** command to query the SNMP community word of the engine.

HIRSCHMANN IT

A **BELDEN** BRAND