AVCOMM EdgeCommander

User Manual

AVCOMM Technologies Inc.
333 West Loop North, Suite 460 Houston, TX 77024, USA | info@avcomm.us | www.avcomm.us

AVCOMM Technologies Inc.

EdgeCommander

User Manual

About This Manual

This user manual is intended to guide a professional installer to install and configure the EdgeCommander. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this EdgeCommander.

Disclaimer

Avcomm reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required, or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to Avcomm. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. Avcomm assumes no responsibility for its use by the third parties.

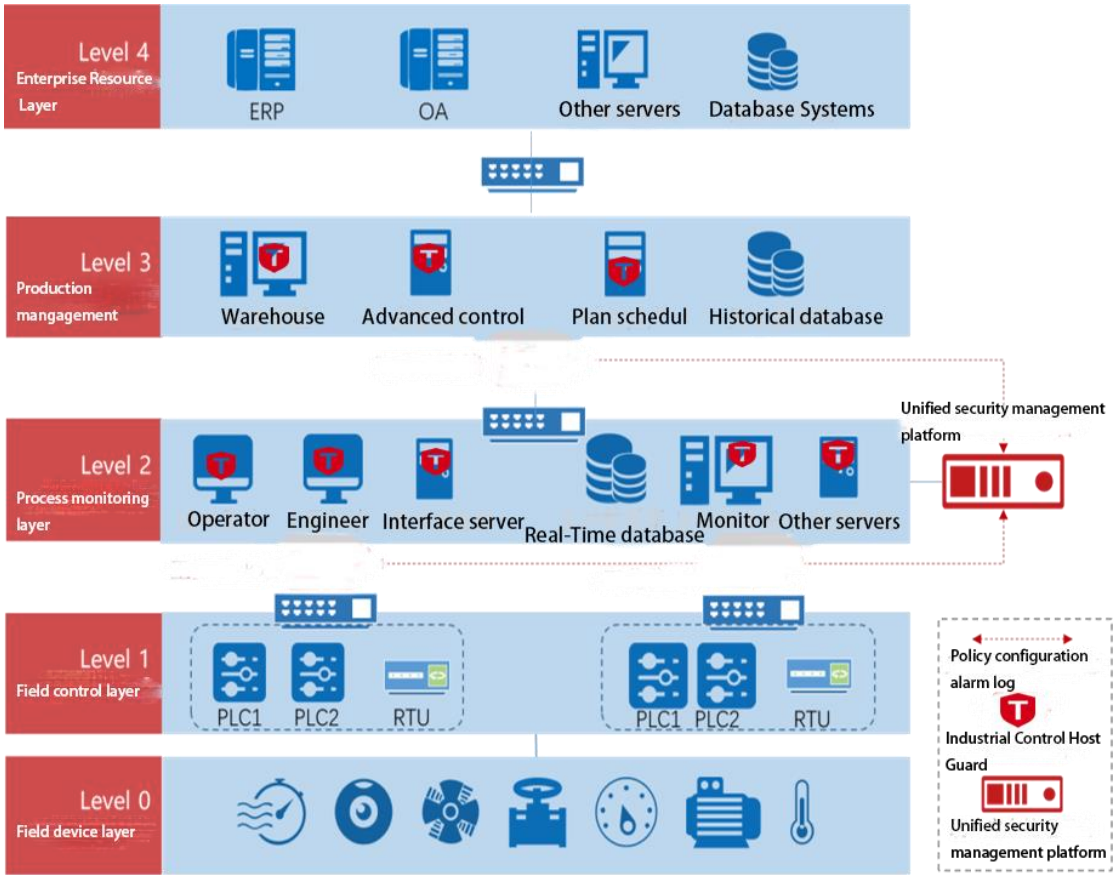
Avcomm Online Technical Services

At Avcomm, you can use the online service forms to request the support. The submitted forms are stored in server for Avcomm team member to assign tasks and monitor the status of your service. Please feel free to write to www.avcomm.us if you encounter any problems.

Contents

1. Overview of Unified Security Management

1.1. Unified Security Management Networking Diagram



1.2. Product Description

The AVCOMM unified security management platform can conduct centralized management of industrial firewalls, intelligent monitoring terminals and IEG reinforced workstations as produced by AVCOMM, able to provide Web management to the outside.

The administrator can manage AVCOMM products installed in the system via the Web management interface in a unified manner, including to:

- View the current working status of the installed industrial firewall, the intelligent monitoring terminal and the IEG.
- View the firewall policy and the whitelist policy of a deployed industrial firewall or configure the firewall policy and the whitelist policy of a new industrial firewall, view and process the generated alarm logs and the interception records on illegal messages.

- View the industrial protocol whitelist monitoring policy, the protocol violation policy, the no-traffic policy and abnormal traffic baseline configuration, etc. of a deployed intelligent monitoring terminal, or configure the industrial protocol whitelist monitoring policy, the protocol violation policy, the no-traffic policy and abnormal traffic baseline configuration, etc. of a new intelligent monitoring terminal, view and process relevant log alarms.
- View the security policy of a deployed IEG or configure the security policy of a new IEG, view and process log alarms.
- Configure system-related database backup policy, trusted host and management users.

Notably, intelligent monitoring terminals for industrial firewalls and monitoring & audit are accessed to the network interlinked with the unified security management platform through their own dedicated management network ports, and IEG reinforced workstations are accessed to the network interlinked with the management platform through existing physical connections.

Intelligent monitoring terminals for industrial firewalls and monitoring & audit and the unified security management platform have a default IP when they leave the factory, which needs to be changed to an IP address that can be used by customers in a specified way. See the following for specific change methods.

1.3. **Operating Steps**

The process flow chart for the unified security management, briefly introduces the basic operating steps for the unified security management platform to control the industrial firewall, the intelligent monitoring terminal and the IEG. See relevant sections for the specific operations (the unified security management platform is hereinafter referred to as the "Management Platform").


Change the IP address of the management platform device
Start and log in the management platform
Industrial firewall
Intelligent monitoring terminal
The host guard
Set the DEVICE IP using CLI commands
Set the DEVICE IP using CLI commands
Install the Host Guard client
Set the connection management platform IP using the CLI command
Set the connection management platform IP using the CLI command
Set the IP address of the management platform
Set to the learning mode when the device goes online
Set to the learning mode when the device goes online
Change to the alarm mode and issue the corresponding whitelist template
Change to the run mode
Change to the guard mode

1.4. About the Manual

The Manual is mainly for the Super Administrator, Administrator, and the Auditor of a customer's network security system. It introduces how to configure and manage industrial firewalls, host reinforcement, monitoring & audit, and system configuration. During configuration, online help may be available to help you to view the details. The following basic knowledge is required when reading the Manual:

- ✓ Information system management
- ✓ Common browser operations
- ✓ Basic network knowledge

If you want to be proficient in the configuration and management of industrial firewalls, host reinforcement, monitoring & audit, as well as system configuration & management, please read the Manual carefully.

1.5. How to Use the Manual

The Manual mainly give a detailed description of industrial firewalls, host reinforcement, monitoring & audit, and system configuration as much as possible.
For more information, please visit: www.avcomm.us.

1.6. Provisions of Graphical Interface Format

Formats	Meanings
<>	The angle brackets "<>" indicate button names, such as "click <Save>".
[ ]	The square brackets "[]" indicate window names, menu names and data tables, such as "popup the [Firewall Management] window".
/	Multilevel menus are separated by "/". For example, the multi-level menu [File/New/Folder] indicates the menu item [Folder] under the submenu [New] of the menu [File].

2. Log in the Unified Security Management Platform

2.1. Start the Unified Security Management Platform

The management platform starts before the devices that it controls. According to the instructions given the *Installation Manual*, after checking that the management platform hardware has been properly configured, connecting the power cord, and setting the power button of the management platform to the "ON" position, and the management platform will start. Generally, the management platform automatically completes the entire startup process. The old-version management platform (with 6 network ports) is to connect the network cable with ETH4 as default. The new-version management platform (with only 2 network ports) is to connect the network cable with Network Port 1 as default. For both old and new management platforms, 192.168.8.8 is the default IP address available (this is the default IP address of the management platform, which can be modified later voluntarily).

After the startup of the management platform, the Google Chrome can be enabled on a host that is available to the management platform online (the Google Chrome is recommended), enter https://192.168.8.8:8440/ or a website similar to the following:

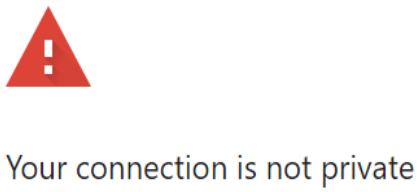
https://192.168.8.8:8440 (new version) or

http://192.168.8.8:8080 (old version)

to access to the management platform for subsequent login and configuration.

🕮 **Description:**

If the browser reports an error as shown in the following figure, simply click " Advanced " below the browser page, then select " Proceed to 192.168.4.204 (unsafe) ".

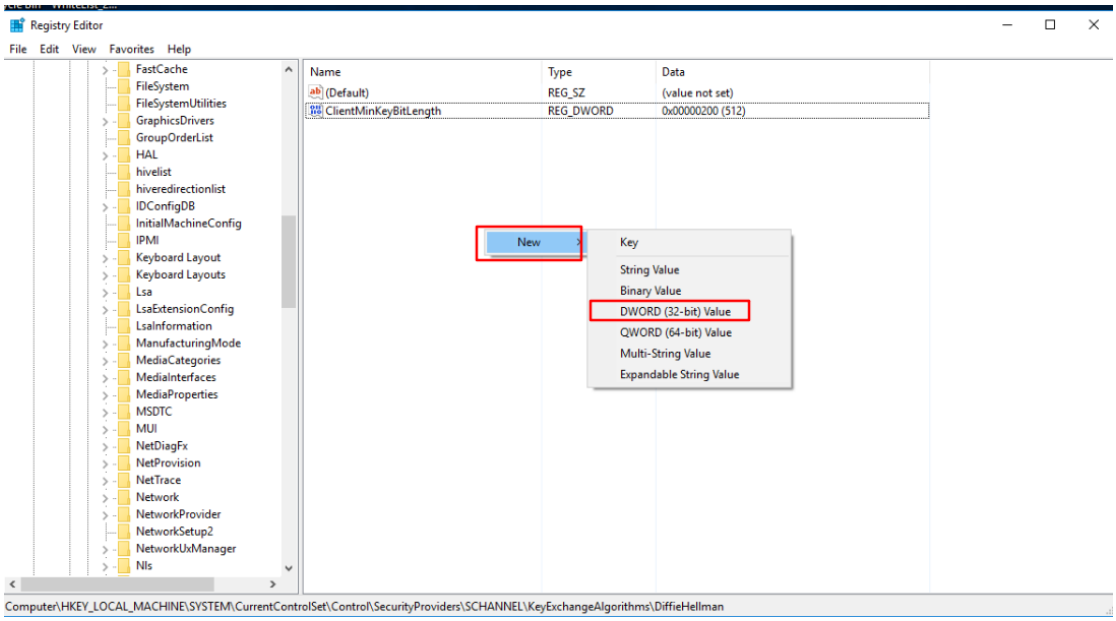


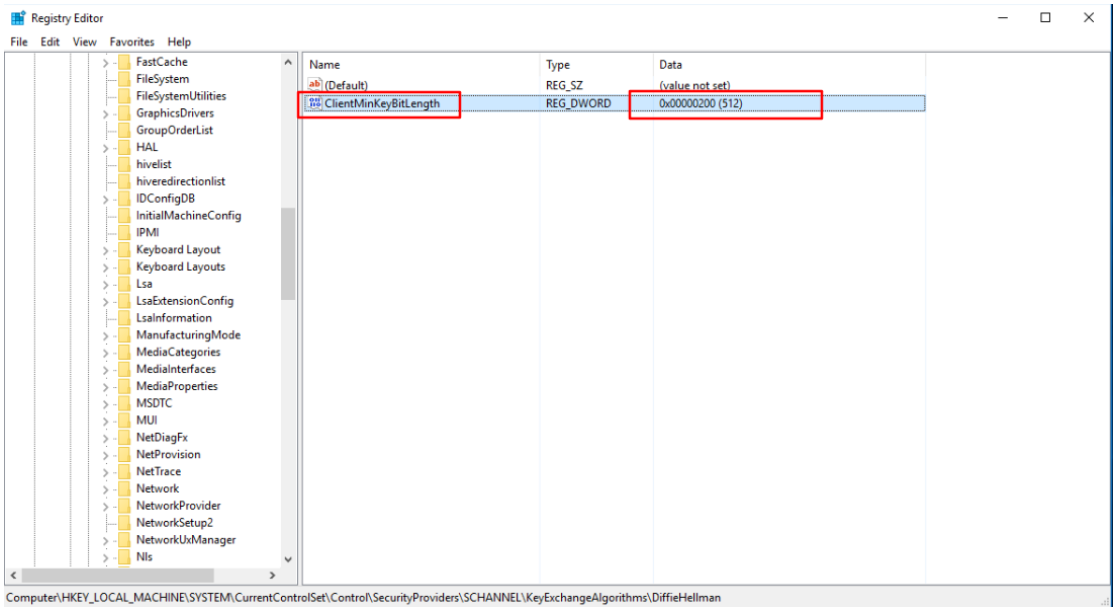
🕮 **Description:**

If the IE browser is not accessible, open the registry and find the following registry path:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

Right-click and select New, then select DWDRD (32-bit), change the name to ClientMinKeyBitLength and modify the data to 00000200.





2.2. **Log in the Management Platform**

2.2.1.**Normal Login**

After the startup of the management platform, enter the correct management page address of the management platform in the browser. After the pop-up of the login dialog box as shown in Fig.2-1, enter the correct username and password, and click <Login> to enter the configuration page of the system.

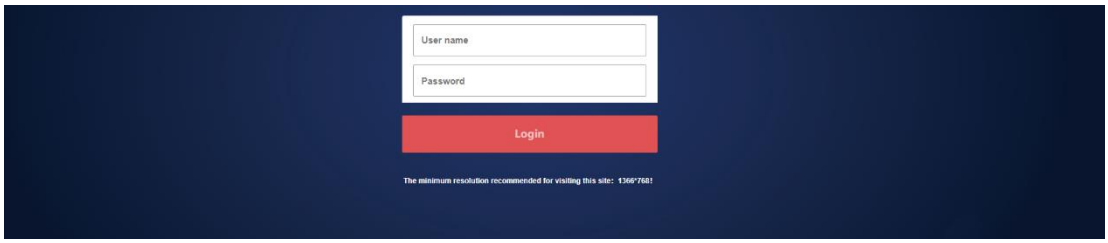


Fig.2-1 Page after the Startup of the Management Platform

Currently, the management platform supports users with three roles. If it is the first time to log in the management system, a user will be defaulted to log in as "Admin" with a default password "Admin@123". After entering the system, users with different roles will have different permissions. Users who can create other roles are system operators.

Roles included in the system are system operator, configuration administrator, and audit administrator. If custom users are configured, they can be used later for decentralized management.

2.2.2.Two-Factor Authentication Login

If the user has connected the USBKey, after the startup of the management platform, enter the correct page address of the management platform in the browser to pop up a login dialog box as shown in Figures 2-2 and 2-1.

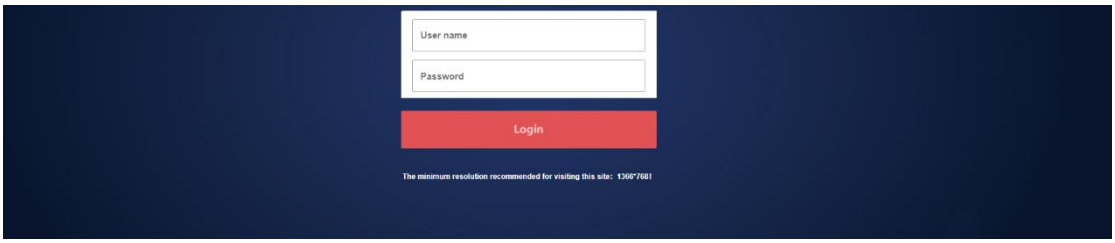


Fig.2-2 Page after the Startup of the Management Platform after Having Connected the USBKey

If the user has not connected the USBKey, please enter the correct username and password, click <Login> to enter the configuration page of the system.

If the user logged in has connected to the USBKey without installing the USBKey plug-in, please download the USBKey plug-in first and install it correctly. If the USBKey plug-in has been installed, enter the correct username and password, insert the USBKey of the user logged in, enter the correct USBKey PIN code, click <Login> to enter the configuration page of the system.

2.3. View the Management Platform Version

After logging in the management platform, click <About> to view the version information on the management platform. (As shown in Fig.2-3):

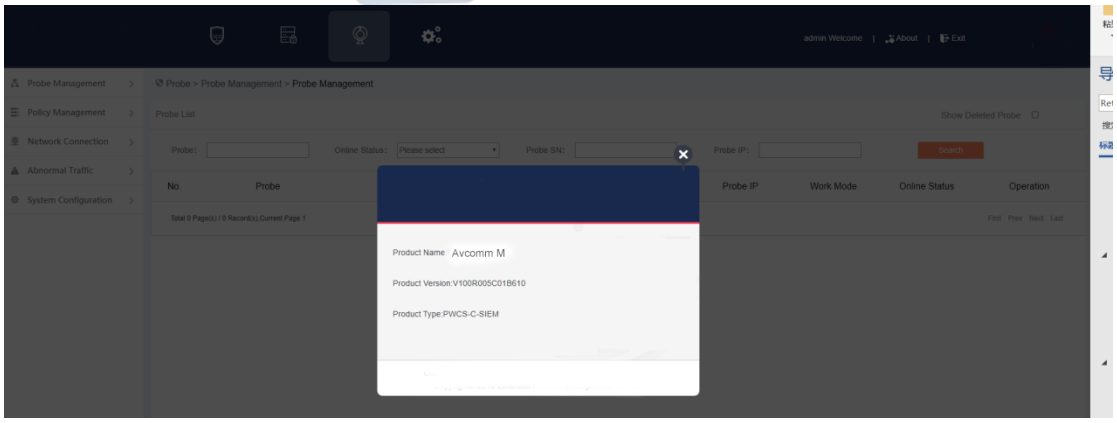


Fig.2-3 Version Information on Management Platform

2.4. Exit the Management Platform

Click <Exit> to exit the management platform (as shown in Fig.2-4):

Fig.2-4 management platform exit.

3. Industrial Firewall

3.1. Introduction to Products

3.1.1.Product Overview

The industrial firewall series independently developed by AVCOMM are collected called as industrial firewalls (also can be called as trusted gateways or gateways). The product series current has three models, namely, S2106/S2112/S2124. Both hardware and software of these products have fully independent intellectual property rights, therefore, we can resolutely put an end to the hidden dangers of the back door. The products have a variety of network access modes (supporting both electrical and optical ports), based on centralized management and decentralized deployment in view of management forms. The unified security management platform for configuration management of industrial firewalls is an integral part of a product. The platform adopts a B/S architecture. The administrator can access to the machine on the management platform at will for convenient access and management, which can greatly improve the operation & maintenance efficiency, and effectively lower the maintenance costs. The product hardware is independently designed in full line with industrial standards and can be deployed and applied to various complex industrial production environments. The hardware has been certified by

the top standards of the industry, such as CE, CC, and FCC, etc., which can work steadily for a long time, thus greatly shortening the system downtime for customers. The industrial firewall software adopts an architecture design that is autonomously controllable in full. Main function module cooperates with each other, fully resolve, judge and control all data circulating in a customer's industrial control network, effectively safeguard the transmission of regular production data, fully put an end to the dispersion and dissemination of illegal data and viruses in the customer's industrial control network, thus guaranteeing the customer's long-term and steady production to the maximum extent.

3.1.2.Appearance and Description

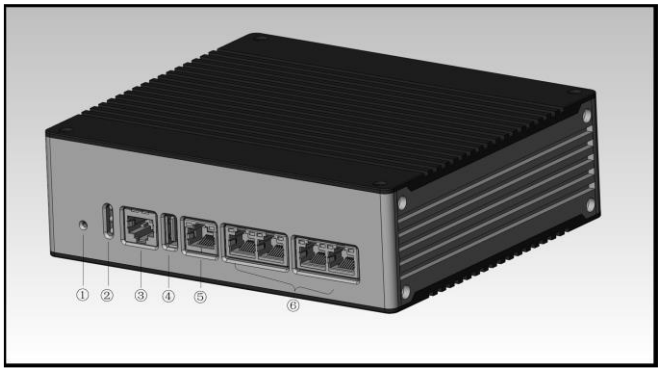


Fig.3-1 Appearance of S2100 in the Product Series

① Reset button
② LED indicator light
③ Console serial port, RS232
④ USB 2.0 interface
⑤ Management network port, 10/100/1000BASE-T adaptive Ethernet port
⑥ Service network port, 10/100/1000BASE-T adaptive Ethernet port; there are two pairs, with those connected closely as a pair. Any one of the two pairs can be used as the entrance and the other as the exit. Do not cross the two pairs.

3.1.3.Instruction to Indicator Lights

There are three indicator lights on the device, namely PWR, RUN and BP

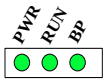


Fig.3-2 Indicator Lights

Tab.1 Instruction to Indicator Lights of Industrial Firewall

Indicator Lights	**Panel Screen Printing**	**Status**	**Instructions**
power indicator light	PWR	NC	It is not powered on or a power failure occurs to the host

		NO in green	The power supply is normal, the host is powered on normally
Running indicator light	RUN	NC	The device is not powered on or breaks down
		Flashing in green	The device works regularly
		Flashing in red	The device fails or undergoes a network attack.
Bypass indicator light	BP	NC	The BPYASS function is not started
		NO	The BYPASS function is enabled
Ethernet port indicator light	MGMT ETH1/ETH2/ETH3/ETH4	NC	The corresponding interface is in an unconnected state
		Color of indicator lights	The green color indicates that the current operation is based on a gigabit rate. The orange color indicates that the current operation is based on a megabit rate
		The indicator light is normally on	The interface has been established
		The indicator light flashes	The interface is sending and receiving data

3.1.4.Technical Specifications

Tab.2 Technical Specification for Industrial Firewalls

Model	**S2106**	**S2112**	**S2124**
Features			
Firewall functions	Status detection packet filtering firewall		
In-depth message resolving	The in-depth message resolving of OPC, Siemens S7, Modbus-TCP/Modbus-RTU, Ethernet/IP (CIP), MMS, IEC104, DNP3, FINS, PROFINET and other		

	protocols, support for the dynamic port of OPC, OPC, Siemens S7, Modbus-TCP, Ethernet/IP (CIP), MMS, IEC104, DNP3 read-only, message format check, integrity check, support for OPC 3.0 specifications distributed by the OPC Foundation.		
Whitelist function	Whitelist based access control policy		
Intelligent learning rules	Help to generate rules by intelligent protocol detection		
Rule test mode	Provide test modes to verify the correctness of security rules and business applicability		
Three-level permission management	The administrator permissions are separately divided for the approval administrator, the configuration administrator and auditor		
Local cache of logs	The security logs can be sent to the log server or to a local cache		
IP/MAC address binding	Support manually or learning to establish the IP, MAC binding relationship, avoiding address spoofing		
User-defined whitelist application	Identify the industrial control protocol according to the customer's actual business on site, so as to facilitate the preparation free of misinformation		
Unknown device detection	Quickly discover illegally connected devices		
Session management	Inquiry ongoing sessions in real time and individually set the session aging time		
Performance characteristics			
Number of data collection points	More than 100,000 points		
Packet delay	Less than 100μs based on the full configuration policy		
Concurrent connections	300000	300000	300000
User limit	Unlimited		
Bypass function	Auto bypass when in case of a power failure or system exception		
Hardware specification			

Processor	Dedicated multi-core network processor	Dedicated multi-core network processor	Dedicated multi-core network processor
Memory	DDR3 1G	DDR3 1G	DDR3 2G
Log storage	4G	4G	4G
Business port	6 gigabit combo port	8 gigabit ports +4 gigabit combo ports	16 gigabit ports +6 gigabit combo ports +2 gigabit SFP+ ports
Bypass	3 RJ45 interface	6 RJ45 interface	11 RJ45 interface
Management port	1 port 10/100/1000 Mbps adaptive	1 port 10/100/1000 Mbps adaptive	1 port 10/100/1000 Mbps adaptive
Serial interface	RJ45 debugging port	RJ45 debugging port	RJ45 debugging port
USB interface	1 port, USB 2.0	1 port, USB 2.0	1 port, USB 2.0
Dimensions/power supply/operating environment			
Working environment	Temperature: -40 ~ 75℃ Humidity: 5%-95%, no condensation	Temperature: -10 ~ 60℃ Humidity: 5%-95%, no condensation	Temperature: -10 ~ 60℃ Humidity: 5%-95%, no condensation
Storage environment	Temperature: -40 ~ 85℃ Humidity: 5%-95%, no condensation	Temperature: -40 ~ 85℃ Humidity: 5%-95%, no condensation	Temperature: -40 ~ 85℃ Humidity: 20%-80%, no condensation
MTBF	250,000 hours	250,000 hours	250,000 hours
Power supply	9-36VDC，Redundant power supply	100-240V AC，Redundant power supply	100-240V AC，Redundant power supply
Peak power	Typical power consumption 14.5W, Max 25W	Typical power consumption 26W, Max 46W	Typical power consumption 29W, Max 50W

Dimensions (WxDxH) mm	89x150x135mm	440*400*44mm	440*400*44mm
Installation method	35mm standard DIN rail clamping	Standard 19" rack mounting	Standard 19" rack mou nting
Protection grade	IP40	IP40	IP40
Authentication	CE, CB	CE, CB	CE, CB

3.2. Startup and Login

3.2.1.Startup of Industrial Firewall

According to the Hardware Installation Manual for Industrial Firewalls, the industrial firewall is installed to a specified position, guaranteeing that the power connector of the industrial firewall is normal. After connecting it to the required power supply, the industrial firewall will begin to start properly. The console port can be used to monitor the industrial firewall startup process as per the Installation Manual.

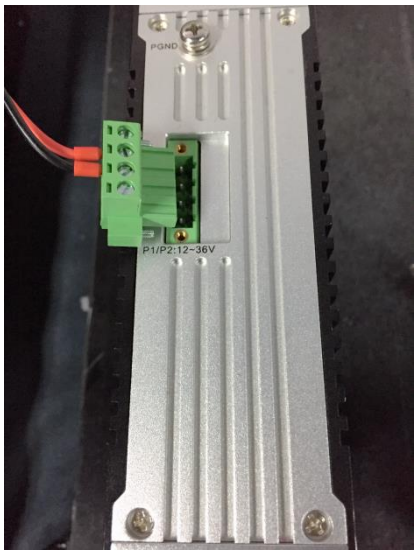


Fig.3-3 Powering on Industrial Firewall by Using Power Cord Supplied

After the industrial firewall is started, a new industrial firewall with no security policy configured will default to the operation mode in the "initial status", under which the industrial firewall exists in a transparent manner, intercepting no messages. If the security policy has been configured, the started industrial firewall will use the security configuration available before the last shutdown.

The industrial firewall shall be connected to the management platform to go online normally before it can be configured. Please insert the network cable into the MGMT port when connecting the management platform. The default IP address of all industrial firewalls is set to 192.168.8.6 when leaving the factory, which can be changed to the MGMT port address of the industrial firewall before or after connecting to the network for the management platform. Before the management platform can manage the industrial firewall regularly, the command line interface of the industrial firewall can configure the address of the management port and set the address of the management

platform to be connected. The command line of industrial firewall shall be introduced in the following section. Refer to 3.2.2.4 Change the IP Address of Management Port when setting the address of MGMT port of industrial firewall, and 3.2.2.5 Set the Management Platform Address when setting the management platform address to be connected.

3.2.2.CLI Application

CLI (Command Line Interface) is a text-like command interface between users and devices. A user enters text commands and submits them to the device to execute the corresponding commands by pressing Enter, so as to configure and manage the device, and confirm the configuration result by viewing the output information.

Since some operations of the device need to be completed in this interface, after the industrial firewall device is started, some necessary configuration needs to be done using the CLI command, such as to set the address of the management platform to be connected.

The industrial firewall device supports a variety of ways to enter the CLI interface, such as to connect directly through the Console port or enter the CLI interface after logging in the device via Telnet/SSH, etc. Either way, the default username when logging in the device is: AVCOMM, and the default password is: AVCOMM. The CLI interface of the device is shown below.

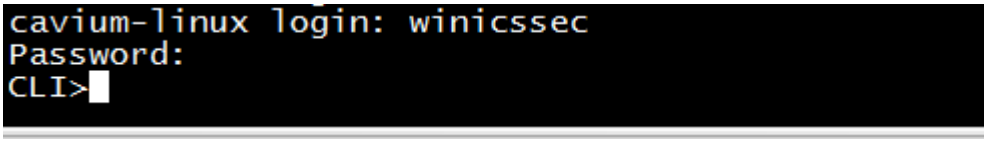


Fig.3-4 CLI Interface

Introduction to Common Commands:

3.2.2.1.Help

CLI>help

Display the help information.

3.2.2.2.System statistics related.

CLI>show pkt stat

View message statistics at all levels.

CLI>show mgmtip

View the IP address information on the management port.

CLI>show fpa

View the FPA information, mainly on various memory statistics.

CLI>show mem pool

View the mem pool information.

3.2.2.3. Enter the system configuration view.

CLI> config

Enter the system configuration view for the following configuration.

3.2.2.4. Change the IP address of the management port.

Note: to configure, use the config command to enter the system view

CLI#set mgmtip <ip> [netmask]

Change the IP address of the device management port.

For example: change the IP address of the management port of Industrial Firewall A to 192.168.8.6. The full command of the mask 255.255.255.0 is as follows:

CLI# set mgmtip 192.168.8.6 255.255.255.0

3.2.2.5. Set the address of the management platform.

CLI>show serverip

Check the IP address of the unified security management platform as configured in the industrial firewall

CLI#set serverip <IPV4ADDR: serverip>

Set the IP address of the unified security management platform to which the industrial firewall needs to be connected.

For example: the address of the management platform is 192.168.8.8, then the complete command is as follows:

CLI>set serverip 192.168.8.8

CLI>config

Set the industrial firewall gateway command,

For example: if the gateway address of 192.168.1.1 needs to be added, the complete command is as follows:

CLI# set mgmtgw 192.168.1.1

3.3. Firewall Management

3.3.1. Introduction to Functions

An industrial firewall is the object of the management platform management. All policy configurations are specific to a certain industrial firewall, for instance, only when the firewall security policy rules are distributed to a specific industrial firewall, can such rules work. To facilitate the management of multiple industrial firewalls with the same service, they system has also introduced the concept of firewall grouping.

Firewall grouping is the unified distribution and control when configuring industrial firewalls with the same service. The grouping of operations will affect all online industrial firewalls under such a group, so as to configure industrial firewalls of the same group in a unified manner. If the industrial firewall has an individualized

configuration, it shall be removed from its own group.

3.3.2.Firewall Management

After successfully opening the browser and logging in the Web management interface of the management platform, find [Industrial Firewall] in the upper menu bar, click the button (as shown in Fig.3-5), then find [Firewall Management/Firewall Management] in the left navigation bar; click on the left side of the menu [Firewall Management] (as shown in Fig.3-6) to see the Firewall Management page in the display page on the right side (as shown in Fig.3-7):

Fig.3-5 Industrial Firewall in Upper Menu Bar

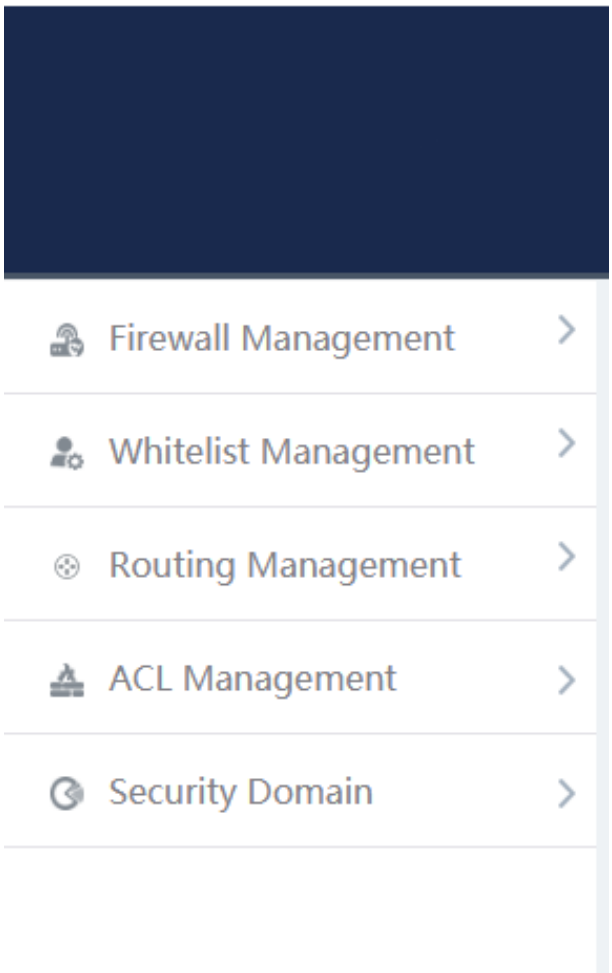


Fig.3-6 Firewall Management in Navigation Bar

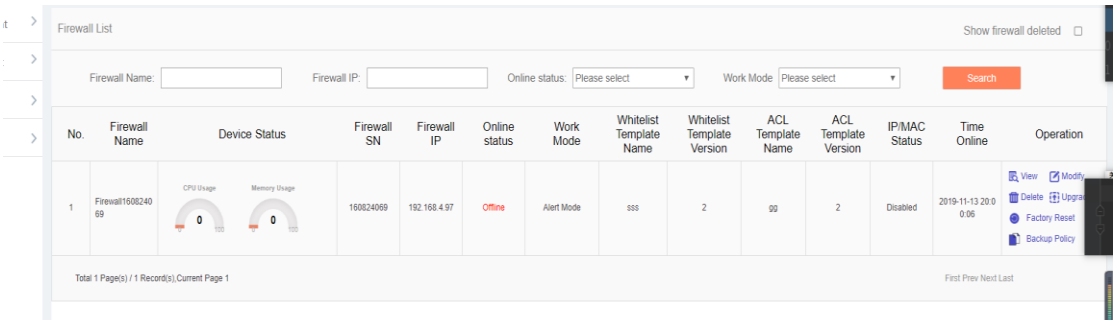
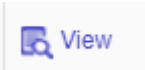
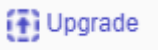
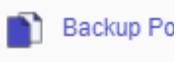


Fig.3-7 Firewall Management Display Page

View the current running status of the industrial firewall, with the following meanings:

Tab.3 Instruction to Firewall Management List Display

Column Names	**Instructions**
Firewall Name	The name given by the system or users for each industrial firewall, for example: "Industrial Firewall, Control Room, Production Workshop 1"
Device Status	Current running status of industrial firewalls, including CPU and memory utilization ratio. If a certain value is always overloaded within 1min, a corresponding alarm will be generated.
Firewall SN	The unique identification number of the industrial firewall automatically assigned by the system; an identification number represents a unique industrial firewall
Firewall IP	IP address of the management network port of the industrial firewall
Online status	The current industrial firewall is connected to the management platform (that is, online) or not connected (that is, offline)
Work Mode	Under which operation mode the current industrial firewall is in, the new industrial firewall is defaulted to "initial state".
Whitelist Template Name	The template name of the whitelist rules that are applied to the industrial firewall, if blank, it means that currently the industrial firewall has no whitelist rules set yet
Whitelist Template Version	The template version of the whitelist rules that are applied to the industrial firewall, the version and the template ID uniquely determine a set of whitelist rules, each edit whitelist and save, with the version number automatically +1 after each time the whitelist is edited and saved.
ACL Template Name	The template name of the ACL rules that are applied to the industrial firewall, if blank, it means that currently the industrial firewall has no ACL rules set yet

ACL Template Version	The template version of the ACL rules that are applied to the industrial firewall, the version and the template ID uniquely determine a set of ACL rules, each edit ACL template and save, with the version number automatically +1 after each time the ACL template is edited and saved.	
Time Online	The last time the industrial firewall goes online	
Operation	View 	View more detailed information on industrial firewalls, view the authorized function of each industrial firewall under the sub-page
	Modify 	Modify and set the information, operation mode, whitelist template and security policy rules, etc. of industrial firewall
	Delete 	Delete the offline industrial firewall, unable to delete the online industrial firewall. After deleting the industrial firewall, click "Display Deleted Ones" to view and restore the information
	Upgrade 	Upgrade the software running on the industrial firewall online. Only when the industrial firewall is online can this operation be conducted, refer to Section 3.3.4 Firewall Upgrade
	Restore the factory settings. 	One-key reset the factory settings of fire walls devices
	Back up all policy applications 	Copy all policies being applied on the source device to one or more other online and non-learning devices for distribution

3.3.2.1. Information view

Click <View> in the "Operation" property column of [Industrial Firewall Management], display the detailed information on industrial firewall (as shown in Fig.3-8):

Firewall > Firewall Management > View

Firewall Basic Information

Firewall Name:	Firewall160824069 View authorization information
Firewall SN:	160824069
Firewall IP:	192.168.4.97
Software version:	0.0.0.0
Group:	
Online status:	Offline
Physical Location:	
Time Online:	2019-11-13 20:00:06
Remarks:	

Work Mode Information

Work Mode:	Protection Mode

Deploy Mode Information

Deploy Mode:	Transparent Mode

Applied Whitelist Template Setting (* Prompt: Remove the firewall from group to set individual whitelist for the firewall!)

Whitelist Template Name:	whitelist_390

Firewall security Policy Template

Security Policy Template Name:	ACL-LHB

Firewall static routing configuration

Functional state: disabled	
Firewall Interface Configuration:	
Static Routing Table Name:	

IP/MAC Addr. Binding

Functional state: enabled	IP-MAC Configuration

Session Aging Time

TCP Aging Time:	1 Minute(s)
UDP Aging Time:	1 Minute(s)

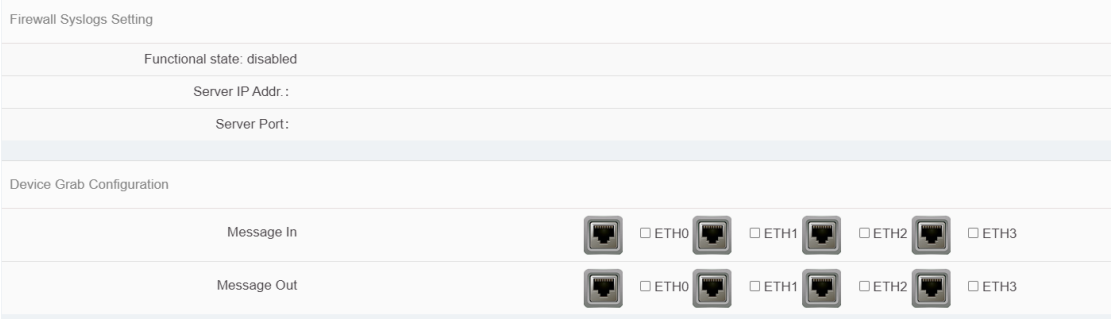


Fig.3-8 Industrial Firewall Information View Page

In addition to the more detailed information on the device, the most important thing in this page is the authorization information. Click <View authorization information> to open the authorization information page. For operations relating to more specific authorization information, please refer to the Section 3.3.3 Authorization Management.

Click <Back> in this page and go back to the [Firewall List Display] page.

3.3.2.2. **Modify firewall.**

Click <Modify> under the operation column of [Firewall List] (as shown in Figure.3-9) to open the industrial firewall information modification page, which separately modifies "Basic Information on Industrial Firewall", "Information on Operation mode", "Applied Whitelist Template Settings", "Firewall Security Policy Template", "IP/MAC Address Binding" (as shown in Fig.3-10):

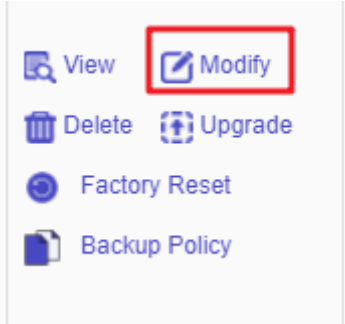
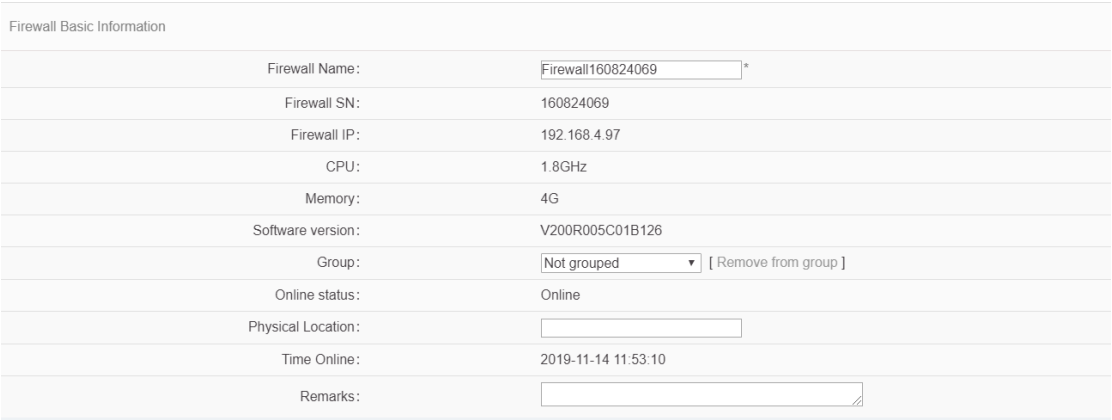


Fig.3-9 Modify Button



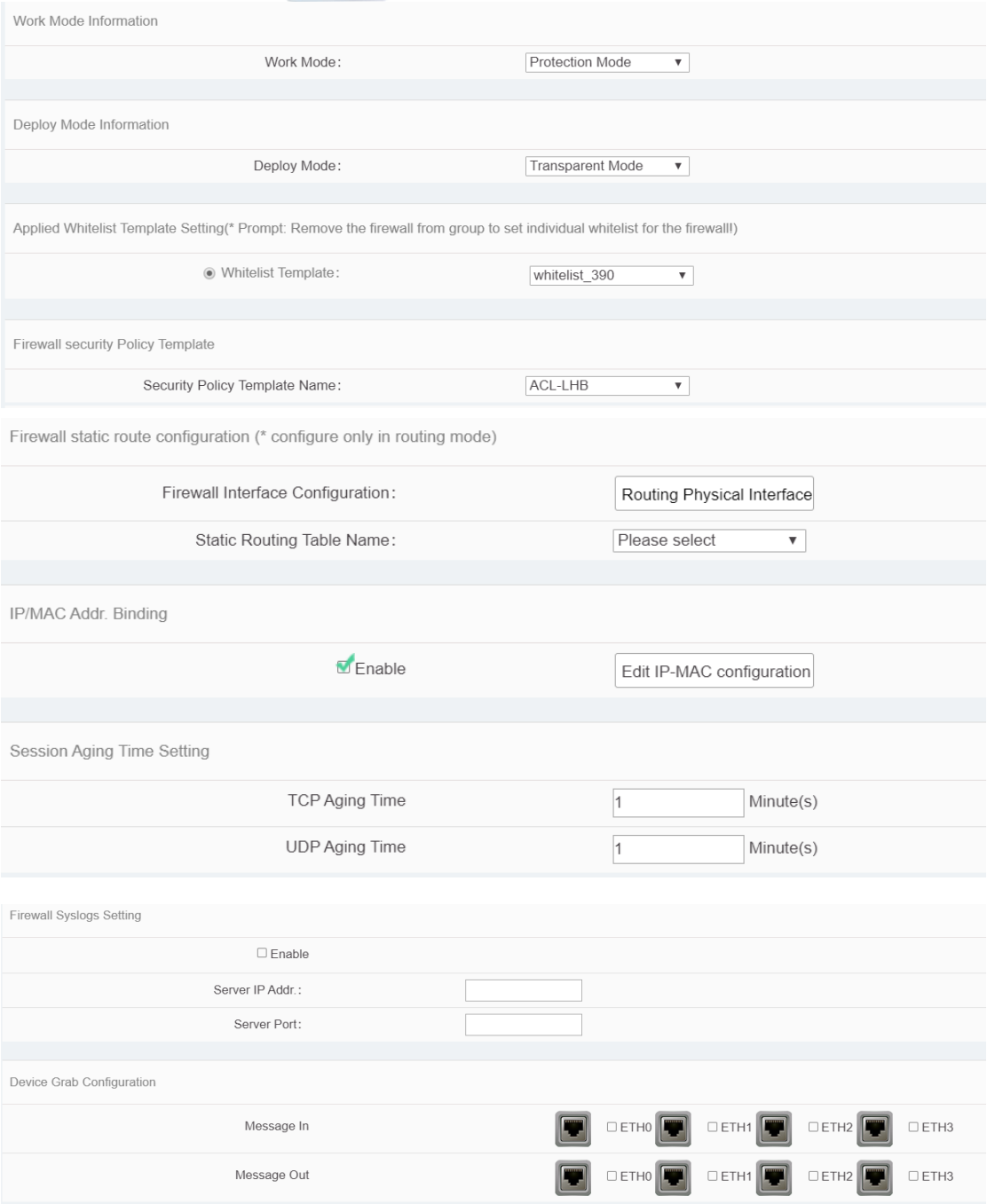


Fig.3-10 Industrial Firewall Modification Page

Tab.4 Instruction to Industrial Firewall Modification Information

Column Names	**Instructions**
Firewall Name	Define a meaningful name for an industrial firewall that is easy to understand and remember. Modify this when configuring an industrial firewall
Physical Location	The physical location of the department or where an industrial firewall belongs to, for example, "Control Room, Production Workshop 1", optional
Remarks	Optional, additional explanatory information

Operation mode	1. If the current mode is Learning Mode, only items Learning Completed and Learning Mode are available in the drop-down mode list of the industrial firewall. 2. If the current state is Learning Completed, items Learning Mode, Alarm Mode and Protection Mode are available in the drop-down mode list of the industrial firewall. 3. If the current mode is Alarm Mode, items Learning Mode and Protection Mode are available in the drop-down mode list of the industrial firewall. 4. If the current mode is Protection Mode, items Learning Mode and Alarm Mode are available in the drop-down mode list of the industrial firewall. 5. If the user changes the mode to Learning Mode, the whitelist template settings below will turn gray out and become inoperable 6. If the user changes from Learning Mode to Learning Completed, an edit box for whitelist template generation will appear in this case, allowing the user to name the whitelist template generated by learning. 7. If the industrial firewalls are grouped, then the user cannot change the operation mode and the whitelist template, which can be operated only after quitting the group.
Whitelist Template	For the whitelist rule template currently used by the industrial firewall, only when the industrial firewall changes to Alarm Mode or Protection Mode, the edit box will be highlighted. In this case, a whitelist template must be selected before saving it.
Security Policy Template Name	The security policy template currently used for the industrial firewall, optional
IP/MAC Addr. Binding	Configure IP/MAC address binding rules
Session Aging Time Setting Device Grab Configuration	Set the session aging time for TCP and UDP connections. Check grab network port, support to capture the message of any one or more ports including eht0, eth1, eth2, eth3, eth4, and eth5. It is possible to specify to capture the incoming, outgoing or two-way message of each port. The

	management platform stores the captured messages according to the device ports, and can to query and download the messages. Message query and Download can view all messages captured network port capture packet to capture all messages by network port grab package, which can be downloaded And download.	
Operation	Save	All modification information will be saved to the database and taken into effect and returned to the industrial firewall information list display page.
	Back	Ignore all modifications and go back to the industrial firewall information list display page.

3.3.2.3. Delete a firewall.

Click <Delete> under the operation column of [Firewall List] to delete the offline industrial firewall that is no longer in use. (As shown in Fig.3-11):

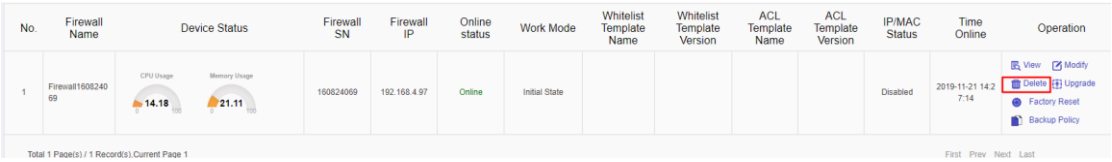


Fig.3-11 Delete an Industrial Firewall Button

However, please note that the online industrial firewall cannot be deleted. When clicking "Delete", a corresponding prompt will be given.

3.3.2.4. Retrieve firewalls.

In the [Firewall List] page, industrial firewalls can be retrieved according to the conditions (as shown in Fig.3-12):

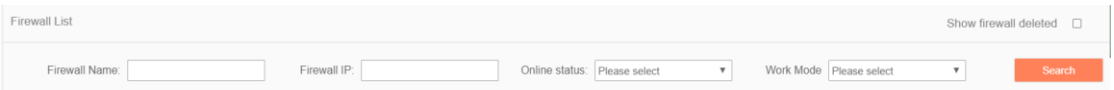


Fig.3-12 Retrieve Firewalls

3.3.3. Authorization Management

A license means a permit, it is a contractual form for device suppliers to authorize the use scope and deadline,

etc. of product features. The License can dynamically control whether certain features of a product are available or not. Users can purchase a License to activate certain features and functions as needed. For this product, only one activated License file exists in each industrial firewall device, and the activation of a new License will invalidate the old one.

Currently, the device supports the following methods to activate a License:

- Manually activate it through the unified security management platform

  After purchasing or updating a License and obtaining the License authorization certificate, the device under management shall be authorized or the authorization shall be updated by logging in the specified page of the unified security management platform.

Industrial firewall authorization management consists of three components: the authorization tool, the industrial firewall and the unified security management platform. The authorization tool belongs to AVCOMM and is only available to specified users within the Company.

3.3.3.1. Check authorization.

Click the left navigation bar [Firewall Management], open the page and select to view the authorized industrial firewall, click <View> under the operation column, with the button (as shown in Fig.3-13) available in the opened page:

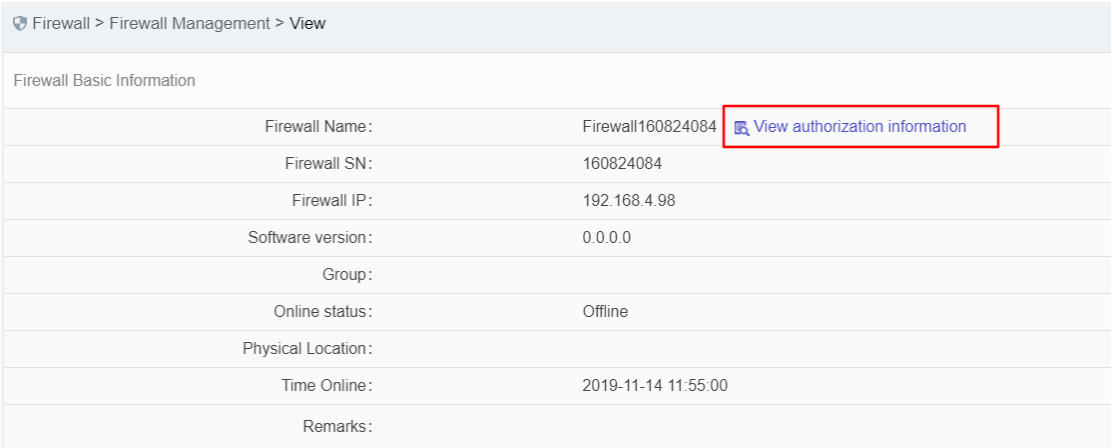
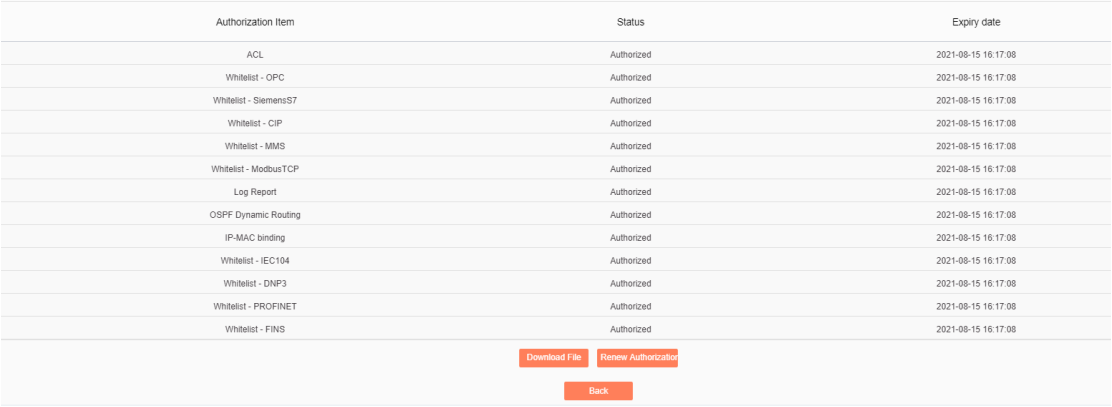


Fig.3-13 Authorization Information on Industrial Firewalls

➢ View the authorization information.

Click <View authorization information> to pop up a specific authorization information page (as shown in Fig.3-14):



Authorization Item	Status	Expiry date
ACL	Authorized	2021-08-15 16:17:08
Whitelist - OPC	Authorized	2021-08-15 16:17:08
Whitelist - SiemensS7	Authorized	2021-08-15 16:17:08
Whitelist - CIP	Authorized	2021-08-15 16:17:08
Whitelist - MMS	Authorized	2021-08-15 16:17:08
Whitelist - ModbusTCP	Authorized	2021-08-15 16:17:08
Log Report	Authorized	2021-08-15 16:17:08
OSPF Dynamic Routing	Authorized	2021-08-15 16:17:08
IP-MAC binding	Authorized	2021-08-15 16:17:08
Whitelist - IEC104	Authorized	2021-08-15 16:17:08
Whitelist - DNP3	Authorized	2021-08-15 16:17:08
Whitelist - PROFINET	Authorized	2021-08-15 16:17:08
Whitelist - FINS	Authorized	2021-08-15 16:17:08

Download File Renew Authorizatio

Back

Fig.3-14 Authorization Details View Page

This page displays the authorization details for the current industrial firewall.

- Download File

  Obtain the authorization file of the industrial firewall, which can be sent to the manufacturer for subsequent update of the authorization information.

- Renew Authorization

  Update the authorization information on the current industrial firewall.

- Back

  Close the current page and return to the industrial firewall view page. Get the authorization file.

In the opened industrial firewall authorization details page, click <Download File> to download the authorization file, which can be sent to the manufacturer and used by the subsequent manufacturer as a basis for updating the new authorization to the user.

3.3.3.2. Update the firewall authorization information.

In the opened industrial firewall authorization details page of, click <Renew Authorization > to pop up the authorization file selection dialog box, to update the latest authorization file obtained by the user from the manufacturer to a specified industrial firewall (as shown in Fig.3-15):

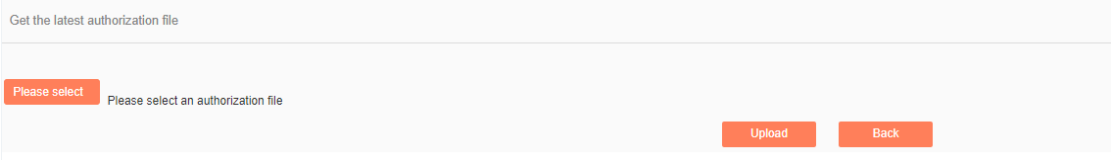


Fig.3-15 Select New Authorization File to be Updated to Industrial Firewall

- Please select...

  Click Please select to pop up the file selection dialog box.

  Find the new authorization file (for example: a file that is named with the device ID and suffixed with ".dat"), double-click the file or select <Open>, then click <Upload>. The browser will upload this file to the management platform of the server first, then notify the industrial firewall. The industrial firewall will update the authorization. Upon the successful updating, the user will be able to view the page for the new authorization information.

- Back

  Clicking <Back> will not execute any operations, but directly go back to the industrial firewall authorization details page instead.

3.3.4.Firewall Upgrade

When a new industrial firewall version that is more powerful in functions and more stable in operation is launched, users can upgrade the industrial firewall device remotely through the unified security management platform.

After opening the [Firewall Management] page, click <Upgrade> under the operation column of [Firewall Information Display List] to pop up the dialog box [Firewall Upgrade] (as shown in Fig.3-16):

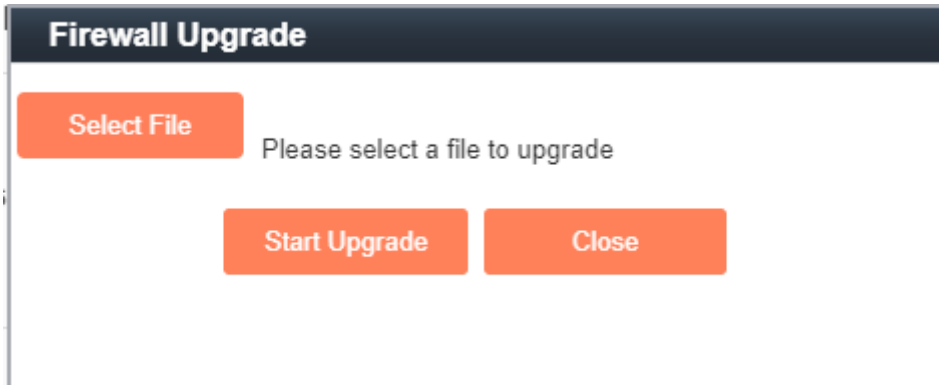


Fig.3-16 Industrial Firewall Upgrade File Selection

- Select File

Click "Select File" to pop up the file selection dialog box. Find the new upgrade file (for example: sys-fw.tar.gz), double-click the file or select <Open>.

- Start Upgrade

Upon clicking this button, the browser will firstly upload the upgrade file to the server where the unified security management platform is located, and then notify and distribute the upgrade file to the industrial firewall, which will execute specific upgrade operation.

- Close

Click <Close> will not execute any operations, but directly go back to the [Firewall Information Display List] page instead.

3.3.5.IP/MAC Address Binding

Find [Firewall Management/Firewall Management] in the left navigation bar, click <Modify> to open the industrial firewall modification page. (As shown in Fig.3-17):

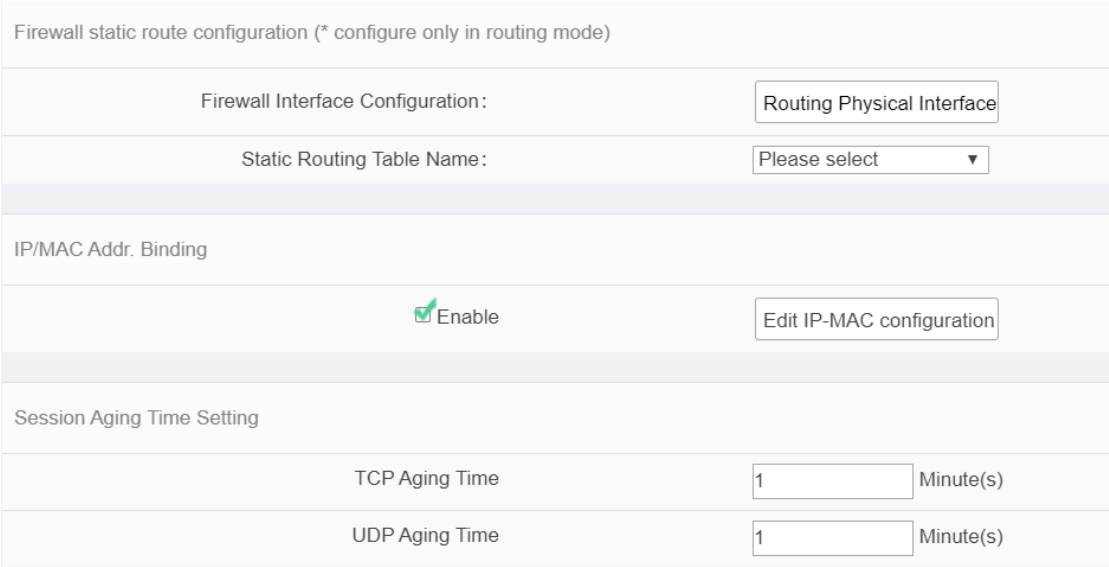


Fig.3-17 IP/MAC Configuration in Industrial Firewall Management Modification Page

3.3.5.1. **Rule configuration**

This feature can be "enabled" for a single industrial firewall or a group of industrial firewalls. Only after the function is enabled can the configuration be edited.

If "IP/MAC Address Binding" is enabled, click <Edit IP/MAC Configuration> and skip to the IP/MAC Configuration page (as shown in Fig.3-18):

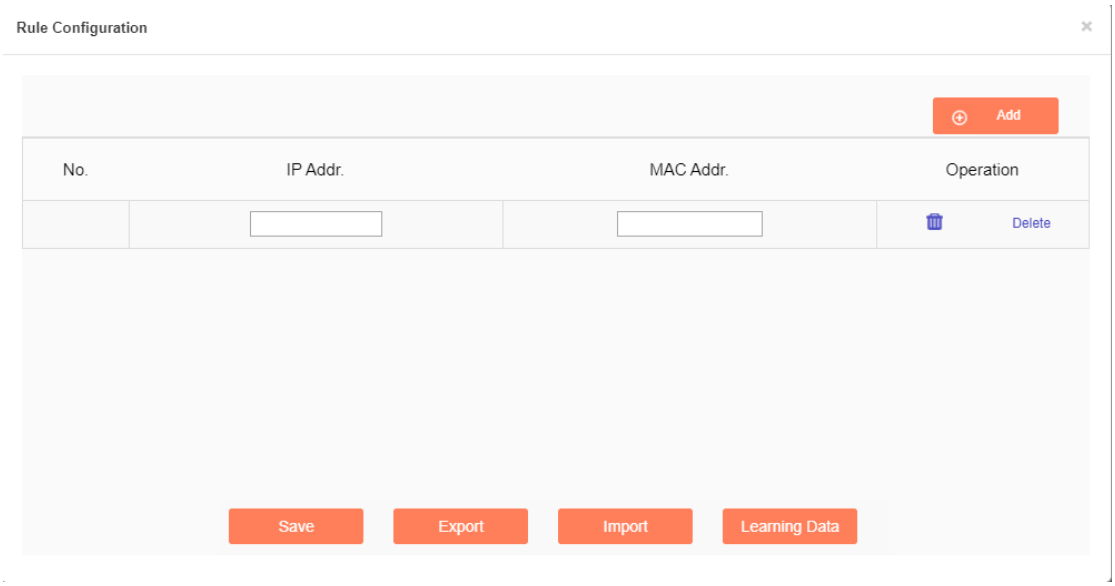
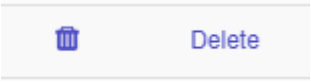


Fig.3-18 Rule Configuration Page

Click <Add> to add rules, click 

to delete current rules, click <Save> to save rules.

3.3.5.2. Learning data

Click <Learning Data> and skip to the Learning Data page (as shown in Fig.3-19):

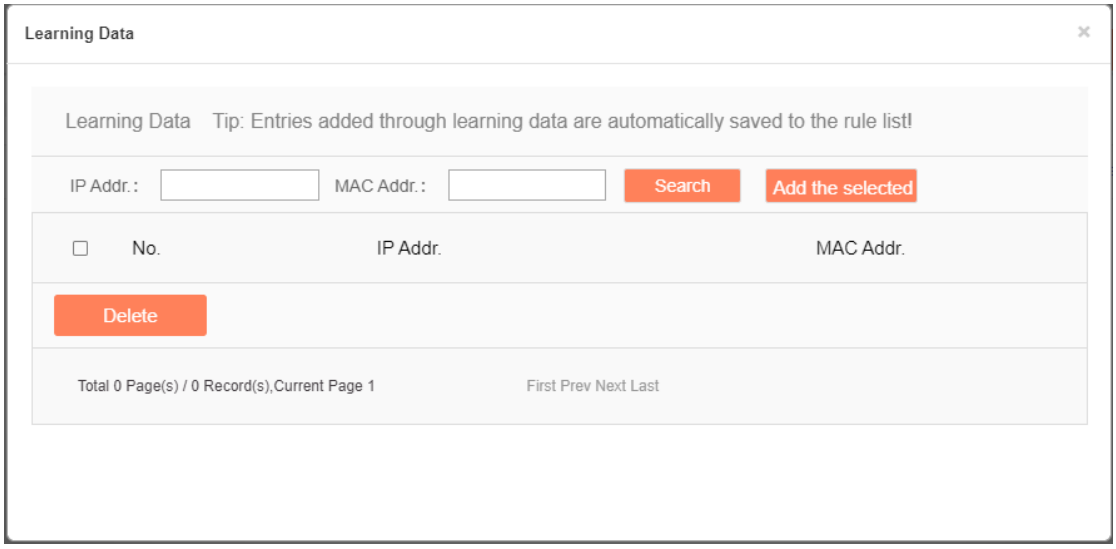


Fig.3-19 Learning Data Page

Search the learning data according to the IP address and the MAC address conditions, click <Delete> to delete the selected data (as shown in Fig.3-20):

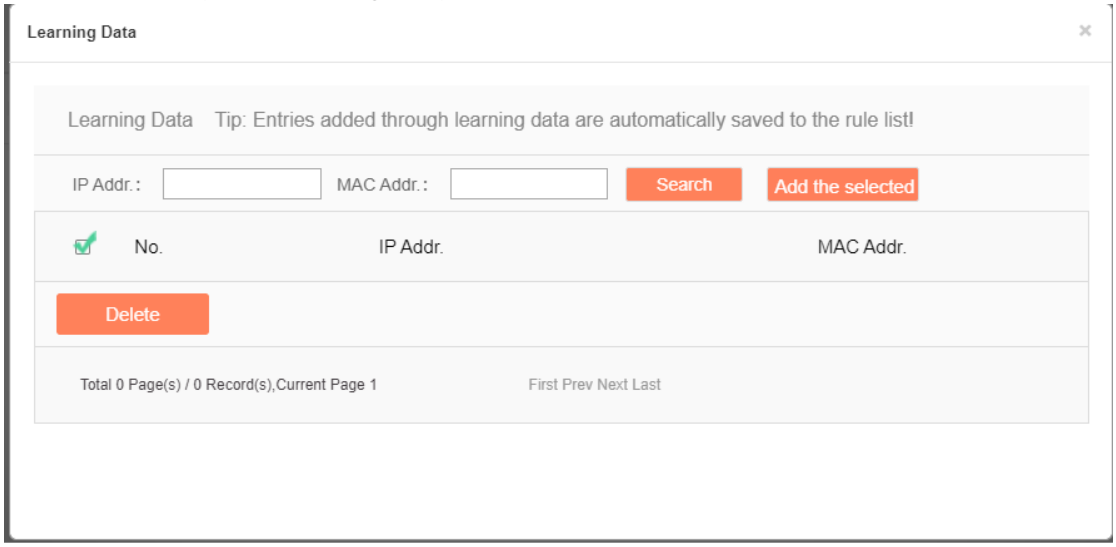


Fig.3-20 Delete Learning Data

Click <Add the selected> to add the selected rule to the rule configuration list (as shown in Fig.3-21):

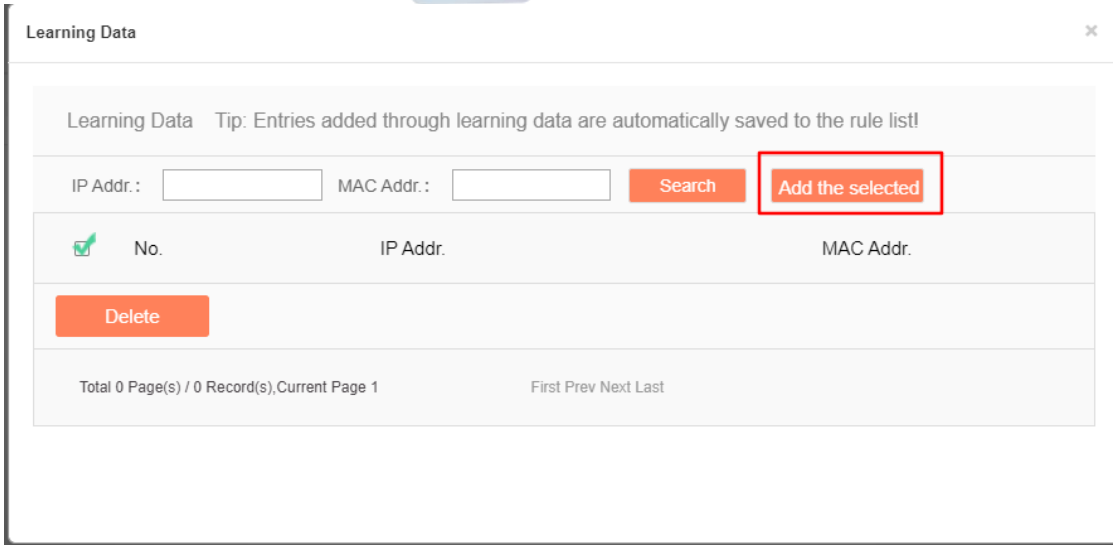


Fig.3-21 Adding Learning Data

3.3.6.Group Management

Find [Firewall Management/Group Management] in the left navigation bar, click "Open" (as shown in Fig.3-22) to see the Group List Information Display page in the display page on the right (as shown in Fig.3-23):

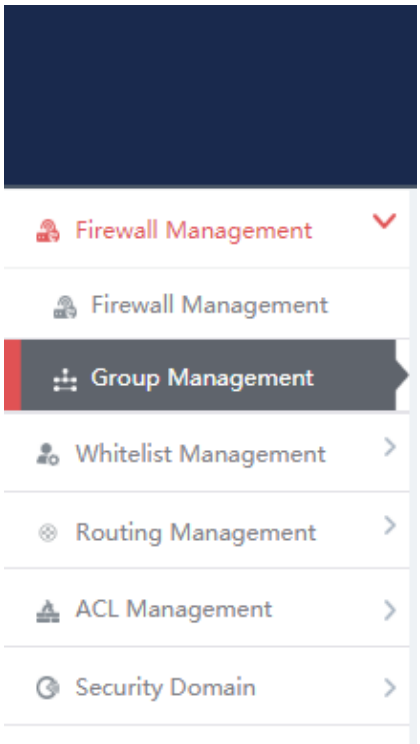


Fig.3-22 Group Management in Navigation Bar

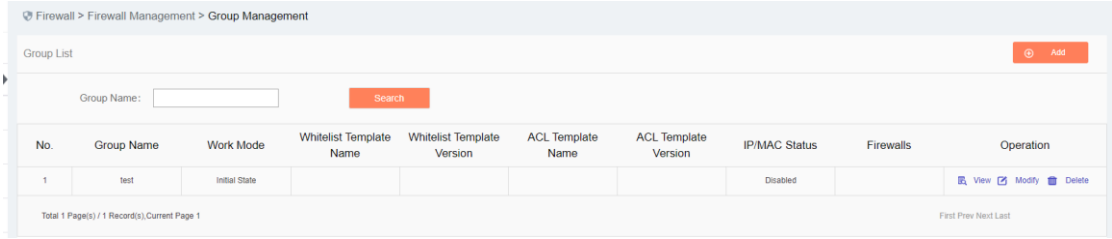


Fig.3-23 Group List Display Page

View the information on all industrial firewall groups in the system here, with the meaning as follows:

Tab.5 Instruction to Group Management List Display

Column Names	**Instructions**	
Group Name	an industrial firewall group name that is easy to remember, for example "6#DCS Industrial Firewall Group"	
Work Mode	The operation mode which currently all industrial firewalls under the group are in, which means being in the initial status if without any additions	
Whitelist Template Name	The name of the whitelist rule template applied to all industrial firewalls under the group; If blank, it means that no whitelist rule is currently set in the group	
Whitelist Template Version ACL Template Name ACL Template Version IP/MAC Status	The version of the whitelist rule template applied to all industrial firewalls under the group. The name of the ACL template applied to all industrial firewalls under the group; If blank, it means that no whitelist rule is currently set in the group. The version of the ACL template applied to all industrial firewalls under the group. The state of IP/MAC Binding Status, Enable means on,Disbale means off	
Firewalls	Industrial firewalls contained in the group	
Operation	View	View more detailed information on the group
	Modify	Modify and set group information, operation modes, whitelist templates, firewall rules, industrial firewalls contained and so on
	Delete	Delete the industrial firewall group; cannot deletes a group containing industrial firewalls

3.3.6.1. Add a group.

Click <Add> on the right side of the firewall group list tab under [Group Management] (as shown in Fig. 3-24), with the Firewall Group Add page popped up (as shown in Fig. 3-25):

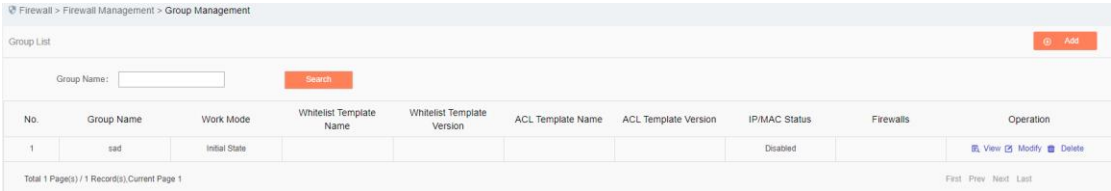


Fig.3-24 Firewall Group Add Buttons

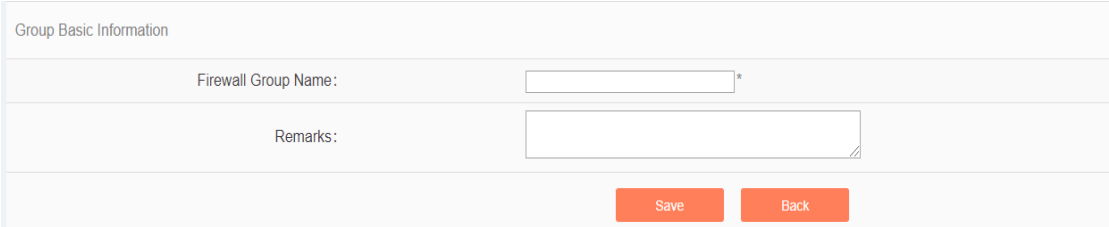


Fig.3-25 Firewall Group Add Page

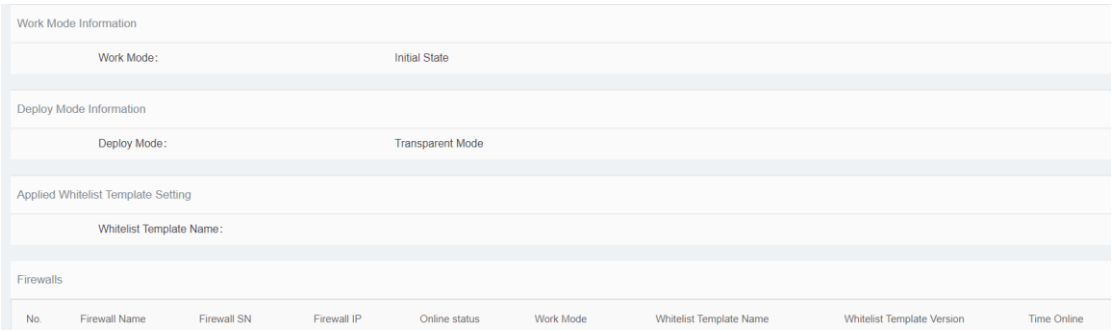
Tab.6 Instruction to Firewall Group Add Information

Column Names	Instructions
Firewall Group Name	Define a meaningful name for the group that is easy to understand and remember
Remarks	Optional, additional explanatory information

In the adding process, enter the industrial firewall group name and other information to be noted, click <Save> to finish adding, and view the newly added group in the industrial firewall group list.

3.3.6.2. Information view

Click <View> under the operation column of [Group List] to display the detailed group information (as shown in Fig.3-26):



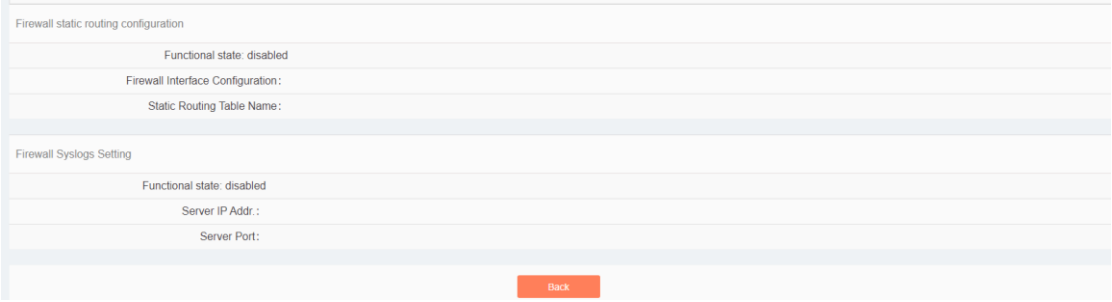


Fig.3-26 Group Information View Page

Click <Back> and go back to the [Group List] page.

3.3.6.3. **Modify a group.**

Click <Modify> under the operation column of [Group List] (as shown in Fig.3-27) to open the [Group Information Modification] page, which can separately modify basic information on the group, operation modes of the group, whitelist template currently applied to the group and IP/MAC address binding configuration (as shown in Fig.3-28):

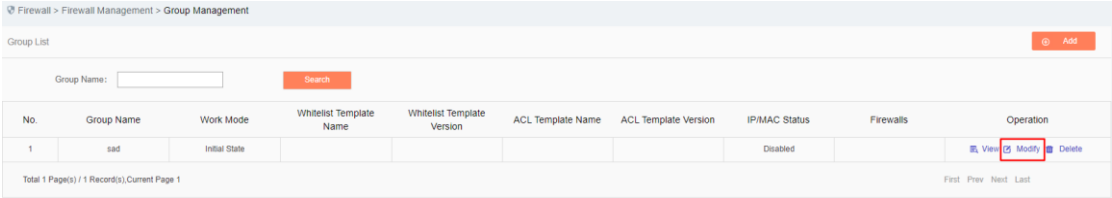
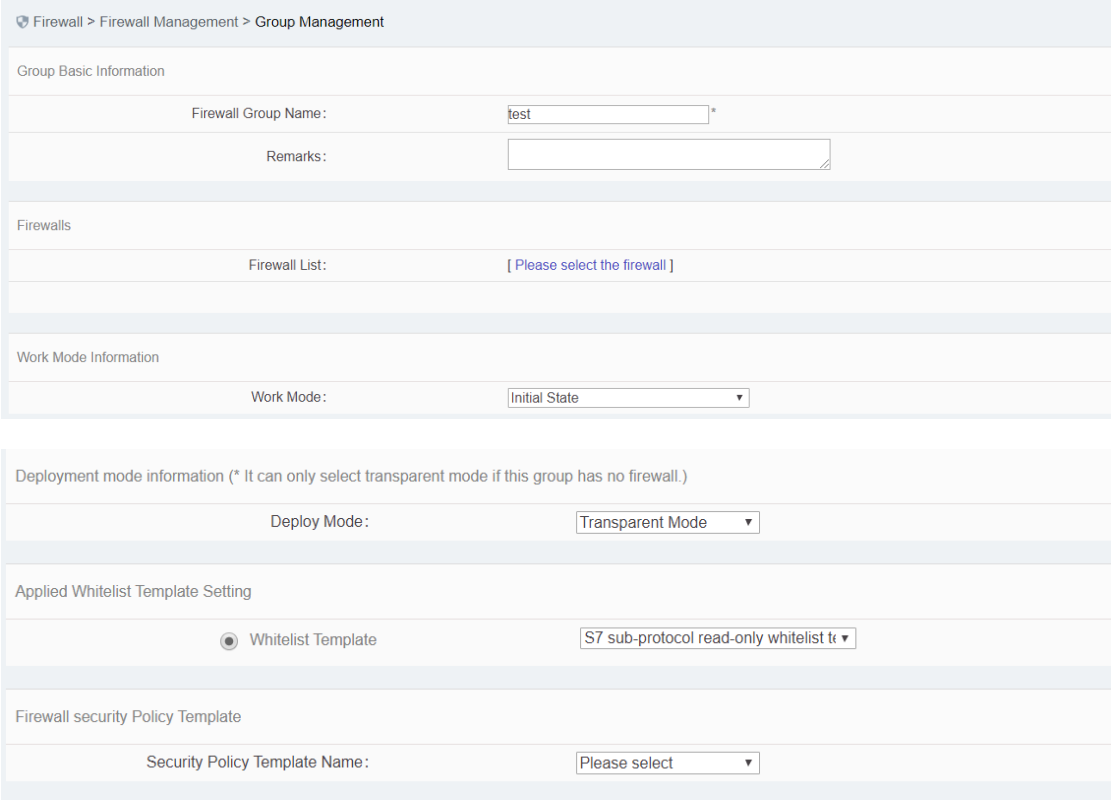


Fig.3-27 Modify Button



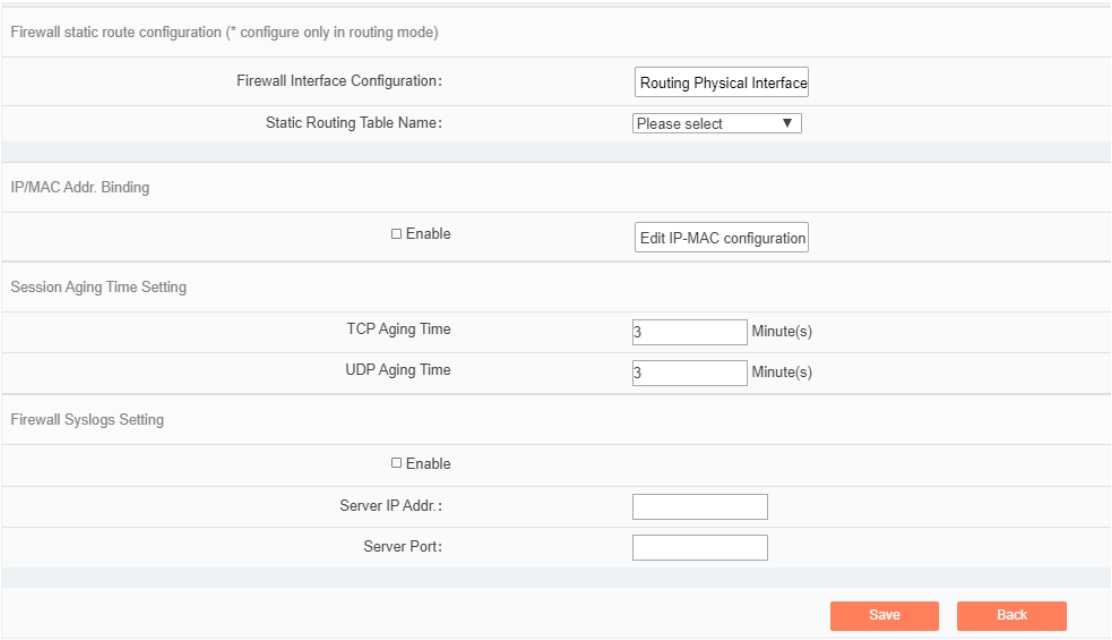


Fig.3-28 Group Information Modification

Tab.7 Instruction to Firewall Group Modification Information

Column Names	**Instructions**
Firewall Group Name	Define a meaningful name for the group that is easy to understand and remember
Remarks	Optional, additional explanatory information
Firewall List	All industrial firewalls under the current group can be edited by clicking <Select a Firewall>
Work Mode	1. If the current mode is Learning Mode, only items Learning Completed and Learning Mode are available in the drop-down operation mode list 2. If the current state is Learning Completed, items Learning Mode, Alarm Mode and Protection Mode are available in the drop-down operation mode list 3. If the current mode is Alarm Mode, items Learning Mode and Protection Mode are available in the drop-down operation mode list 4. If the current mode is Protection Mode, items Learning Mode and Alarm Mode are available in the drop-down operation mode list 5. If the user changes the mode to Learning Mode, the whitelist template settings below will turn gray and become inoperable

	6. If the user changes from Learning Mode to Learning Completed, an edit box for whitelist template generation will appear in this case, allowing the user to name the whitelist template generated by learning 7. If the operation mode of the group is changed, the operation modes of all industrial firewalls under the group will be changed	
Whitelist Template	It means the whitelist rule template name used by the industrial firewall. Only when the operation mode is changed to Alarm Mode or Protection Mode, the edit box will be highlighted. In this case, a whitelist template must be selected to save it. Changes will affect all industrial firewalls under the group	
Security Policy Template Name	It means the security policy template name used by the group. Changes will affect all industrial firewalls under the group	
IP/MAC Addr. Binding	Enable and edit IP/MAC address binding	
Session Aging Time Setting	Set the session aging time for TCP and UDP connections	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the [Group Information Display List] page
	Back	Ignore all modifications and go back to the [Group Information Display List] page

3.3.6.4. **Add a firewall to the group.**

In the opened [Group Information Modification] page, click <Please select the firewall> to open the [Please select the firewall] page (as shown in Fig.3-29):

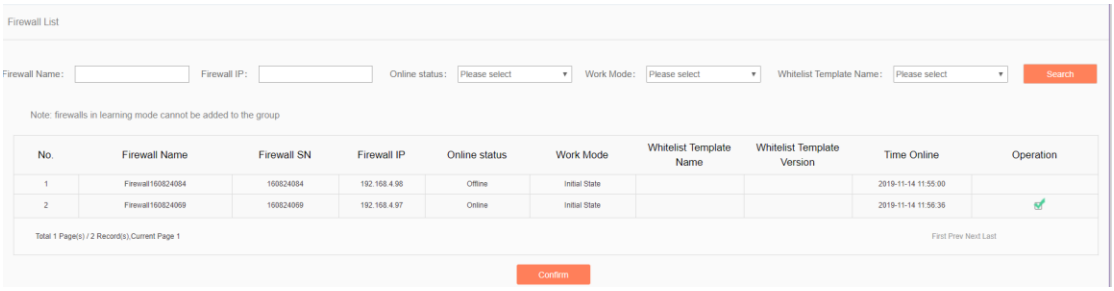


Fig.3-29 Page of Selecting a Firewall in the Group

Select the required industrial firewall in the opened page, click "Select" in the last row of "Operations"; deselect "√" in the column to cancel. Click <Confirm> to complete the operation after the operation is done.

3.3.6.5. Delete a group.

Click <Delete> under the <Operation> column of [Firewall Group List] to delete a group that is no longer used. (As shown in Fig.3-30):

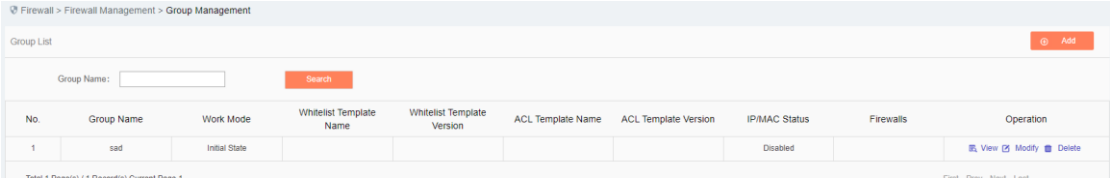


Fig.3-30 Group Delete Buttons

The group cannot be deleted if a firewall is contained under it. All industrial firewalls under the group shall be removed before deleting the group.

3.3.6.6. Retrieve a group.

In the [Firewall Group List] page, retrieve the group based on certain criteria (as shown in Fig. 3-31):

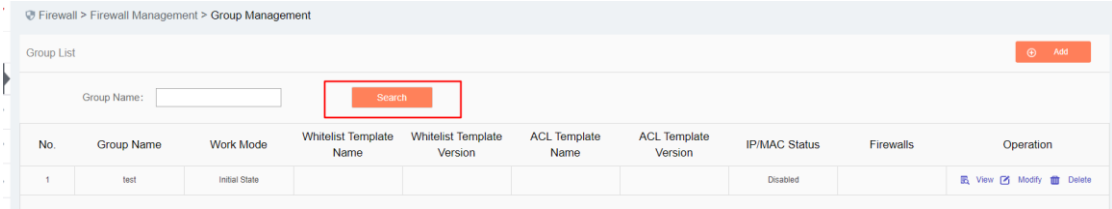


Fig.3-31 Retrieve a Group

3.3.7. Firewall Syslog Configuration

3.3.7.1. Configuration process

After logging in the management platform, the user opens the [Firewall] ->[Firewall Management] page to display the added firewalls. In this page, the user selects the firewall with its configuration to be modified, then clicks <Modify> to and goes to the firewall modification page, finding the sub-item "Firewall Syslog Configuration". After clicking <Enable>, the page sets the relevant controls for Syslog service configuration to editable. See the following table for the contents that can be set:

Tab.8 Instruction to Firewall Syslog Configuration

Configuration Item Name	Description	Remarks
Server IP Address	The IP address of Syslog server, which supports both IPv4 and IPv6 formats. IPv4 is	

	represented with the dotted decimal system, and up to one address can be configured at the same time	
Server Port	Number of ports used for sending Syslog in range 1-65535	

When clicking <Enable> again, relevant controls are not editable.

See the diagram below:

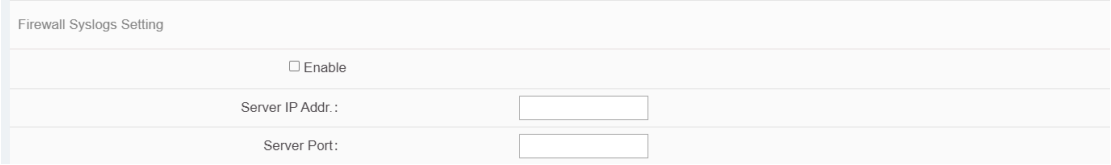


Fig.3-32 Syslog Configuration Subitems in Firewall Modification Page

3.4. Whitelist Management

3.4.1.Introduction to Functions

Industrial control system security issues are different from traditional IT network security issues, which pay more attention to serviceability and reliability, thus different in view of technical concepts and product realization.

The industrial control system emphasizes certainty, so what kind of traffic ought to be transmitted in the network must be clear and controllable. However, the traditional "blacklist" idea pays more attention to the identification and blocking of threats, which needs to frequently update the "blacklist feature library" of a product. Secondly, only when an accident occurs can the features of new threats be extracted and identified. Thirdly, understatement and misinformation often occur to such a product. To solve these problems, AVCOMM industry firewalls by using the industrial protocol in-depth resolving technology, realize the powerful industrial protocol whitelist function, helping customers to identify, define and control legal commands circulating at an industrial site via an intelligent learning engine. However, for unknown commands, whether causes damage on the industrial site or not, the firewalls will not allow them to "go through the wall", with the protection transforming from |"passively" adding a blacklist feature after being damaged to "actively" defining a legal traffic, thus avoiding unknown threats and attacks, in compliance with the required certainty and controllability for industrial sites.

The protection concept of industrial firewalls changes from "black" to "white" and from "passive defense" to "active protection". It is completely and especially applicable to sites for various industrial production network systems. Therefore, an important innovation of industrial firewall is whitelist management.

Whitelist management of the management platform can facilitate users to view, edit and use a whitelist.

3.4.2.Template Management

Click [Whitelist Management/Template Management] in the left navigation bar (as shown in Fig.3-33) and go to the [Whitelist Template Management] page (as shown in Fig.3-34):

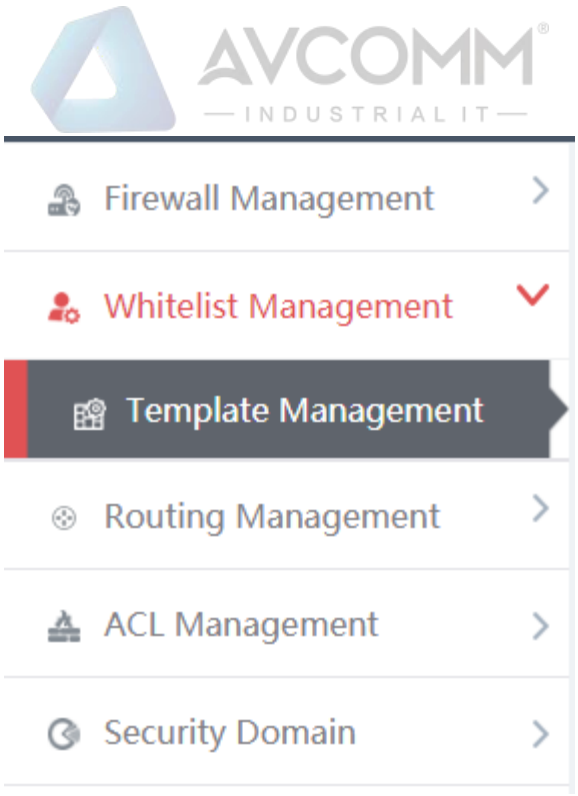


Fig.3-33 Select Whitelist Template Management

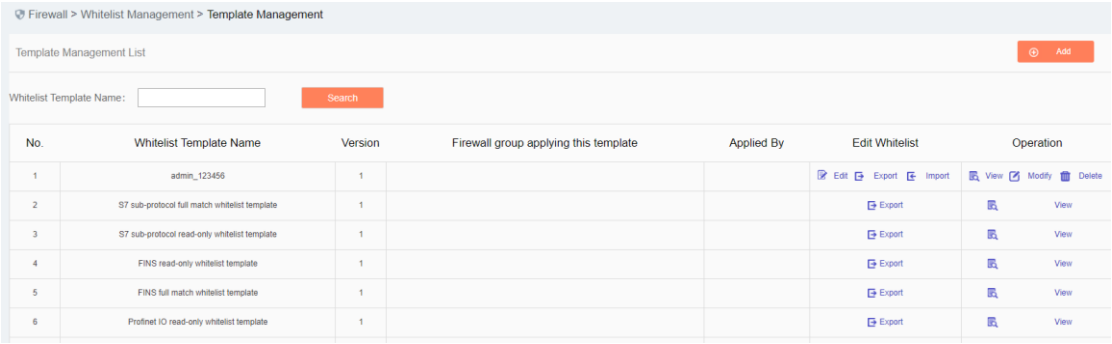


Fig.3-34 Whitelist Template Management

View information on all whitelist templates in the system here, with the meanings given below:

Tab.9 Instruction to Whitelist Template List Display

Column Names	**Instructions**
Whitelist Template Name	A whitelist template name that is easy to remember, for example "Whitelist Learned from Data Collection System 1"
Version	The version of Whitelist rule template, the version and the template ID uniquely determine a set of whitelist rules. The version number will automatically +1 after each time the whitelist is edited and saved
Firewall group applying this template	All firewall groups that are using this whitelist template
Applied By	All independent industrial firewalls that are using the whitelist template

Edit Whitelist	Edit	Click and go to the specific whitelist item edit page for each industrial protocol
	Export	Export the current whitelist rules in Excel format When clicked
	Import	Import the current whitelist rules in Excel format When clicked
Operation	View	View more detailed information on whitelist templates
	Modify	Modify and set the whitelist template. This button is not available to the whitelist template that are built-in the system
	Delete	Delete a whitelist template; cannot delete a whitelist template in use. This button is not available to the whitelist template that are built-in the system

3.4.2.1. **Add a whitelist template.**

Open [Template Management] in the left navigation bar, click <Add> on the right of the template management list TAB (as shown in Fig.3-35) to pop up the Whitelist Template Add page (as shown in Fig.3-36):

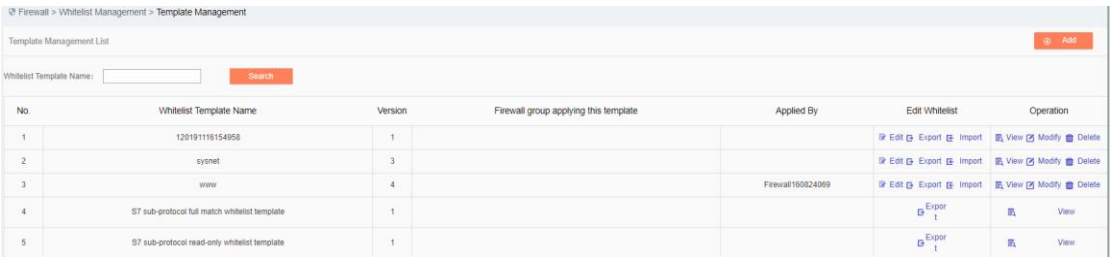


Fig.3-35 Whitelist Template Add Button

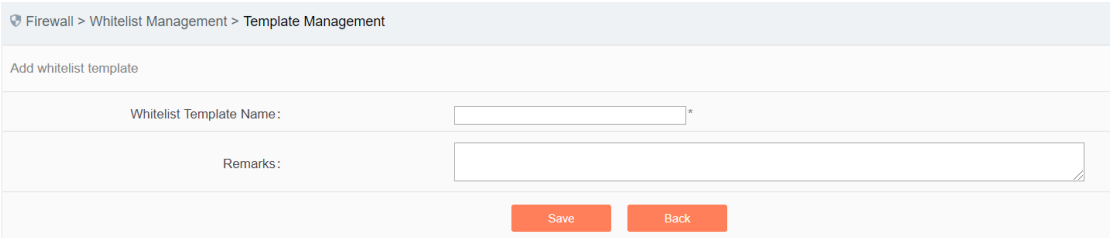


Fig.3-36 Whitelist Template Add Page

Tab.10 Instruction to Whitelist Template Add Information

Column Names	**Instructions**
Whitelist Template Name	Define a meaningful whitelist template name that is easy to understand and remember
Remarks	Optional, additional explanatory information

3.4.2.2. Information view

Open the [Template Management List] of whitelist, click <View> under the operation column in the display list to display the detailed information on whitelist template (as shown in Fig.3-37):

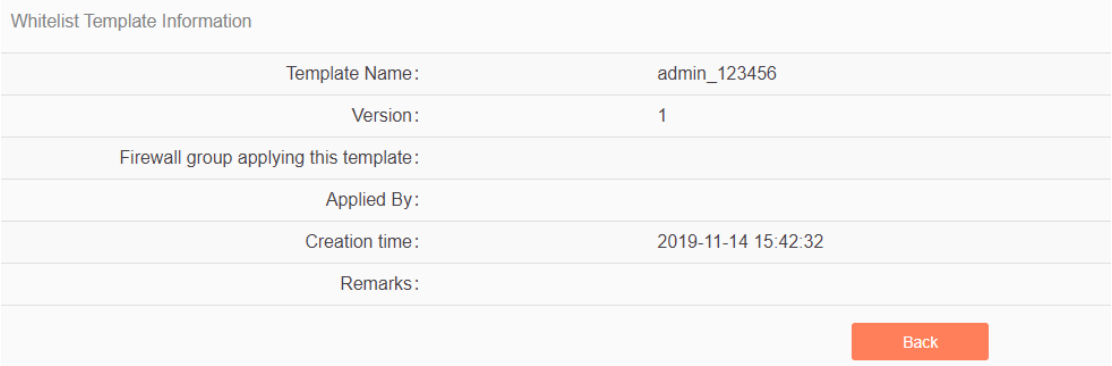


Fig.3-37 Whitelist Template Information View Page

Click <Back> and go back to the [Whitelist Template List Display] page.

3.4.2.3. Modify a whitelist template.

Open the [Template Management] of the whitelist, click <Modify> under the operation column in the display list (as shown in Fig.3-38) to open the [Whitelist Template Information Modification] page, separately modify the basic information on the whitelist template (as shown in Fig.3-39):

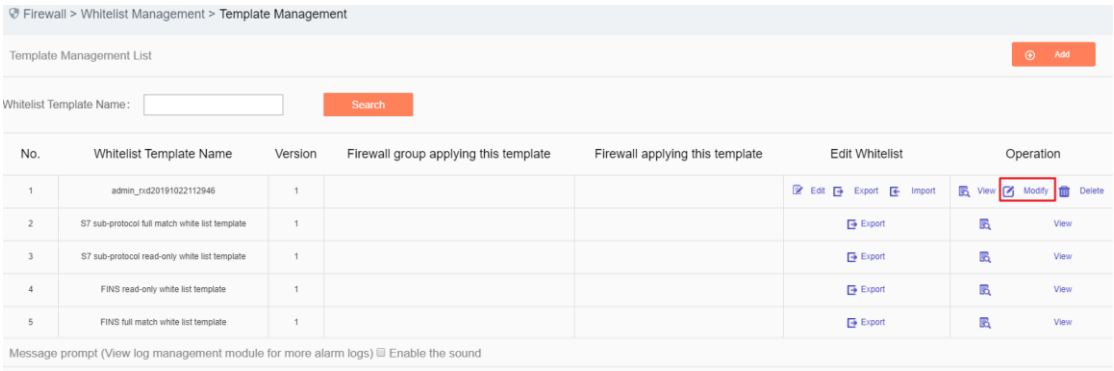


Fig.3-38 Whitelist Template Modification Buttons

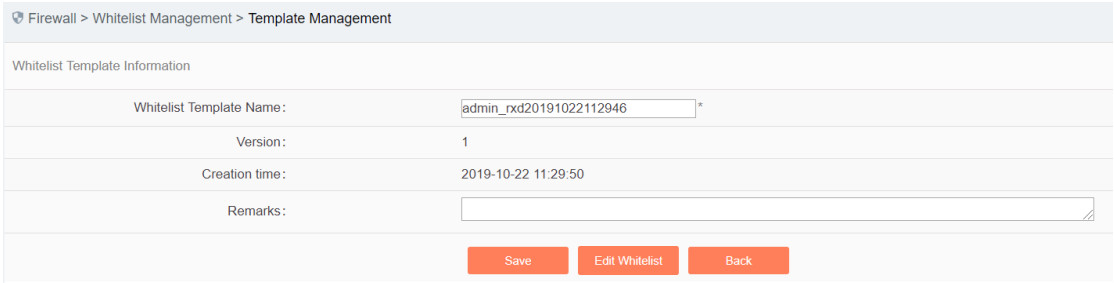


Fig.3-39 Whitelist Template Modification Page

Tab. 11 Instruction to Whitelist Template Modification Information

Column Names	Instructions

Whitelist Template Name	Define a meaningful whitelist template name that is easy to understand and remember	
Remarks	Optional, additional explanatory information	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the Whitelist Template Information List Display page
	Edit Whitelist	Click and go to the Whitelist Edit page for each specific industrial protocol
	Back	Ignore all modifications and go back to the Whitelist Template Information List Display page

3.4.2.4. Delete a whitelist template.

Click <Delete> under the operation column in the [Template Management] information display list of the whitelist to delete a whitelist template that is no longer used. (As shown in Fig.3-40):

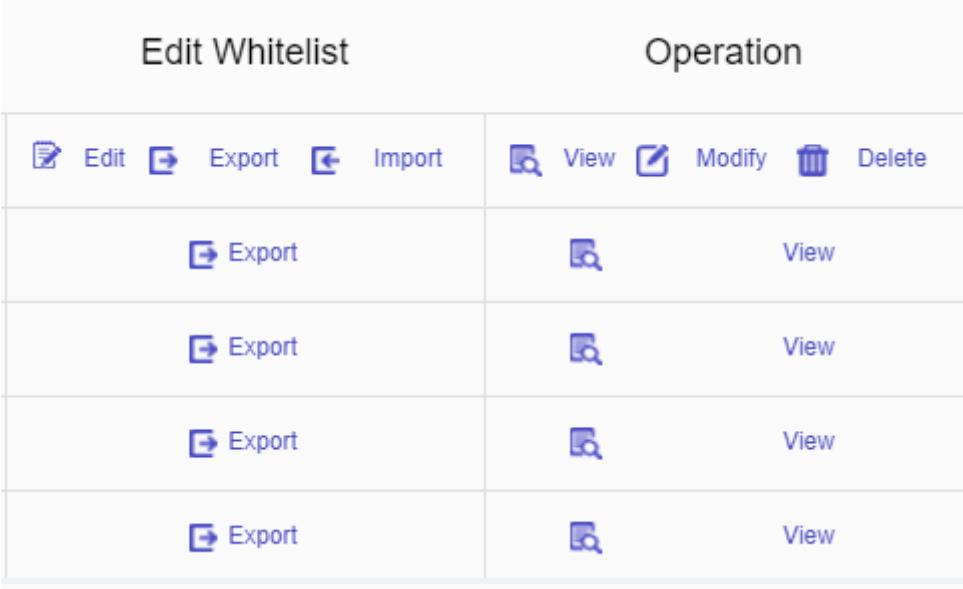


Fig.3-40 Whitelist Template Delete Button

3.4.2.5. Retrieve a whitelist template.

In the [Template Management] information display list of the whitelist, retrieve a whitelist template the whitelist template based on the conditions (as shown in Fig.3-41):

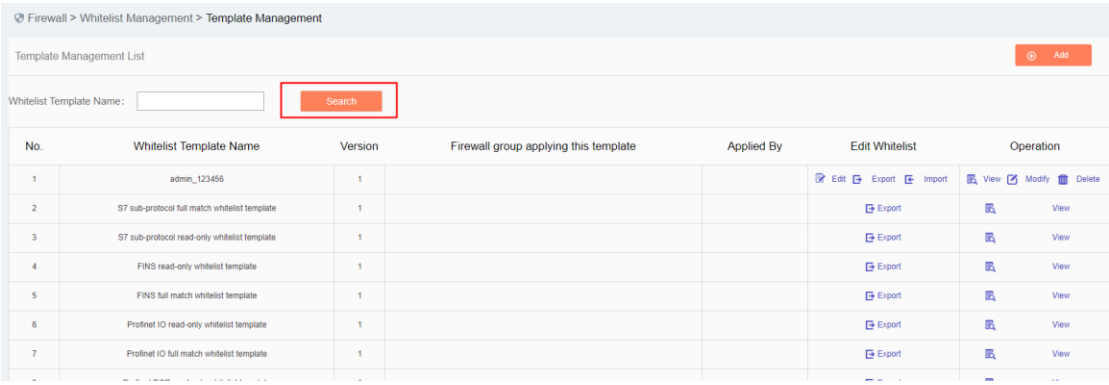


Fig.3-41 Retrieves a Whitelist Template

3.4.3.Whitelist Template Rule Management

Whitelist template rule items refer to the rules of a specific industrial protocol in a whitelist template. Its management is the core of whitelist template management. All templates depend on each specific whitelist item. Currently, industrial firewalls support whitelists of following standard industrial protocols:

OPC Classic 3.0, Siemens S7, Modbus TCP, Ethernet/IP (CIP), MMS, IEC 104, DNP3, FINS, PROFINET，

Industrial firewalls intend to support whitelists of all common industrial protocols in the near future.

Ways to enter the [Whitelist Template Rule Management] page:

The first path: click <Edit> in the [Whitelist Management]-[Template Management]-[Edit Whitelist] column;

The second path: click <Modify> in the [Whitelist Management]-[Template Management]-[Operation] column (as shown in Fig.3-42), click <Edit Whitelist> in the opened [Whitelist Template Modification] page (as shown in Fig.3-43):

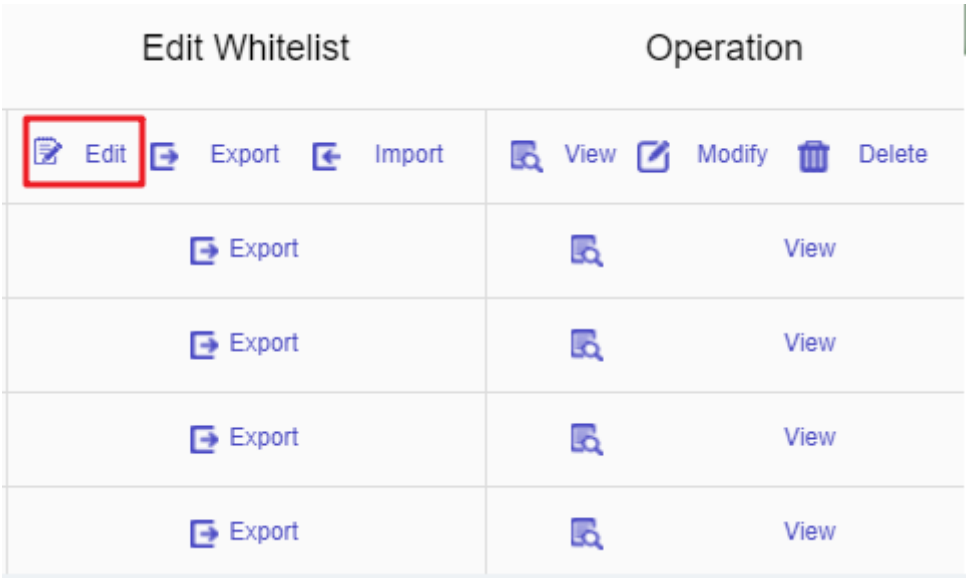


Fig.3-42 Edit Button

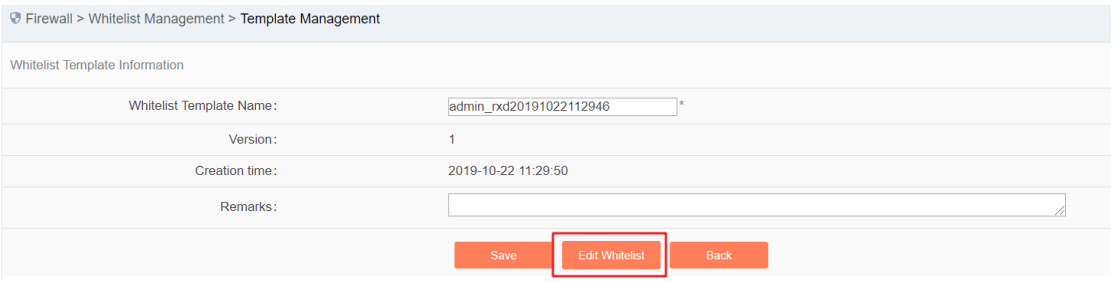


Fig.3-43 Whitelist Edit Button

OPC and Modbus protocols are used as examples to guide how to manage whitelist items. Other protocols will be similar but different in specific fields. Therefore, no more detailed description will be given here.

3.4.3.1. Add an OPC whitelist item.

After opening the [Template Management] of the whitelist, click <Edit> under the "Edit Whitelist" column and go to the specific rule edit page, click <Add> on the right of this page (as shown in Fig.3-44) to automatically add a new whitelist line at the bottom of the OPC whitelist item list (as shown in Fig.3-45):

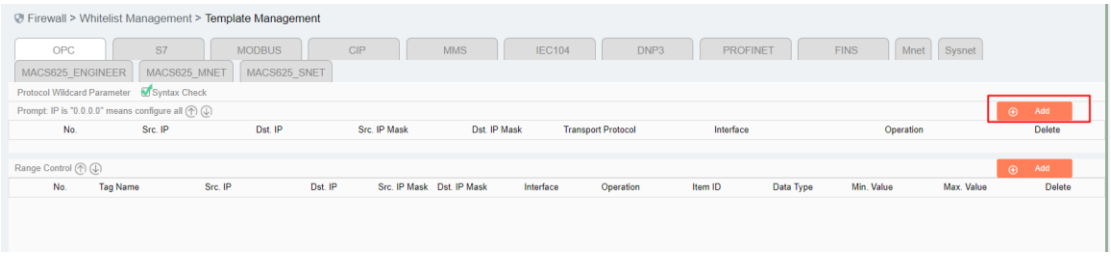


Fig.3-44 Whitelist Template Add Button

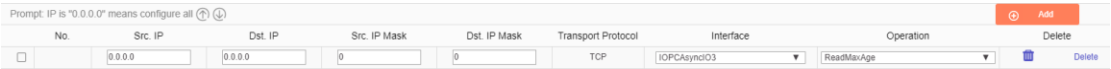


Fig.3-45 Whitelist Template Added Successfully

Tab.12 Instruction to OPC Whitelist Item Field

Column Names	Instructions
Src. IP	IP address to initiate an OPC data request, dotted in decimal format
Dst. IP	Destination IP address requesting the OPC data, dotted in decimal format
Src. IP mask	The mask of the source IP, with the value taken usually from 0 to 32
Dst. IP mask	The mask of the destination IP, with the value taken usually from 0 to 32
Interface	The name of an interface in the OPC protocol specification, taken from the drop-down box.
Operation (Method Name)	A method under a specific interface as defined in the OPC protocol specification, taken from the drop-down box.

Operation	Save	Save all modification information to the database and make it come into effect, and go back to the Whitelist Template Information List Display page
	Back	Ignore all modifications and go back to the Whitelist Template Information List Display page

3.4.3.2. View OPC whitelist items.

After entering the [Whitelist Template Rule Management] page, with OPC whitelist items displayed by default, click different TABs to display the whitelist items of corresponding tabs (as shown in Fig.3-46):

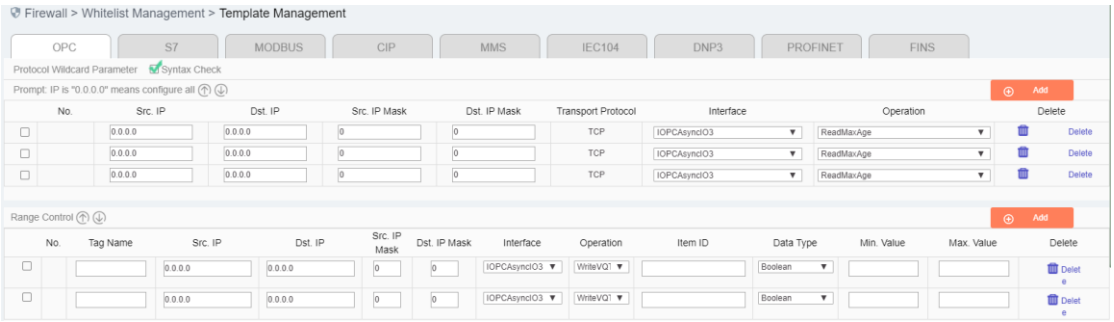


Fig.3-46 OPC Whitelist Information View Page

Click <Back> and go back to the [Whitelist Template List Display] page.

3.4.3.3. Modify an OPC whitelist item.

After entering the [Whitelist Template Rule Management] page, click the edit box under a whitelist item to change the source IP, destination IP, source IP mask, destination IP mask, interface name and method name of a whitelist item, click <Save> after the modification.

3.4.3.4. Modify an OPC range.

After entering the [Whitelist Template Rule Management] page, click the edit box under a whitelist item to change the point alias, source IP, destination IP, source IP mask, destination IP mask, interface name, method name, ItemID, data type, minimum and maximum, click <Save> after the modification.

3.4.3.5. Delete an OPC whitelist item.

After entering the [Whitelist Template Rule Management] page, click <Delete> on the far right of a whitelist

item to delete the corresponding whitelist item. (As shown in Fig.3-47):

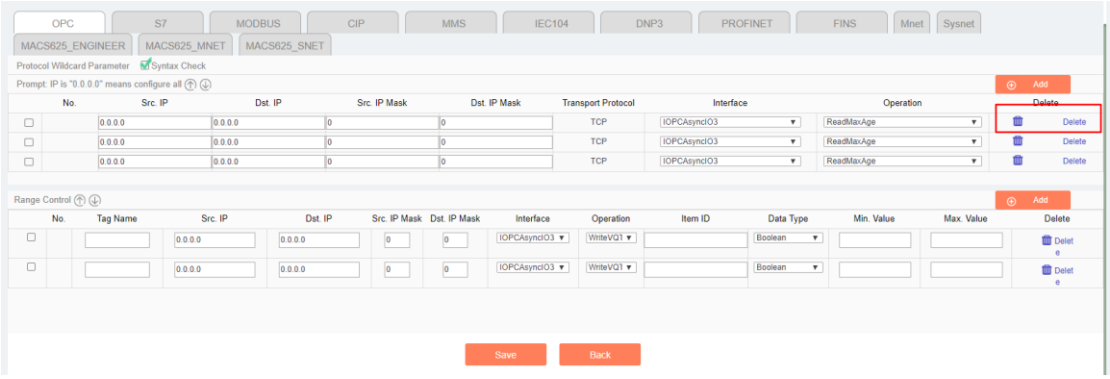


Fig.3-47 Whitelist Template Delete Button

3.4.3.6. Modbus protocol whitelist configuration

The resolving depth of Modbus protocol is different from other industrial protocols. Industrial firewalls can be resolved to a specific value transmitted by Modbus protocol. Therefore, the rule configuration of Modbus protocol in the whitelist template is mainly divided into three parts, namely protocol wildcard parameter, basic whitelist, and range control.

Notably, protocol wildcard parameters mainly have three check options as shown in the following diagram:

Fig.3-48 Modbus Protocol Wildcard Parameter Configuration Item

- Syntax Check

With this option enabled, messages will be discarded and alarm by default if they do not conform to protocol syntax in the protection mode. Other operation modes will not lose packets, but corresponding alarm information will be available in the alarm mode.

- Reset

After enabling this option, if any message is discarded, the industrial firewall will send a Reset message to both sides of Modbus communication to release connection resources.

- Connection Tracking Check

With this option enabled, messages will be discarded and alarmed by default if the connection status is abnormal in the protection mode. Other operation modes will not lose packets, but corresponding alarm information will be available in the alarm mode.

3.4.3.7. Basic Modbus whitelist items

The configuration here is similar to that of the OPC protocol. Refer to the OPC protocol related parameter configuration method.

3.4.3.8. Modbus range control

Check the Global Enable option first by using Modbus range control, (as shown in Fig.3-49):

Fig.3-49. Modbus Range Enable Item

After enabling range control, the following byte order can be edited. It is recommended to use the default configuration and adjust it accordingly if the default configuration does not match the site.

"Point table configuration" is the most important for the range function. The meanings of each field in point table configuration are explained in the following table.

Tab.13 Instruction to Modbus Click Field

Column Names	Instructions
Tag Name	A meaningful alias that represents an address in Modbus
Src. IP	IP address to initiate an OPC data request, dotted in decimal format
Dst. IP	Destination IP address requesting the OPC data, dotted in decimal format
Src. Mask	The mask of the source IP, with the value taken usually from 0 to 32
Dst. Mask	The mask of the destination IP, with the value taken usually from 0 to 32
Function	Modbus protocol function code
Address	The starting address of a point operated by the Modbus protocol
Data Type	The data type of points
Offset	The offset in the address for a specific type of data that is operated based on some function codes, for example: when the data type as operated based on 06 Function Code is of the BOOL type, it needs to specify which bit in the address indicates the BOOL value, with 0 taken by default
High8/Low8	Which byte is used in the address when operating a specific type of data based on some function codes, for example, when the data type as operated based on 06 Function Code (which can operate a 2-bit address) is of the Byte type (1-bit), it needs to specify which bit (8-bit) in the operated address, which is high 8 bits by default
Min. value	Minimum value that is allowed to operate
Max. value	Maximum value that is allowed to operate

For adding, modifying, editing, and deleting a range rule item, please refer to the basic Modbus item operation.

3.4.3.9. Whitelist rule item learning append.

Either learned or manually created whitelist templates can be appended with new learned rules when the learning is completed.

Firstly, switch the industrial firewall to be learned again to Learning Mode. For specific operation, please refer to 3.3.2.2 Modification.

Then, after the appropriate learning process, switch the industrial firewall to Learning Completion. In this case, the operation mode of the [Firewall Information Modification] page will provide existing whitelist templates in the system, (as shown in Fig.3-50):

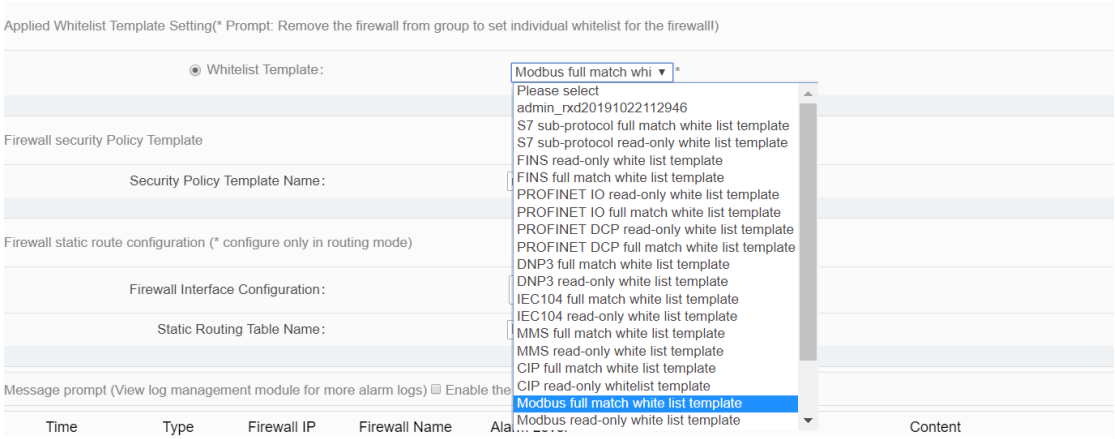


Fig.3-50 Select Existing Whitelist Templates in Case of Learning Completion

When selecting one of the templates and clicking <Save>, the newly learned whitelist rule item will automatically remove the duplicated ones and be added to the selected whitelist template. If there are more than 3000 industrial protocol rules in the template, the template will be highlighted in red in the [Template Management] page, as shown in Fig.3-51, and cannot be distributed to the industrial firewall. The user needs to manually merge the templates highlighted in red below to less than 3,000 entries before distributing them to the industrial firewall.

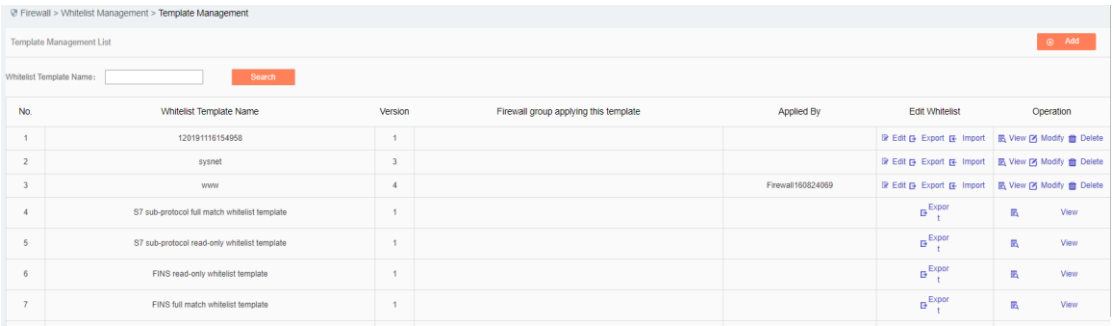


Fig.3-51 One of the Templates with over 3,000 Protocol Rules

3.5. Route Management

3.5.1.Introduction to Functions

In the user network, the board card, as a router device, is not directly connected with other router devices. Instead, the board card forwards data to the network segment where each interface is located. In this case, it is unnecessary to configure the static route table, only to configure the interface IP instead. The network segments where an interface is located can forward data mutually.

In the user network, the board card, as a router device, is connected with some interfaces of the device and the interface of other router device. In this case, the board card forwards data from another network segment s (not the network segment where the interface is located). It is necessary to configure the interface IP and the static route table. The network segments where an interface is located can forward data mutually.

3.5.2.Static Route

3.5.2.1. Page navigation

After logging in the management platform, the configuration administrator clicks [Firewall] to find [Route Management] on the left side of the navigation bar, as shown in the figure.

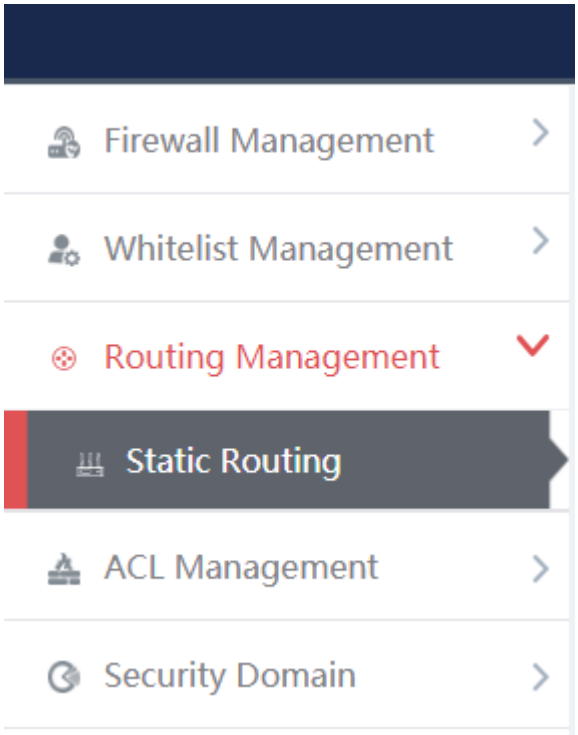


Fig.3-52 Static Route Navigation

3.5.2.2. Retrieve a static route management list.

In the [Static Route Management List] display list page, retrieve the static route management list according to the screening conditions, as shown in the figure

Fig.3-53 Screening Conditions for Static Route Table

3.5.2.3. Add the static route management list.

In the [Static Route Management List] display list page, click [Add] to add a new static route table template, as shown in the figure

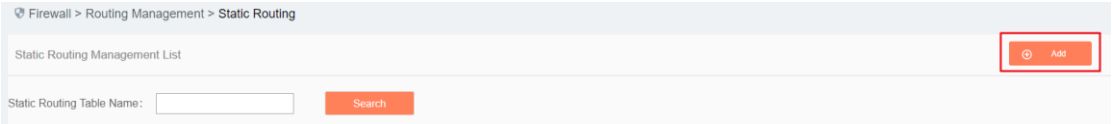


Fig.3-54 Add the Static Route Management Template

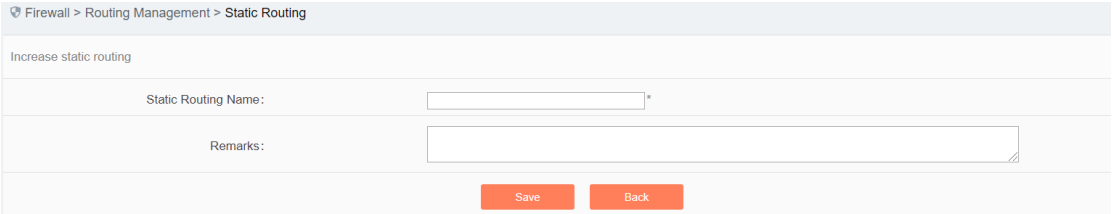


Fig.3-55 Add the Static Route

Tab.14 Instruction to Adding a Static Route Template

Column Names	Instructions	
Static Route Name	The template name allows only Chinese characters, numbers, letters, underscores, and hyphens, with a total length cannot exceed 32 characters	
Remarks	Add the remark information for the template	
Operation	Save	Save the added template
	Back	Go back to the template display list page without saving it

3.5.2.4. Edit a static route management list.

In the [Static Route Management List] display list page, click [Edit] to edit the static route configuration of the static route table template, as shown in the figure

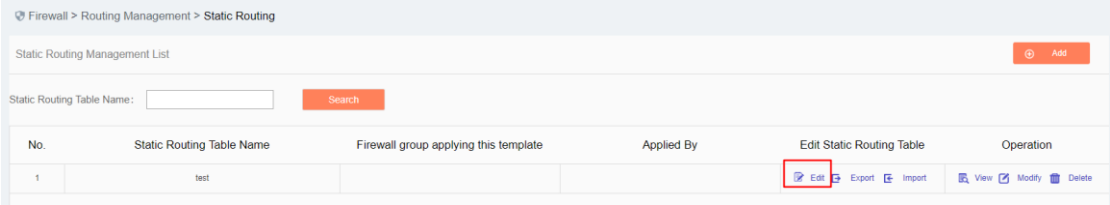


Fig.3-56 Edit a Static Route Table Template

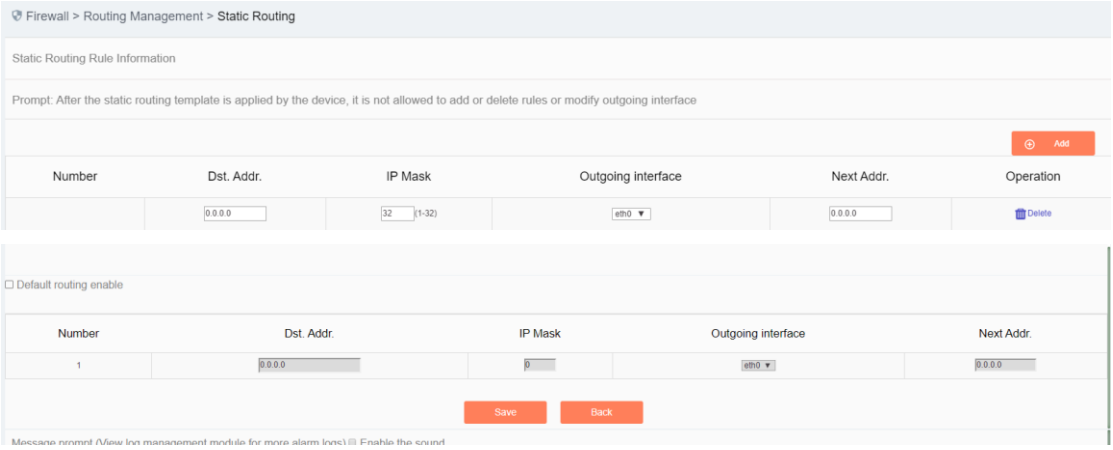


Fig.3-57 Static Route Rule Information

Tab.15 Instruction to Filling in Static Route Rule Items

Column Names	**Instructions**	
Dst. Addr.	Legitimate IP address	
IP Mask	Numbers 1-32	
Outgoing interface	Outgoing interface content	
Next Addr.	Legitimate IP address	
Operation	Add	Add the static route rule information
	Default routing enable	Allow to edit default route enable
	Save	Save the static route rule information
	Back	Go back to the static route template list page without saving it

Tab.16 Content of Default Route Enable List

Column Names	**Instructions**
Dst. Addr.	Legitimate IP address
IP Mask	Numbers 1-32
Outgoing interface	Outgoing interface content

Next Addr.	Legitimate IP address

3.5.2.5. Export the static route management list.

Click <Export> under the operation column in the [Static Route Management List] template display list, export the whitelist information list of the template in Excel format.

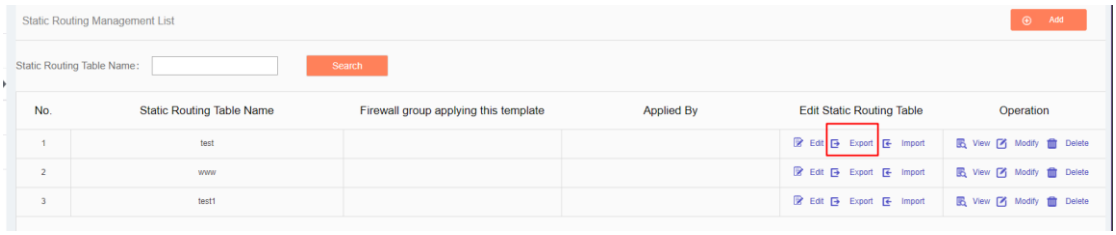


Fig.3-181 Export Static Route Table Template

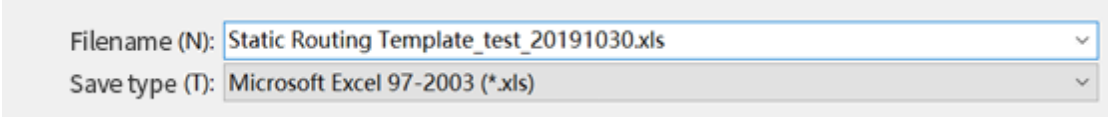


Fig.3-58 Excel Generated by Static Route Table

3.5.2.6. Import a static route management list.

Role: import [Policy Template Rule Information] in Excel format

Click <Import> under the operation column in the [Template Management List] template display list to pop up the [Import Excel] page.

1） Click [Select File] to select an edited Excel template

2） Click <Import Excel> to execute the import operation.

3） Click <Close> to abandon the import operation, close the [Excel import] page.

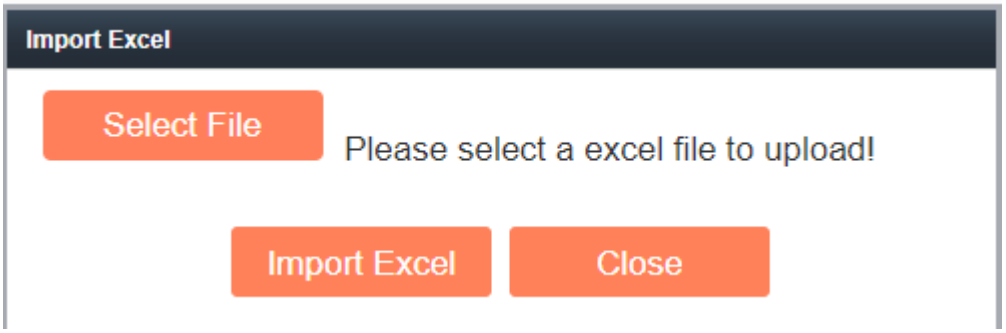


Fig.3-59 File Selection

3.5.2.7. View a static route management list

Click <View> under the operation column in the [Static Route Management List] template display list to display the static route information as shown in the figure

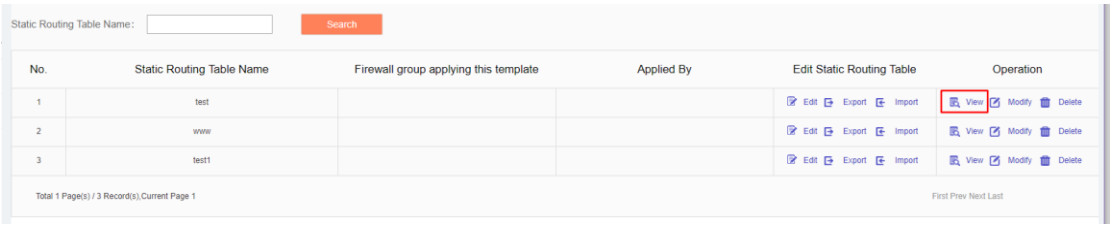


Fig.3-60 View the Static Route Table

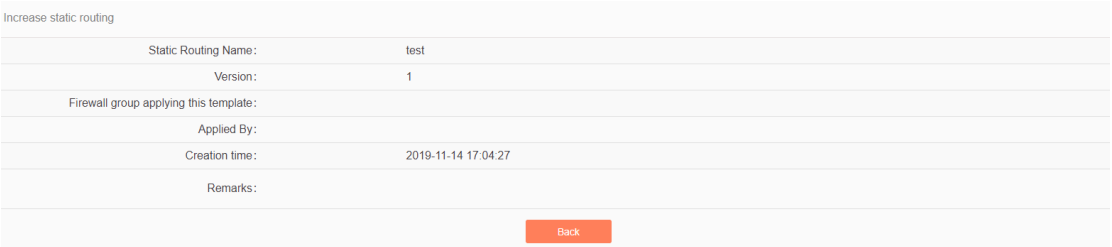


Fig.3-61 Static Route Information

Click <Back> and go back to the static route management list page.

3.5.2.8. Modify a static route management list.

Click <Modify> under the operation column in the [Static Route Management List] template display list to display the static route information as shown in the figure

Fig.3-62 Modify the Static Route Table

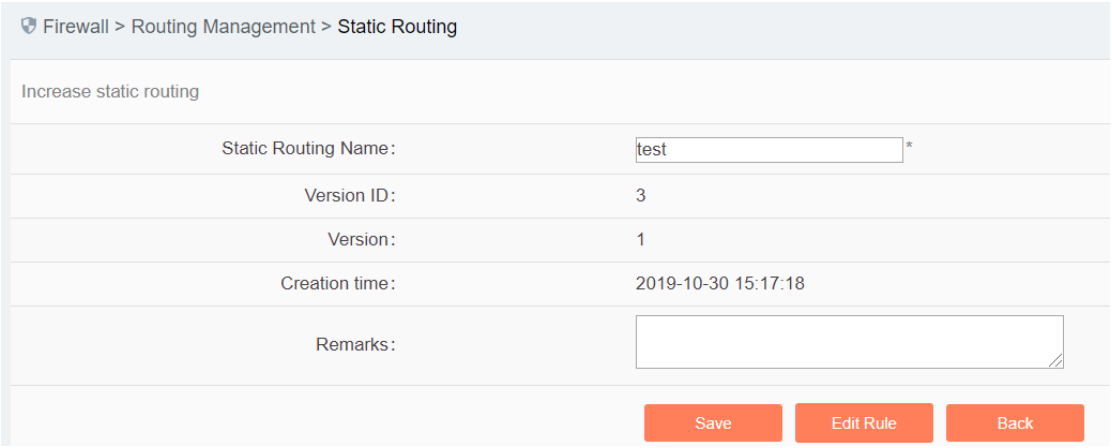


Fig.3-63 Static Route Information

Tab.17 Instruction to Static Route Modification Page Buttons

Column Names	**Instructions**	
Operation	Save	Save the modified static route information
	Edit Rule	Enter the static route rule information page

	Back	Go back to the static route template list page without saving it

3.5.2.9. Remove the static route management list.

In the [Static Route Management List] display list page, click [Delete] to delete the static route template, as shown in the figure

Fig.3-64 Static Route Table Template

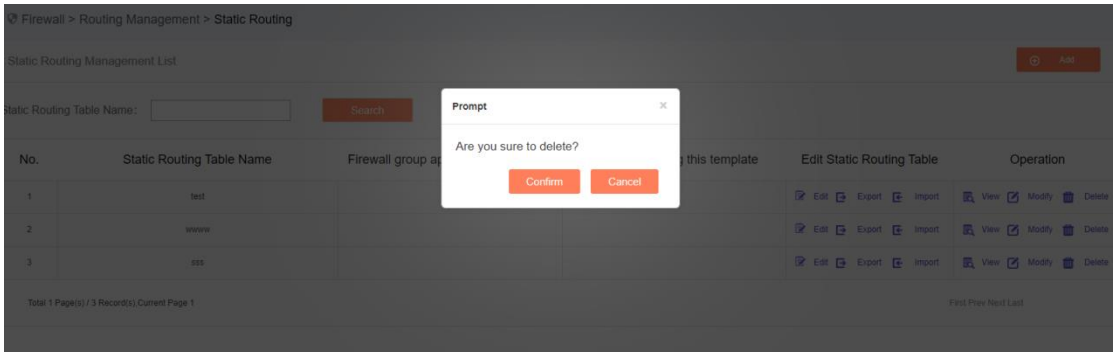


Fig.3-65 Confirmation Box

Click <Cancel> to abandon the deletion or click <Confirm> to execute the delete operation.

3.6. ACL Management

3.6.1. Introduction to Functions

As a type of firewall products, the built-in firewall management function of industrial firewalls is one of its basic functions. Currently, industrial firewalls adopt the status detection firewall mechanism to achieve the corresponding security control.

Here is a brief introduction to the status detection firewall. It adopts the status detection packet filtering technology, which is an extension of traditional packet filtering. The status detection firewall has a check engine interception data packet at the network layer, and it extracts information on the status of the application layer, based on which a decision is made on whether to accept or reject the connection. This technology provides a highly secure solution with good adaptability and scalability. The status detection firewall also typically includes agent-level services that provide additional support for application-specific data content. The status detection technology is optimal to provide limited support for UDP protocol. It treats all UDP packets passing through the firewall as a virtual connection. When the reverse response group arrives, a virtual connection is deemed as having been established. The status detection firewall overcomes the limitations of packet filtering firewalls and application proxy servers. It detects the addresses of "to" and "from", requiring no agent for each application accessed to.

3.6.2.Security Policy Template Management

Click [ACL Management/Security Policy] in the left navigation bar (as shown in Fig.3-66), go to the [Security Policy Management] page (as shown in Fig.3-67):

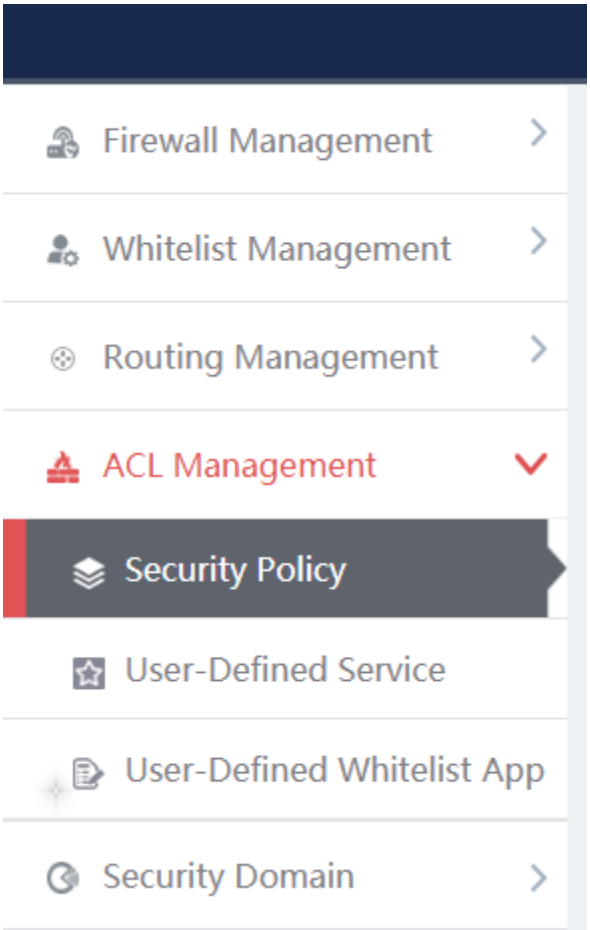


Fig.3-66 Selecting Security Policy Management

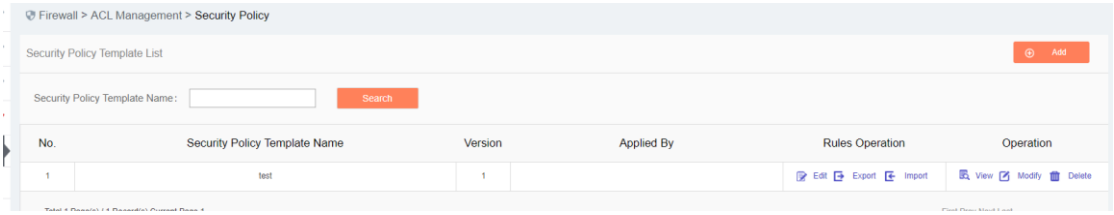


Fig.3-67 Security Policy Management

View the information on all security policy templates in the system, with the meanings given below:

Tab.18 Instruction to Security Policy Template List Display

Column Names	Instructions

Security Policy Template Name	A security policy template name that is easy to remember, for example "6#DCS Inbound Security Policy Template"	
Version	The version of security policy template, the version and the template ID uniquely determine a set of security policy rules. The version number will automatically +1 after each time the security policy is edited and saved	
Applied By	All independent industrial firewalls that are using this security policy template	
Rules Operation	Edit	Click to enter the specific security policy rule item edit page
	Export	Click and then export the current security policy rule in Excel format
	Import	Click to import the security policy rule in Excel format to the current security policy rules
Operation	View	View more detailed information on security policy templates
	Modify	Modify and set the information on security policy templates
	Delete	Delete a security policy template. The security policy template in use cannot be deleted

3.6.3.Add a Security Policy Template

Open [Firewall Management/Security Policy Management], find <Add> on the right in [Security Policy Template List], click it to pop up the security policy template add page (as shown in Fig.3-68):

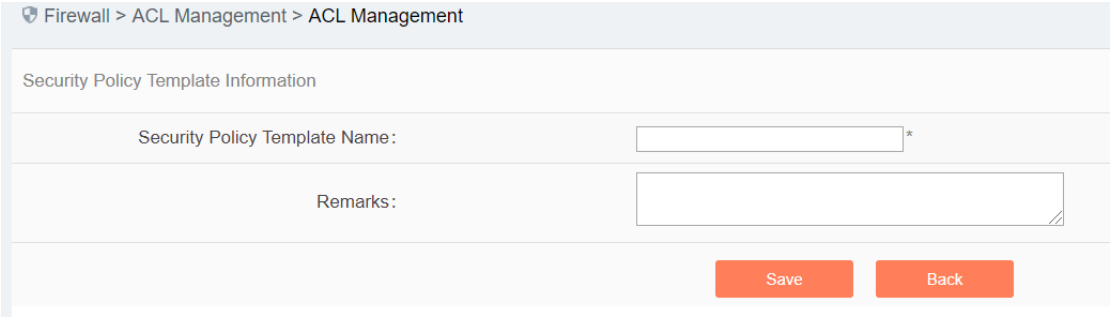


Fig.3-68 Security Policy Template Add Page

Tab.19 Instruction to Security Policy Template Add Information

Column Names	Instructions
Security Policy Template Name	Define a security policy template name that is easy to understand and remember

Remarks	Optional, additional explanatory information

3.6.3.1. Information view

Click <View> under the operation column in the [Firewall Management/Security Policy Management] template display list to display the detailed information on security policy templates (as shown in Fig.3-69):

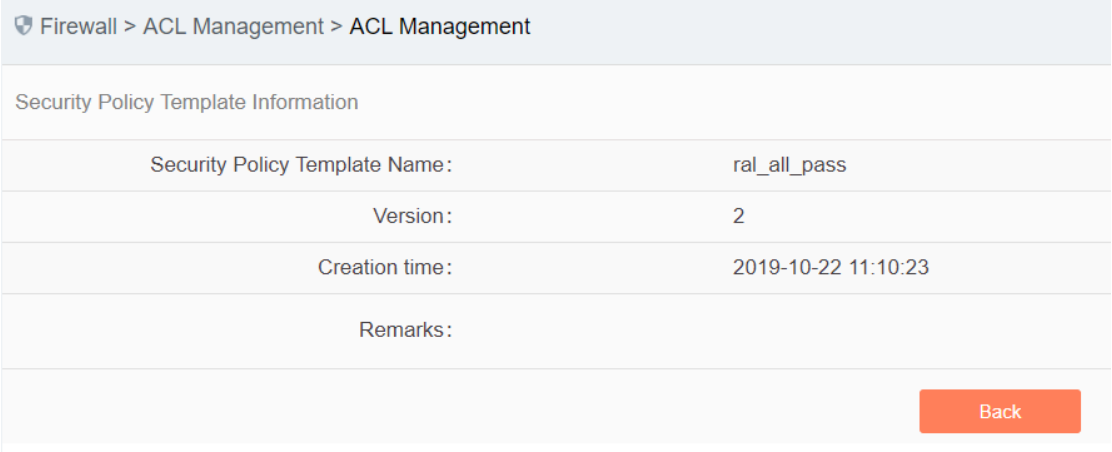


Fig.3-69 Security Policy Template Information View Page

Click <Back> and go back to the return to the [Security Policy Management] page.

3.6.3.2. Modify a security policy template.

Click <Modify> under the operation column in the [Security Policy Management] security policy template list to open the [Security Policy Template Information] modification page, which can modify the basic information on security policy templates (as shown in Fig.3-70):

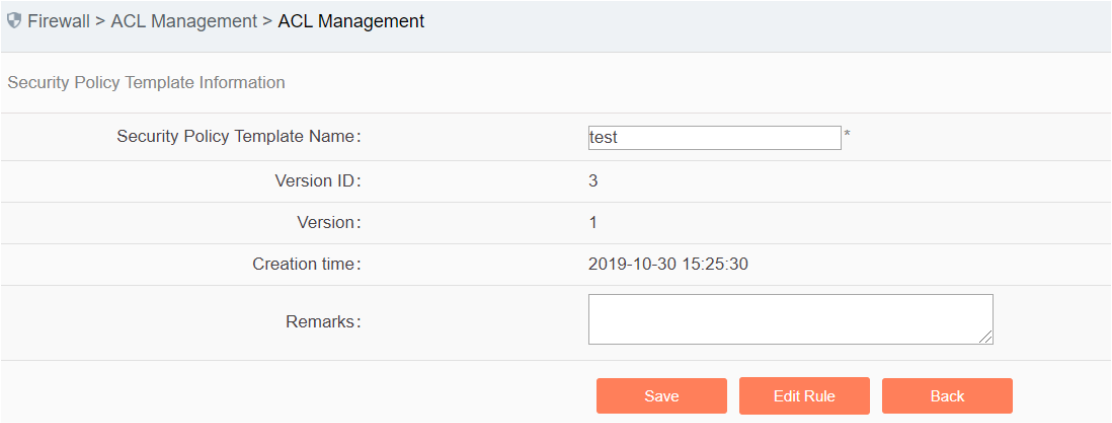


Fig.3-70 Security Policy Template Modification Page

Tab.20 Instruction to Security Policy Template Modification Information

Column Names	Instructions

Security Policy Template Name	Modify the name of the security policy template	
Remarks	Optional, additional explanatory information	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the [Security Policy Management] page
	Edit Rule	Click to enter the specific security policy rule item edit page
	Back	Ignore all modifications and go back to the [Security Policy Management] page

3.6.3.3. Delete a security policy template.

Click <Delete> under the operation column in the [Security Policy Management] security policy template list to delete security policy template that are not used any longer.

Note: the template cannot be deleted if it is being used by an industrial firewall or an industrial firewall group.

3.6.3.4. Retrieve a security policy template.

In the [Security Policy Management] display list page to retrieve a security policy template based on conditions. (As shown in Fig.3-71):

Fig.3-71 Retrieve a Security Policy Template

3.6.4. Security Policy Template Rule Item Management

The management of security policy rule items is the core of security policy management. All templates depend on each specific security policy rule item.

To enter the [Security Policy Rule Item Management], click <Edit> under the security policy rule maintenance column in the [Security Policy Management] display list, or click <Edit Rule> after entering the [Security Policy Template Information] modification page (as shown in Fig.3-72):

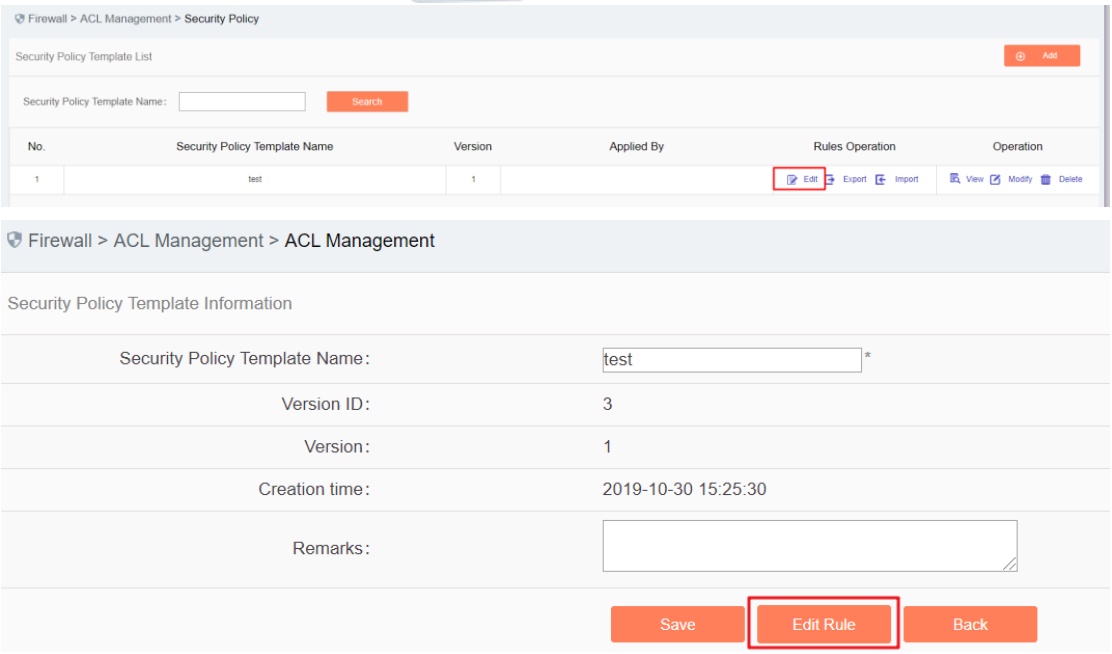


Fig.3-72 Security Policy Rule Edit Button

3.6.4.1. Add a security policy rule.

After entering the [Policy Template Rule Information] page, click <Add> on the right (as shown in Fig.3-73) to automatically add a line of new rules at the bottom of the security policy rule list (as shown in Fig.3-74):

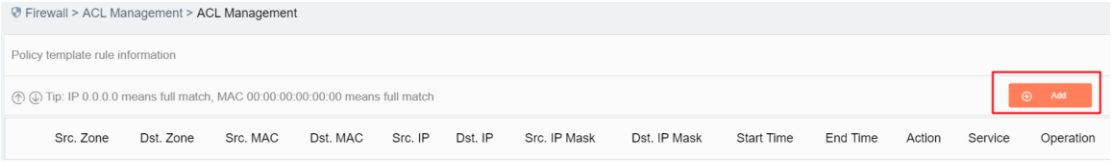


Fig.3-73 Security Policy Rule Add Buttons

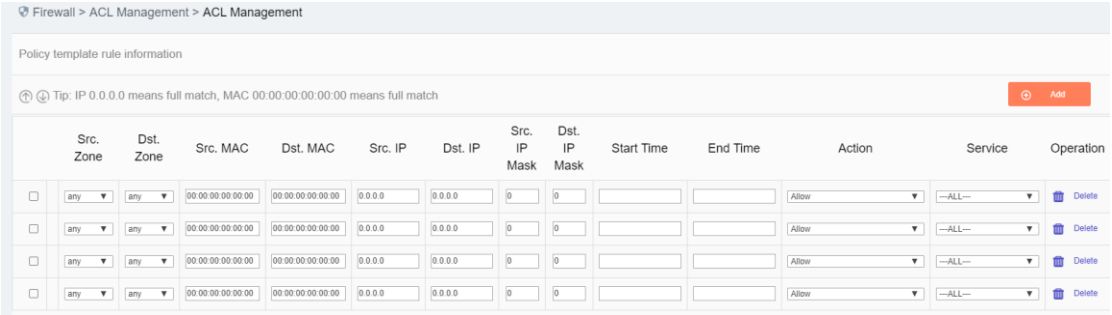


Fig.3-74 New Security Policy Rules

Tab.21 Instruction to Security Policy Rule Fields

Column Names	Instructions
Src. Zone	The security area initiating a data request, with "any" indicating full match
Dst. Zone	The destination security area for the data request, with "any" indicating full match

Src. MAC	The MAC address initiating a data request, in format of "00:00:00:00:00:00"	
Dst. MAC	The destination MAC address requesting the data, in the format of "00:00:00:00:00:00"	
Src. IP	The IP address initiating a data request, in dotted decimal format	
Dst. IP	The destination IP address requesting data, in dotted decimal format	
Src. IP mask	The mask of the source IP, with the value taken usually from 0 to 32	
Dst. IP mask	The mask of the destination IP, with the value taken usually from 0 to 32	
Start Time	The starting point-in-time at which the rule takes effect	
End Time	The last point-in-time at which the rules are no longer valid	
Action	When the rule is hit, the firewall processes the packet, passes, blocks, or passes and logs it	
Service	The service types supported by the rule	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the security policy management template list display page
	Back	Ignore all modifications and go back to the security policy management template information list display page

3.6.4.2. View a security policy rule item.

After entering the [Policy Template Rule Information] page to view the specific security policy rule item under the current policy template. (As shown in Fig.3-75):

Fig.3-75 Security Policy Rule Item Information View Page

If the template is new, the rule item is blank when viewed, and the rules can be viewed after completing the corresponding add operation as per the following section. Click <Back> and go back to the [Security Policy Management] template list display page.

3.6.4.3. Modify a security policy rule.

After entering the [Policy Template Rule Information] page, click the edit box under a specific security policy rule to modify the source Security Zone, destination Security Zone, source MAC, destination MAC, source IP, destination IP, source IP mask, destination IP mask, start time, end time, an execution action and service of a specific security policy rule, click <Save> after the modification.

3.6.4.4. Delete a security policy rule.

After entering the [Policy Template Rule Information] page, click the <Delete> on the far right of a specific security policy rule to delete the corresponding security policy rule. (As shown in Fig.3-76):

Fig.3-76 Security Strategy Rule Delete Button

Click <Save> after deleting it.

3.6.5. User-Defined Service

In addition to using services pre-defined by the management platform, users can also define their own services provided by other servers in the network.

Click [ACL Management/User-Defined Service] in the left navigation bar (as shown in Fig.3-77) to open the [User-Defined Service] page.

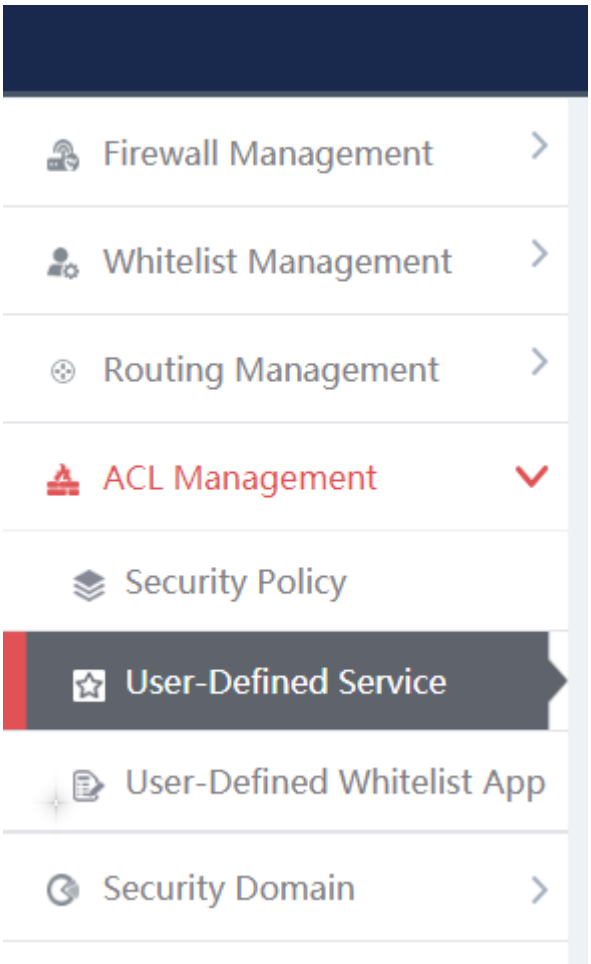


Fig.3-77 Selecting a custom service.

3.6.5.1. **Add a User-Defined service.**

After entering the [User-Defined Service] page, click <Add> on the right (as shown in Fig.3-78) to pop up the custom service add page (as shown in Fig. 3-79):

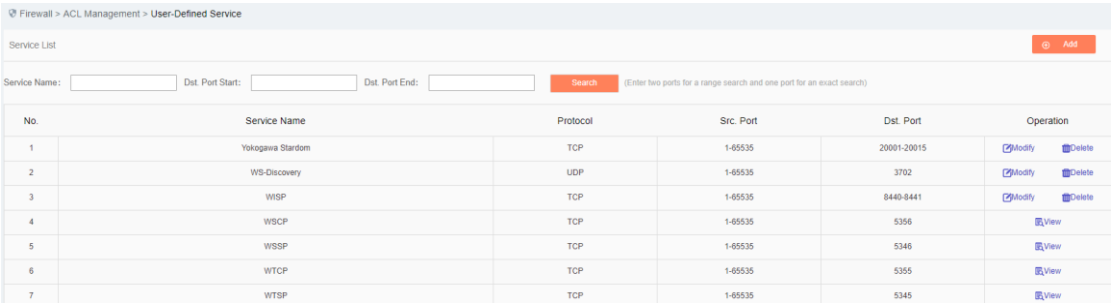


Fig.3-78 Custom Service Add Button

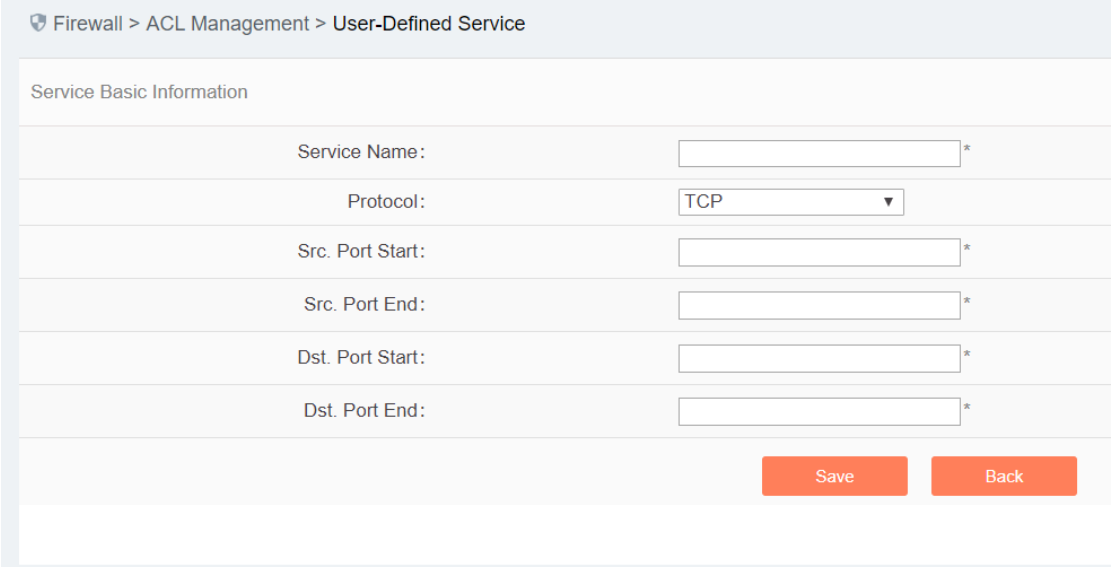


Fig.3-79 Custom Service Add Page

Tab.22 Instruction to custom service Add Fields

Column Names	**Instructions**	
Service Name	The custom application name that cannot conflict with an existing one	
Protocol	Drop down to select the transport layer protocol on which the service depends	
Src. Port Start	The source start port used by the service, from 1 to 65535, enter 1 if not available	
Src. Port End	The Source end port used by the service, from 1 to 65535, enter 65535 if not available	
Dst. Port Start	The destination start port used by the service, from 1 to 65535	
Dst. Port End	The destination end port used by the service, from 1 to 65535, same to that of the destination start port if there is only one port	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the custom service list display page
	Back	Ignore all modifications and go back to the custom service list display page

3.6.5.2. View a user-defined service.

After entering the [User-Defined service] page to view the built-in and customized services of the current system. (As shown in Fig.3-80):

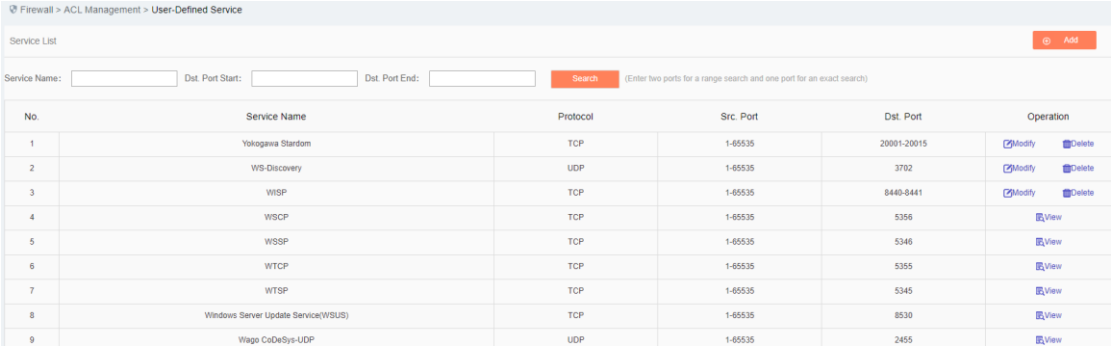


Fig.3-80 Custom service Information View Page

3.6.5.3. Modify a user-defined service.

After entering the [User-Defined service] page, click <Modify> under the operation column TO modify the custom service and modify the page (as shown in Fig.3-81):

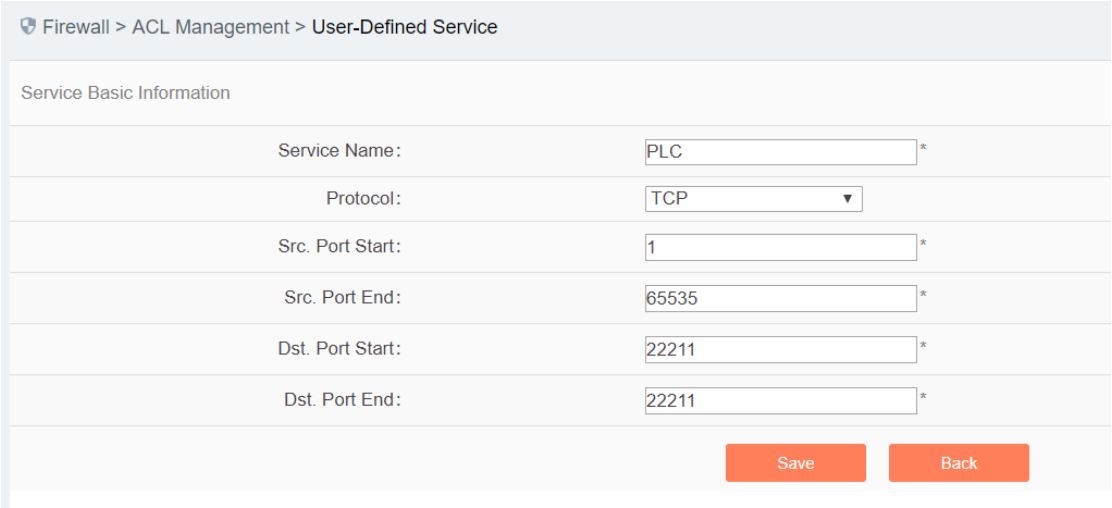


Fig.3-81 Custom service Modification Page

See 3.6.5.1 Adding a custom service for the meaning of each field.

3.6.5.4. Delete a user-defined service.

After entering the [User-Defined service] page, click <Delete> on the far right of a user-defined service to delete the corresponding custom service. (As shown in Fig.3-82):

Fig.3-82 Custom service Delete Button

Note: custom services that are being used by a security policy cannot be deleted

3.6.6.User-Defined Whitelist Applications

In certain industrial sites, the protocol running in the application layer and the port running by default for the protocol may have changed. In this case, it may not accurately identify an industrial protocol simply by opening the default port specified in the protocol in the firewall security policy rules or adopting the traditional DPI technology. Therefore, AVCOMM industrial firewalls can solve the above problem by adding custom whitelist applications.

Click [ACL Management/User-Defined Whitelist App] in the left navigation bar (as shown in Fig. 3-83) to open the [User-Defined Whitelist App] page (as shown in Fig.3-84):

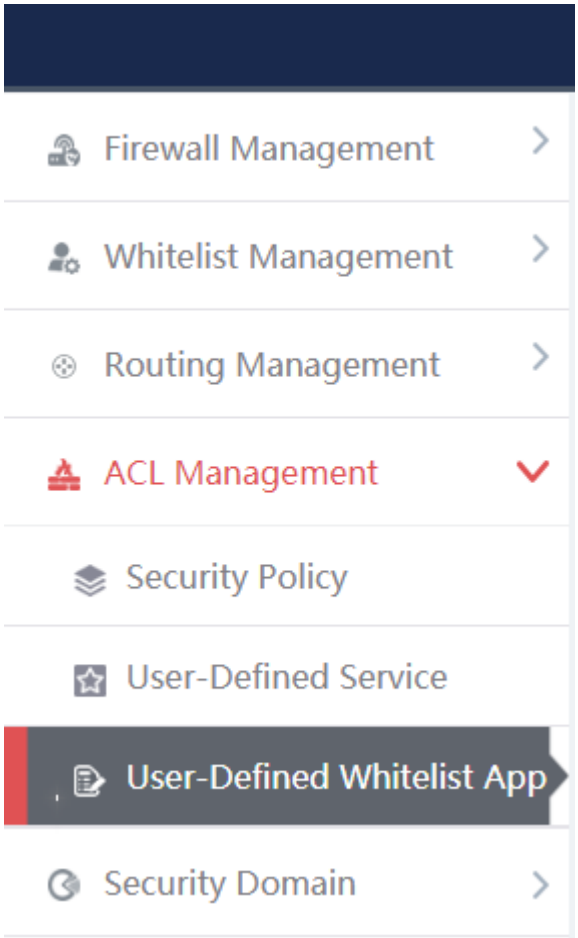


Fig.3-83 Selecting a User-Defined Whitelist Application

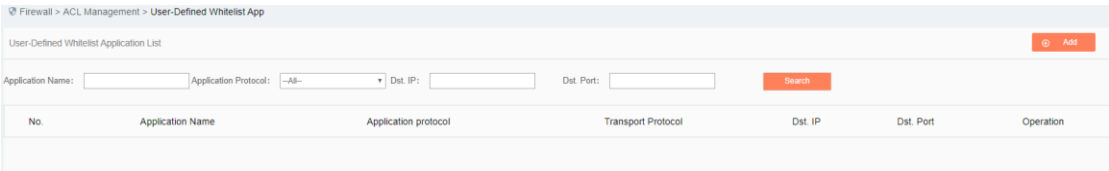


Fig.3-84 Selecting a User-Defined Whitelist Application

3.6.6.1. Add a User-Defined Whitelist Application

After entering the [User-Defined Whitelist Application] page, click <Add> on the right (as shown in Fig.3-85) to pop up the user-defined whitelist application add page (as shown in Fig.3-86):

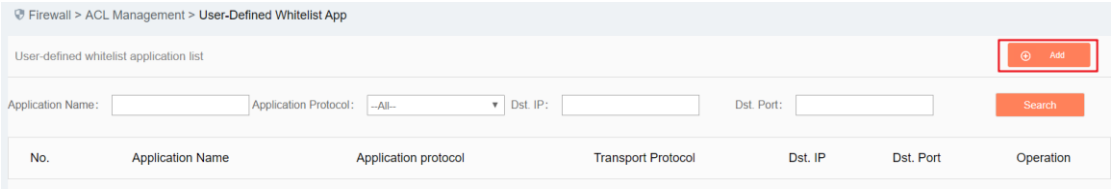


Fig.3-85 User-Defined Whitelist Application Add Button

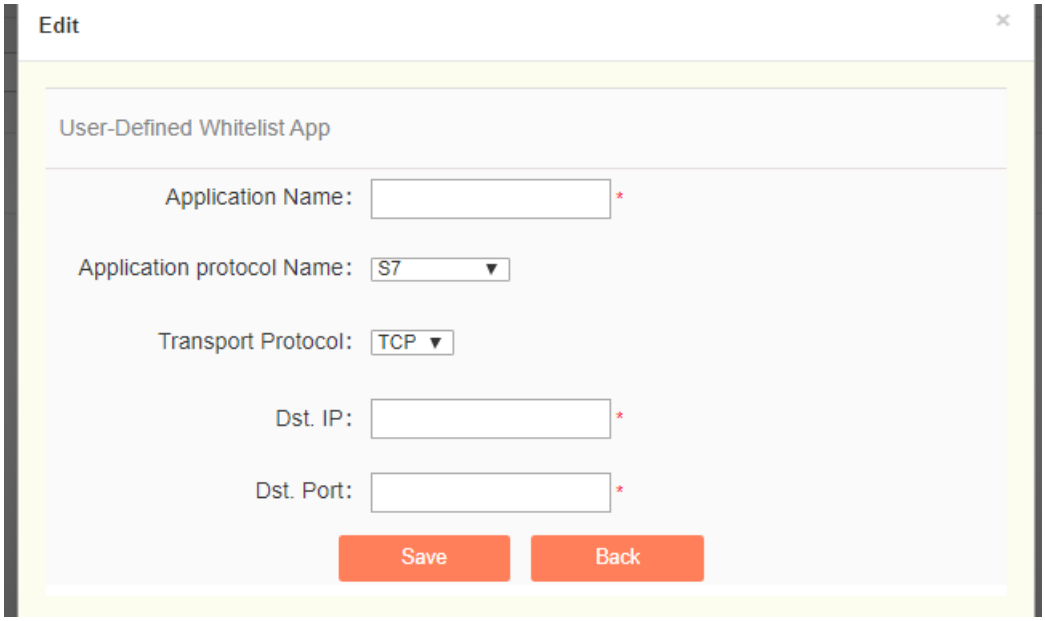


Fig.3-86 User-Defined Whitelist Application Add Page

Tab.23 Instruction to Custom Whitelist Application Add Fields

Column Names	Instructions	
Application Name	The custom whitelist application name that cannot conflict with the existing one	
Application protocol Name	Drop down to select the industrial protocol with the application layer to be customized	
Transport Protocol	Drop down to select the transport layer protocol on which the service depends	
Des. IP	Provide the device IP address of the industrial protocol server	
Dst. Port	A new port to replace the default port for this industrial protocol	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the custom whitelist application list display page
	Back	Ignore all modifications and go back to the custom whitelist application list display page

3.6.6.2. View a user-defined whitelist application.

After entering the [user-defined Whitelist Application] page to view the current user-defined whitelist applications. (As shown in Fig.3-87):

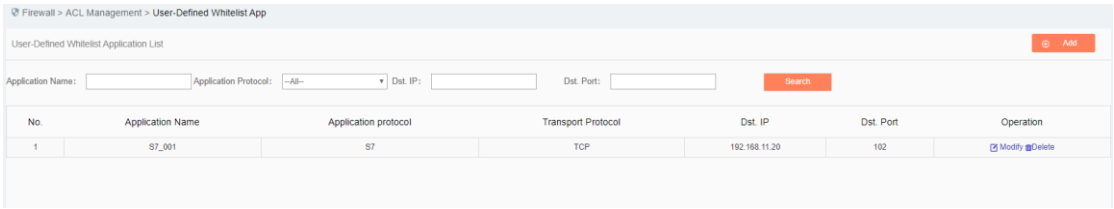


Fig.3-87 User-Defined Whitelist Application Information View Page

3.6.6.3. Modify a custom whitelist application.

After entering the [User-Defined Whitelist Application] page, click <Modify> under the operation column to modify the user-defined whitelist application and modify the page (as shown in Fig. 3-88):

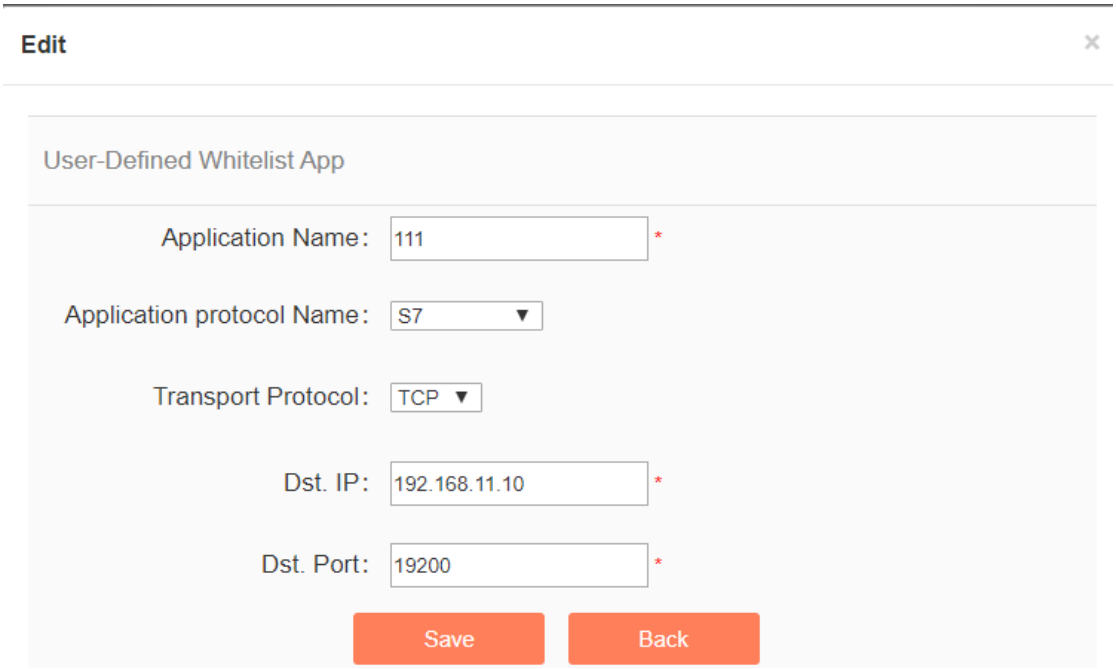


Fig.3-88 User-Defined Whitelist Application Modification Page

See 3.6.6.1 Adding a User-Defined Whitelist Application for the meaning of each field.

3.6.6.4. Delete a user-defined whitelist application.

After entering the [User-Defined Whitelist Application] page, click the <Delete> on the right of a custom whitelist application to delete the corresponding custom whitelist application. (As shown in Fig.3-89):

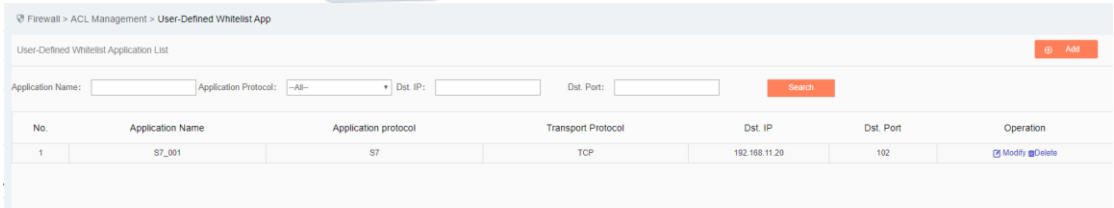


Fig.3-89 User-Defined Whitelist Application Delete Button

Note: user-defined whitelist applications that are being used by a security policy cannot be deleted

3.7. Security Domain Management

3.7.1.Introduction to Functions

The traditional interface-based policy configuration mode needs to configure security policies for each interface, which brings a great burden to the network administrator. The maintenance workload of security policies increases exponentially, thus increasing the probability of security risks introduced due to the configuration. Different from the traditional interface-based policy configuration mode, mainstream firewalls in the industry solve the above problems by configuring security policies around the Security Domain.

A so-called Security Domain is an abstract concept, which can be divided into two ways:

- By interfaces.

The Security Domain can include three layers of common physical interfaces and logical interfaces and can also include two layers of physical Trunk interfaces +VLAN. Interfaces that are of the same Security Domain generally have consistent security requirements in view of security policy control.

- By IP addresses.

The Security Domain that is divided by IP address realizes security policy control according to the source IP address or destination IP address of a service message.

With the introduction of the Security Domain concept, the security administrator can implement layered policy management by classifying interfaces or IP addresses with the same security requirements (into different domains). By introducing the Security Domain concept, it not only simplifies the policy maintenance complexity, but also realizes the separation of network service and security service.

The management platform adopts interface division to realize Security Domain management.

3.7.2.Add a Security Domain

Click <Add> (as shown in Fig. 3-90) on the right of the [Security Domain Management] Security Domain list tab to pop up the Security Domain add page. (As shown in Fig.3-90):

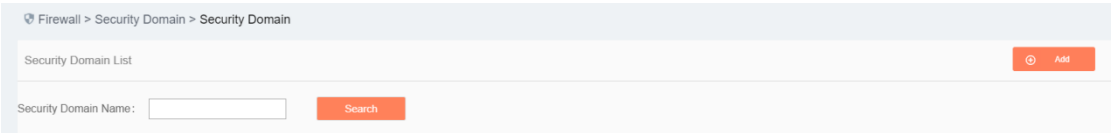


Fig.3-90 Security Domain Add Button

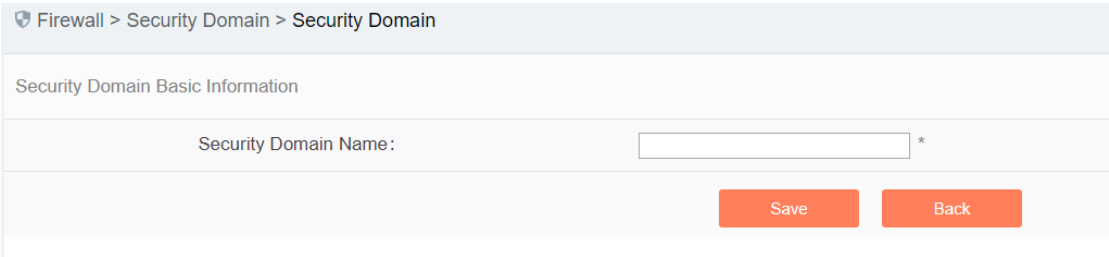


Fig.3-91 Security Domain Add Page

Tab.24 Instruction to Security Domain Add Information

Column Names	Instructions
Security Domain Name	A Security Domain name that is easy to remember

3.7.3.View a Security Domain

Click [Security Domain/Security Domain] in the left navigation bar, enter the [Security Domain] page (as shown in Fig.3-92):

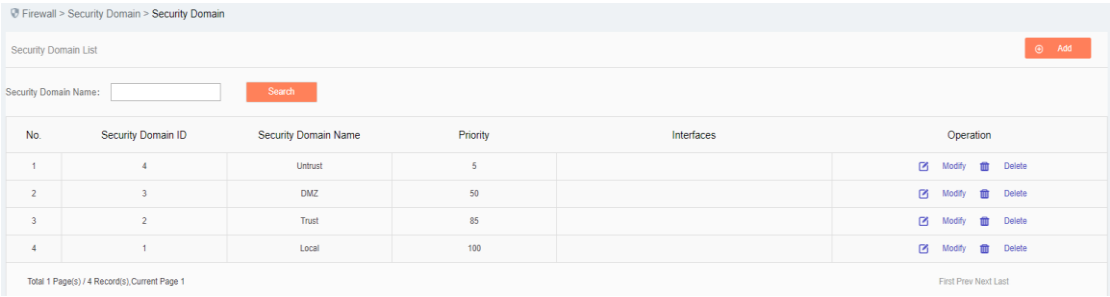


Fig.3-92 Security Domain Management Page

There are two basic Security Domain types, that is, Security Domains built in by the system, and Security Domains created by a user himself. The former only allows to modify the priority, including these two properties of firewalls; the latter can modify all other properties except ID. View all the Security Domain information in the system here, with the following meanings given as below:

Tab.25 Instruction to Security Domain List Display

Column Names	Instructions	
Security Domain ID	The unique identification number of a Security Domain, which is automatically assigned by the system	
Security Domain Name	A Security Domain name that is easy to remember	
Priority	Set the priority of a Security Domain	
Interfaces	All industrial firewall interfaces contained in a Security Domain	
Operation	Modify	Modify and set the Security Domain information

	Delete	Delete a Security Domain

3.7.4.Modify a Security Domain

Click <Modify> under the operation column in the [Security Domain Management] Security Domain list to open the [Security Domain Basic Information] modification page (as shown in Fig. 3-93), which can modify the basic information on the Security Domain.

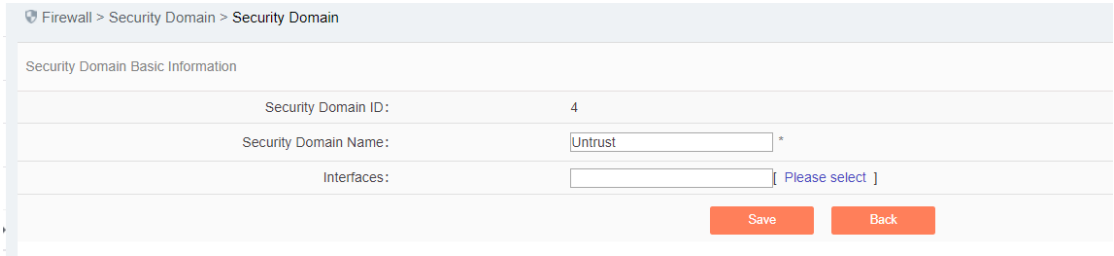


Fig.3-93 Information on Security Domain Modification

The most important thing here is to modify the corresponding interface of the Security Domain. Click <Please select> in the [Security Domain Basic Information] page to pop up the page for selecting interfaces included in a Security Domain, (as shown in Fig.3-94):

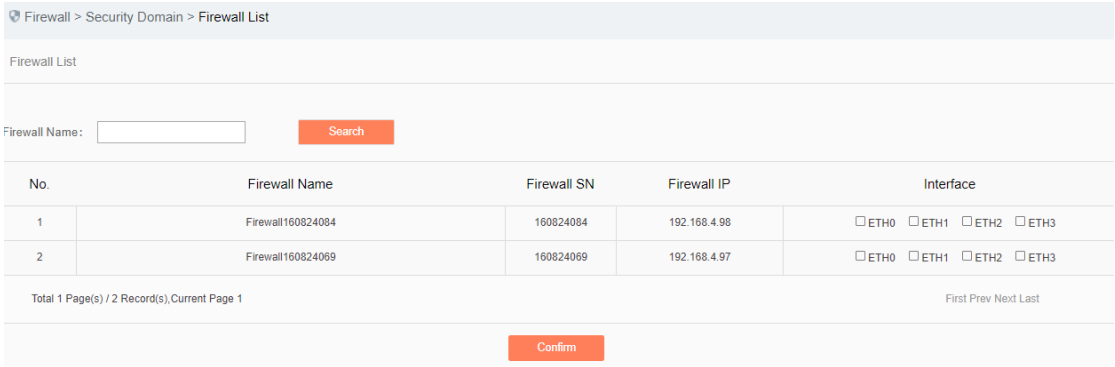


Fig.3-94 Selecting Firewall Interfaces Included in a Security Domain

For an interface corresponding to a specific industrial firewall that is included in a Security Domain, the network connected to such an interface shall be the Security Domain.

For example:

If the Security Domain Trusted contains ETH1, the interface for "Industrial Firewall, Production Domain 1", and a security policy includes a pass policy from Trusted to any Security Domain, then it means that all sessions initiated from ETH1 can pass.

3.7.5.Delete a Security Domain

Click <Delete> under the operation column in the [Security Domain Management] Security Domain list to delete the Security Domain that is no longer used.

Note: The Security Domain built into the system cannot be deleted, nor can the Security Domain being used by the security policy rules.

3.7.6.Retrieve a Security Domain

In the [Security Domain Management] security display list page, a Security Domain can be retrieved based on the conditions. (As shown in Fig.3-95):

Fig.3-95 Retrieve a Security Domain

3.8. Log Management

3.8.1.Introduction to Functions

Log management can buffer or redirect logs generated by system events or packet filtering actions to the log receiving server. By analyzing and archiving the log contents, the administrator can check the security bugs in the network detected by the industrial firewall, understanding that when someone has tries to violate the security policy rules and the whitelist template rules to access the network. In addition, real-time logging can be used to detect ongoing intrusions and prohibit them.

Note:

Only auditor has the permission for log management.

3.8.2.Whitelist Alarm Log

Whitelist alarm logs are generated by messages flowing through the industrial firewall that violate the whitelist rules for the industrial firewall. It is possible to generate such a log only when the industrial firewall is in alarm mode or protection mode.

3.8.2.1.Log list

Click [Log Management/Whitelist Alarm Log] in the left navigation bar (as shown in Fig. 3-96), go to the [Whitelist Alarm Log] list page (as shown in Fig. 3-97):

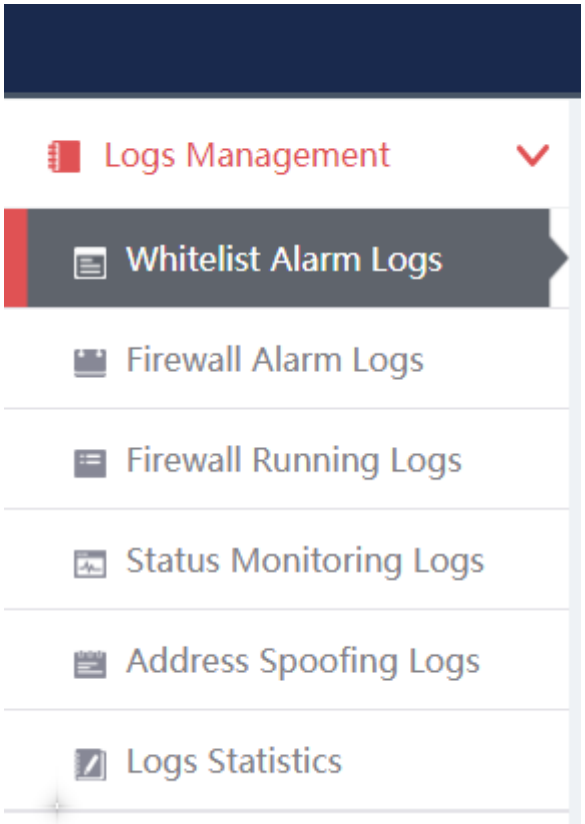


Fig.3-96 Whitelist Alarm Log Menu

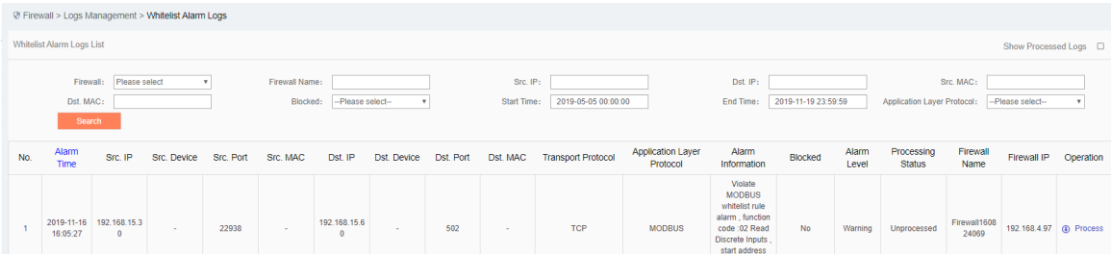


Fig.3-97 Whitelist Alarm Log List Page

View all the log information on whitelist alarms here, with the meaning given below:

Tab.26 Instruction to Whitelist Alarm Log Display

Column Names	**Instructions**
Firewall Name	A firewall name that is generated by the system or named by users, which is easy to remember
Firewall IP	The IP address assigned by the industrial firewall, in dotted decimal format
Src. IP	The IP address initiating a data request, in dotted decimal format
Src. Device	Display "-" if there is no device name, otherwise display the name of the source device
Src. Port	The port used by the machine initiating the data request

Dst. IP	The destination IP address requesting data, in dotted decimal format	
Dst. device	Displays "-" when there is no device name, otherwise displays the name of the destination device	
Dst. Port	The port used by the target machine of the request	
Transport Protocol	The protocol type of transport layer used by a message	
Application Layer Protocol	Specific application types	
Alarm information	Information on alarm description	
Blocked	Whether to release or block the processing of a message	
Alarm Level	Refer to 5.6.2 Instruction to Alarm Levels for the level of possible damage caused by alarms	
Processing Status	Whether alarms have been viewed and processed	
Alarm Time	Time when an alarm occurs	
Operation	Process	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Display Processed Logs> on the right side of the [Whitelist Alarm Log] whitelist alarm log list tab to view processed alarms. (As shown in Fig.3-98):

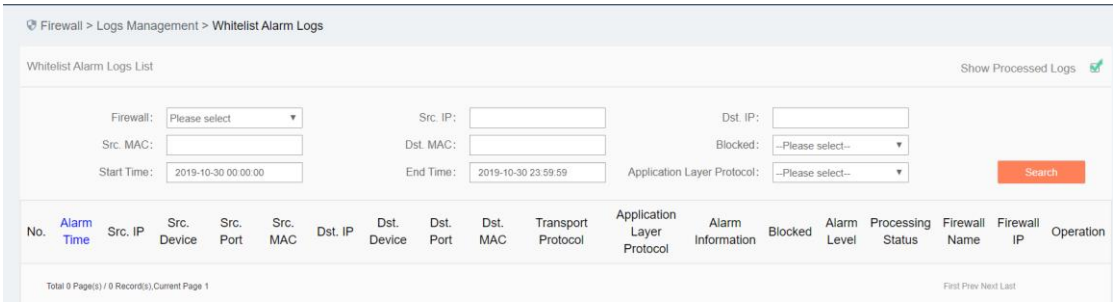


Fig.3-98 Displaying Processed Whitelist Alarm Log List Page

3.8.2.2. Processing a log

Click <Process> under the operation column in the [Whitelist Alarm Log] display list to display the [Whitelist Alarm Log Information] processing page as shown in the figure below. (As shown in Fig.3-99):

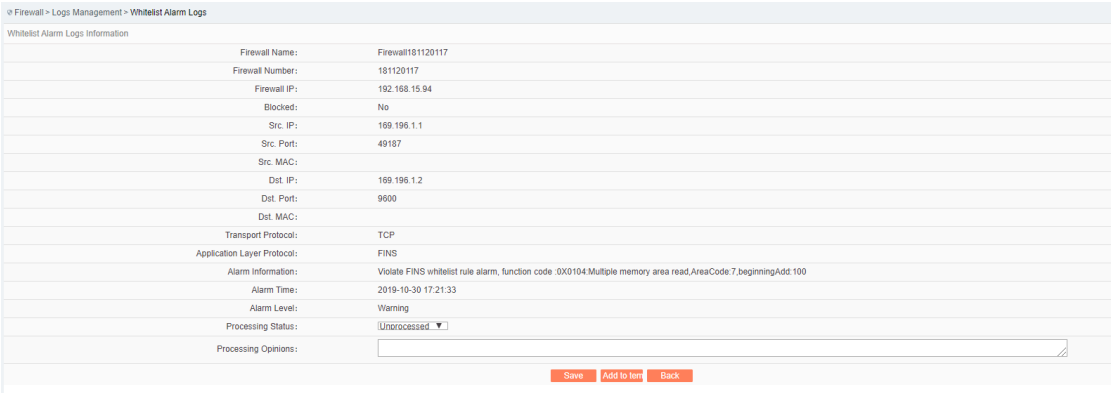


Fig.3-99 Whitelist Alarm Processing Page

Click the drop-down box of processing status, select "Close", fill in the relevant opinions in the processing opinions field and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the list of [Whitelist Alarm Log] page by default.

Or do not select "Close" but fill in the processing opinions instead.

3.8.2.3. Retrieve a log.

In the [Whitelist Alarm Log] list page, the logs can be retrieved based on conditions. (As shown in Fig.3-100):

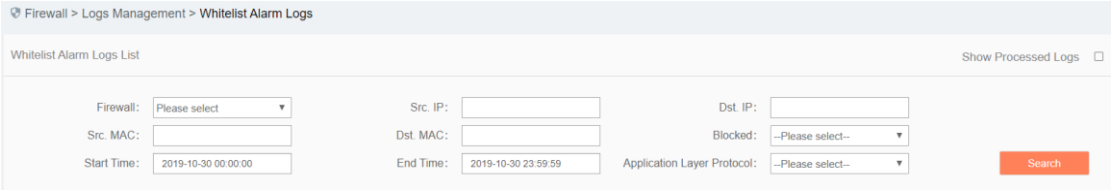


Fig.3-100 Retrieving a Whitelist Alarm Log

3.8.3. Firewall Alarm Logs

Firewall warning logs are generated by messages flowing through the industrial firewall that violate the security policy rules of the industrial firewall. Regardless of the operation mode of the industrial firewall, as long as messages violate the security policy rules, this type of warning will be generated.

3.8.3.1. Log list

Click [Log Management/Firewall Alarm Log] in the left navigation bar (as shown in Fig. 3-101), enter the [Firewall Alarm Log] list page (as shown in Fig.3-102):

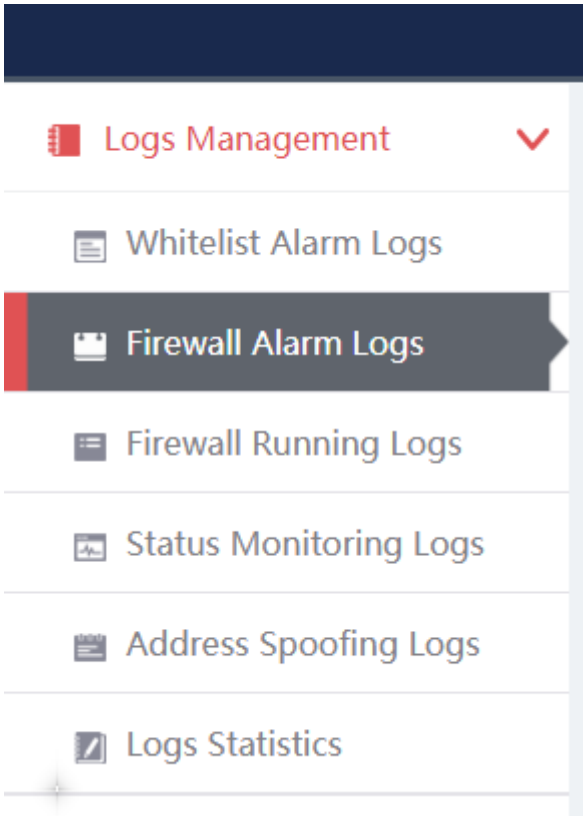


Fig.3-101 Firewall Alarm Log Menu

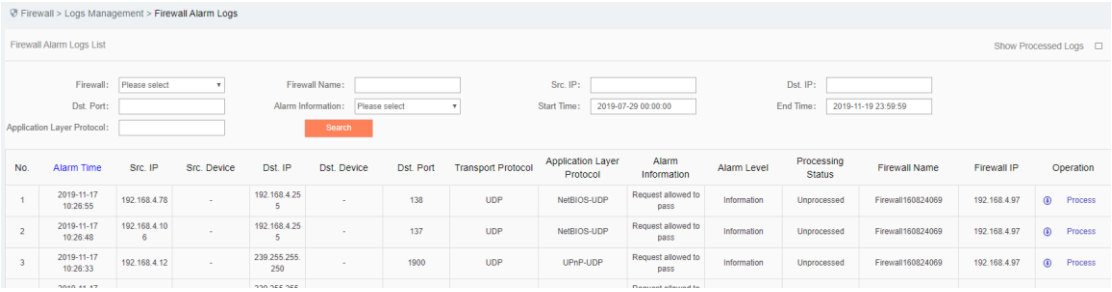


Fig.3-102 Firewall Alarm Log List Page

View all log information on firewall alarms here, with the meanings given below:

Tab.27 Instruction to Firewall Alarm Log Display

Column Names	**Instructions**
Firewall Name	An industrial firewall name that is generated by the system or named by users, which is easy to remember
Firewall IP	The IP address assigned by the industrial firewall, in dotted decimal format
Src. IP	The IP address initiating a data request, in dotted decimal format
Dst. IP	The destination IP address requesting data, in dotted decimal format
Dst. device	Displays "-" when there is no device name, otherwise displays the name of the destination device

Dst. port	The port used by the target machine of the request	
Transport Protocol	The protocol type of transport layer used by the message	
Application Layer Protocol	Specific application types	
Alarm Information	Information on alarm description	
Alarm Level	Possible damage levels that may be caused by alarms	
Processing Status	Whether alarms have been viewed and processed	
Alarm Time	Time when an alarm occurs	
Operation	Process	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Show Processed Logs> on the right side of the [Firewall Alarm Log] firewall alarm log list tab to view processed alarms. (As shown in Fig.3-103):

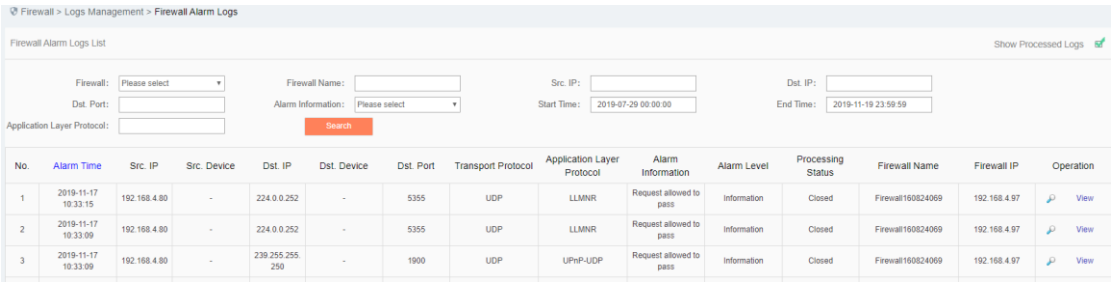


Fig.3-103 Displaying Processed Firewall Alarm Log List Page

3.8.3.2. **Processing a log**

Click <Process> under the operation column in the [Firewall Alarm Log] display list to display the [Firewall Alarm Log Information] processing page as shown in the following figure. (As shown in Fig.3-104):

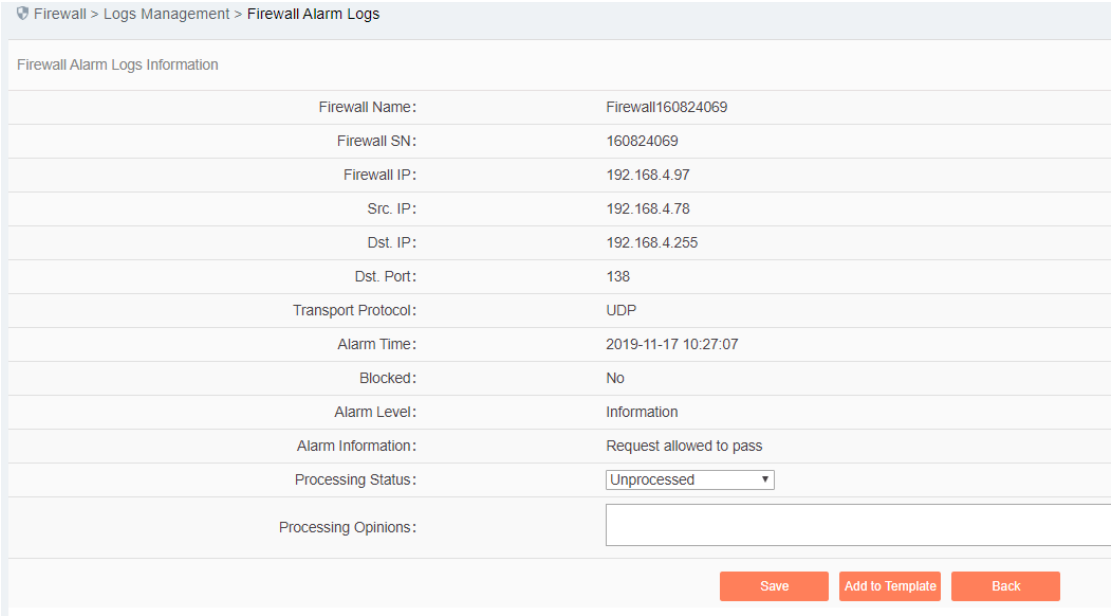


Fig.3-104 Firewall Alarm Processing Page

Click the drop-down box of processing status, select "Back", fill in the relevant opinions in the processing opinions field and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the list of [Firewall Alarm Log] page by default.

Or do not select "Close" but fill in the processing opinions instead.

3.8.3.3. Retrieve a log.

In the [Firewall Alarm Log] list page, the logs can be retrieved based on conditions. (As shown in Fig.3-105):

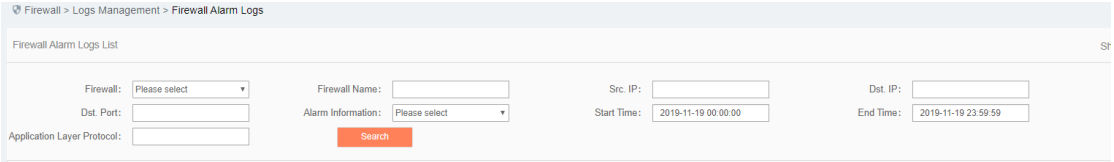


Fig.3-105 Retrieving a Firewall Alarm Log

3.8.4. Firewall Run Log

Firewall run log is a log to record the running status of industrial firewalls.

3.8.4.1. Log List

Click [Log Management/Firewall Run Log] in the left navigation bar (as shown in Fig. 3-106), enter the [Firewall Run Log] list page (as shown in Fig.3-107):

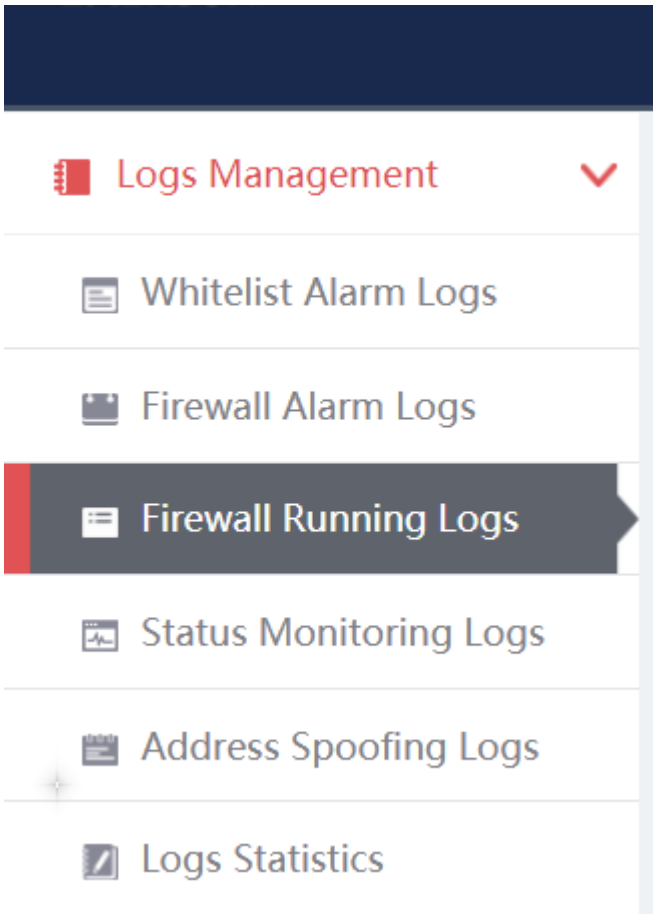


Fig.3-106 Firewall Run Log Menu

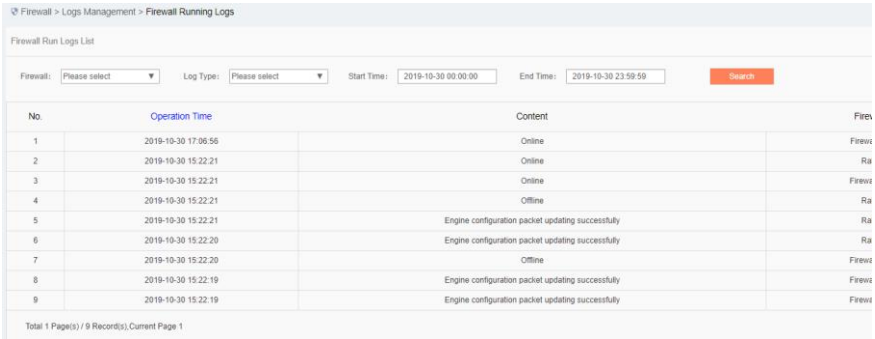


Fig.3-107 Firewall Run Log List Page

View the information on all industrial firewalls run logs, with the meanings given below:

Tab.28 Instruction to Firewall Run Log Display

Column Names	**Instructions**
Firewall Name	An industrial firewall name that is generated by the system or named by users, which is easy to remember
Firewall IP	The IP address assigned by the industrial firewall, in dotted decimal format
Content	Subsequent running status of industrial firewalls after logs are generated

Operating Time	Log generation time

3.8.4.2. Retrieve a log.

In the [Firewall Run Log] list page, the logs can be retrieved based on conditions. (As shown in Fig.3-108):

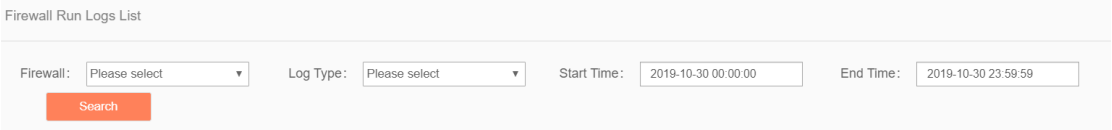


Fig.3-108 Retrieving a Firewall Run Log

3.8.5. Status Monitoring Logs

Refer to 3.8.4 Introduction to Firewall Run Logs for relevant operations.

3.8.6. Address Spoofing Logs

Address spoofing logs are generated by messages flowing through the industrial firewall that violate IP/MAC rules for the industrial firewall. It is possible to generate such a log only when the industrial firewall is in alarm mode or protection mode.

3.8.6.1. Log list

Click [Log Management/Address Spoofing Log] in the left navigation bar (as shown in Fig. 3-109), enter the [Address Spoofing Log] list page (as shown in Fig. 3-110):

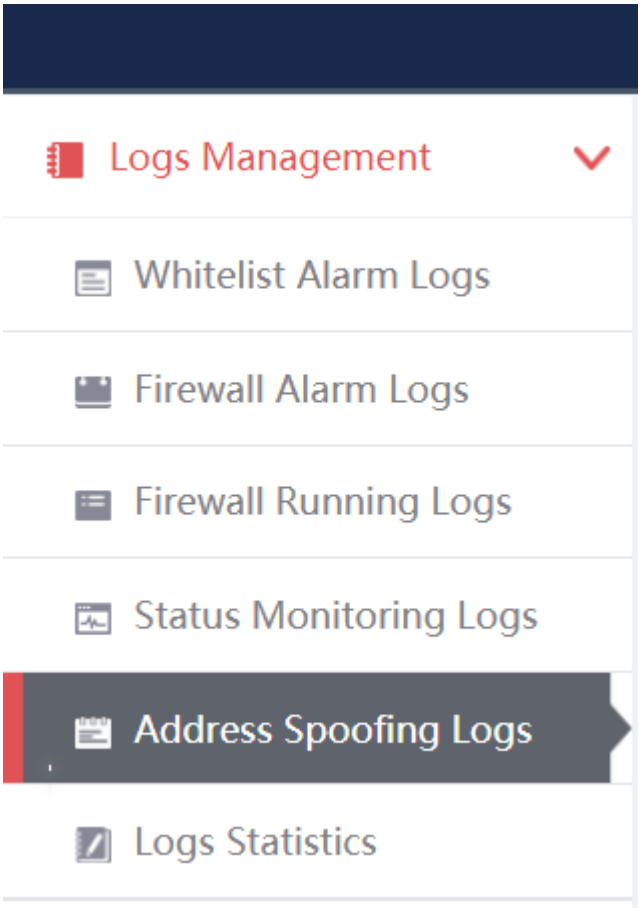


Fig.3-109 Whitelist Alarm Log Menu

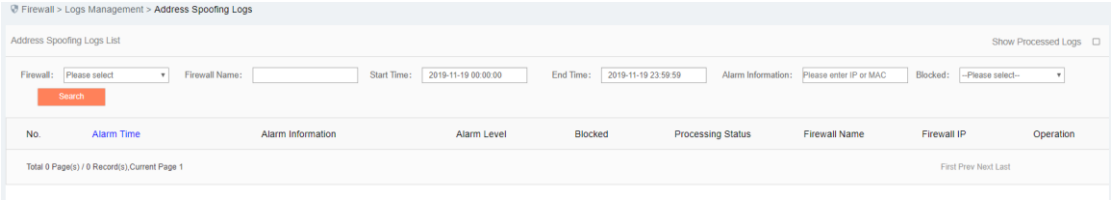


Fig.3-110 Address Spoofing Log List Page

View the information on all address spoofing log s, with the meanings given below:

Tab.29 Instruction to Address Spoofing Log Display

Column Names	**Instructions**
Firewall Name	An industrial firewall name that is generated by the system or named by users, which is easy to remember
Firewall IP	The IP address assigned by the industrial firewall, in dotted decimal format
Alarm Information	Information on alarm description
Blocked	Whether to release or block the processing of a message
Alarm Level	Warning of possible damage levels

Processing Status	Whether alarms have been viewed and processed	
Alarm Time	Time when an alarm occurs	
Operation	Process	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Display Processed Log> in the right side of the [address spoofing log] address spoofing log list tab to view processed logs. (As shown in Fig.3-111):

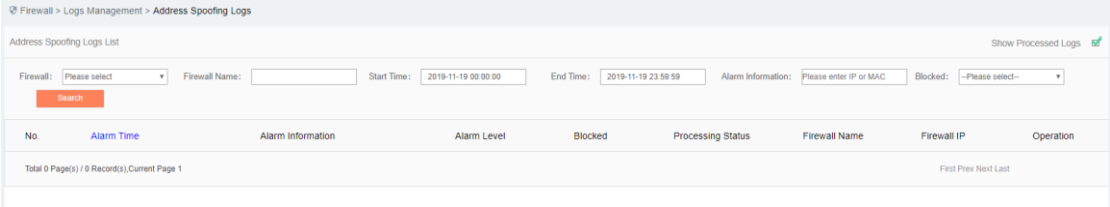


Fig.3-111 Displaying Processed Address Spoofing Log List Page

3.8.6.2. Processing a log

Refer to other log processing methods.

3.8.6.3. Retrieve the logo.

Refer to other log processing methods.

3.8.7. Log Statistics

Log statistics is divided into two modes, one is for the number of the four types of alarms for all industrial firewall devices, and the other for the number of the four types of alarms for a single industrial firewall device.

3.8.7.1. Display

Click [Log Management/Log Statistics] in the left navigation bar (as shown in Fig.3-112), enter the [Log Statistics] list page (as shown in Fig.3-113):

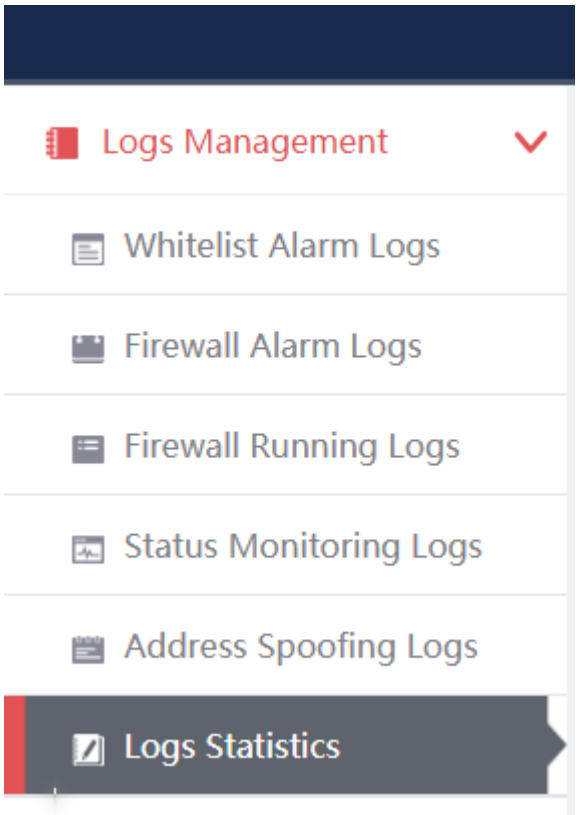


Fig.3-112 Log Statistics Menu

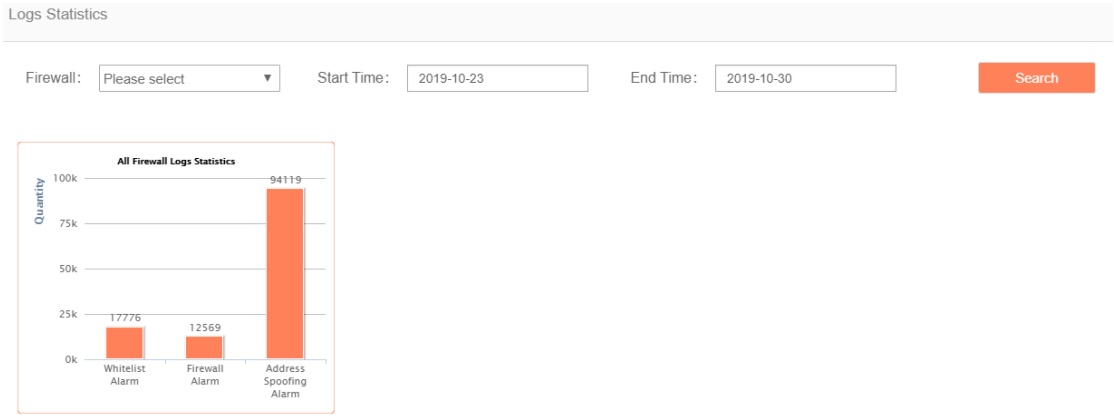


Fig.3-113 Log Statistics Page

3.8.7.2. **Retrieve statistics.**

In the [Log Statistics] page, which can retrieve the statistical data based on conditions. (As shown in Fig.3-114):

Fig.3-114 Retrieving Log Statistical Data

4. Industrial Endpoint Guard (IEG)

4.1. Introduction to Products

The IEG module is used to manage and monitor the management module of IEG. IEG is the host security software that is designed and developed based on AVCOMM's "soft trusted" technology with its own intellectual property rights, which aims at defects in traditional anti-virus software and combines the workstation security protection characteristics of an industrial control system.

The host security software innovatively introduce the application program whitelist management technology into industrial control network security protection. Only programs that are in the whitelist are allowed to run in the system, and all application programs that are not included in the whitelist are not allowed to run.

The software can manage and configure multiple industrial control hosts through the USM. Various alarm information and logs that are generated by the industrial control host during operation will be summarized to the management platform for data collection and analysis.

4.2. System Permissions

The system operator, administrator, and auditor (separately Sysoperator, admin and audit) shall be managed uniformly in the management platform. For the IEG module, the administrator and the auditor will be synchronized and used when installing the IEG client, with its permissions given below:

- Administrator: has all configuration management permissions.
- Sysoperator: has the user management authority of unified security management platform and industrial control host guard (Windows version).
- Auditor: has log audit related permissions

4.3. Real-time Alarm

When the auditor successfully logs in the unified management platform, click the "IEG" tab to enter. The upper part mainly displays system information, with the menu list of the system module on the left and the real-time and recent alarm information interfaces on the right (as shown in Fig.4-1):

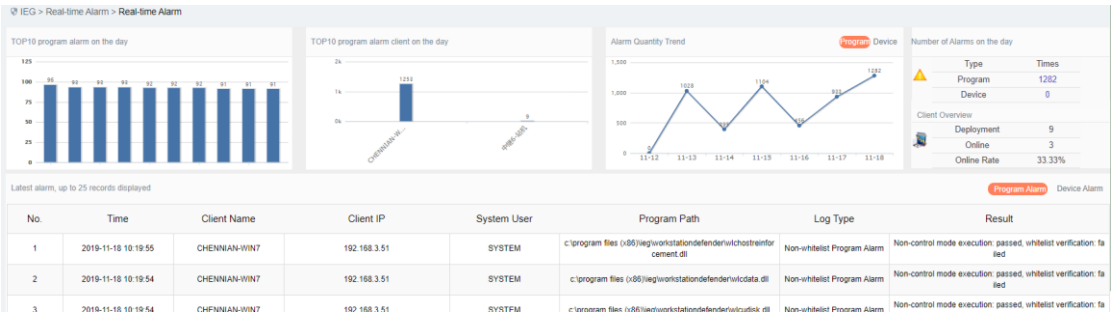


Fig.4-1 Real-time Alarm Page

The real-time alarm interface is the default display interface upon the successful login of the management

platform, which mainly includes 6 parts: statistics of TOP10 alarm programs on the day, statistics of TOP10 alarm clients on the day, alarm quantity trend, total alarms on the day, terminal overview and recent alarm.

- TOP 10 program alarm statistics on the day: the pie chart shows the TOP 10 records with the most alarm times of all programs on the day according to the classified statistics of program paths in view of all program alarms on the day. When there are fewer than 10 records, only existing records are displayed.
- Statistics of TOP 10 program alarm client on the day: bar chart shows the TOP 10 records with the most alarm times of all programs on the day according to IP classification statistics. When there are fewer than 10 records, only existing records are displayed.
- Alarm quantity trend: display the alarm quantity trend of program alarms and peripheral alarms in recent 7 days in the form of broken line graph. Switch between the two and display the program alarm quantity trend by default.
- Number of alarms on the day: display the number of program alarms and peripheral alarms on the day in the form of a list. Click the number and go to the program alarm or peripheral alarm interface.
- Terminal overview: displays the quantity of deployed and online clients, as well as the online rate, in the form of a list. Click the quantity value of deployed (or online) clients and go to the client monitoring interface.
- Recent alarm (up to 25 records displayed): display the latest 25 alarm records on program alarms and peripheral alarms in the form of a list, switch between the two and display program alarms by default.

4.4. Log Management

4.4.1.Log Classification

Through the log management module, the auditor can query and export program alarms, peripheral alarms, firewall alarm logs, operating system logs, IEG run logs, access control alarms.

- Program alarm: the client reports the generated program alarm log to the management platform, and all program alarms of the day are displayed by default in the program alarm interface list. The administrator can query related logs by setting conditions. Interface (as shown in Fig.4-2).
- Device alarm: the client reports the generated device alarm log to the management platform, and all device alarms of the day are displayed by default in the device alarm interface list. The administrator can query related logs by setting conditions. Interface (as shown in Fig.4-3 Device Alarm).
- Firewall log: the client reports the generated firewall log to the management platform, and all host firewall alarms of the day are displayed by default in the firewall log interface list. The administrator can query related logs by setting conditions. Interface (as shown in Fig.4-4).
- Operating system log: the client reports the generated operating system log to the management platform, and all operating system logs of the day are displayed by default in the operating system log interface list. The administrator can query related logs by setting conditions. Interface (as shown in Fig.4-5).
- IEG run log: the client will make a log of online & offline, CPU overload and memory overload, and all IEG run logs of the day are displayed by default in the log interface list. The administrator can query related logs by setting conditions. Interface (Fig.4-6).
- Access control alarm: the client reports the generated consolidated alarm log of the host to the management platform, and all access control alarms of the day are displayed by default in the access

control alarm interface list. The administrator can query related logs by setting conditions. Interface (Fig.4-7).

- Operating system login/logout log: check the login/logout information on the operating system user of the operating system where the client is located. The administrator query information by setting conditions. Interface (as shown in Fig.4-8):

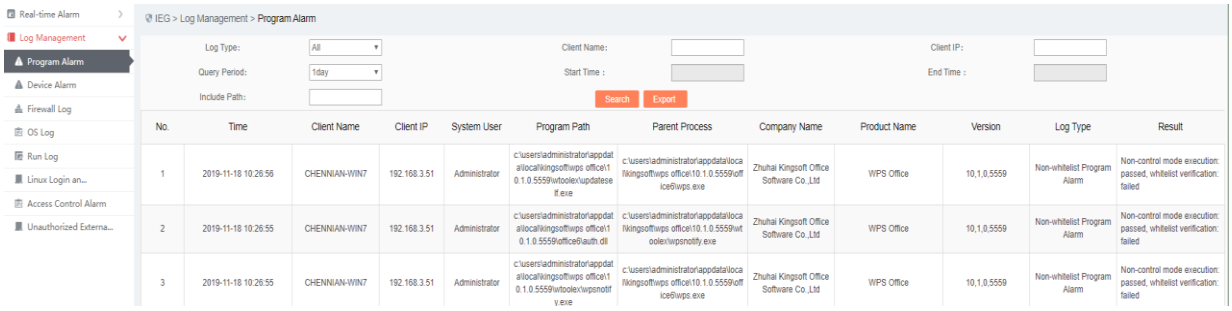


Fig.4-2 Program Alarm

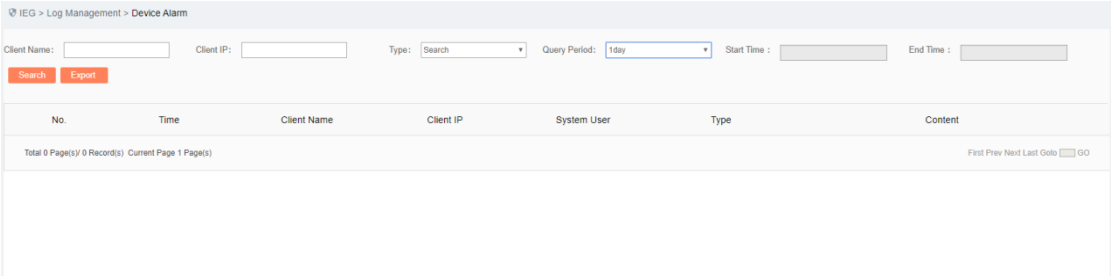


Fig.4-3 Device Alarm

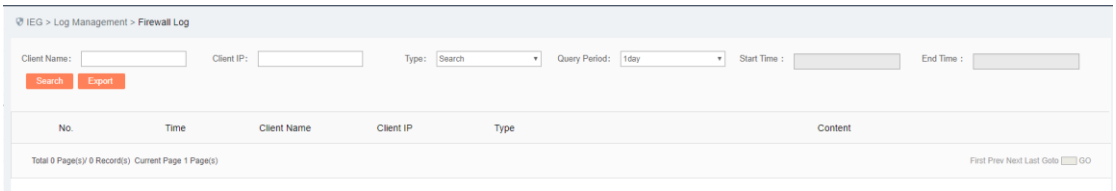


Fig.4-4 Firewall Alarm Log

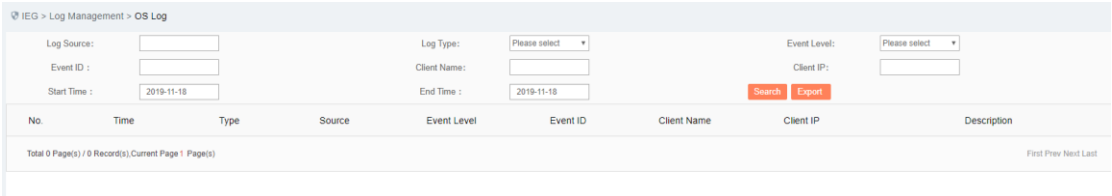


Fig.4-5 Operating System Log

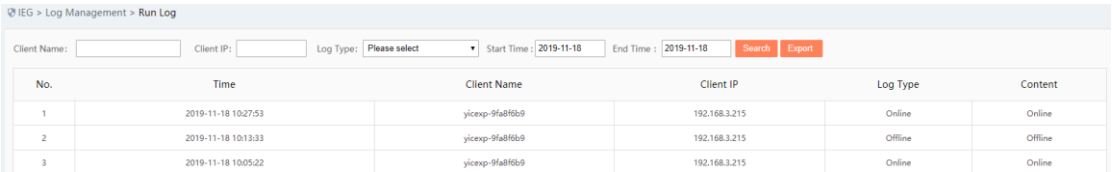


Fig.4-6 Run Log

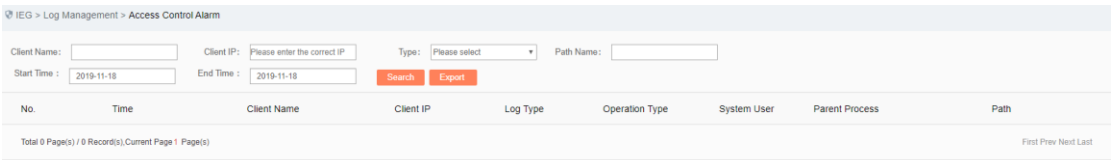


Fig.4-7 Access Control Alarm

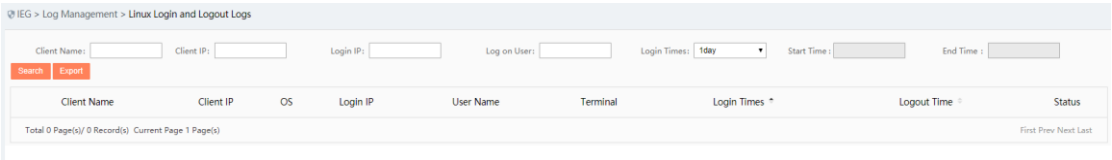


Fig.4-8 Linux Login and Logout Log

4.4.2.Log Query and Export

The above program alarms, peripheral alarms, firewall alarm logs, operating system logs, run logs, operating system login/logout logs, access control alarms and illegal outreach alarms can be queried and exported.

- Query: enter the legal keyword for query conditions, click "Query" to query the relevant log.
- Export: upon clicking "Export", the auditor can export the results to EXCEL files according to the query conditions.

4.5. IEG Management

Through the IEG management module, the administrator can conduct client status monitoring, group management, client group management, uninstalling or mandatorily uninstalling of the client, and distribute the client upgrading notice.

4.5.1.Client Monitoring

Client monitoring: query the client's status according to the keywords listed in the group tree [Client List] and refresh each status item of the client every 10 seconds. The administrator can click <Set Alias> to set an alias for the client, and click <Refresh> to manually refresh the client status. The default page of the interface displays the current status of all clients, can also filter and display the policy overview information of the client according to the query conditions. The operation functions include "More", "View Boot System Load Files", "Set Alias" and "Refresh". (As shown in Fig.4-9):

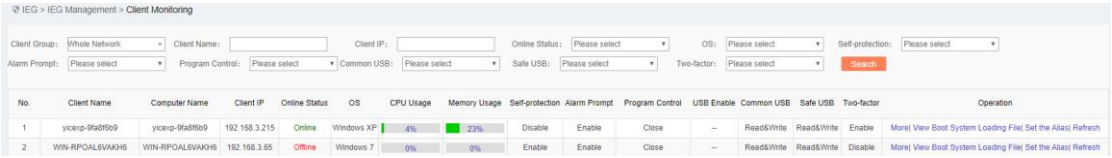


Fig.4-9 Client Monitoring

4.5.2.Group Management

Add, delete, and modify system organization. In the interface (as shown in Fig.4-10), the newly added organizational structure is in the red box. When organizations are added through the organization management interface, the administrator can divide the clients into different organizations.

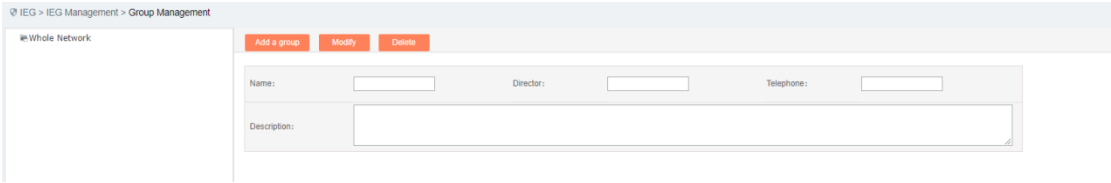


Fig.4-10 Group Management

4.5.3.Client Group

Client group: provide functions such as to query the clients in the organization node, add clients to the basic-level organization node created by the administrator in the organization management interface, delete or delete in batches the added clients from the organization node. Interface (as shown in Fig.4-11):

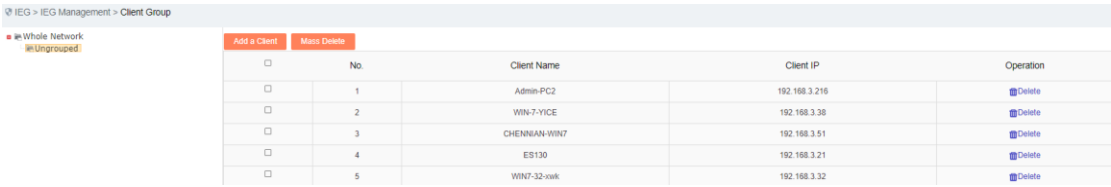


Fig.4-11 Client Group

4.5.4.Client Uninstallation

Client uninstallation: provide functions including client uninstallation, forced client uninstallation and real-time command action log display. The client displayed in this interface is different from the one displayed in the corresponding interface for IEG. If the client is uninstalled mandatorily, the management platform will stop monitoring the client immediately. Uninstalling the client, and after the client returns a message for successful uninstall, the management platform will no longer monitor the client. A specified client can be quickly and precisely found according to the query keyword. The interface displays the latest instruction action log of the day by default. The uninstall here does not affect the uninstall of the same function of the IEG. Click <Delete> to delete all command action logs with one click. Interface (as shown in Fig.4-12):

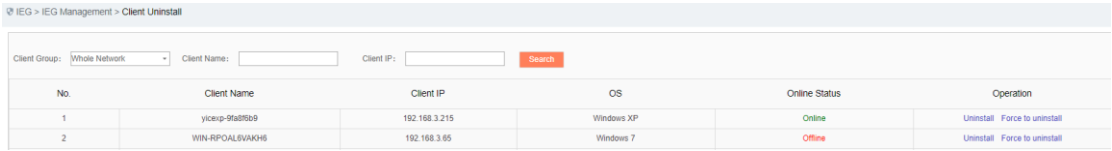


Fig.4-12 Client uninstallation

4.5.5.Client Upgrading

Client upgrading: this function only supports the IEG of Linux operating system, An upgrade notice is distributed to the client for upgrade via the management platform. After receiving the message, the client will actively request the upgrade package and upgrade. (As shown in Fig.4-13):

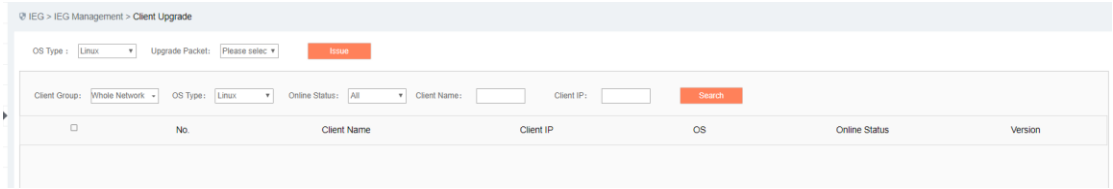


Fig.4-13 Client upgrading

4.6. Program Whitelist

Through the program whitelist module, the administrator can enable or disable each client program whitelist related function. The program whitelist related functions include: scan exception template, process audit template, system integrity check, whitelist management, program control, alarm processing, process audit. Complete the operation quickly by creating a template. Find a specified client quickly and accurately according to keyword query. The interface displays the latest command action log of the day by default. Click <Clear a Message Log> to delete all instruction action logs with one click.

Based on scan exception template and process audit template, including to add, delete or modify, etc., the administrator can enable and disable each client function, with templates created including scan exception template and process audit template.

4.6.1.Scan Exception Template

Scan exception template: add, delete, modify and query scan exception templates. After adding the scan exception template, click <Rule Configuration> to add the exception path that is not scanned.

Template operation interface, currently only supports Windows client (as shown in Fig.4-14):

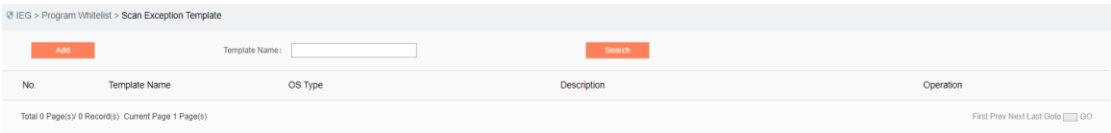


Fig.4-14 Scan Exception Template

Template configuration interface, (as shown in Fig.4-15):

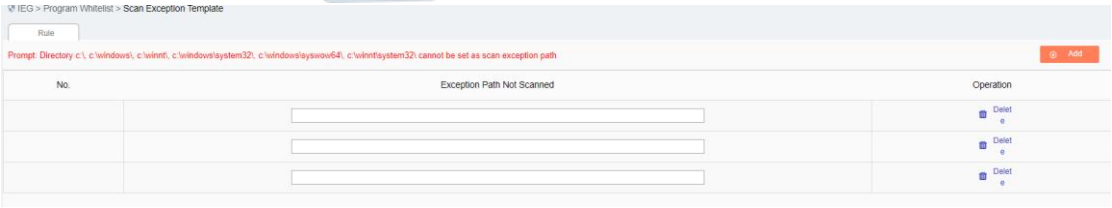


Fig.4-15 Template Configuration Interface

4.6.2.Process Audit Template

Process audit template: add, delete, modify, and query process audit templates. After adding the process audit template, click <Rule Configuration> to add the process name to be audited.

Template operation interface, including Windows and Linux templates (as shown in Fig.4-16):

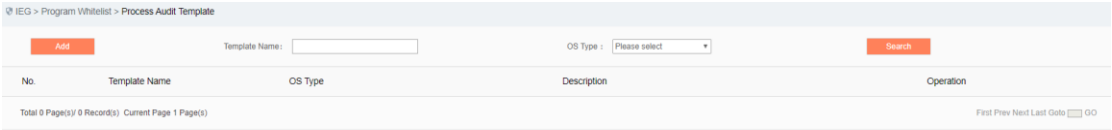


Fig.4-16 Process Audit Template

Template configuration interface (as shown in Fig.4-17):

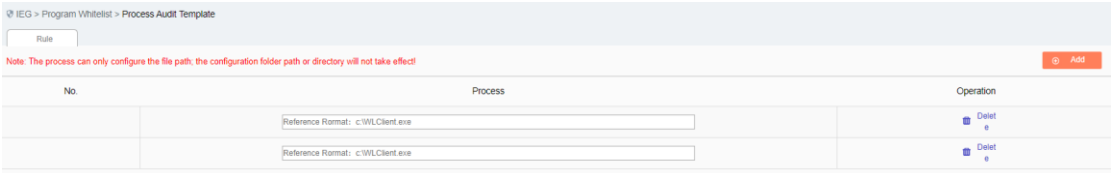


Fig.4-17 Template Configuration Interface

4.6.3.System Integrity Check

Give an "Enable" or "Disable" Instruction to the client for system integrity check. Upon successful execution of the client, refresh the interface automatically (as shown in Fig.4-18):

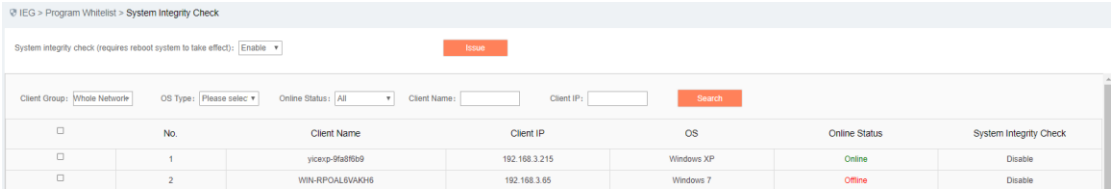


Fig.4-18 System Integrity Check Interface

4.6.4.Whitelist Management

Whitelist management includes to set the scan exception path. By setting the scan exception path, specify

a path that is not scanned when the whitelist is generated. The scan exception template is required for setting the scan exception template, which is configured in the [Scan Exception Template]. The user can distribute the scan exception path to the specified client by adding the scan exception template. By default, the system will upload the default scan exception to the management platform when booting. Scan exception templates can be generated by scanning exceptions for a single device. Interface (as shown in Fig.4-19):

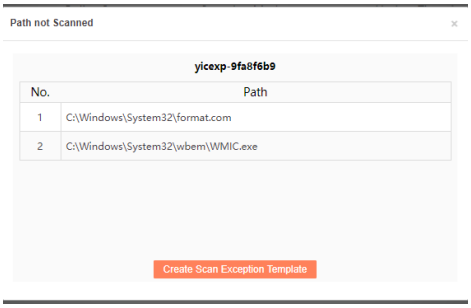


Fig.4-19 No Scan Path Interface

Upon the completion of whitelist exception path configuration, give the scan command to the specified IEG via the whitelist management page and view the scan status, after the scan is finished, view the whitelist list and its quantity, and support to export the whitelist as csv. Interface (as shown in Fig.4-20):

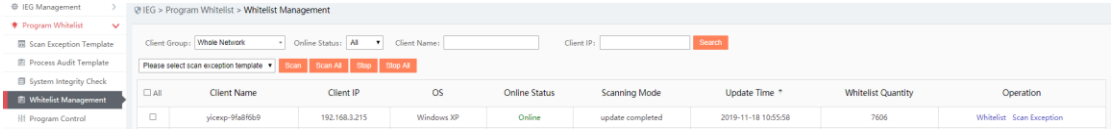


Fig.4-20 Whitelist Management Interface

View the whitelist interface (as shown in Fig.4-21):

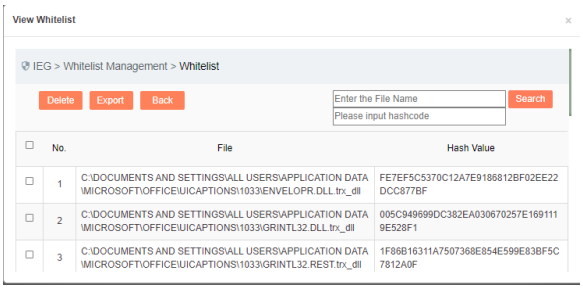


Fig.4-21 Viewing the Whitelist Interface

4.6.5.Program Control

Enable or disable client program control. Upon the successful execution of the client, refresh the interface automatically (as shown in Fig.4-22):

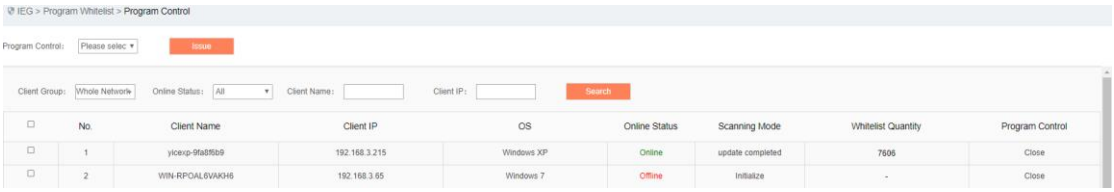


Fig.4-22 Program Control Interface

- Disable: when disabled, executable files that are not in the whitelist can be executed, with no alarm log generated.
- Intercept and alarm: when enabled, scan the computer-generated program whitelist database, and enable security protection. Executable files that are not in the whitelist cannot be executed, with an alarm log generated.
- Alarm: when enabled, scan the computer generated program whitelist database and enable security protection. Executable files that are not in the whitelist can be executed, with an alarm log generated.

4.6.6.Alarm Processing

Add non-whitelist program alarm log information intercepted by the whitelist into the whitelist, retrieve and export according to the conditions. The interface (as shown in Fig.4-23):

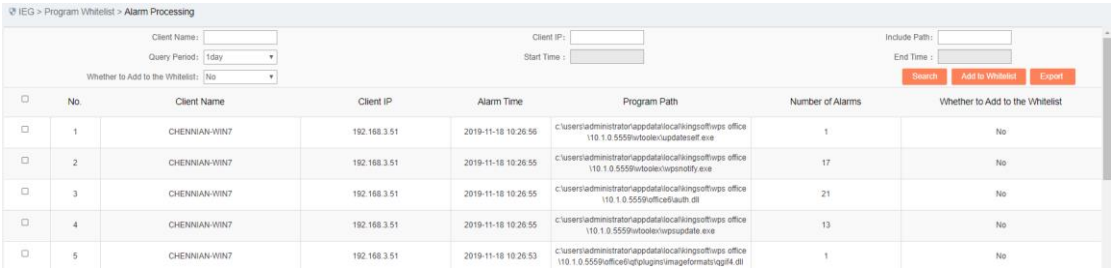


Fig.4-23 Alarm Processing Interface

4.6.7.Process Audit

Add a process audit template when using the function, with the process audit template set in [Process Audit Template]. Distribute the “Disable” or "Enable (Specific Template)" process audit policy to the client, refresh the interface automatically upon the successful execution of the client (as shown in Fig.4-24):

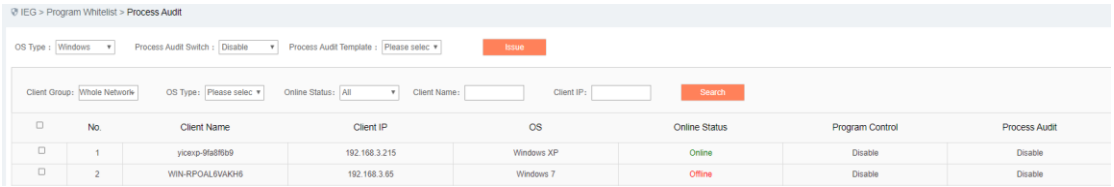


Fig.4-24 Process Audit Interface

After the process audit interface distributes the corresponding process audit template, IEG will report the policy based on this. By accepting the policy, View Policy Details in the above figure can be clicked to view the specific policy information. As shown in Fig.4-25 Client Policy Details, a Generate a Policy button is at the bottom of the interface. By clicking the button, a policy template can be generated and included in the process audit template.

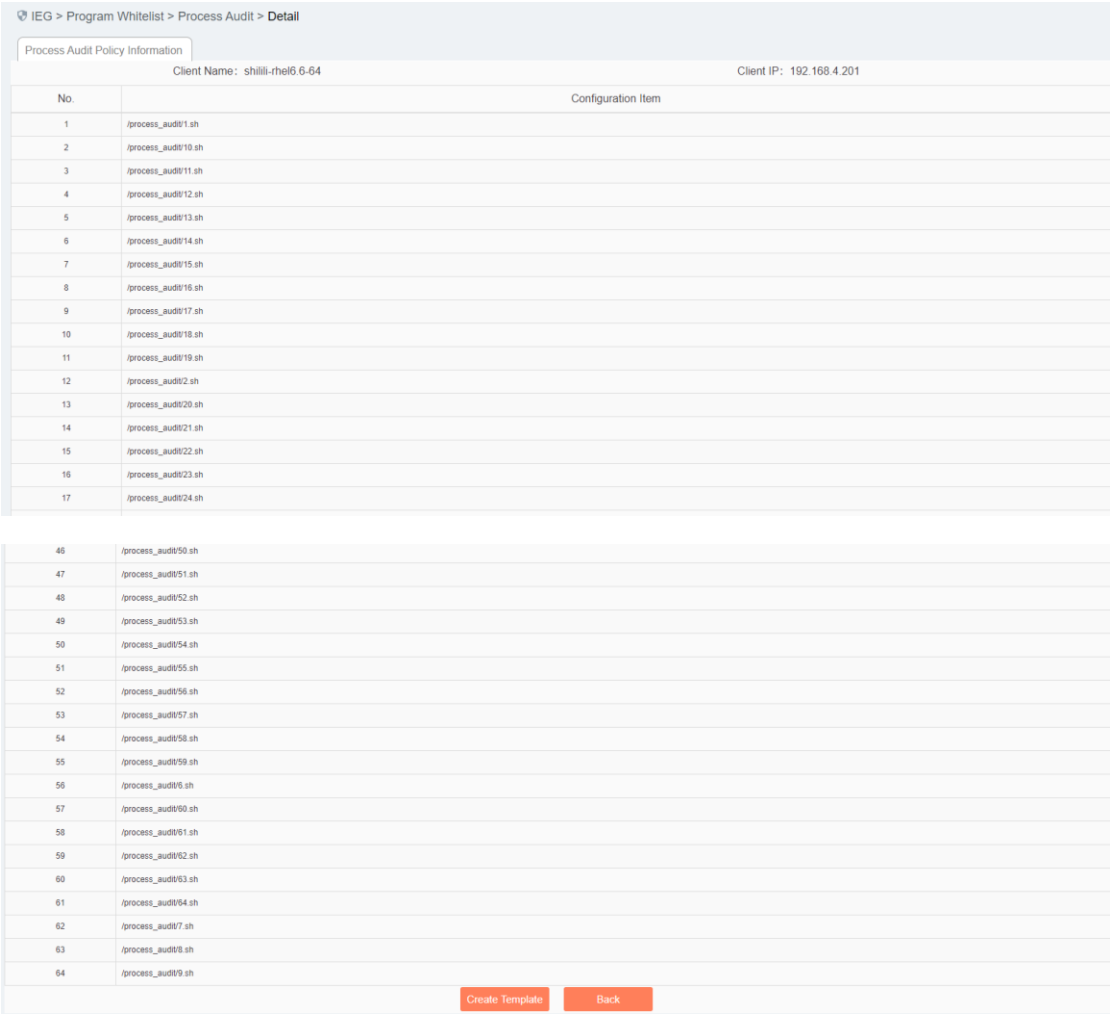


Fig.4-25 Process Audit Interface

4.7. Security Baseline

The security baseline configuration is divided into several levels: expert level, important level, intelligent level, and custom level. In the meantime, the security baseline restore default configuration function is also provided. When distributing Restore Default Configuration, the system is restored to the configuration when installed. The client security baseline configuration can be synchronized in two ways: client self-configuration and management platform distribution. When the management platform distributes the configuration, follow the process of configuration prior to distribution.

4.7.1.Safety Baseline Template

Expert level, important level and intelligent level are the default templates of the system. The custom level configuration template can be edited. All templates are capable of copying. A default template cannot be edited, but with its configuration viewed only. The copied template can edit the template and carry out rule configuration, distributing different templates for different clients.

Template Definition Interface (as shown in Fig.4-28):

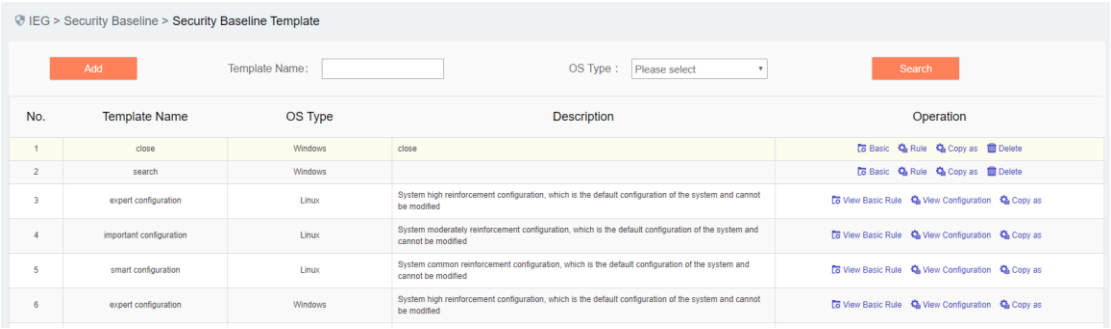


Fig.4-28 Security Baseline Default Template Interface

Windows Default Expert Template Configuration Page (as shown in Fig.4-29):

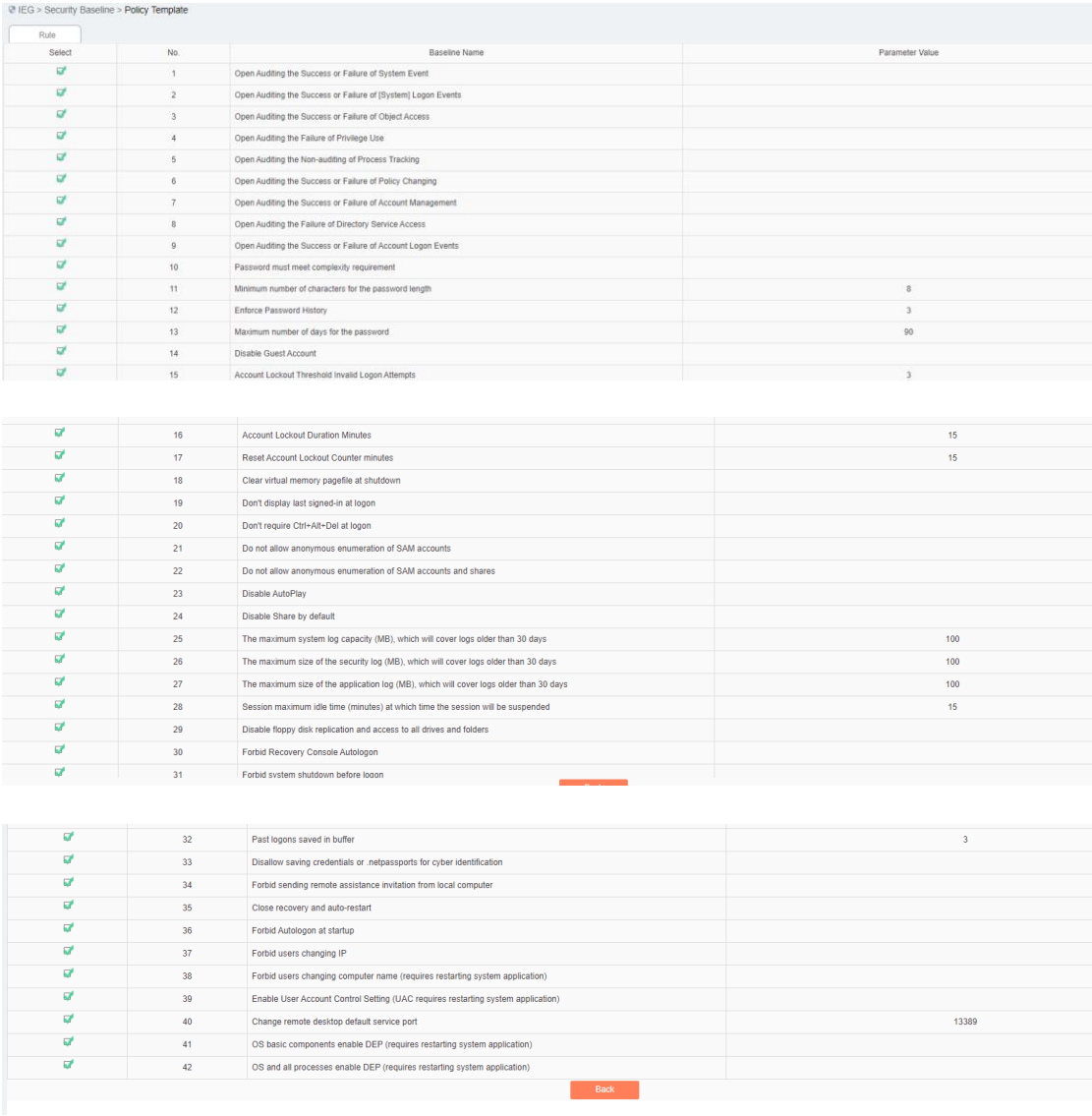


Fig.4-29 Windows Expert Template Page

Linux Default Expert Template Page (as shown in Fig.4-30)

IEG > Security Baseline > Policy Template

Rule

Select	No.	Baseline Name	Parameter Value
☑	1	Set the limit minutes for the account login timeout (restart for linx 42)	15
☑	2	Minimum number of characters for the password length	8
☑	3	The new password is at least 3 characters different from the old password	
☑	4	The new password must contain at least 1 capital letter	
☑	5	The new password must contain at least 1 lowercase letter	
☑	6	The new password must contain at least 1 numeric	
☑	7	The new password must contain at least 1 special character	
☑	8	pwdfailntimes	3
☑	9	Maximum number of days for the password	90
☑	10	The minimum password usage period is 0 days	
☑	11	/etc/passwd/ file permissions 644	
☑	12	/etc/shadow/ file permissions 640	
☑	13	UMASK Defaults to 022	
☑	14	Enable the limit number of reserved history commands	200
☑	15	The system must enable the audit service	
☑	16	The system must create a log file	
☑	17	Ensure that system log files can only be appended	
☑	18	Ensure that the contents of the polled history log file cannot be modified	
☑	19	The system must enable the audit service	
☑	20	The system must create an audit log file	
☑	21	Backup Firewall Policy	
☑	22	BASH shell-breaking vulnerability detection	
☑	23	OpenSSL Heart Bleeding Vulnerability Detection	
☑	24	System firewall on state detection	
☑	25	Only the UID of the ROOT account is 0	
☑	26	Detect default accounts that are not needed in the system	
☑	27	Rename the ROOT Account Name	
☑	28	Disable ROOT account remote login	
☑	29	Non-owner file is forbidden in the system command directory	
☑	30	The 777-permission file is forbidden in the system command directory	
☑	31	Ordinary users can switch to ROOT account	
☑	32	FTP service shutdown status detection	
☑	33	Disable FTP anonymous login	
☑	34	The root directory free space cannot be less than 10%	
☑	35	The system supports the RDP protocol.	
☑	36	Disable TELNET remote management mode	
☑	37	Use encrypted remote management mode	
☑	38	Web service shutdown status detection	
☑	39	Mail service shutdown status detection	
☑	40	Syncookie Function On-state Detection	
☑	41	OS DEP startup status detection (requires restart)	
☑	42	Prohibit giving permission to change host IP address	
☑	43	Forbid non root users changing computer name	
☑	44	Only SSH is allowed when users log in remotely	
☑	45	The password must not contain the account name.	
☐	46	Restrict SSH remote login for a specified IP address range host	
☑	47	Limit SSH maximum connection, Pre-warning when the connection exceeds the designated value	500
☑	48	Public key authentication is prohibited for login between hosts, and password authentication mode should be used.	

Back

Fig.4-30 Linux Expert Template Page

Template Copy (Fig. 4-31):

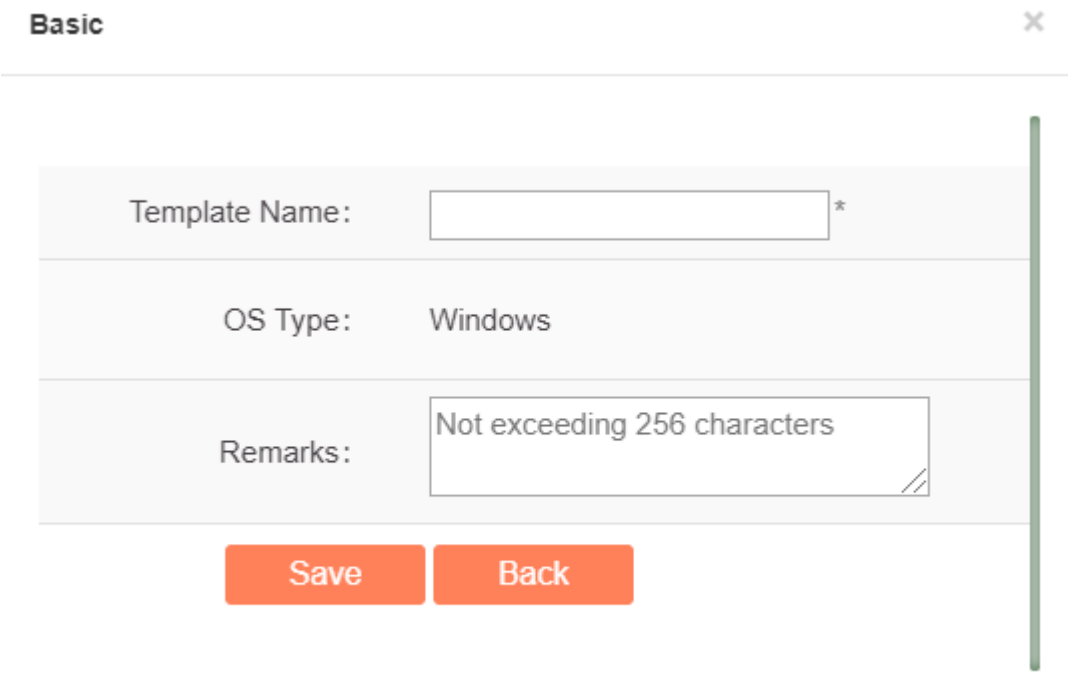


Fig.4-31 Template Copy Interface

The copied template can have the option to edit rules (as shown in Fig.4-32), which cannot be illustrated due to the document. Please be subject to the actual page:

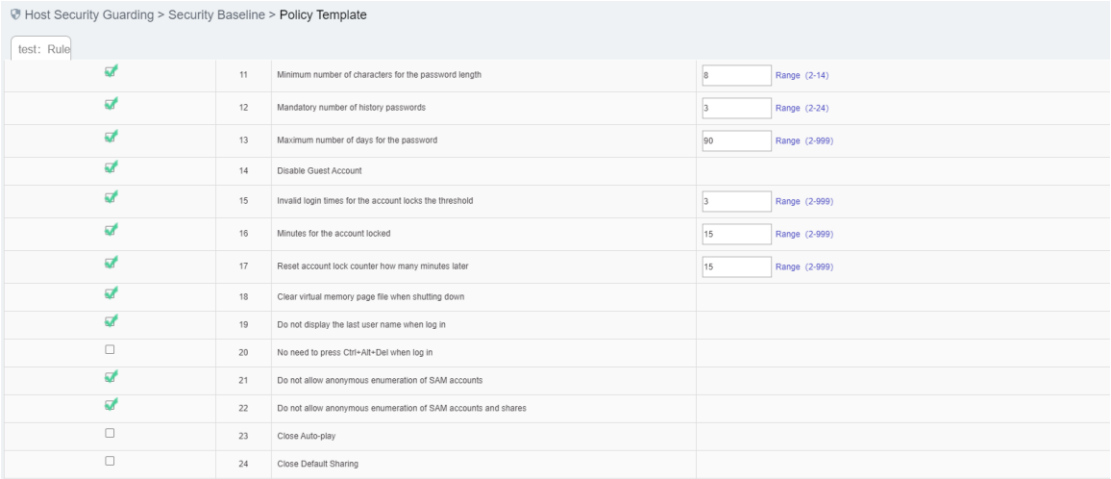


Fig.4-32 Copied Template Rule Edit Interface

Linux copied template configuration rules can also edit SSH remote login rules, bind SSH remote login IP segments, users, and time periods (as shown in Fig. 4-33):

Fig.4-33 Editing SSH Remote Logon Rules

4.7.2.Security Baseline Configuration

The security baseline policy configuration is distributed by Windows and Linux clients respectively. After the successful execution of the client, the policy configuration information can be displayed by clicking View a Policy. When viewing the policy information here, the reinforcement items of Windows and Linux clients are different. See the following figure Policy Configuration Interface for the specific change (as shown in Fig. 4-34):

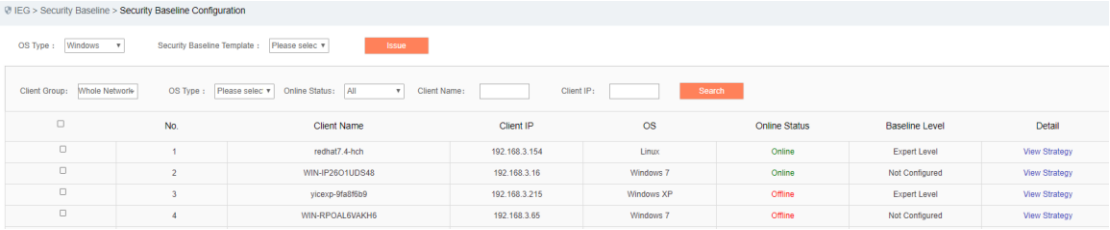


Fig.4-34 Policy Configuration Interface

Windows Client View Policy (as shown in Fig.4-35):

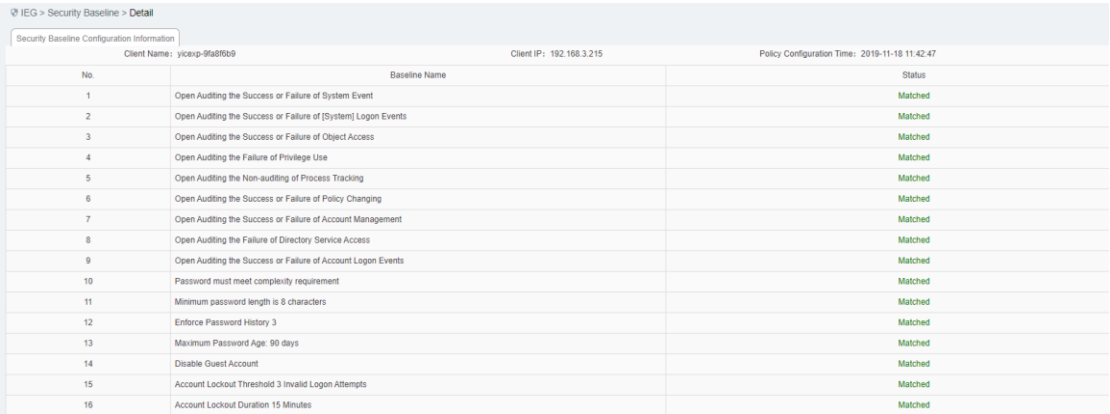


Fig.4-35 Windows Client Configuration View

Windows Client View Policy 2 (as shown in Fig.4-36):

17	Reset Account Lockout Counter in 15 Minutes	Matched
18	Clear virtual memory pagefile at shutdown	Matched
19	Don't display last signed-in at logon	Matched
20	Don't require Ctrl+Alt+Del at logon	Matched
21	Do not allow anonymous enumeration of SAM accounts	Matched
22	Do not allow anonymous enumeration of SAM accounts and shares	Matched
23	Disable AutoPlay	Matched
24	Disable Share by default	Matched
25	System logs reach 100M. Override logs before 30 days	Matched
26	Security logs reach 100M. Override logs before 30 days	Matched
27	App logs reach 100M. Override logs before 30 days	Matched
28	15 minutes idle time is required before suspending a session	Matched
29	Disable floppy disk replication and access to all drives and folders	Matched
30	Forbid Recovery Console Autologon	Matched
31	Forbid system shutdown before logon	Matched
32	Past logons saved in buffer 3	Matched
33	Disallow saving credentials or .netpassports for cyber identification	Matched
34	Forbid sending remote assistance invitation from local computer	Matched
35	Close recovery and auto-restart	Matched
36	Forbid Autologon at startup	Matched
37	Forbid users changing IP	Not Matched
38	Forbid users changing computer name (requires restarting system application)	Matched
39	Enable User Account Control Settings (UAC, Need to Restart System Application)	This system is not supported
40	Change remote desktop default service port 13389	Matched
41	OS basic components enable DEP (requires restarting system application)	Matched
42	OS and all processes enable DEP (requires restarting system application)	Not Matched

Back

Fig.4-36 Old Windows Client Configuration View

Linux Client View Policy (as shown in Fig.4-37):

IEG > Security Baseline > Detail

Security Baseline Configuration Information

Client Name: redhat7.4-hch Client IP: 192.168.3.154 Policy Configuration Time: 2019-11-18 11:56:39

No.	Baseline Name	Status
1	Set account login timeout limit to 15 minutes	Matched
2	Password length is at least 8 characters	Matched
3	The new password is at least 3 characters different from the old password	Matched
4	The new password must contain at least 1 capital letter	Matched
5	The new password must contain at least 1 lowercase letter	Matched
6	The new password must contain at least 1 numeric	Matched
7	The new password must contain at least 1 special character	Matched
8	Password login failed 3 times will lock the account 5 minutes	Matched
9	The maximum password period is 90 days	Matched
10	The minimum password usage period is 0 days	Matched
11	/etc/passwd/ file permissions 644	Matched
12	/etc/shadow/ file permissions 640	Matched
13	UMASK Defaults to 022	Matched
14	Enable history command retention limit to 4	Matched
15	The system must enable the audit service	Matched
16	The system must create a log file	Matched
17	Ensure that system log files can only be appended	Matched
18	Ensure that the contents of the polled history log file cannot be modified	Matched
19	The system must enable the audit service	Matched
20	The system must create an audit log file	Matched
21	Backup Firewall Policy	Matched
22	BASH shell-breaking vulnerability detection	Manual Configuration is Recommended
23	OpenSSL Heart Bleeding Vulnerability Detection	Matched
24	System firewall on state detection	Matched
25	Only the UID of the ROOT account is 0	Matched
26	Detect default accounts that are not needed in the system	Manual Configuration is Recommended
27	Rename the ROOT Account Name	Manual Configuration is Recommended
28	Disable ROOT account remote login	Manual Configuration is Recommended
29	Non-owner file is forbidden in the system command directory	Matched
30	The 777-permission file is forbidden in the system command directory	Matched
31	Ordinary users can switch to ROOT account	Matched
32	FTP service shutdown status detection	Matched
33	Disable FTP anonymous login	Manual Configuration is Recommended
34	The root directory free space cannot be less than 10%	Matched
35	The system supports the RDP protocol.	Manual Configuration is Recommended
36	Disable TELNET remote management mode	Matched
37	Use encrypted remote management mode	Matched
38	Web service shutdown status detection	Matched
39	Mail service shutdown status detection	Matched
40	Syncookie Function On-state Detection	Matched
41	OS DEP startup status detection (requires restart)	Matched
42	Prohibit giving permission to change host IP address	Matched
43	Forbid non root users changing computer name	Matched
44	Only SSH is allowed when users log in remotely	Matched
45	The password must not contain the account name.	Matched
46	Restrict SSH remote login for a specified IP address range host	Manual Configuration is Recommended
47	Limit the maximum number of SSH connections and alert when the number of connections exceeds 500	Matched
48	Public key authentication is prohibited for login between hosts, and password authentication mode should be used.	Matched

Back

Fig.4-37 Linux Client Configuration View

4.8. Device Management

Device management is divided into "Windows device management" (device management corresponding to the old version), "Linux device management" and "registered USB management".

4.8.1.Windows Device Management

Security USB: the built-in security encryption chip is used with the IEG software. The security USB cannot be operated on a host without the IEG installed.

Common USB: a USB storage device that can be automatically loaded on any host.

Control the common USB, security USB, CD-ROM and WLAN operation permissions of the client.

Common USB control: control the use permission of common USB, including forbidden,read only and read&write

Security USB control: control the use permission of security USB, including prohibition of use, read only use and out of control

CD-ROM and WLAN control: control the enabling and disabling of CD-ROM and WLAN

After the successful execution of distributing a policy to the client, the interface will be automatically refreshed, Device Control Interface (as shown in Fig.4-38):

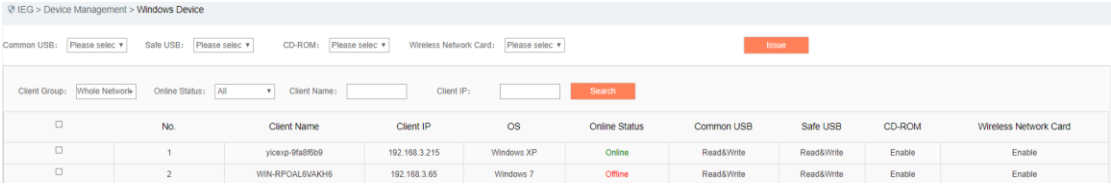


Fig.4-38 Peripheral Control Interface

4.8.2.Linux Device Management

Linux Device Management currently only provides USB switch control to enable and disable USB control. In the disabled state, the USB can do any operation without being controlled, In the enable state, the operation of the registered USB will be controlled by the relevant policies of the registered USB management (as shown in Fig.4-39):

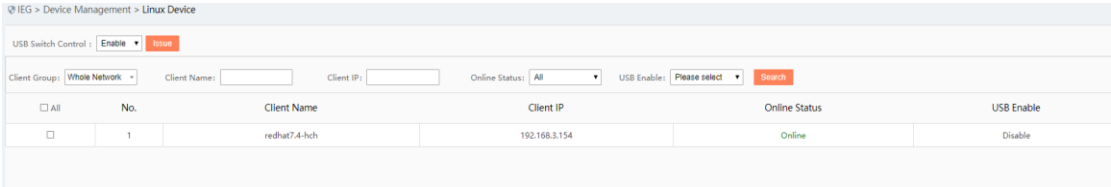


Fig.4-39 Linux Device Management

4.8.3.Registered USB Management

Control USB registration, unregistration, read and write execution functions, query the corresponding USB according to the query conditions. (As shown in Fig.4-40):

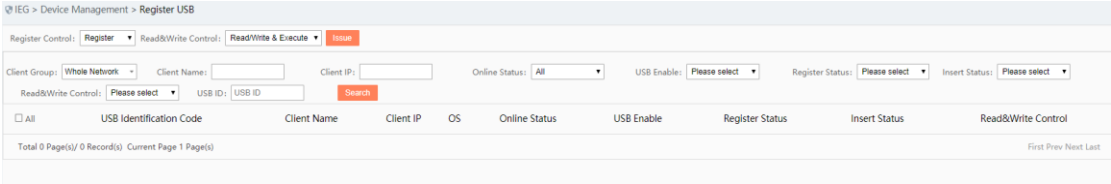


Fig.4-40 Registered USB Management

4.9. Access Control

Through the functions of registry protection template, file protection template, subject template and object template function, including to add, delete or modify, etc., the administrator can enable or disable each function of the client.

Note: Linux does not support the registry protection template.

4.9.1.Registry Protection Template

Registry protection template: add, delete, modify, and query the registry protection template. After adding the registry protection template, click <Rule Configuration> to add the registry key to be protected. This function is only limited to protect the registry key values under the HKEY_LOCAL_MACHINE keyword. Rules can be imported and exported.

Registry template configuration interface (as shown in Fig.4-41, Fig.4-42 Registry Rule Configuration Interface):

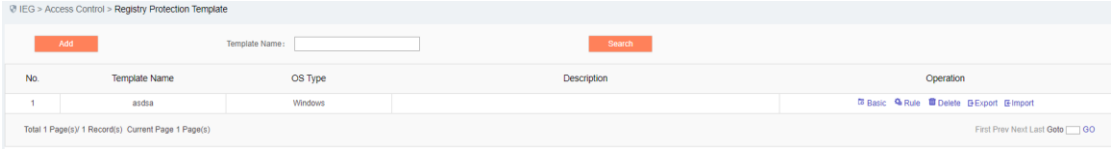


Fig.4-41 Registry Template Configuration Interface

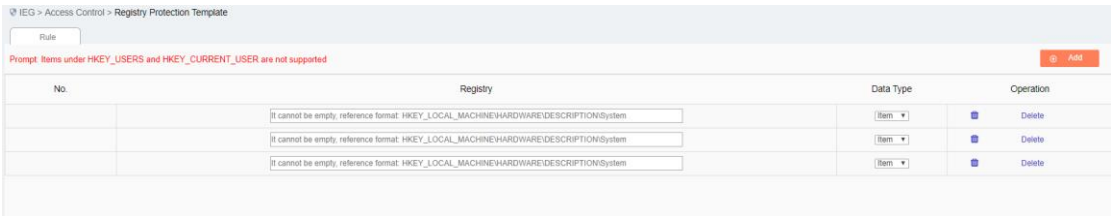


Fig.4-42 Registry Rule Configuration Interface

4.9.2.File Protection Template

File protection template: add, delete, modify, and query the configuration file template. After adding the file

protection template, click <Rule> to add the configuration file to be protected. You can configure Linux templates or windows templates. Rules can be imported and exported.

File protection template configuration interface (as shown in Fig. 4-43 and Fig. 4-44):

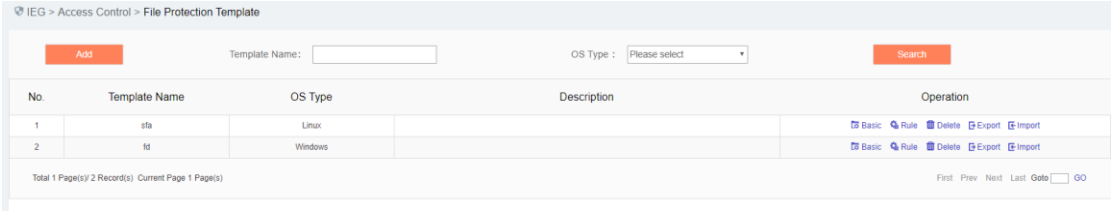


Fig.4-43 File Protection Template Configuration Interface

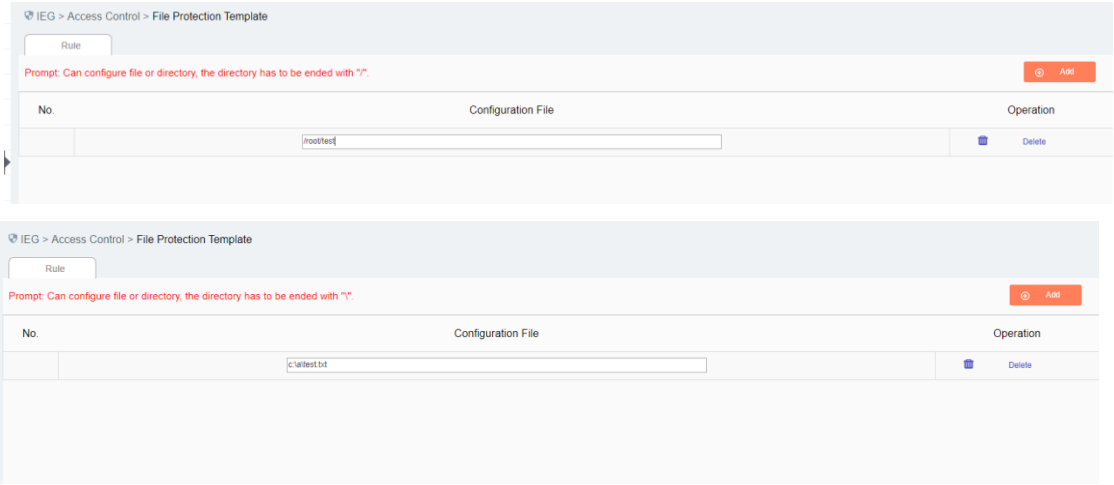


Fig.4-44 File Protection Rule Configuration Interface

4.9.3.File Protection Exception Template

File protection exception template: add, delete, modify, and query configuration file protection exception templates. After adding the file protection exception template, click <Rule> to add the configuration file requiring protect exception. Rules can be imported and exported.

File protection exception template configuration interface (as shown in Figs.4-45 & 4-46):

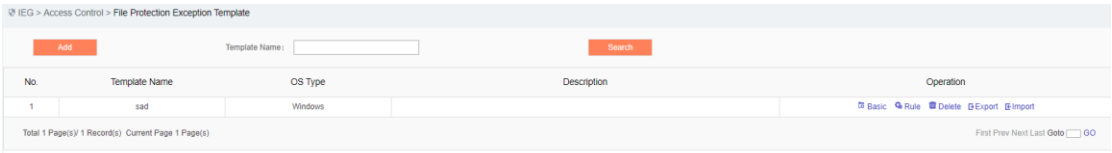


Fig.4-45 File Protection Exception Template Configuration Interface

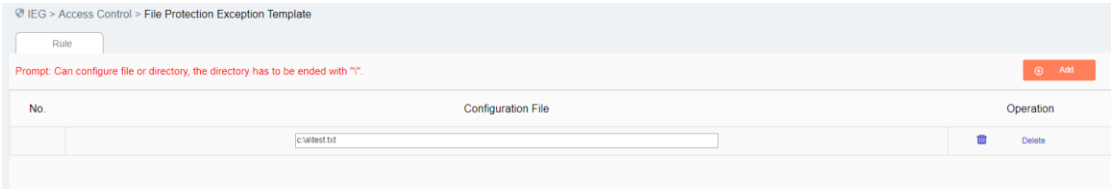


Fig.4-46 File Protection Exception Rule Configuration Interface

4.9.4.Registry Protection Policy

Registry protection: when choose alarm mode (Intercept And Alarm/Warning), the specified registry entry is not allowed to be modified. When chose alarm mode (Disabled), the above registry entry is allowed to be modified, and registry entry to be protected can be specified via <Configure>. This function is only limited to protect registry keys under the HKEY_LOCAL_MACHINE keyword. Using this function requires setting the registry protection template, which is set in [Access Control -> Registry Protection Template].

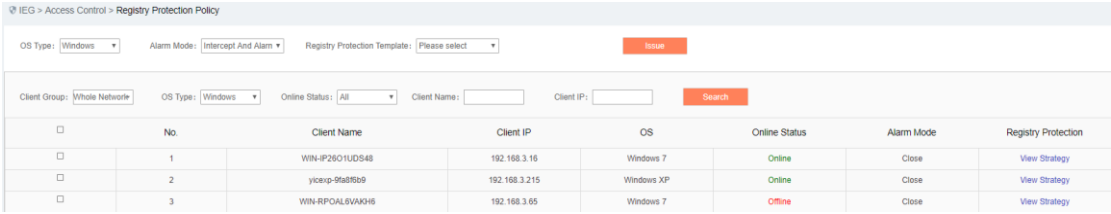


Fig.4-56 Registry Protection Policy Interface

4.9.5.File Protection Policy

Configuration file protection: when choose alarm mode (Intercept and Alarm/Warning), the specified system file is not allowed to be modified. When choose alarm mode(disabled), the above file is allowed to be modified, and a directory or file to be protected can be specified by the configuration button. To use this function, set the configuration file protection template first, which is set in [Access Control --> File Protection Template]. Add the alarm mode in the file protection policy interface (as shown in Fig.4-57), accept the file protection template and file protection exception template as reported from the client at the same time.

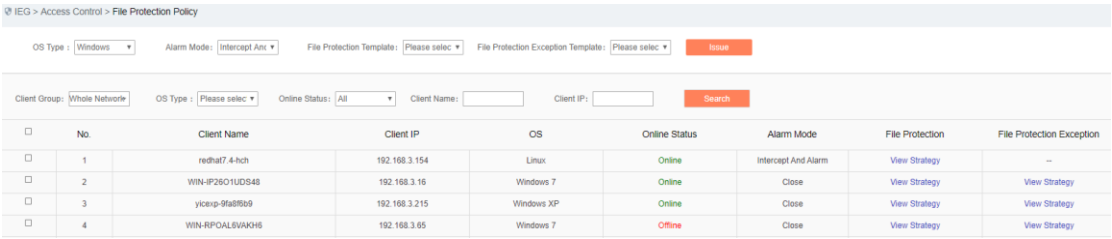


Fig.4-57 File Protection Policy Interface

4.10. Two-factor Authentication

4.10.1. User Template

The user template is applicable to create templates used by a customer on the client. Specific functions are as follows:

1) Basic functions including to add, delete and modify basic information. Click <Add> to pop up the Create Template Page. As shown in the figure below, click <Save> to complete the creation successfully after filling in the

information. (Note: template names are not repeatable.) The template list page can conduct fuzzy query according to the template name, click the delete button behind the template to delete the template. (As shown in Fig.4-69):

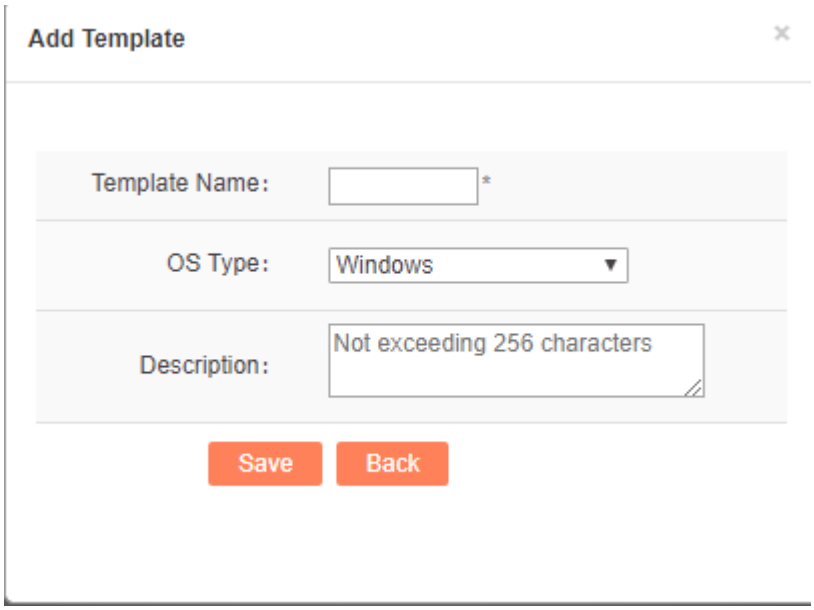


Fig.4-69 User Template Add Interface

2) Click the basic rules behind the template to modify the template name and the remark information.

3) Click the rule configuration behind the template to carry out user management, including user creation, deletion, password modification, USBKey binding, USBKey unbinding and PIN code reset. (Note: download and install the USBKey plug-in when used for the first time. This page provides the link for downloading) (as shown in Fig.4-70):

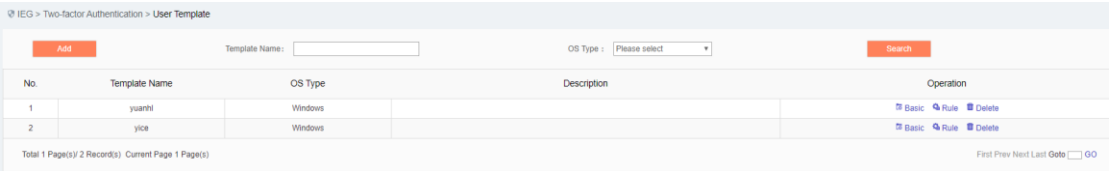


Fig.4-70 User Template List Interface

4) User creation. Click <Add> in the rule configuration page of the template to pop up the user creation page, as shown in the figure below. There are two ways to fill in the user role, the default one is the drop-down button, and the contents in the drop-down option are the common user group information reported from the client. The second way is to click the toggle button behind the user role. The user role can be entered manually after clicking the custom user group. (Note: manually entered user roles must exist on the client, otherwise the creation fails after distribution). There are two options for authentication mode, the default one is normal password mode, or the USBKey password mode, which needs to insert the USBKey tool, that is, Ukey for short. After inserting the USBKey, change the modified name later. If there is no USBKey information in the drop-down box of the inserted page, click <Refresh a List>, click <Save> to complete the creation successfully after entering the information. (As shown in Fig.4-71/4-72):

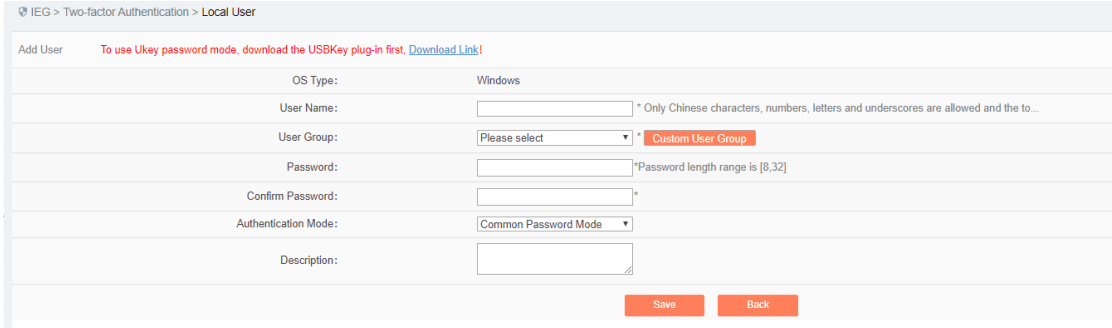


Fig.4-71 Add User Interface Normal Password

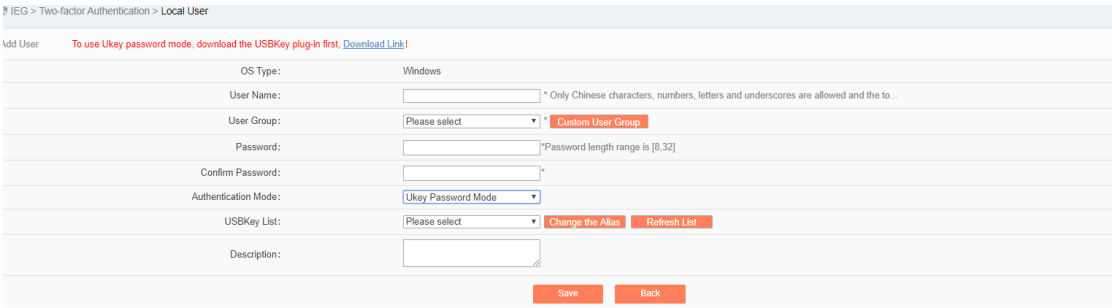


Fig.4-72 Add User Interface Normal USBKey Password

5) To modify the password means to modify the password of this user (as shown in Fig.4-73):

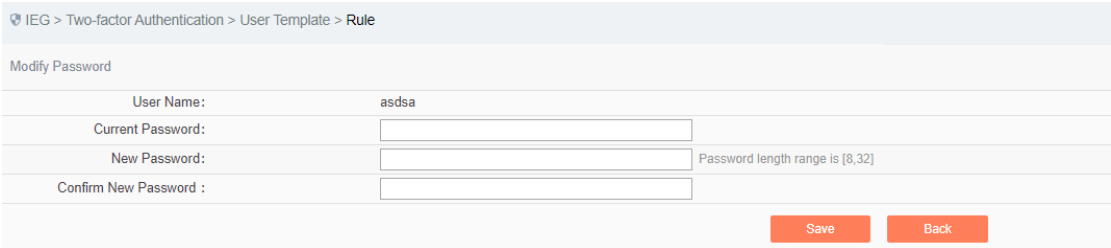


Fig.4-73 Modify Password Interface

6) USBKey binding, USBKey unbinding and PIN code reset. When the user selects the normal password authentication mode, USBKey binding appears behind the user. Click <USBKey Binding> to pop up a USBKey list, select the USBKey and click to save it (as shown in Fig.4-74):

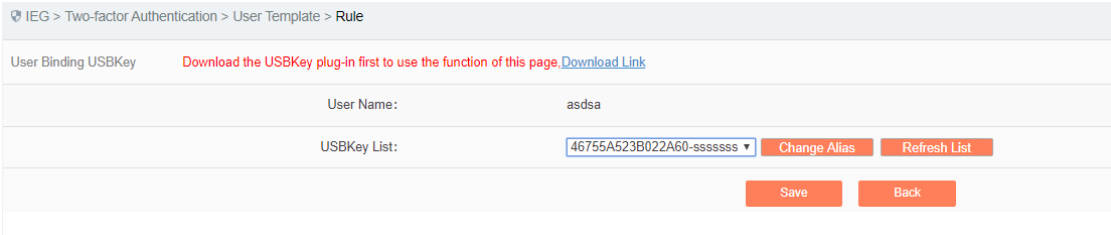


Fig.4-74 User Binding USBKey Interface

When the user is in the USBKey password authentication mode, USBKey unbinding, and PIN code reset will appear behind the user list. Clicking <USBKey Unbinding>, the user authentication mode will be changed to normal password mode. Click to reset the PIN code, with the PIN code of the USBKey set to the default value. The default value is Admin@123.

4.10.2. Authentication Policy

This function is mainly used to distribute the client's authentication policy command. By selecting and

matching various policies, the user distributes to a single or a batch of clients (as shown in Fig.4-75):

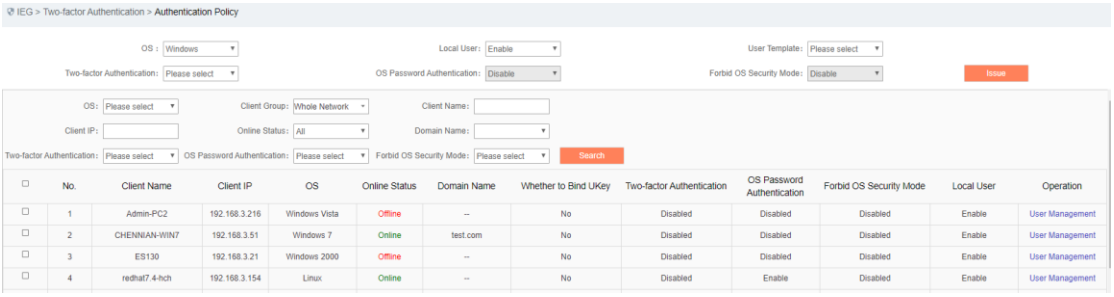


Fig.4-75 Authentication Policy Interface

1) Notably, the enabling and disabling of USBKey authentication is to control client authentication. The user can login with the USBKey and the password only when enabled. Enabling USBKey authentication requires a user binding USBKey on the client or a client joining in the domain.
2) For local users, when enabled, the existing user can use the operating system at the client normally; when disabled, the existing user cannot use it, and only the user distributed and created under the management platform can use it.
3) The user template, that is, the template created by the user template module. The template is overwritten when distributed, that is, to keep the existing users of the system and the users of the template only. When the management platform template is blank, all users created in the management platform at the client will be deleted.
4) OS password authentication, that is, the password authentication switch of the operating system where the client is located. (the OS system password turns off can only turn off the two factor switch, not the operating system switch.).
5) Disable the OS security mode, the security mode of the operating system is not available when enabled, with the security mode of the operating system available when disabled.
6) User management in the client operation column for Windows, click <User Management> to pop-up the user information reported from the client. As shown in the figure below, carry out USBKey binding, USBKey unbinding and PIN code reset for locally created users. (As shown in Fig.4-76):

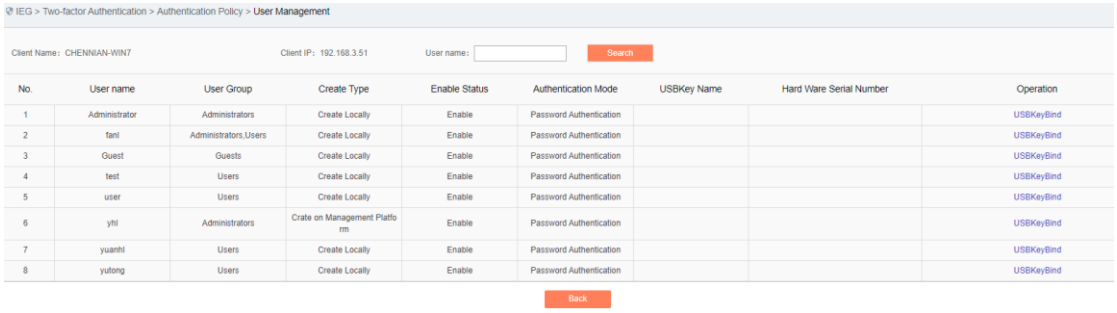


Fig.4-76

User Management Interface

7) User management in the client operation column for Linux, click <User Management> to enter the user management page at the client. (As shown in Fig.4-77):

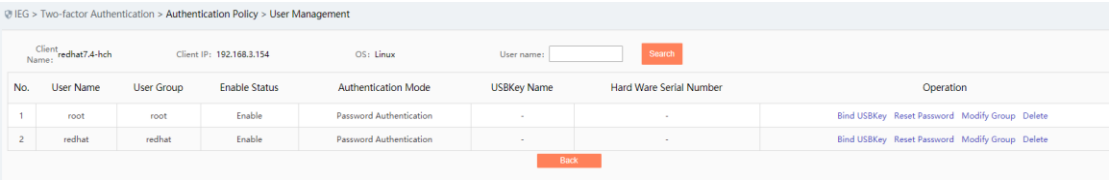


Fig.4-77 User Management Interface

4.10.3. Domain User Binding Information

Domain user management information mainly involves domain related operations, carrying out USBKey binding and unbinding for users joining the domain. The data in the list is added and reported from the client. (As shown in Fig.4-78):

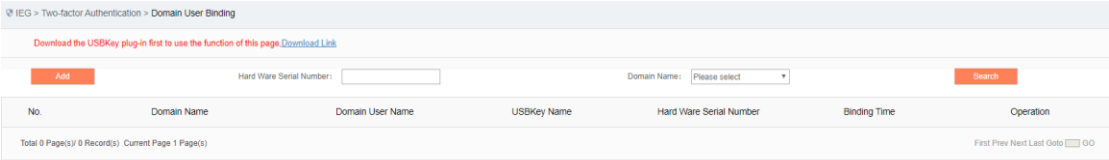


Fig.4-78 Domain User Binding List Interface

1) Click <Add> to add the domain user USBKey binding relationship (as shown in Fig.4-79):

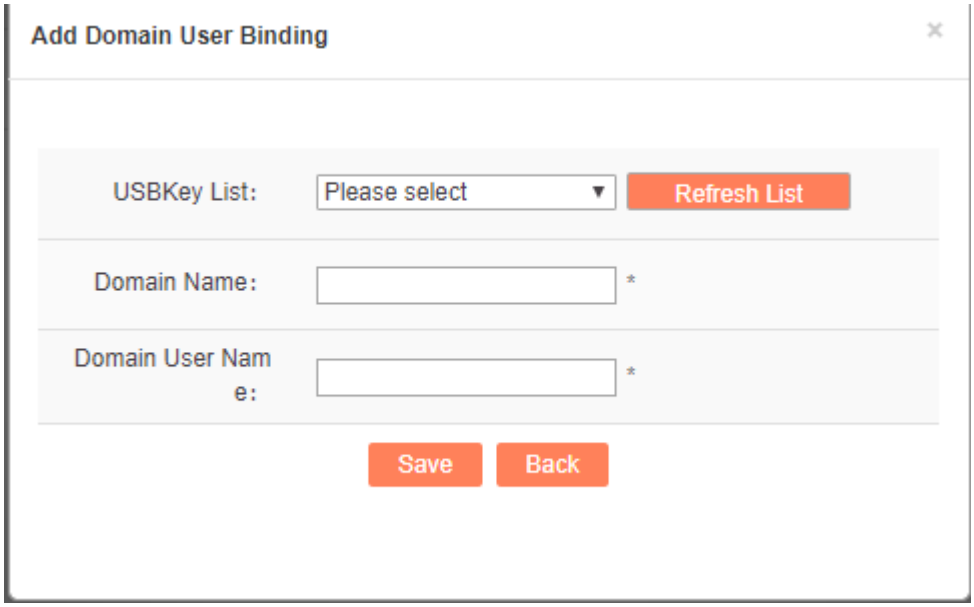


Fig.4-79 Domain User Binding Interface

2) Unbinding & unbinding. Only by inserting the corresponding USBKey can unbinding be done and deleted successfully.

4.11. Basic Configuration

Through the basic configuration module, the administrator can carry out basic system configuration, system operation log audit, authorization and uploaded non-whitelist file configuration.

4.11.1. Basic Configuration

This function controls the client (including Windows and Linux clients) to enable or disable the client self-

protection and alarm prompt.

Self-protection: when enabled, all configurations, registry entries and processes required for normal operation of this product are not allowed to be modified; when disabled, the above items are allowed to be modified.

Alarm prompt: when enabled, the operating system taskbar will pop up bubbles to prompt alarm information while generating real-time alarm; when disabled, bubbles will no longer be popped up to prompt alarm information.

Note: the Linux client is incapable of alarm prompt.

Function interface (as shown in Fig.4-86 Basic Configuration Interface):

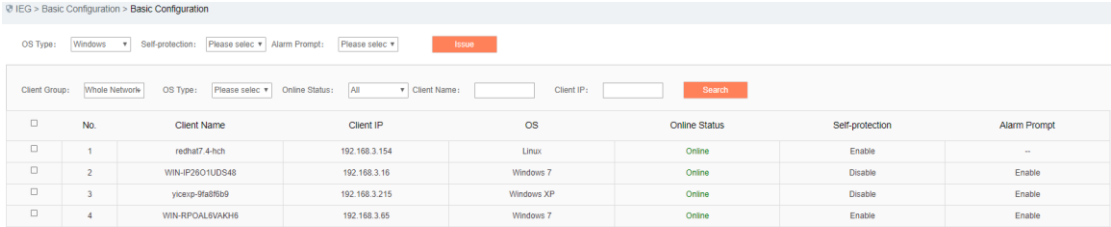


Fig.4-86 Basic Configuration Interface

4.11.2. Operating System Log Audit

The client can set the time to audit the operating system logs through this interface and distribute it to the specified client. Interface (as shown in Fig.4-87):

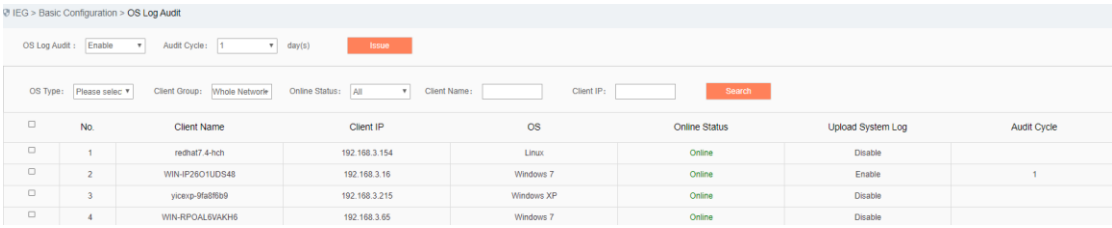


Fig.4-87 Operating System Log Audit Interface

4.11.3. Authorization Management

The administrator can view the current authorization information through this interface (as shown in Fig.4-88). When authorization expires or the administrator needs to add authorization nodes, the update authorization operation can be executed. Before installing the IEG server version, the unified management platform must import the authorization file first. Click <Please select the authorization file> to pop up the selection window (as shown in Fig.4-89), select the correct .lcs file and click <Open>. Click <Start to Upload> in the [Authorization Management] interface, upload the selected license file to the USM. The authorization management function list of the IEG module is: program whitelist, access control, security baseline, two-factor authentication, network whitelist, illegal outreach and peripherals management.

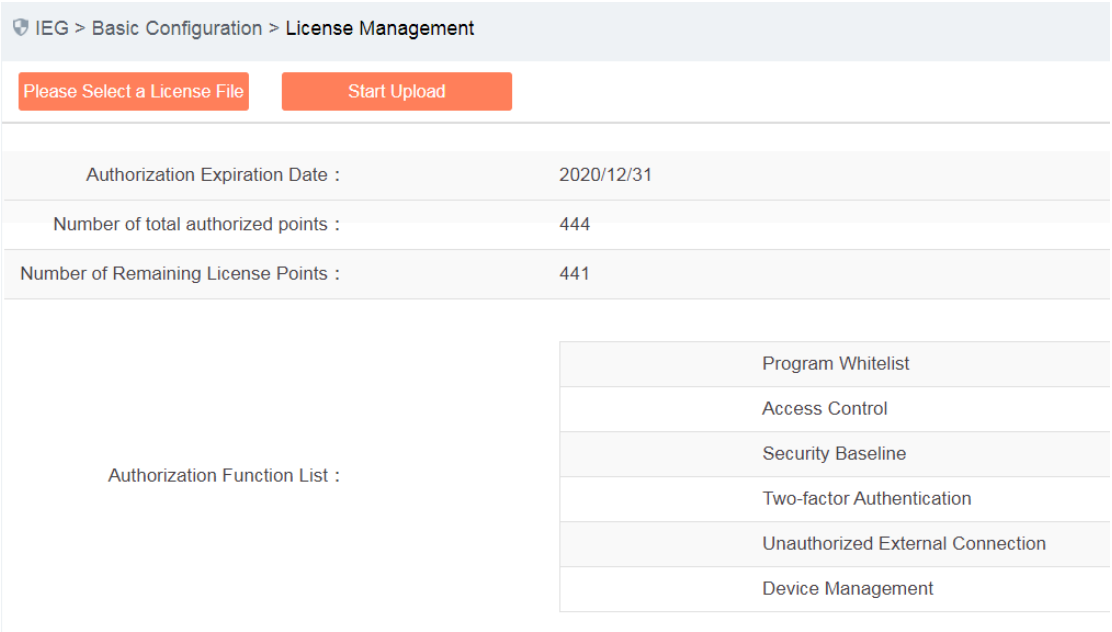


Fig.4-88 Authorization Management

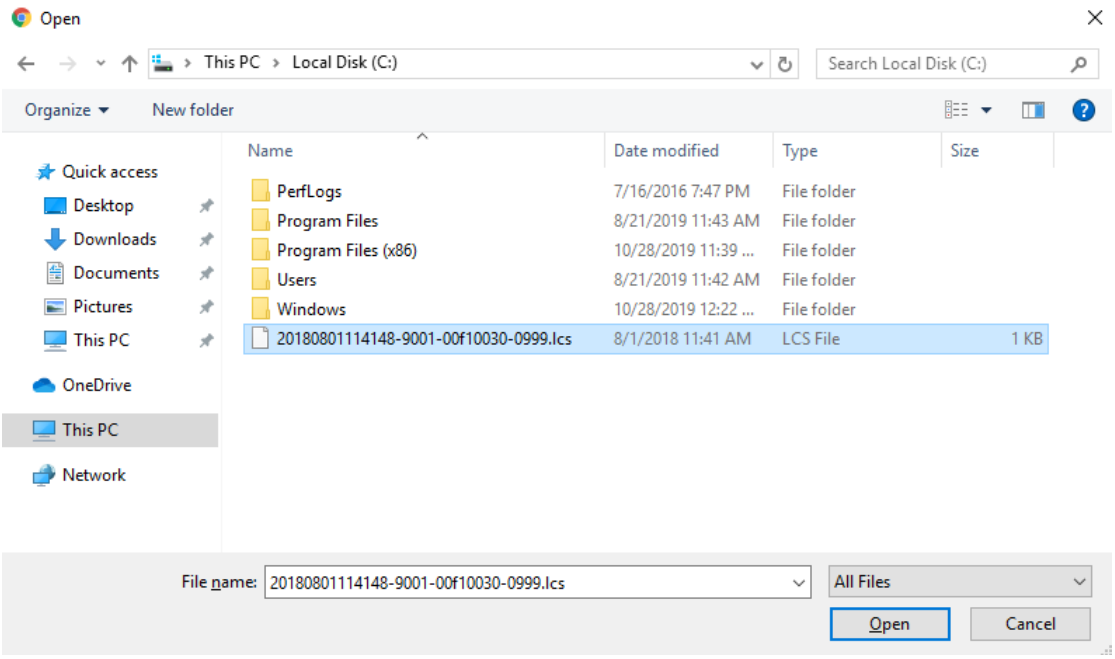


Fig.4-89 Selecting a License File

4.11.4. Upload a Non-Whitelist File

When this function is enabled, if the registered IEG client system has executed the executable program in the non-whitelist, and the executable program is less than 5M, the executable program will be uploaded to the unified safety management platform for future audit.

Functional interface (see Fig.4-90):

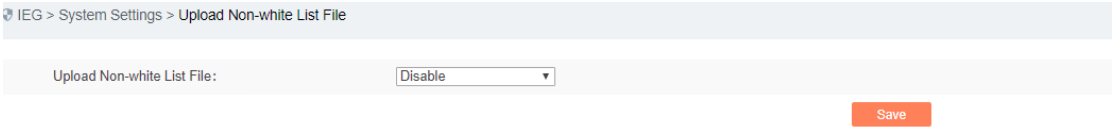


Fig.4-90 Uploading a Non-whitelist File.

4.11.5. Installation Package Management

The function of the installation package management page function is to easily save, download and manage the installation package files of IEG and other programs. It is convenient to upload and download, with enhanced convenience and improved work efficiency. Interface (as shown in Fig.4-91):

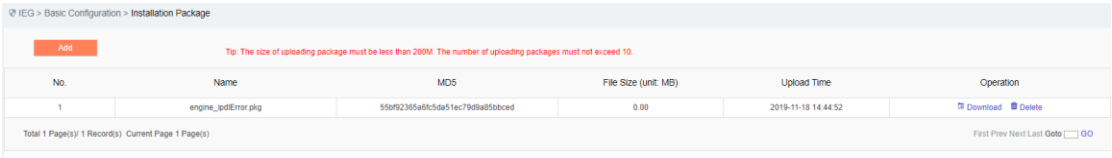


Fig.4-91 Installation Package Management Interface

Click <Add> to pop up the installation package page. Allow to upload a single file with a size up to 200M and up to 10 files uploaded in total (as shown in Fig.4-92):

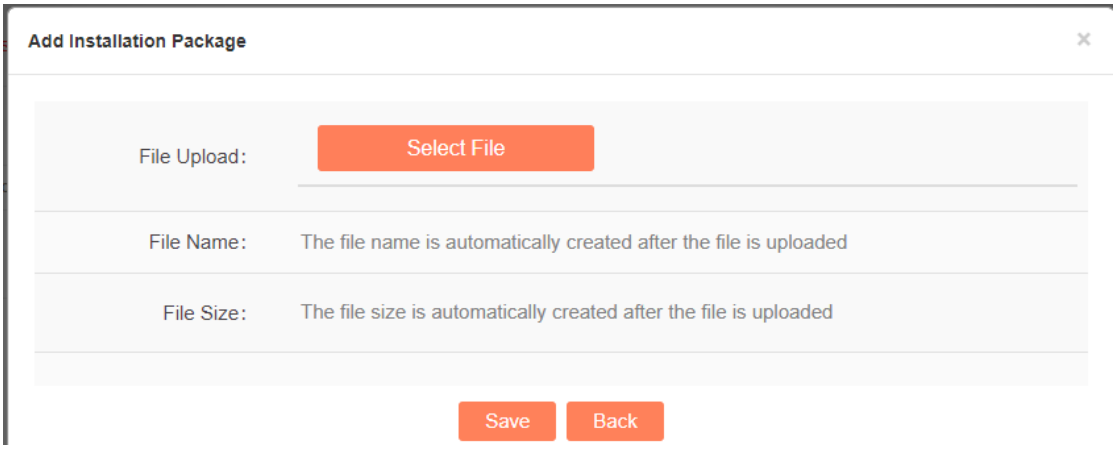


Fig.4-92 Add Installation Package Page

Click <Save> to save the uploaded file and go back to the installation package management list display page. Click <Back> to cancel the operation and go back to the installation package management list display page.

In the installation package management list display page, click <Download> in any installation package operation, allowing to download the corresponding files to local; click <Delete> in any installation package operation, allowing to delete the corresponding files (as shown in Fig.4-93):

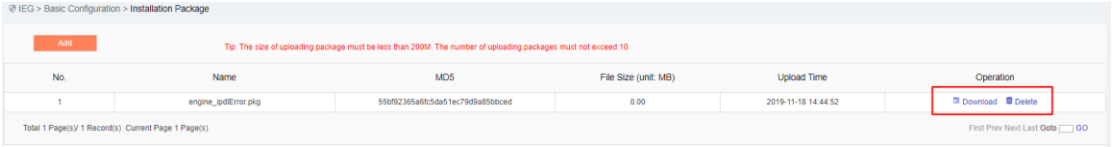


Fig.4-93 Installation Package Operation Button

5. Monitoring Audit

5.1 Introduction to Products

5.1.1 Product Overview

AVCOMM monitor audit is the leading audit product of industrial control industry. Its innovative advanced independently developed hardware is excellent in performance, low in power consumption and suitable for a variety of complex industrial production site environments. The software is of completely independent research and development. Combined with the independently developed hardware, it gives full play to the advantage of the hardware, supports network connection status detection, industrial protocol in-depth resolving, industrial protocol detection, historical traffic data audit of the entire network, network anomaly detection, key industrial event detection, user-defined rules alarm and industrial protocol industrial no traffic detection.

AVCOMM monitor audit is an information security audit system dedicated for the industrial control network. It adopts bypass deployment, of "zero risks" to the industrial production process. Based on the in-depth resolving (DIP, Deep Packet Inspection) of communication messages for the industrial control protocol (e.g., IEC104, S7, DNP3, Modbus TCP, OPC), it can detect network attacks, mis operation by users, illegal operation by users, illegal device access and the spread of worms, viruses and other malicious software in real time in view of the industrial protocol and give real-time alarms. In the meantime, it makes a detailed record on all network communication behaviors, including the command-level industrial control protocol communication records. It provides a solid foundation for security accident investigations on the industrial control system.

AVCOMM monitor audit, is widely used in power, oil, petrochemical, rail transit, tobacco, coal, iron & steel, advanced manufacturing and other industries.

AVCOMM monitor audit generally adopts decentralized deployment and centralized management. The product consists of two major components: **UM** and **intelligent monitoring terminal**. Notably, the intelligent monitoring terminal hardware device is distributed and deployed at the mirror port of the customer's network switch or connected into the specified network to receive centralized management of the management platform.

5.1.2 Appearance and Description

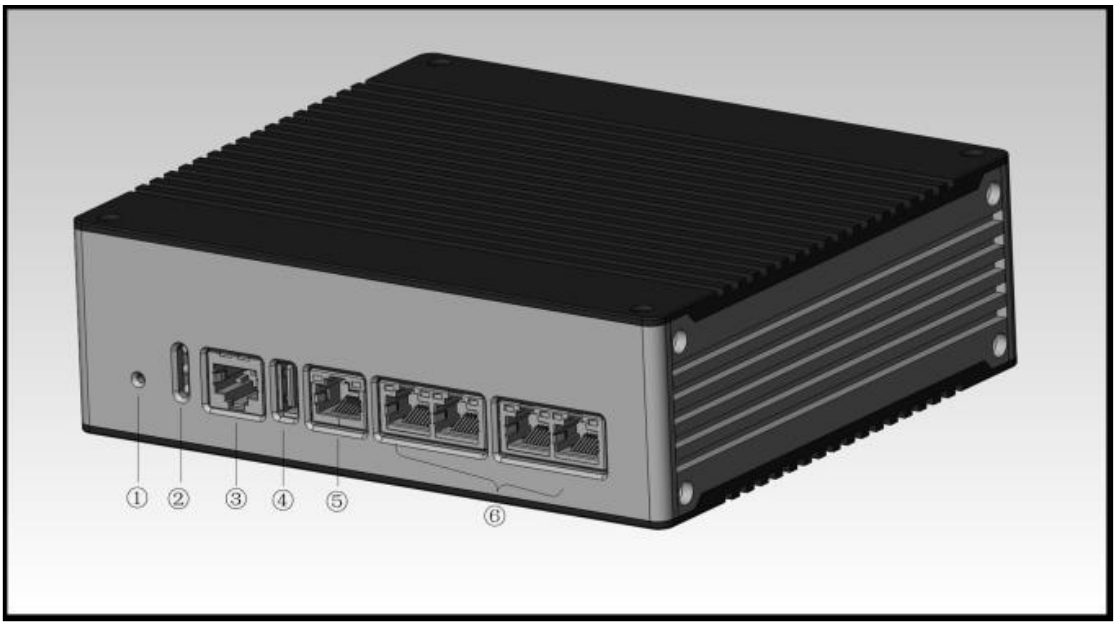


Fig.5-1 Appearance of Intelligent Monitoring Terminal

① Reset button
② LED indicator light
③ Console serial port, RS232
④ USB 2.0 interface
⑤ Management network port, 10/100/1000BASE-T adaptive Ethernet port
⑥ Service port, 10/100/1000BASE-T adaptive Ethernet port

5.1.3.Indicator Light Description

There are three indicator lights on the device, namely PWR, RUN and BP

Fig.5-2 Indicator Light

Tab.30 Instruction to Intelligent Monitoring Terminal

Indicator Light	**Panel Screen Printing**	**Status**	**Instructions**
Power light	PWR	NC	It is not powered on or a power failure occurs to the host
		NO in green	The power supply is normal, and the host is powered on normally

Run light	RUN	NC	The device is not powered on or breaks down
		Flashing in green	The device works regularly
		Flashing in red	The device fails or undergoes a network attack.
Bypass indicator light	BP	NC	The bypass function is not enabled
		NO	The bypass function is enabled
Ethernet electrical interface indicator light	MGMT ETH1/ETH2/ETH3/ETH4	NC	The corresponding interface is in an unconnected status
		Color of indicator lights	The green color indicates that the current operation is based on a gigabit rate. The orange color indicates that it is currently operating at 100 megabits
		The indicator light is normally on	The interface has been established
		The indicator light flashes	The interface is sending and receiving data

5.1.4.Technical Specifications

Tab.31 Technical Specifications for Intelligent Monitoring Terminals

Level-1 Demand Classification	Title	Description	Specification items	Specific Parameters or Indicators
Network Anomaly Detection	Protocol communication record	Conduct in-depth resolving for communication messages of the industrial control protocol, recording the communication logs on the industrial control protocol.	Recorded industrial protocols include	OPC DA, HAD, A&E, DX
				Modbus TCP
				Siemens S7
				DNP3
				IEC104
				CIP
				MMS

		Record the network connection information for non-industrial control protocols or industrial control protocols. Record contents include time (start, end), source MAC, source IP address, source port, destination MAC, destination IP address, destination port, protocol, number of messages (uplink, downlink), number of bytes (uplink, downlink).		PROFINET
				FINS
			Configure whether to record industrial control protocol session information in the command line of the terminal	Support
			The one-month record on each industrial control protocol for a single table supports up to	10 million entries
			Record all network session information by default	Support
			Set rules of whether to record certain session information	Support
			When setting a rule, the configuration items for the rule include	Source IP, destination IP, source IP mask, destination IP mask, protocol, start source port, end source port, start destination port, end destination port, and execution action
			This rule is included in a template, with each template specification supporting up to	1,000 entries
			The one-month record on industrial control protocol supports up to	10 million entries
	Modeling normal communication behaviors	Based on the communication record on industrial control protocol, the industrial control communication model whitelist is established by self-learning, that is, the	Industrial protocols that can establish a whitelist include	OPC DA, HAD, A&E, DX, OPC protocols support dynamic port tracking
				Modbus TCP
				Siemens S7
				DNP3

		normal communication behaviors are modeled. Support the administrator to manually adjust the industrial control communication model whitelist.		IEC104
				CIP
				MMS
				PROFINET
				FINS
			Total rules included in each whitelist template can support up to	3,000 entries (either in view of learning or manually adding)
	Abnormal communication behavior detection	Compare the current industrial control protocol communication behavior with the whitelist, and give an alarm for behaviors deviating from the whitelist	Add an alarm event to the whitelist with one click	Yes, but alarms for violating Modbus TCP range, OPC DA range, Siemens S7 range do not support to add into the whitelist with one click.
			For one month, such alarms can support up to	10 million entries
	Abnormal traffic	Monitor the inflow and outflow traffic of the device, give an alarm when exceeding the baseline value	Graphical display of abnormal traffic	Support
			Abnormal traffic statistics cycle	5 minutes
			Abnormal traffic alarm confirmation and alarm status linkage	Support
			Manual configuration of abnormal traffic baselines	Support
Network attack detection	Industrial control protocol attack detection	To detect and alarm the format of the industrial control protocol messages that do not conform to its specification	Industrial protocols that can be detected include	OPC DA, HAD, A&E, DX
				Modbus TCP
				Siemens S7
				DNP3
				IEC104
				CIP
				MMS
				PROFINET
				FINS

			Support not to detect a specific protocol of some IPs, with no-detection rules that can configure up to	1,000 entries
			For one month, the system supports up to	10 million entries
	User-defined warning rules	Allow the administrator to customize the industrial control protocol communication alarm rules and give an alarm for communication behaviors meeting the alarm rules.	Industrial control protocols supporting User-defined alarm setting include:	OPC DA, HAD, A&E, DX
				Modbus TCP
				Siemens S7
				DNP3
				IEC104
				CIP
				MMS
				PROFINET
				FINS
			Each protocol supports up to	1,000 entries
			For one month, support up to	1 million entries
	Detection based on parameter thresholds	Set a detection threshold for specific process status parameter and the control signal, give an alarm for events exceeding the threshold.	Protocols supporting range control include	Modbus TCP, OPC DA, Siemens S7
			This rule supports up to	3,000 entries, including the whitelist rules.
			For one month, support up to	10 million entries, including the Modbus whitelist rules.
Key event detection	No traffic detection	Within the set time, a service of a single IP (such as Modbus) receives no message, thus requiring an alarm.	Specify that this function can be enabled or disabled on the terminal	Support
			No traffic time range	5-86,400 seconds
			This rule supports up to	1,000 entries
			For one month, support up to	100,000 entries
	Key event detection	Give an alarm for engineer station configuration change, control instruction changes, PLC download,	Key event definition	Built in the system
			User-defined key events	Not support
			Key events include	The write operation

		load change and other key events.		For S7 protocol: 26 request downloads, 27 start download, 28 complete downloads, 29 request upload, 30 start upload, 31 complete uploads, 40CPU start, 41CPU stop
			This rule supports up to	1,000 entries
			For one month, support up to	1 million entries
Network connection statistics	Network connection view	Network connection real-time view, real-time graphical display of all network connections within the monitoring range, and abnormal network connections highlighted in red. Network connection history view, graphical display of all network connections within the monitoring range for a certain time period, and abnormal network connections highlighted in red. Double-click an IP to display details of each connection connected to such an IP. Support filtering based on source and destination IP addresses, only displaying connection views related to a certain IP address. Supports filtering based on source and destination ports, only displaying connection views related to a certain port.	Provide a connection with the configuration interface well-configured.	Support
			Exception connections need to be stored in the database and used in the history view from being established to ended	Store historical connection data for up to 3 months
			Connection details include time (start, end), source MAC, source IP address, source port, destination MAC, destination IP address, destination port, protocol, number of messages (upstream, downstream), number of bytes (upstream, downstream)	There is no upper limit for the number of entries displayed in real time
			Real-time views display: number of nodes connected by each IP node; number	Support

		Support filtering based on source and destination MAC addresses, only displaying connection views related to a certain MAC address.	of ports enabled; number of upstream and downstream messages	
			IP configuration displayed or hide in the connection diagram	Support
			The configuration items in the connection baseline include: source IP, destination IP, destination port	Support up to 1,000 entries
			The network traffic baseline configuration items include: source IP, destination IP, number of upstream bytes and downstream bytes	Support up to 1,000 entries
	Traffic statistics	Provide statistics of real-time, historical minutes, historical days (customizable range), etc. of network traffic and number of messages.	Real-time traffic display is realized in three specifications	For the last 60 minutes, one point for the horizontal axis refers to every 5 minutes
				Last 24 hours
				Last 30 days
			The history view can customize statistics objects (select which host to make statistics), and the traffic and messages can be reflected in the same view	Support
	Order statistics	The hosts and network devices sorted by outflow, inflow and total traffic within a certain time range are shown in a bar chart,	Traffic TOP N can be set	N range: 1-50
			The type of traffic statistics is available for drop-down options	Drop-down options include all, send and receive

		which can skip to detailed messages. The hosts and network devices sorted according to the number of outflow, inflow and total messages within a certain time range are shown in a bar chart, which can skip to detailed messages. The hosts and network devices sorted by outflow, inflow and total connection ports within a certain time range are shown in a bar chart, which can skip to detailed messages. The hosts and network devices sorted by connection ports within a certain time range are shown in a bar chart, which can skip to detailed messages.	Message number TOP N can be set	N range: 1-50
			The type of message statistics is available for drop-down options	Drop-down options include all, send and receive
			Port statistics TOP N can be set	N range: 1-50
			The type of port statistics is available for drop-down options	Drop-down options include all, source port and destination port
			All statistics can be configured with a time range	Support
Operation mode support	The system can work in multiple modes	Learning mode: the system collects learning data in this mode to assist in generating whitelist rules. In this mode, there is no alarm for the whitelist, with other alarms normally generated	Effective time for switching the mode	<3s
		Operation mode: for messages violating the whitelist rules and the protocols, give an alarm for messages of user-defined rules, no traffic rules and key events, which can be viewed in the management center		
Deployment mode support	The terminal device can be	According to the actual network requirements, the	Bypass deployment	Support

	deployed in many ways	terminal supports various deployment modes	Serial deployment	Support
			Bypass forwarding deployment	Support
Performance	Time accuracy	Time accuracy of communication records	Time accuracy requirement	<1ms
	Number of terminals	Depending on different server configurations, the number of terminals that are online at the same time as supported by each type of server are different	The low-end server supports up to	10 terminals
Session management	Session table query	Maximum timeout	Maximum query time, beyond which the query will stop	30s
		Maximum number of sessions	Maximum number of sessions supported by a single intelligent monitoring terminal	120000
	Session aging time	TCP default time	Factory default TCP session aging time	3 minutes
		TCP session aging time setting	A session aging time range can be set	1-120 minutes
		UDP default time	Factory default UDP session aging time	3 minutes
		UDP session aging time setting	A session aging time range can be set	1-120 minutes
Management functions	Policy management	Provide a friendly user management interface to manage policies	Industrial protocol whitelist template management	Support
			Protocol parameter configuration	Support
			Protocol detection exception template management	Support
			No traffic detection template management	Support
			Key event detection template management	Support

			User-defined rules	Support
			Network session audit template management	Support
	Alert statistics	make statistics and summarize all alarm information in the system	Alarms supported include	Industrial protocol whitelist alarm
				Industrial protocol alarm
				No traffic alarm
				User-defined alarm
			Graphical display	Support, including histograms, pie charts and trend charts
			Statistical result export	Support PNG, JPG, SVG and PDF format export
	Authorization control	The intelligent monitoring terminal is authorized to play the role in monitoring and audit	A special tool authorizes the specified device	Support
			The management platform can view, download and update the authorization, with the result prompted when updating	Support
			It is in the yellow background color when the authorization is less than 1 month, and in the red background color in case of expired authorization	Support
	Terminal device status view	The status information on the device can be viewed in real time in the management interface	Information refresh time	<5s
			Statuses that can be viewed include	CPU usage
				Memory usage
				Hard disk usage

	Upgrade management	All components within the system can be upgraded seamlessly	Automatic upgrade of the management platform	Not support
			Manual upgrade of the management platform	Support
			Automatic upgrade of the intelligent monitoring terminal	Not support
			Manual local upgrade of the intelligent monitoring terminal	Support
			The management platform upgrades the intelligent monitoring terminal	Support
	Remote management	Able to configure and manage policies in the system remotely	Manage the system based on the Web method	Support
	Permission authentication	ID authentication	Need to authenticate the user's ID	Support
			User separation of powers	Support, including the system operator, the configuration administrator, auditor
			Password strength	Length 8-16, a combination of upper and lower case letters, numbers, special characters (#@!~%^&*)
		Trusted host	IP authentication	Support
			MAC authentication	Support, optional
Storage management	All alarms and log data generated by the system will be saved to the server for	Log storage mode	Database	Support, MySQL
		Log storage cycle	Support up to	3 months
		Able to query the logs in the system	A dedicated tool is available for query	Support
			Process alarm incidents	Support

	centralized management		Logs can be retrieved based on specified conditions	Support
		Performance	Regular backup	Yes, up to 3 months
			Maximum number supported for each type of logs	Refer to each functional indicator
			Maximum number supported for each type of alarms	Refer to each functional indicator
	Database backup	The audit management platform supports to back up the data automatically to a specified server. Automatic backup supports two check policies: the disk space reaching the usage limits and the real-time data reaching the specified limits. Also, able to specify to which server the backup is done	Disk usage limits	50%-90%
			Storage cycle usage restrictions	1-99, unit: days
			The server address to which the backup can be set	Support
			Anonymous user backup	Support
System configuration	Decoding engine configuration	Decoding engine loading	Number of decoding engine configuration protocols loaded at the same time for the USM	<16

5.2. Startup and Login

5.2.1.Startup of Intelligent Monitoring Terminal

Based on the intelligent monitoring terminal hardware installation manual, install the intelligent monitoring terminal to a specified position, guaranteeing that the power connector of the intelligent monitoring terminal can work normally. After connecting it with the required power supply, start the intelligent monitoring terminal normally. Use the console port as per the installation manual to monitor the startup process of the intelligent monitoring terminal.

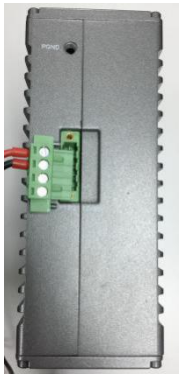


Fig.5-3 Powering on the Intelligent Monitoring Terminal with the Power Cord Provided

After the normal startup of the intelligent monitoring terminal, the new intelligent monitoring terminal will be authorized before it works. With the "initial status" as the default operation mode, the intelligent monitoring terminal has no monitoring policies now, thus will not make any records on all messages from the intelligent monitoring terminal. When starting to monitor, corresponding configurations shall be made in the "policy management" configuration page of the management platform. Then the intelligent monitoring terminal to enable monitoring shall be selected, with the configured policy application assigned to the terminal.

If the intelligent monitoring terminal has been registered to the management platform, then when enabled, the intelligent monitoring terminal will use the policy configuration before the last startup.

5.2.2.Use of CLI

CLI (Command Line Interface) is a text-like command interface between users and devices. A user enters text commands and submits them to the device to execute the corresponding commands by pressing Enter, so as to configure and manage the device, and confirm the configuration result by viewing the output information.

Since some operations of the device are to be completed in this interface, after the device is started, some necessary configuration shall be done using the CLI command, such as to set the address of the management platform connected.

The intelligent monitoring terminal supports multiple ways to enter the CLI interface, such as to directly connect via the Console port or enter the CLI interface by logging in the Telnet/SSH logon device, etc. Either way, the default username when logging in the device is: AVCOMM, and the default password is: AVCOMM. CLI interface of the device. (As shown in Fig.5-4):

```
cavium-linux login: winicssec
Password:

Entering character mode
Escape character is '^]'.

=== WELCOME TO WNT CLI ===

CLI>
```

Fig.5-4 Command Line Interface - Common View

5.2.2.1. Help

CLI>help

Display help information.

5.2.2.2. System statistics related.

CLI>show pkt stat

View message statistics at all levels.

CLI>show fpa

View the FPA information, mainly on various memory statistics.

CLI>show mem pool

View the mem pool memory information.

CLI>config

Enter the system view.

5.2.2.3. Service-related

CLI# show log level

Level: TRACE (5)

View the log level.

CLI# show log plane

View the enabling of a module log

CLI# set log level <level>

Set the log level.

CLI# set log plane <module_id> [dp|mp|ap|cl]

Set/disable a module log.

5.2.2.4. Set the IP address of the management platform.

CLI>show serverip

View the IP address of the management platform configured on the intelligent monitoring terminal.

CLI#set serverip 192.168.8.8

Set the IP address of the management platform to which the intelligent monitoring terminal shall be connected

CLI>config

Set the industrial firewall gateway command,

For example: if the gateway address of 192.168.1.1 needs to be added, the complete command is as follows:

CLI# set mgmtgw 192.168.1.1

5.2.2.5. Set the access mode of the intelligent monitoring terminal.

CLI#set sma deploy mode access.

Set the access mode of the intelligent monitoring terminal to serial deployment.

CLI#set sma deploy mode port-mirror.

Set the access mode of the intelligent monitoring terminal to mirror deployment.

CLI# set sma deploy mode mirror-forward.

Set the access mode of the intelligent monitoring terminal to bypass forwarding deployment

5.2.2.6. Change the IP address of the intelligent monitoring terminal.

CLI#set mgmtip 192.168.8.6

Change the IP address of the intelligent monitoring terminal.

5.3. Intelligent Monitoring Terminal Management

5.3.1. Introduction to Functions

The intelligent monitoring terminal is the management object of the management platform. All configurations aim for specific intelligent monitoring terminals. For example, the whitelist policy rules of intelligent monitoring terminals shall be distributed to a specific intelligent monitoring terminal to play a role.

5.3.2. Intelligent Monitoring Terminal Management

After successfully logging in the management platform, find [Monitoring Audit] in the upper menu bar, click the button, then find [Intelligent Monitoring Terminal Management/Intelligent Monitoring Terminal Management] in the left navigation bar, click the menu (as shown in Fig.5-5) to view the intelligent monitoring terminal management page (as shown in Fig.5-6):

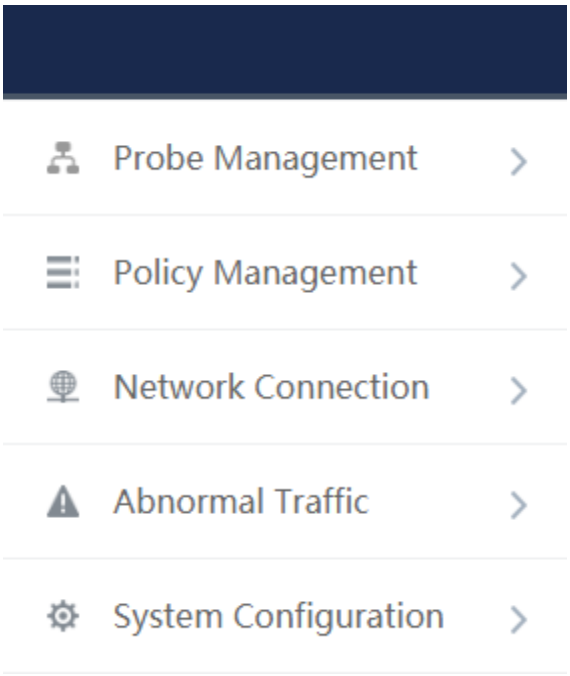


Fig.5-5 Intelligent Monitoring Terminal Management in Navigation Bar

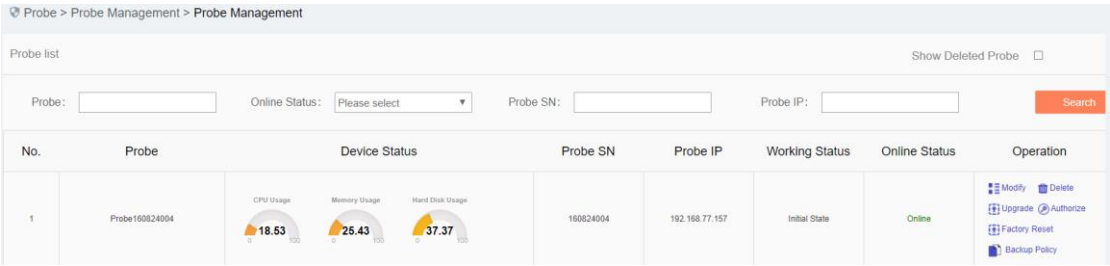


Fig.5-6 Intelligent Monitoring Terminal Management Page

View the current running status of the intelligent monitoring terminal, with the following meanings:

Tab.32 Instruction to Intelligent Monitoring Terminal Management List Display

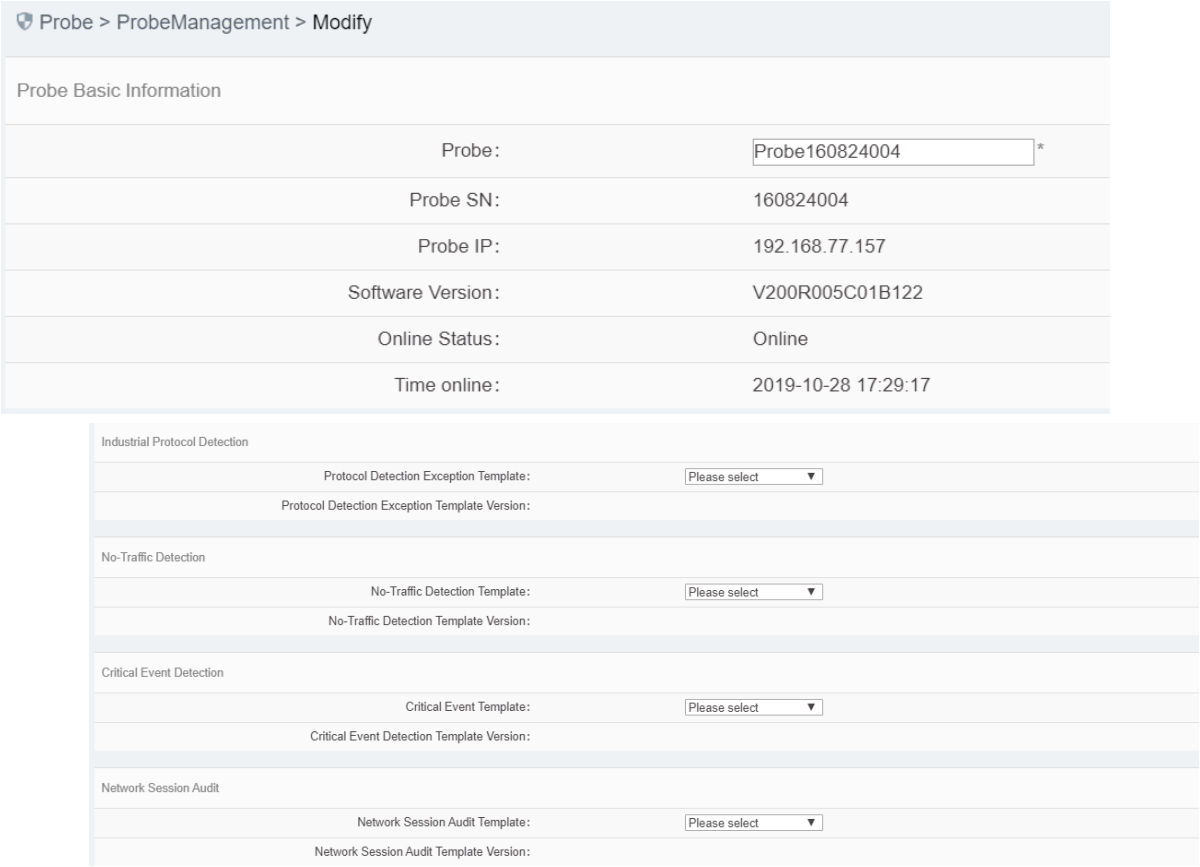
Column Names	**Instructions**
Intelligent monitoring terminal name	A name used by the system or a user for each intelligent monitoring terminal, for example "Intelligent Monitoring Terminal, Control Room, Production Workshop 1"
Device status	Current running status of the intelligent monitoring terminal, including CPU usage, memory usage and hard disc space usage. If a certain value is always overloaded within 1min, a corresponding alarm will be generated.

Intelligent monitoring terminal ID	The unique identification number of the intelligent monitoring terminal automatically assigned by the system. A number represents the unique intelligent monitoring terminal	
Intelligent monitoring terminal IP	IP address of the intelligent monitoring terminal management network port	
Working status	Under which operation mode the intelligent monitoring terminal is currently in, the new intelligent monitoring terminal is defaulted to "initial state".	
Online status	The current intelligent monitoring terminal is connected to the management platform (that is, online) or not connected (that is, offline)	
Operation	details Modify	View more details of the intelligent monitoring terminal, including to change the operating mode of the terminal and adjust the policy
	Delete Delete	Delete the offline intelligent monitoring terminal, not allow deleting online intelligent monitoring terminals. Click "Display Deleted Intelligent Monitoring Terminal" to view and restore the information in view of the deleted intelligent monitoring terminal
	Upgrade Upgrade	Upgrade the software running on the intelligent monitoring terminal online. Conduct the operation only with the intelligent monitoring terminal online. Refer to chapter 5.3.2.3 Intelligent Monitoring Terminal Upgrade
	Authorization Authorize	View and change the authorization items of the intelligent monitoring terminal
	Restore the factory settings. Factory Reset	Restore the specified intelligent monitoring terminal to the factory state, clear all configurations except those authorized for the intelligent monitoring terminal

	Back up all policy applications Backup Policy	Copy all policies being applied on the source device to one or more other online and non-learning devices for distribution

5.3.2.1. Information view

Click <Details> under the operation column in [Intelligent Monitoring Terminal List] to display the detailed information on the intelligent monitoring terminal (as shown in Fig.5-7):



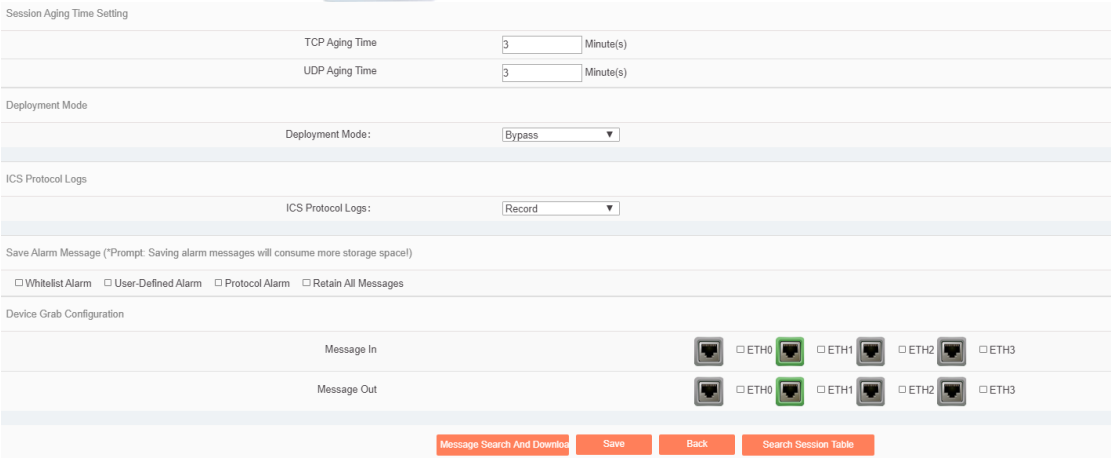


Fig.5-7 Intelligent Monitoring Terminal Information View Page

This page contains more details about the selected device.

Click <Back> in this page and go back to the [Intelligent Monitoring Terminal List Display] page.

Directly modify the intelligent monitoring terminal configuration via <Details>, including basic information on intelligent monitoring terminal, operation mode of intelligent monitoring terminal, whitelist template currently applied to intelligent monitoring terminal, industrial protocol detection template, no traffic detection template, key event detection template, network session audit template and alarm message save configuration.

Tab.33 Instruction to Intelligent Monitoring Terminal Details

Column Names	**Instructions**
Intelligent monitoring terminal name	Define a meaningful name for the intelligent monitoring terminal that is easy to understand and remember
Intelligent monitoring terminal number	Number given when delivering the intelligent monitoring terminal
Intelligent monitoring terminal IP	IP address of the intelligent monitoring terminal management network port
Software version	Software version that is currently used for the intelligent monitoring terminal
Online status	Connection status of the intelligent monitoring terminal and the management platform
Time online	Online time of the intelligent monitoring terminal
Operation mode	1. If the current mode is Learning Mode, only items "Learning Completed", and "Learning Mode" are available in the drop-down operation mode list. 2. If the current mode is Learning Completed, only items "Learning Mode" and "Operation mode" are available in the drop-down operation mode list.

	3. If the current mode is Operation mode, item "Learning Mode" is available in the drop-down operation mode list. 4. If the user changes the mode to Learning Mode, the whitelist template settings below will turn gray and become inoperable 5. If the user changes from Learning Mode to Learning Completed, a whitelist template generation edit box will appear, allowing the user to name the whitelist template generated by learning
Whitelist template name	The whitelist rule template name used by the intelligent monitoring terminal. Only when the intelligent monitoring terminal changes to "running mode" can the edit box be highlighted, and a whitelist template must be selected before it can be saved.
Whitelist template version	The whitelist template version number applied to the intelligent monitoring terminal
Protocol detection exception template	The protocol detection exception template name applied to the intelligent monitoring terminal
Protocol detection exception template version	The protocol detection exception template version number applied to the intelligent monitoring terminal
No traffic detection template	The no traffic detection template named applied to the intelligent monitoring terminal
No traffic detection template version	The no traffic detection template version number applied to the intelligent monitoring terminal
Key event detection template	The Key event detection template name applied to the intelligent monitoring terminal
Key time detection template version	The key time detection template version applied to the intelligent monitoring terminal
Network session audit template	The network session audit template name applied to the intelligent monitoring terminal

Network session audit template version	The network session audit template version number applied to the intelligent monitoring terminal	
TCP aging time	The TCP session aging time of the intelligent monitoring terminal	
UDP aging time	The UDP session aging time of the intelligent monitoring terminal	
Deployment mode	The deployment mode of the intelligent monitoring terminal	
Industrial protocol audit log	Whether the intelligent monitoring terminal sends an industrial protocol audit log	
Warning messages save	Whitelist alarm	Whether the intelligent monitoring terminal saves messages generating a whitelist alarm
	User-defined alarm	Whether the intelligent monitoring terminal saves messages generating a custom alarm
	Protocol alarm	Whether the intelligent monitoring terminal saves messages violating the protocol
	Retain all messages	Whether the intelligent monitoring terminal saves all original messages
Network port grab	Check grab network port, support to capture the message of any one or more ports including eth0, eth1, eth2, eth3, eth4, and eth5. It is possible to specify to capture the incoming, outgoing, or two-way message of each port. The management platform stores the captured messages according to the device port, and can query and download the messages.	
Operation	Save	Save all modification information and make it come into effect, and go back to the intelligent monitoring terminal page
	Back	Ignore all modifications and go back to the intelligent monitoring terminal information list display page
	Query session table	View the session table on the intelligent monitoring terminal
	Message query and download	View all the messages captured by the network port grab, which can be downloaded

5.3.2.2. Delete an intelligent monitoring terminal.

Click <Delete> under the operation column in the intelligent monitoring terminal list to delete offline intelligent monitoring terminals that are no longer in use. (As shown in Fig.5-8):

Fig.5-8 Deleting the Intelligent Monitoring Terminal

5.3.2.3. Intelligent monitoring terminal upgrade

When a new intelligent monitoring terminal version that is more powerful in functions and more stable in operation is launched, users can upgrade the intelligent monitoring terminal device remotely through the management platform.

After opening the [Intelligent Monitoring Terminal Management] page, click <Upgrade> under the operation column in the intelligent monitoring terminal list to pop up the [Please Select an Upgrade File] dialog box. (As shown in Fig.5-9):

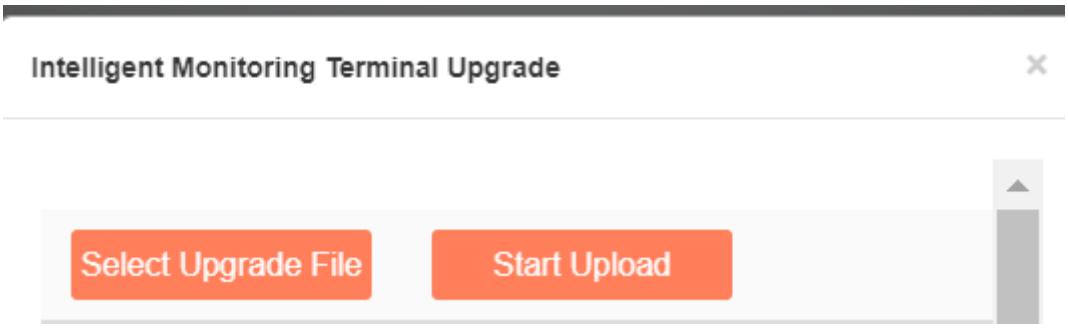


Fig.5-9 Selecting an Upgrade File for Intelligent Monitoring Terminal

- Please select an upgrade file

Click [Please Select an Upgrade File] to pop up the file selection dialog box. Find the new upgrade file (for example: sys-sensor.tar.gz), double-click the file or select <Open>.

- Start upload.

When clicking this button, the browser will first upload the upgrade file to the server where the management platform is located, and then inform the intelligent monitoring terminal, which will execute specific upgrading actions.

- Close

Click <Close> will not execute any operations, but directly go back to the intelligence monitor terminal list page instead.

5.3.2.4. Authorization management

A license means a permit, it is a contractual form for device suppliers to authorize the use scope and deadline, etc. of product features. The License can dynamically control whether certain features of a product are available or

not. Users can purchase a License to activate certain features and functions as needed. For this product, there can only be one License file in active state in each intelligent monitoring terminal device, and activating the new License will invalidate the old License.

Currently, the device supports the following methods to activate a License:

- Manually activated through the management platform

  After purchasing or updating a License and obtaining the License authorization certificate, the device under management shall be authorized or the authorization shall be updated by logging in the specified page of the management platform.

Intelligent monitoring terminal authorization management consists of three components: authorization tool, intelligent monitoring terminal and management platform. The authorization tool belongs to AVCOMM and is only available to specified users within the Company.

5.3.2.4.1. **Check authorization.**

After opening the [Intelligent Monitoring Terminal Management] page, click<Authorization> under the operation column in the intelligent monitoring terminal list to enter the detailed authorization information page. (As shown in Fig.5-10):

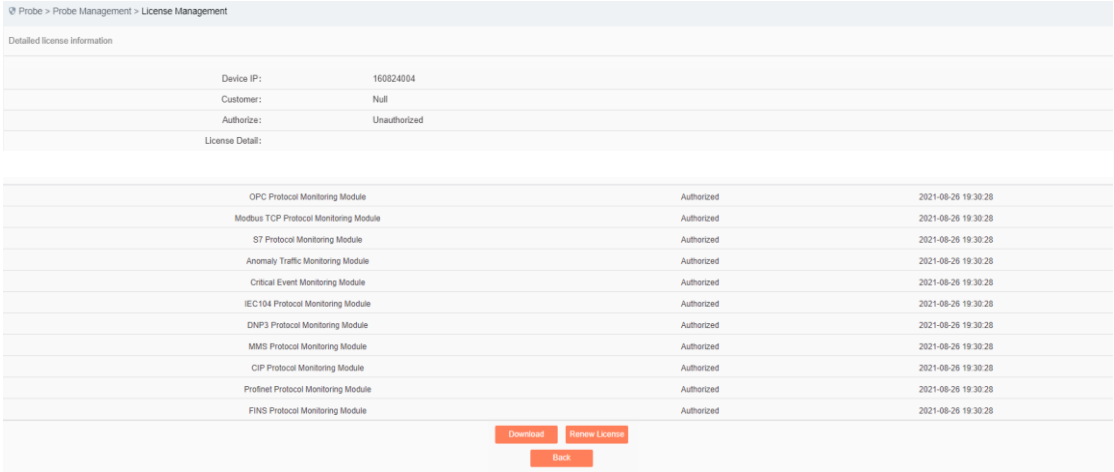


Fig.5-10 Authorization Details View Page

This page displays the authorization details of the current intelligent monitoring terminal.

- Renew License

  Update the authorization information on the current intelligent monitoring terminal

- Download

  Download the authorization file for the current intelligent monitoring terminal.

- Back

  Close the current page and return to the intelligent monitoring terminal management page.

5.3.2.4.2. Update the intelligent monitoring terminal authorization information.

In the opened intelligent monitoring terminal authorization page, click <Update Authorization> to pop up the authorization file selection dialog box to update the latest authorization file obtained by the user from the manufacturer to a specified intelligent monitoring terminal (as shown in Fig.5-11):

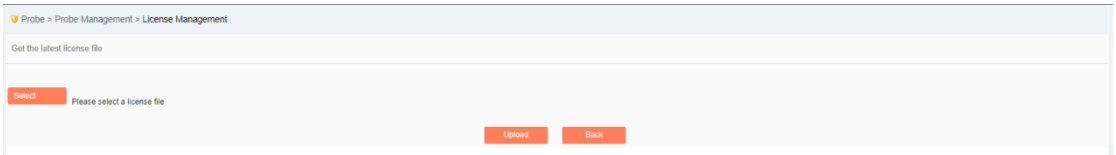


Fig.5-11 Selecting the New Authorization File to be Upgraded to the Intelligent Monitoring Terminal

- Select a file.

  Click "Select a File" to pop up the file selection dialog box.

  Find the new authorization file (for example: a file that is named with the device ID and suffixed with ".dat"), double-click the file or select <Open>, then click <Upload>. The browser will upload this file to the server where the management platform is located first, then notify the intelligent monitoring terminal. The intelligent monitoring terminal will update the authorization. Upon the successful upgrade, the user will be able to view the new authorization information in the authorization page.

- Back

  Clicking <Back> will not execute any operations, but directly go back to the intelligent monitoring terminal authorization details page instead.

5.3.2.5. Retrieve an intelligent monitoring terminal.

In the [Intelligent Monitoring Terminal List] page, intelligent monitoring terminals can be retrieved according to the conditions. (As shown in Fig.5-12):

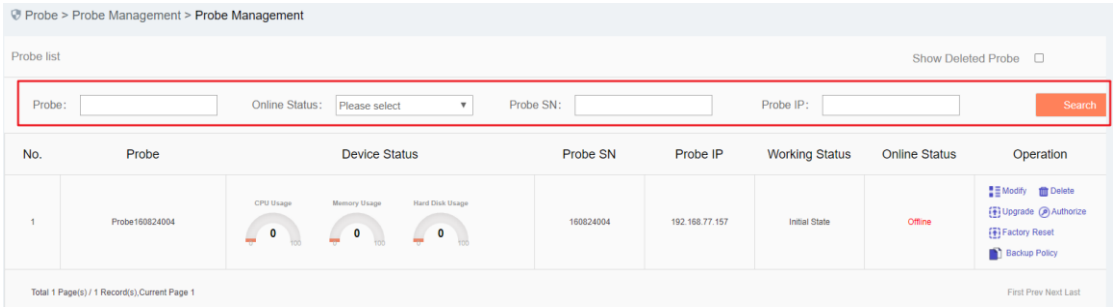


Fig.5-12 Retrieving an Intelligent Monitoring Terminal

5.4. Policy Management

Policy management can manage all monitoring templates used by intelligent monitoring terminals, including industrial protocol whitelist template, protocol parameter configuration, protocol detection exception template, critical event detection template, user-defined rules, network session audit template and no traffic detection template.

5.4.1. Industrial Protocol Whitelist Template

5.4.1.1. Introduction to functions

An important innovation in intelligent monitoring terminals is security policy audit in form of whitelists. Due to the stability of industrial control networks, security audit based on whitelists is an important and efficient way to solve its security issues.

Whitelist management of the management platform can facilitate users to view, edit and use a whitelist.

5.4.1.2. Template management

Click [Policy Management/Industrial Protocol Whitelist Template] in the left navigation bar (as shown in Fig.5-13), enter the [Industrial Protocol Whitelist Template] page (as shown in Fig.5-14):

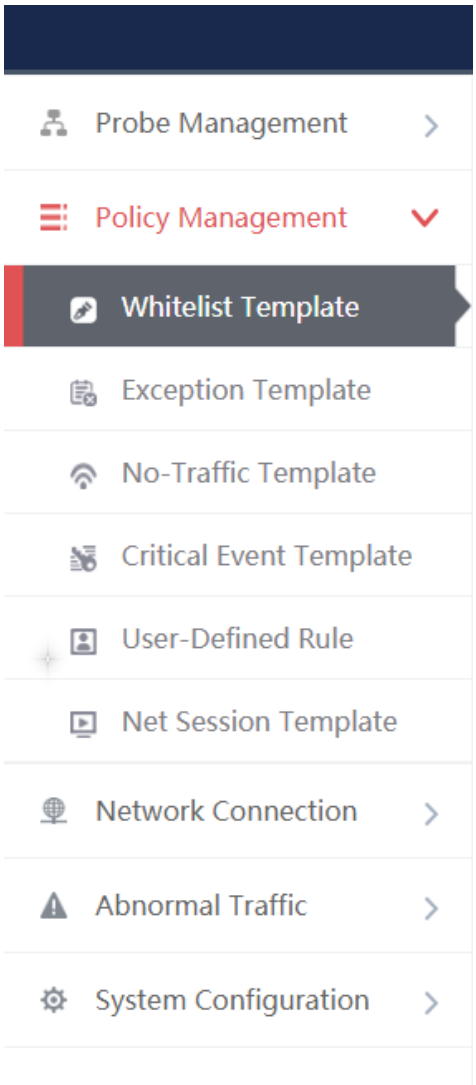


Fig.5-13 Selecting an Industrial Protocol Whitelist Template

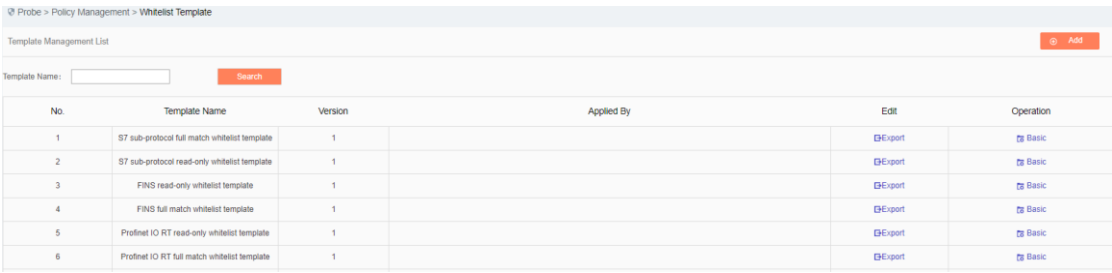


Fig.5-14 Whitelist Template Management

View information on all industrial protocol whitelist templates in the system here, with the meanings given below:

Tab.34 instruction to Whitelist Template List Display

Column Names	**Instructions**	
Template name	A whitelist template name that is easy to remember, for example "Whitelist Learned from Data Collection System 1"	
Version number	The version of the whitelist rule template, the version and the template ID uniquely determine a set of whitelist rules. The version number will automatically plus 1 after each time the whitelist is edited and saved	
Intelligent monitoring terminal using this template	All intelligent monitoring terminals using this whitelist template	
Edit	Import	Industry protocol whitelist rules imported to an excel sheet
	Export	Export the industry protocol whitelist rules from the template to an excel sheet
Operation	Basic configuration	View the basic information on whitelist template. The whitelist template built in the system does not have this button
	Rule configuration	View and modify the whitelist template rule configuration. The whitelist template built in the system does not have this button
	Delete	Delete a whitelist template, cannot delete a whitelist template in use. This button is not available to the whitelist template that is built-in the system

5.4.1.3. **Add a whitelist template.**

Click <Add> on the right side of the [Industrial Protocol Whitelist Template] template management list tab of

policy management (as shown in Fig.5-15) to pop up the whitelist template add page (as shown in Fig.5-16):

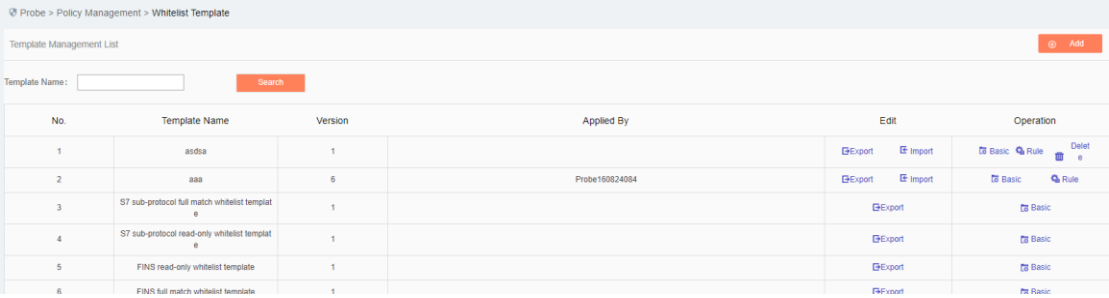


Fig.5-15 Whitelist Template Add Button

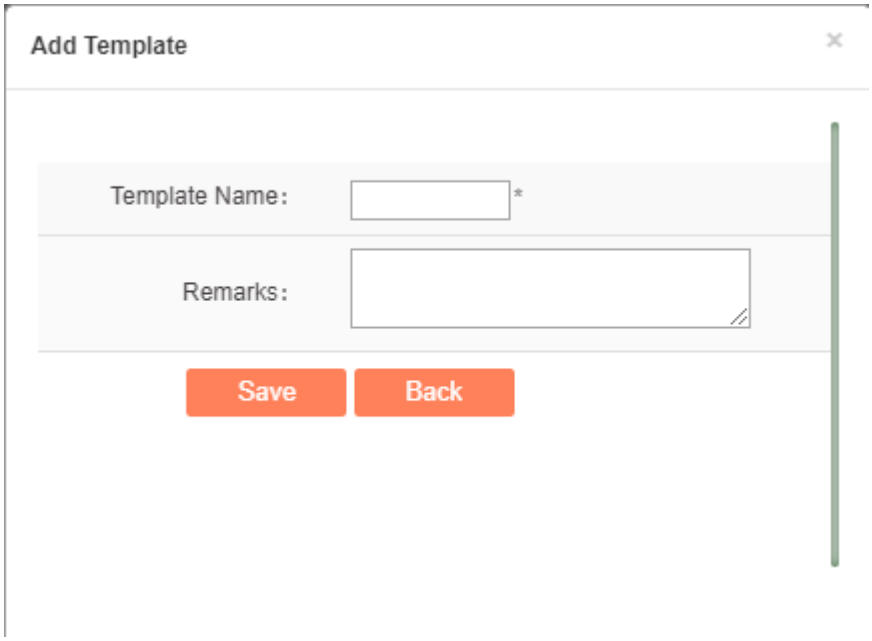


Fig.5-16 Whitelist Template Add Page

Tab.35 Instruction to Whitelist Template Add Information

Column Names	Instructions
Template Name	Define a meaningful industrial protocol whitelist template name that is easy to understand and remember
Remarks	Optional, additional explanatory information

5.4.1.4. Export a whitelist template.

Click <Export> under the operation column in the [Industrial Protocol Whitelist Template] of policy management (as shown in Fig.5-17), export the rules in whitelist template in excel (as shown in Fig.5-18):

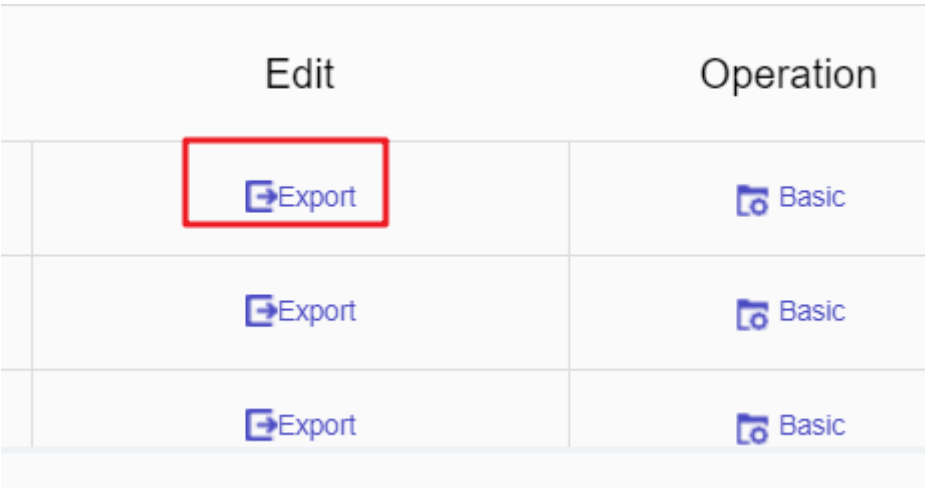


Fig.5-17 Industrial Protocol Whitelist Template Export Button

Click <Export> to export a file named "whitelist template_ {template name}_{date}.xls", for example, the rule file name that is exported on November 18, 2015 and with a template name of "Test" is "whitelist template_test_20151118.xls". The exported excel sheet contains all the rules for the template. (As shown in Fig.5-18):

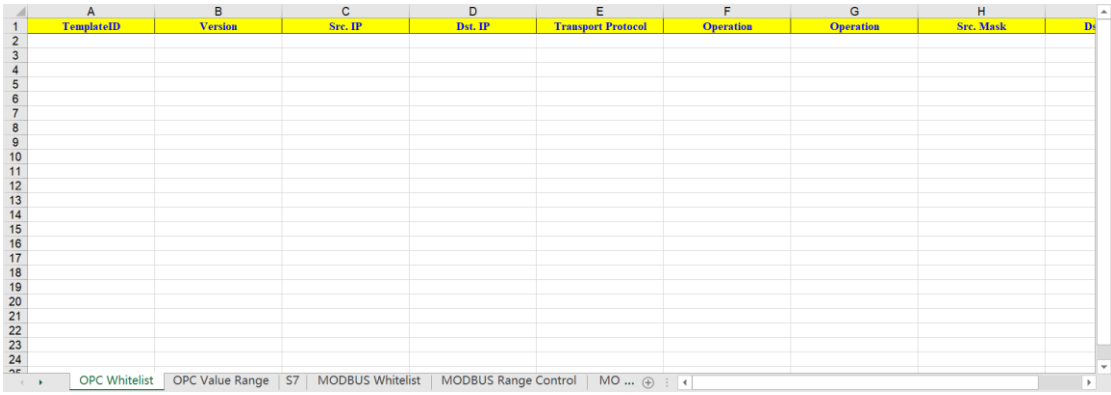


Fig.5-18 Example of Exported an Excel File

5.4.1.5. Import a whitelist template.

Click <Import> under the operation column in the [Industrial Protocol Whitelist Template] display list of policy management (as shown in Fig.5-19), import the rules from the whitelist template saved in an excel sheet into the template (as shown in Fig.5-20):

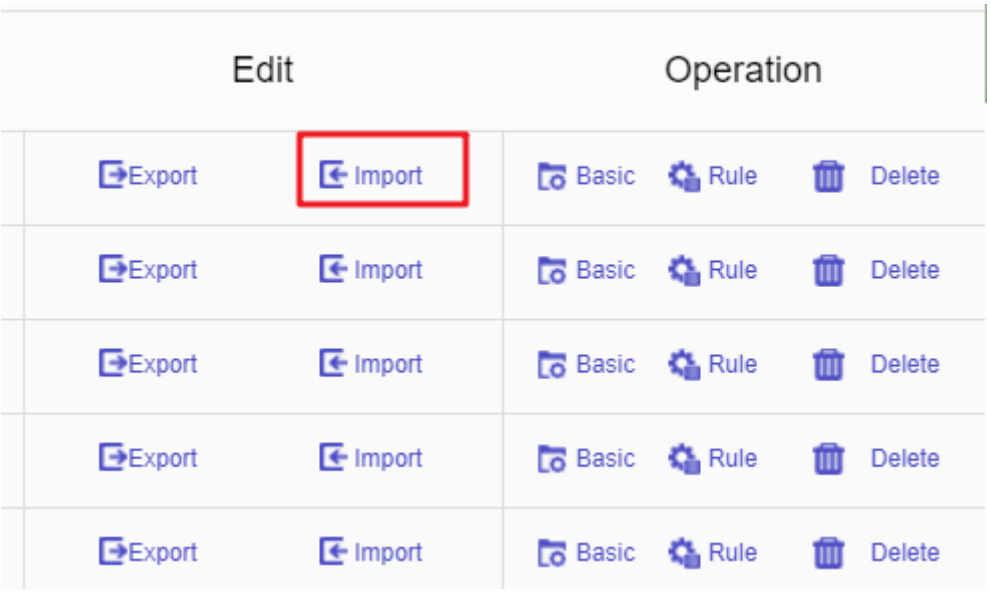


Fig.5-19 Industrial Protocol Whitelist Template Import Rule Button

Click <Import>, select the file to be imported in the dialog box for selecting an excel file, and click <Import Excel> to import the rules. (As shown in Fig.5-20):

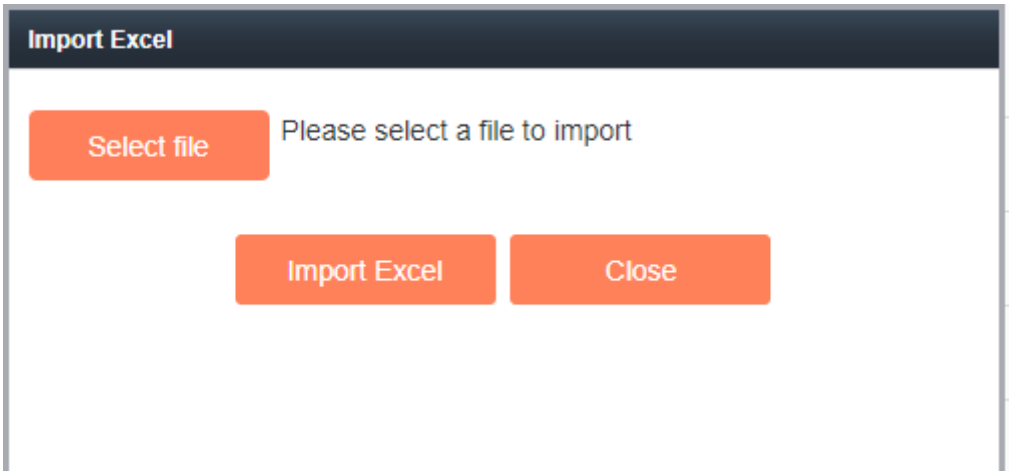


Fig.5-20 Importing the Excel File Selection Dialog Box

5.4.1.6. Basic industrial protocol whitelist template configuration

Click <Basic Configuration> (as shown in Fig.5-21) under the operation column of the [Industrial Protocol Whitelist Template] of policy management, open the [Whitelist Template Information] page to view the basic information on the whitelist template (as shown in Fig.5-22):

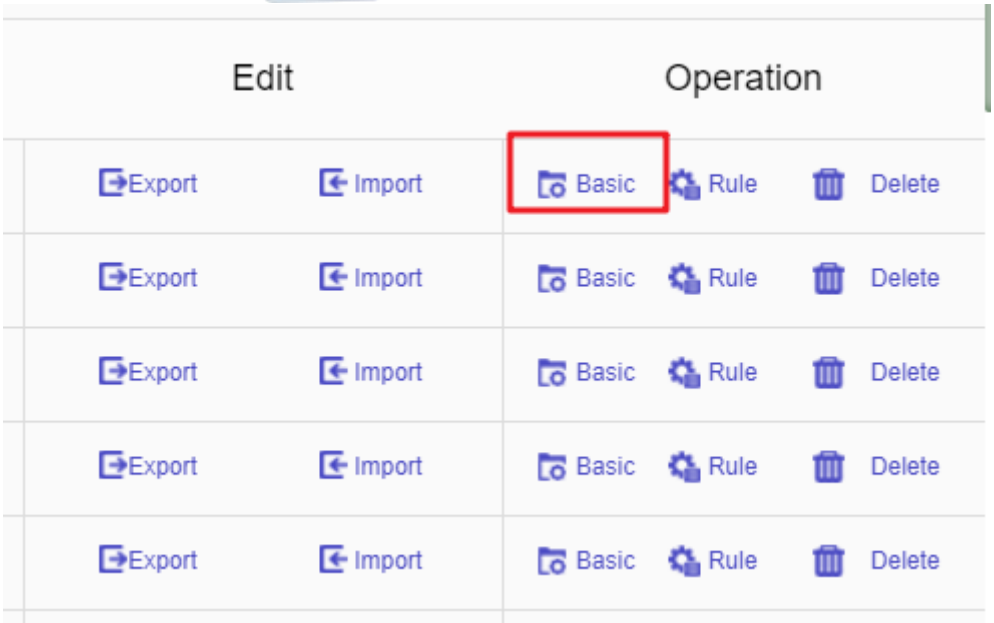


Fig.5-21 Whitelist Template Basic Configuration

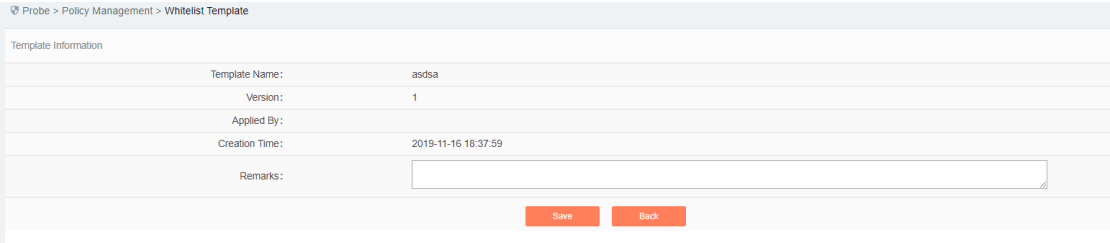


Fig.5-22 Whitelist Template Basic Configuration View Page

Tab.36 Instruction to Whitelist Template Basic Configuration Information

Column Names	Instructions
Template Name	The name of the whitelist template
Version	The version number of the whitelist template, which will automatically plus 1 after being modified each time
Applied By	A list of intelligent monitoring terminals using this template
Creation time	Whitelist template creation time
Remarks	To give additional information, optional

5.4.1.7. Industrial protocol whitelist template rule configuration

The management of industrial protocol whitelist items is the core of whitelist template management. All templates depend on each specific whitelist item. Currently, intelligent monitoring terminals support whitelists of eight standard industrial protocols: OPC, Siemens S7, Modbus, DNP3, IEC104, CIP, MMS, FINS and PROFINET, and will support whitelists of all general industrial protocols in the future.

OPC and Modbus protocols will be taken as an example below to guide how to manage whitelist items. The

case is similar for other protocols, but only with different specific fields.

5.4.1.7.1. View an OPC whitelist item.

Enter the [Rule] page, display the OPC whitelist item by default, click different tabs to display the whitelist item corresponding to the tab. (as shown in Fig.5-23):

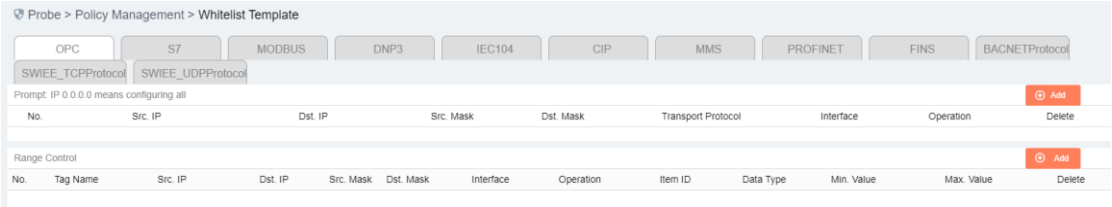


Fig.5 -23 OPC Whitelist Item Information View Page

Click <Back> and go back to the [Industrial Protocol Whitelist Template List Display] page.

5.4.1.7.2. Add an OPC whitelist item.

Enter the [Rule Configuration] page, click <Add> on the right (as shown in Fig.5-24) to automatically add a line of new white items at the bottom of the OPC whitelist item list (as shown in Fig.5-25):

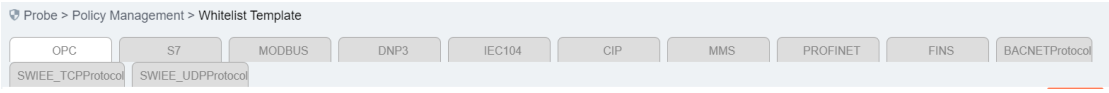


Fig.5-24 Industrial Protocol Whitelist Template Add Button

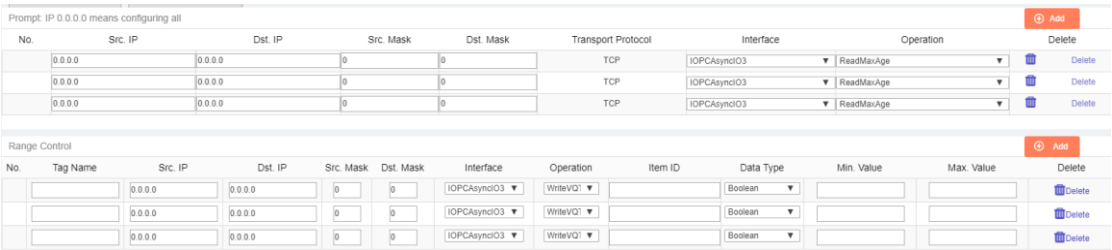


Fig.5-25 Industrial Protocol Whitelist Template Add Page

Tab.37 Instruction to OPC Whitelist Item Fields

Column Names	Instructions
Src. IP	The IP address initiating an OPC data request, in dotted decimal format
Dst. IP	The destination IP requesting OPC data, in dotted decimal format
Transport layer protocol	The transport layer protocol is TCP
Interface	An interface name in the OPC protocol, built in the data dictionary
Operation	A method under an interface specified in the OPC protocol, built in a data dictionary

Tab.38 Instruction to OPC Range Whitelist Item Fields

Column Names	Instructions	
Src. IP	The IP address initiating an OPC data request, in dotted decimal format	
Dst. IP	The destination IP requesting OPC data, in dotted decimal format	
Transport layer protocol	The transport layer protocol is TCP	
Interface	An interface name in the OPC protocol, built in the data dictionary	
Operation	A method under an interface specified in the OPC protocol, built in a data dictionary	
Item ID	Unique identifier of points	
Data type	Value types	
Min. value	Minimum value type	
Max. value	Maximum value type	
Operation	Save	Save all modification information to the database and make it come into effect, go back to the Whitelist Template Information List Display page
	Back	Ignore all modifications and go back to the Whitelist Template Information List Display page

5.4.1.7.3. Modify an OPC whitelist item.

Enter the [Industrial Protocol Whitelist Template] rule configuration page to change the source IP, destination IP, interface name and method name of a whitelist item, click <Save> after the modification.

5.4.1.7.4. Delete an OPC whitelist item.

Enter the [Industrial Protocol Whitelist Template] rule configuration page, click <Delete> on the far right of a whitelist item to delete the corresponding whitelist item. (As shown in Fig.5-26):

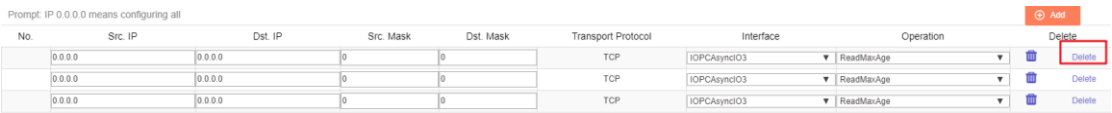


Fig.5-26 Industrial Protocol Whitelist Template Delete Button

The deletion is only provisional. Click Save when making the deletion effective.

Carry out similar operations for other protocols to add, modify and delete an industrial protocol whitelist item.

5.4.1.7.5. Modbus protocol whitelist configuration

The resolving depth of the Modbus protocol is different from that of other industrial protocols. Industrial firewalls can resolve specific values transmitted by the Modbus protocol. Therefore, the rule configuration of the Modbus protocol in whitelist template mainly includes two parts: basic whitelist and range control.

5.4.1.7.6. Basic Modbus whitelist items

The configuration here is similar to that of the OPC protocol. Refer to the OPC protocol related parameter configuration method.

5.4.1.7.7. Modbus range control

To use the Modbus range control function, first check the global enable, (as shown in Fig.5-27):

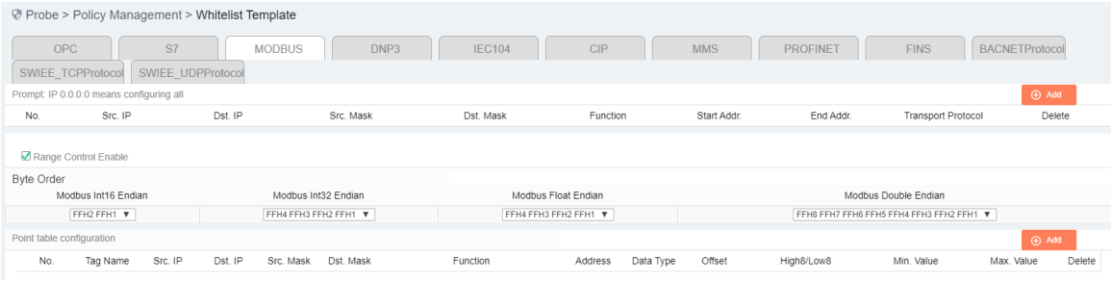


Fig.5-27 Modbus Protocol Range Enablement

After enabling range control, the following byte order can be edited. It is recommended to use the default configuration and adjust it accordingly if the default configuration does not match the site.

"Point table configuration" is the most important for the range function. The meanings of each field in point table configuration are explained in the following table.

Tab.39 Instruction to Modbus Click Fields

Column Names	Instructions
Tag name	A meaningful alias that represents an address in Modbus
Src. IP	The IP address initiating a Modbus data request, in dotted decimal format
Dst. IP	The destination IP requesting Modbus data, in dotted decimal format
Src. Mask	Source IP mask
Dst. Mask	Destination IP mask
Function	Modbus protocol function code
Address	The start addresses for a point operated by the Modbus protocol
Data type	Data type of points

Offset	The offset in the address for a specific type of data that is operated based on some function codes, for example: when the data type as operated based on 06 Function Code is of the BOOL type, it needs to specify which bit in the address indicates the BOOL value, with 0 taken by default
High8/ Low8	Which byte is used in the address when operating a specific type of data based on some function codes, for example, when the data type as operated based on 06 Function Code (which can operate a 2-bit address) is of the Byte type (1-bit), it needs to specify which bit (8-bit) in the operated address, which is high 8 bits by default
Min. Value	Minimum value that is allowed to operate
Max. Value	Maximum value that is allowed to operate

For adding, modifying, editing and deleting a range rule item, please refer to the basic Modbus item operation.

5.4.1.8. Delete a whitelist item.

Click <Delete> under the operation column in the [Industrial Protocol Whitelist Template] information display list of policy management to delete a whitelist template that is no longer in use. The whitelist template being used cannot be deleted. (As shown in Fig.5-28):

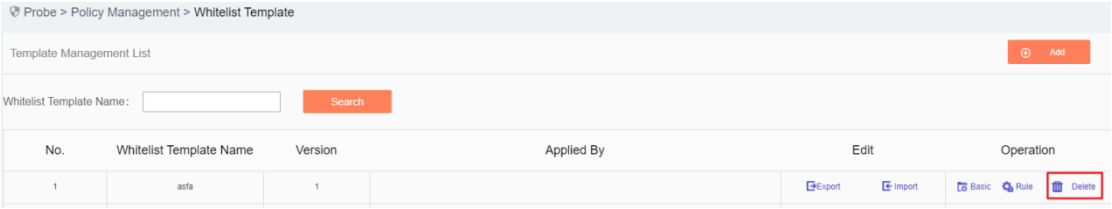


Fig.5-28 Industrial Protocol Whitelist Template Delete Button

5.4.1.9. Retrieve a whitelist template.

In the [Industrial Protocol Whitelist Template] information display list of policy management, the whitelist template can be retrieved according to the conditions. (As shown in Fig.5-29)

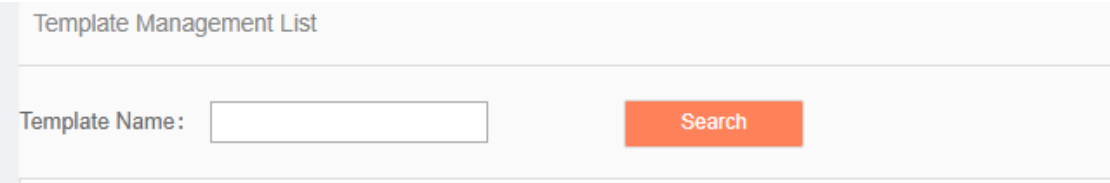


Fig.5-29 Retrieving a Whitelist Template

5.4.2. Protocol Detection Exception Template

5.4.2.1. Introduction to functions

The intelligent monitoring terminal will detect messages according to the industrial protocol. When messages not meeting the protocol are detected, the intelligent monitoring terminal will give an alarm. If customers do not want intelligent monitoring terminals to execute protocol detection on some data connections, they can disable the protocol detection function of intelligent monitoring terminals by configuring the protocol detection exception template.

5.4.2.2. Template management

Click the [Policy Management/Protocol Detection Exception Template] in the left navigation bar (as shown in Fig.5-30), enter the [Protocol Detection Exception Template] page (as shown in Fig.5-31):

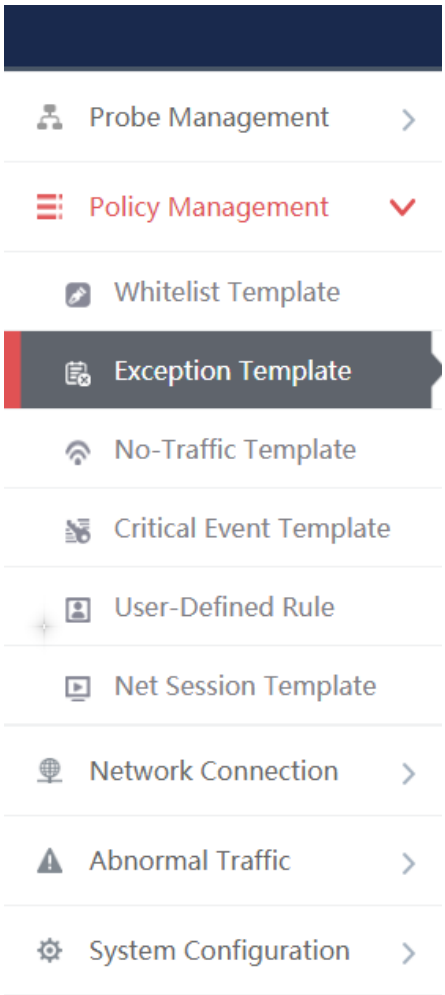


Fig.5-30 Selecting a Protocol Detection Exception Template

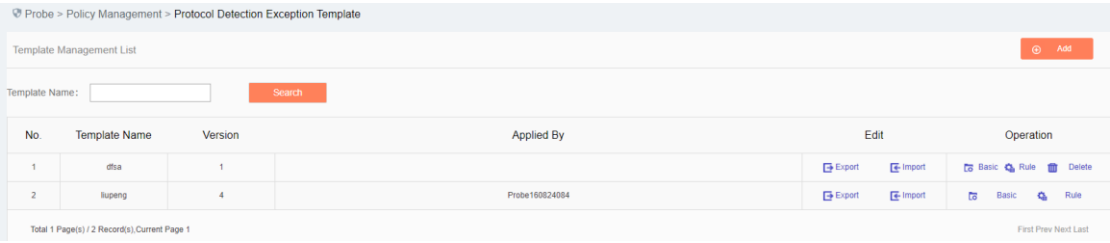


Fig.5-31 Protocol Detection Exception Template Management

View information on all protocol detection exception templates in the system here, with the meanings given below:

Tab.40 Instruction to Protocol Detection Exception Template List Display

Column Names	**Instructions**	
Template Name	A protocol detection exception template name that is easy to remember, for example "Protocol Exception of Data Collection System 1"	
Version	The version of protocol exception template, the version and the template ID uniquely determine a set of protocol exception detection rules. The version number will automatically plus 1 after each time the protocol detection exception rule is edited and saved	
Applied By	All intelligent monitoring terminals that are using this template	
Edit	Import	The protocol detection exception rules imported in an excel sheet
	Export	Export the protocol detection exception rules in the template to an excel sheet
Operation	Basic	View the basic information on protocol detection exception templates
	Rule	View and modify the rule configuration of protocol detection exception templates
	Delete	Delete the template. The template in use cannot be deleted

5.4.2.3. Add a protocol detection exception template.

Click <Add> (as shown in Fig.5-32) on the right of the [Protocol Detection Exception Template] template management list of policy management to pop up the protocol detection exception template add page (as shown in Fig.5-33):

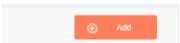


Fig.5-32 Protocol Detection Exception Template Add Button

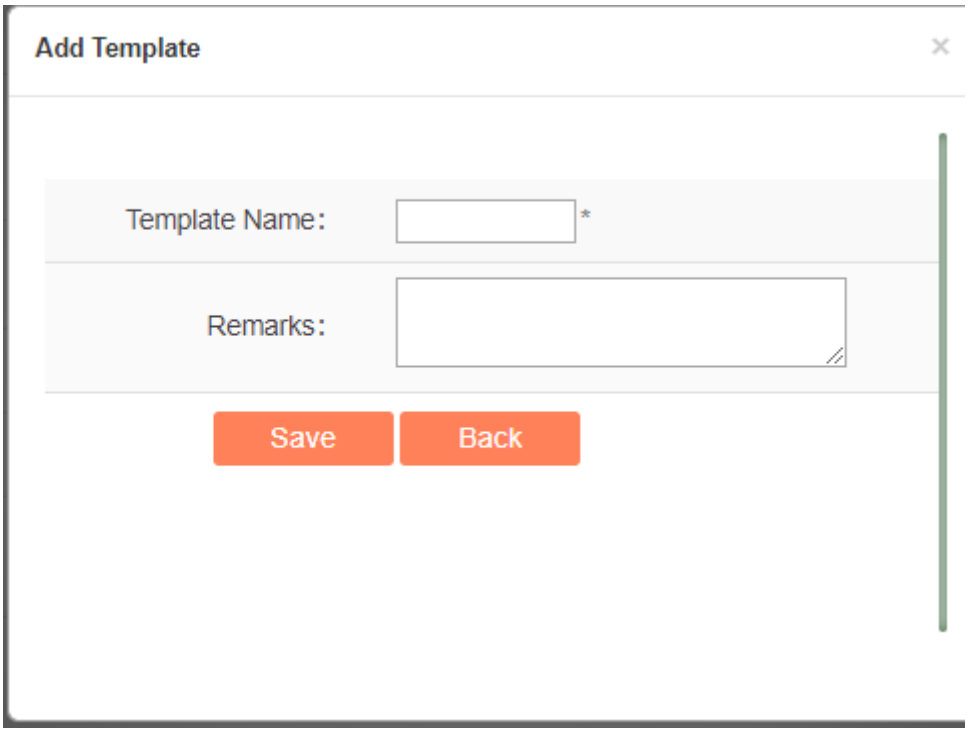


Fig.5-33 Protocol Detection Exception Template Add Page

Tab.41 Instruction to Protocol Detection Exception Template Add Information

Column Names	Instructions
Template Name	Define a meaningful protocol detection exception template name that is easy to understand and remember
Remarks	Optional, additional explanatory information

5.4.2.4. Export a protocol detection exception template.

Click <Export> under the operation column in the [Protocol Detection Exception Template] display list of policy management (as shown in Fig.5-34), export the rules in the protocol detection exception template in an excel sheet (as shown in Fig.5-35):

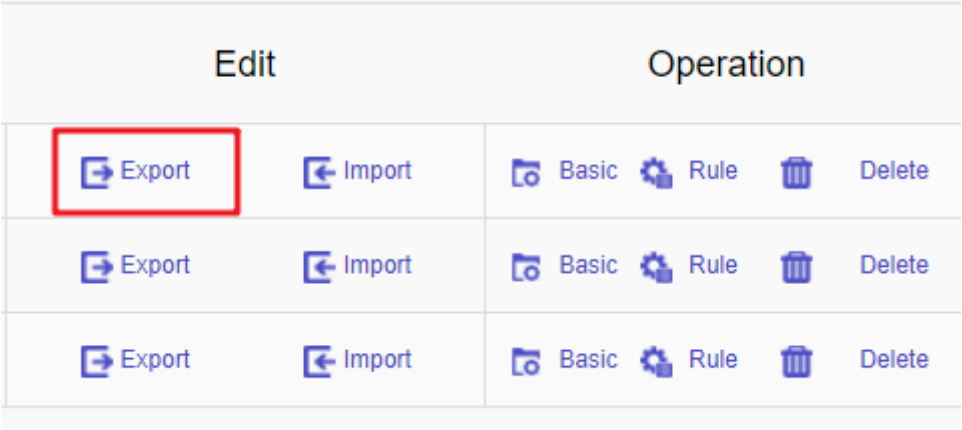


Fig.5-34 Protocol Detection Exception Template Export Button

Click <Export> to export a file named "protocol detection exception template _ {template name}_{date}.xls", for example, the rule file name that is exported on November 18, 2015 and with a template name of "Test" is "protocol detection exception template_test_20151118.xls". The exported excel sheet contains all the rules for the template.

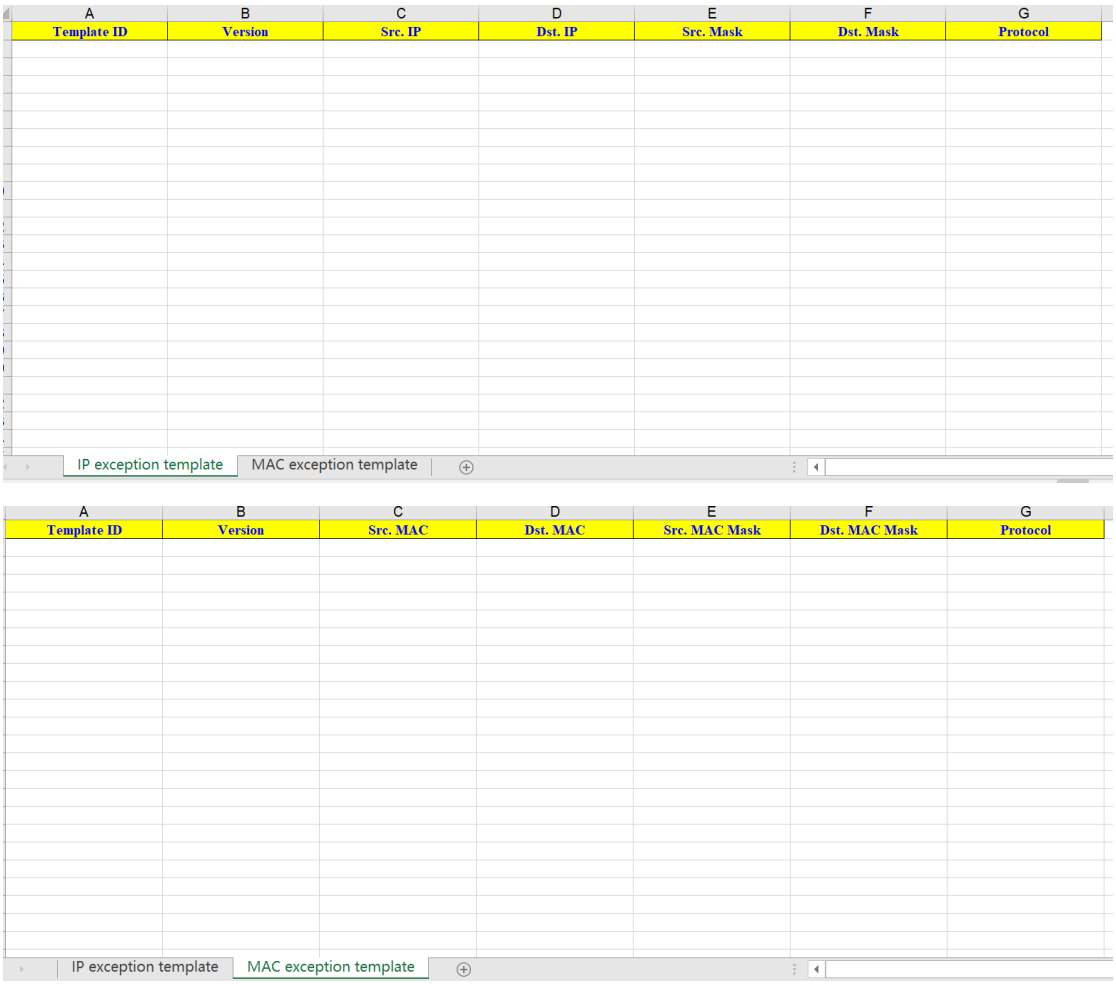


Fig.5-35 Example of an Exported Excel File

5.4.2.5. Import a protocol detection exception template.

Click <Import> under the operation column in the [Protocol Detection Exception Template] display list of policy management (as shown in Fig.5-36), import the rules in the protocol detection exception template saved in excel into the template (as shown in Fig.5-37):

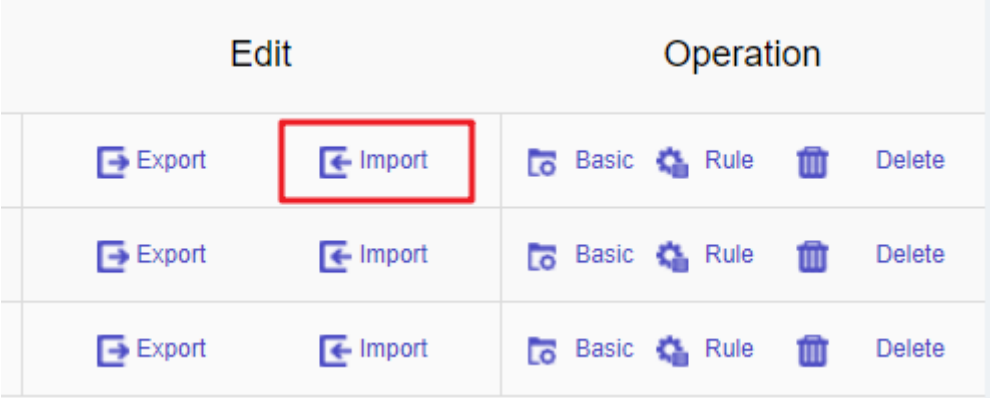


Fig.5-36 Protocol Detection Exception Template Import Rule Button

Click <Import>, select the file to be imported in the dialog box for selecting an excel file, and click <Import Excel> to import the rules.

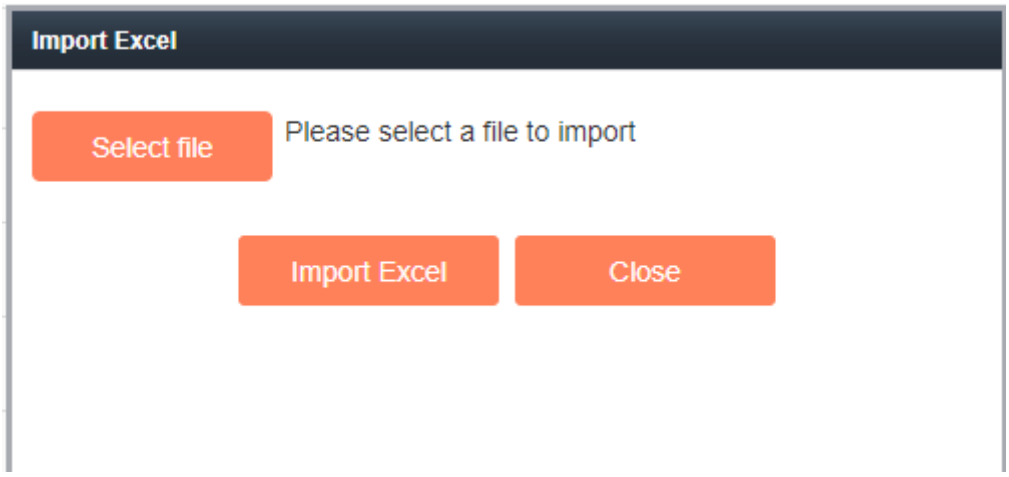


Fig.5-37 Importing the Excel Selection File Dialog Box

5.4.2.6. Basic configuration of protocol detection exception template

Click <Basic Configuration> under the operation column in the [Protocol Detection Exception Template] display list of policy management (as shown in Fig.5-38), open the [Protocol Detection Exception Template] basic configuration page, view the basic information on protocol detection exception templates (as shown in Fig.5-39):

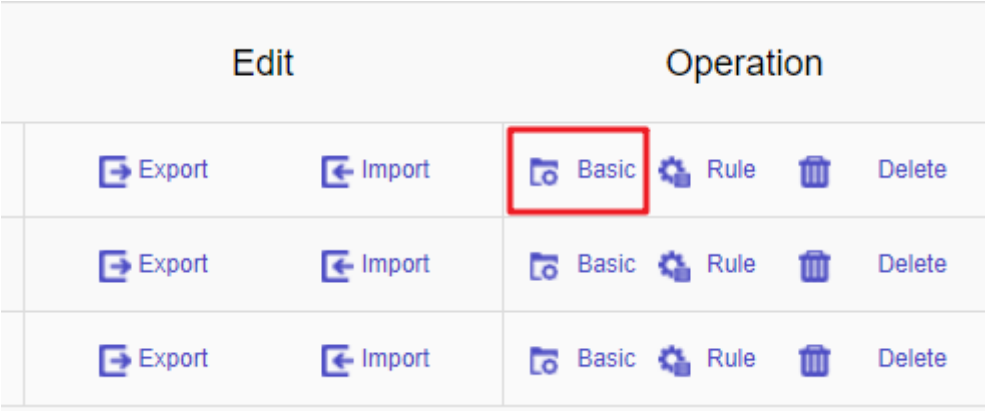


Fig.5-38 Protocol Exception Detection Template Basic Configuration

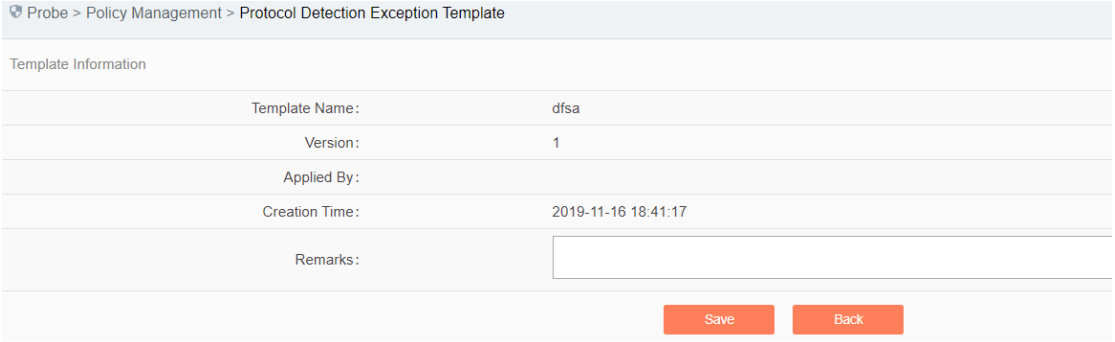


Fig.5-39 Protocol Detection Exception Template Basic Configuration View Page

Tab.42 Instruction to Whitelist Template Basic Configuration Information

Column Names	Instructions
Template Name	The name of the template
Version	The version number of the template, which will automatically plus 1 after being modified each time
Applied By	A list of intelligent monitoring terminals using this template
Creation time	Template creation time
Remarks	To give additional information, optional

5.4.2.7. Protocol detection exception template rule configuration

The management of protocol detection exception rules is the core of protocol detection exception template management. All templates depend on each specific rule.

5.4.2.7.1. View protocol detection exception rules.

Enter the [Rule Configuration] page to display protocol detection exception items, including IP rule and MAC

rule configurations (Fig.5-40):

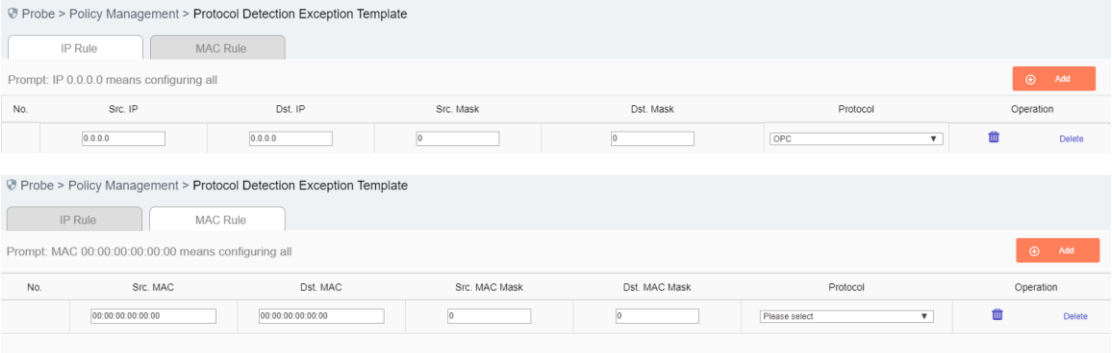


Fig.5-40 Protocol Detection Exception Item Information View Page

Click <Back>, go back to the [Protocol Detection Exception Template List Display] page.

5.4.2.7.2. Add a protocol detection exception rule.

After entering the [Rule Configuration] page, click <Add> on the right (as shown in Fig.5-41) to automatically add a new line of protocol detection exception rules at the bottom of the rule (as shown in Fig.5-42):

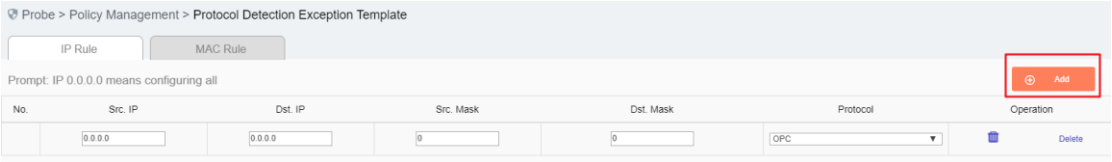


Fig.5-41 Protocol Detection Exception Template Add Button

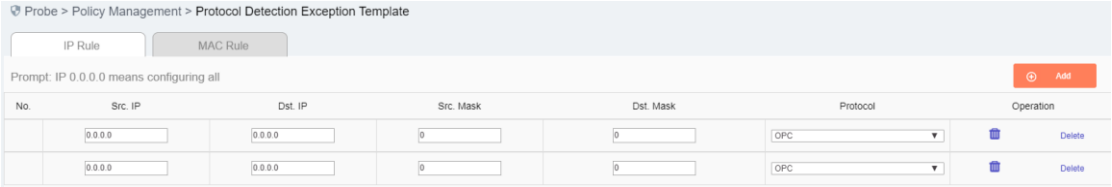


Fig.5-42 Protocol Detection Exception Template Add Page

Tab.43 Instruction to Protocol Detection Exception IP Rule Fields

Column Names	Instructions
Src. IP	The IP address initiating a protocol detection exception connection request, in dotted decimal format
Dst. IP	The destination IP address for protocol detection exception connection, in dotted decimal format
Src. Mask	The mask of the source IP address, generally ranging from 0 to 32
Dst. Mask	The mask for the destination IP address, generally ranging from 0 to 32
Protocol	Industrial protocols for protocol detection exceptions, with options including OPC, Modbus, S7, DNP3, IEC104, CIP, MMS and 853

Operation	Delete	Delete a specified rule, click <Save> to submit the deletion request, re-submit the deleted data to the database modification information, save it in the database and make it come into effect, go back to the protocol detection exception template information list display page at the same time
	Save	Save all modification information to the database and make it come into effect, go back to the protocol detection exception template information list display page at the same time
	Back	Ignore all modifications and go back to the protocol detection exception template information list display page

Tab.44 Instruction to Protocol Detection Exception MAC Rule Fields

Column Names	**Instructions**	
Src. MAC	The MAC address initiating a protocol detection exception connection request	
Dst. MAC	The destination MAC address for protocol detection exception connection	
Src. MAC Mask	A mask for the source MAC address, ranging from 0 to 48	
Dst. MAC mask	A mask for the destination MAC address, ranging from 0 to 48	
Protocol	Industrial protocols of protocol detection exception, with options including PROFINET DCP, PROFINET IORE	
Operation	Delete	Delete a specified rule, click <Save> to submit the deletion request, re-submit the deleted data to the database modification information, save it in the database and make it come into effect, go back to the protocol detection exception template information list display page at the same time
	Save	Save all modification information to the database and make it come into effect, go back to the protocol detection exception template information list display page at the same time

	Back	Ignore all modifications and go back to the protocol detection exception template information list display page

5.4.2.7.3. Modify a protocol detection exception rule.

Enter the [Protocol Detection Exception Rule Configuration] page, change the source IP, destination IP, source IP mask, destination IP mask and protocol of a rule, click <Save> after the modification.

5.4.2.7.4. Delete a protocol to detect exception rule.

Enter the [Protocol Detection Exception Rule Configuration] page, click <Delete> on the far right of a rule to delete the corresponding rule. (As shown in Fig.5-43):

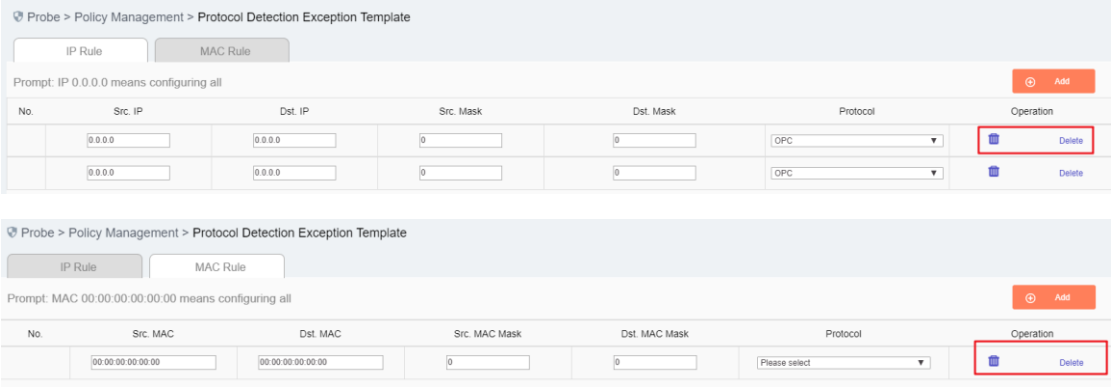


Fig.5-43 Protocol Detection Exception Rule Delete Button

5.4.2.8. Delete a protocol detection exception template.

Click <Delete> under the operation column in the [Protocol Detection Exception Template] information display list of policy management to delete protocol detection exception templates that are no longer in use. The protocol detection exception template being used cannot be deleted. (As shown in Fig.5-44):

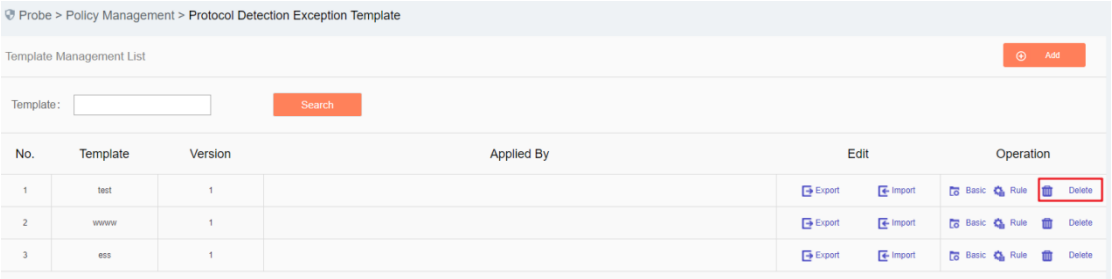


Fig.5-44 Protocol Detection Exception Template Delete Button

5.4.2.9. Retrieve a protocol detection exception template.

In the [Protocol Detection Exception Template] information display list page of policy management, protocol detection exception templates can be retrieved according to conditions. (As shown in Fig.5-45):

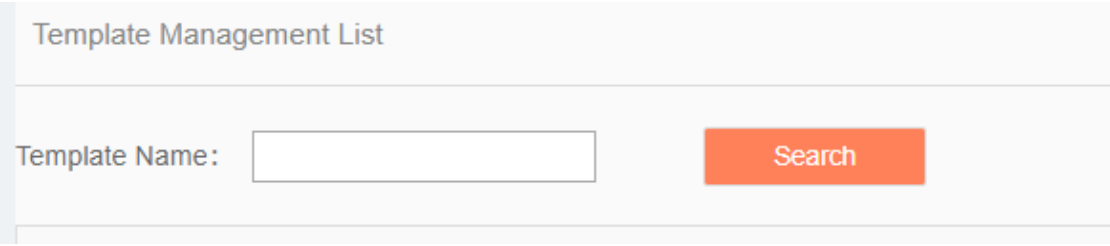


Fig.5-45 Retrieving a Protocol Detection Exception Template

5.4.3. Critical Event Template

5.4.3.1. Introduction to functions

Some key operations are built in the intelligent monitoring terminal, such as engineer station configuration change, control instruction change, PLC download and load change, etc. Users can detect critical events occurred to a specified connection by configuring the critical event detection template.

5.4.3.2. Template management

Click [Policy Management/Critical Event Template] in the left navigation bar (as shown in Fig.5-46), enter the [Critical Event Template] page (as shown in Fig.5-47):

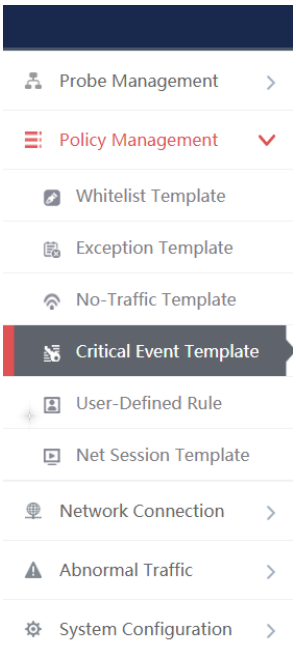


Fig.5-46 Selecting a Critical Event Detection Template

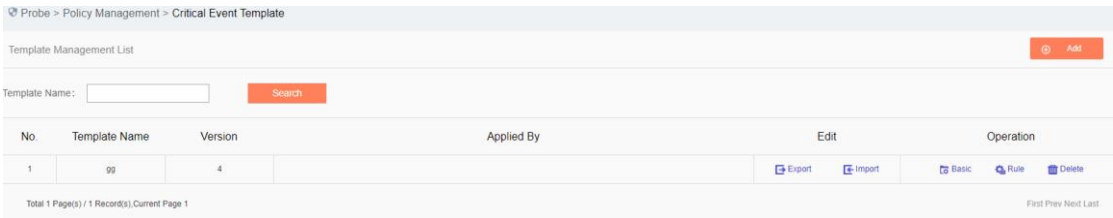


Fig.5-47 Critical Event Detection Template Management

View information on all critical event detection templates in the system here, with the meanings given below:

Tab.39 Instruction to Protocol Detection Exception Template List Display

Column Names	**Instructions**	
Template Name	A critical event detection template name that is easy to remember, for example "Critical Event, Data Collection System 1"	
Version	The version of critical event detection template, the version and the template ID uniquely determine a set of critical event detection rules. The version number will automatically plus 1 after each time the critical event detection rules are edited and saved	
Applied By	All intelligent monitoring terminals that are using this template	
Edit	Import	Critical event detection rules imported to an excel sheet
	Export	Export the critical event detection rules in the template to an excel sheet
Operation	Basic	View the basic information on the critical event detection template
	Rule	View and modify the critical event detection template rule configuration
	Delete	Delete the template. The template in use cannot be deleted

5.4.3.3. **Add a critical event detection template.**

Click <Add> on the right side of the [Critical Event Detection Template] template management list tab of policy management (as shown in Fig.5-48) to pop up the critical event detection template add page (as shown in Fig.5-49):

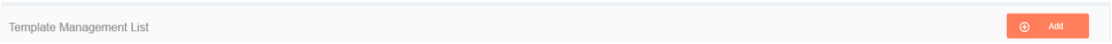


Fig.5-48 Protocol Detection Exception Template Add Button

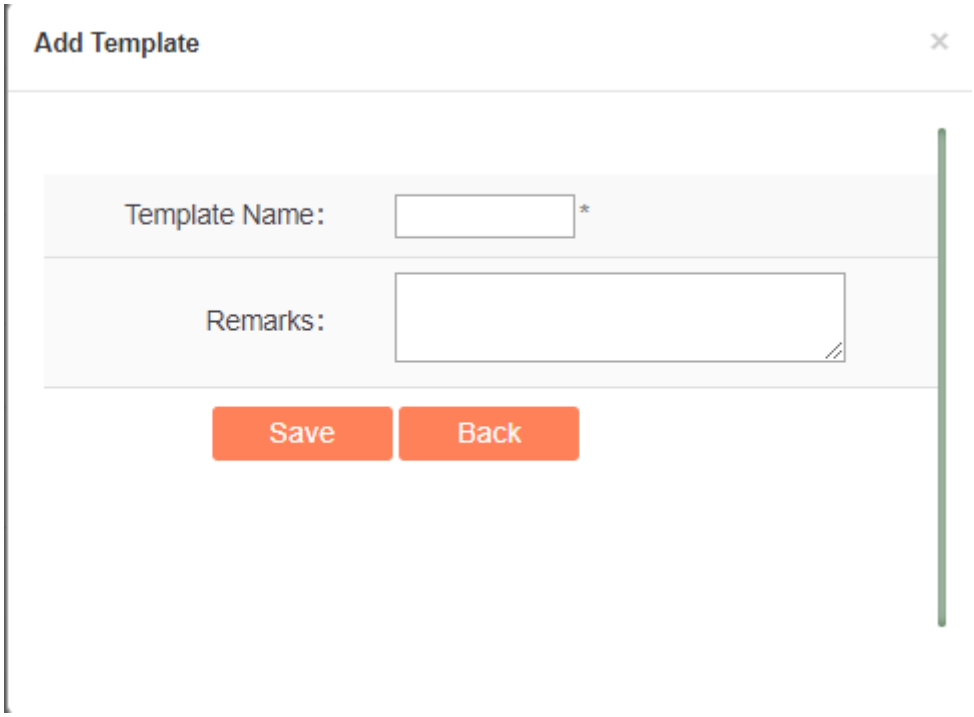


Fig.5-49 Protocol Detection Exception Template Add Page

Tab.40 Instruction to Critical Event Detection Template Add Information

Column Names	Instructions
Template Name	Define a meaningful critical event detection template name that is easy to understand and remember
Remarks	Optional, additional explanatory information

5.4.3.4. Export a critical event detection template.

Click <Export> (as shown in Fig.5-50) under the operation column of [Critical Event Detection Template] display list of policy management, export the rules in the protocol detection exception template in an excel sheet (as shown in Fig.5-51):

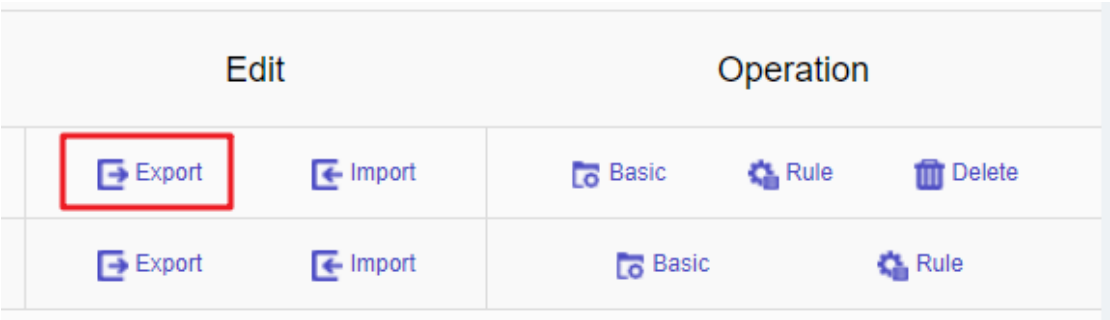
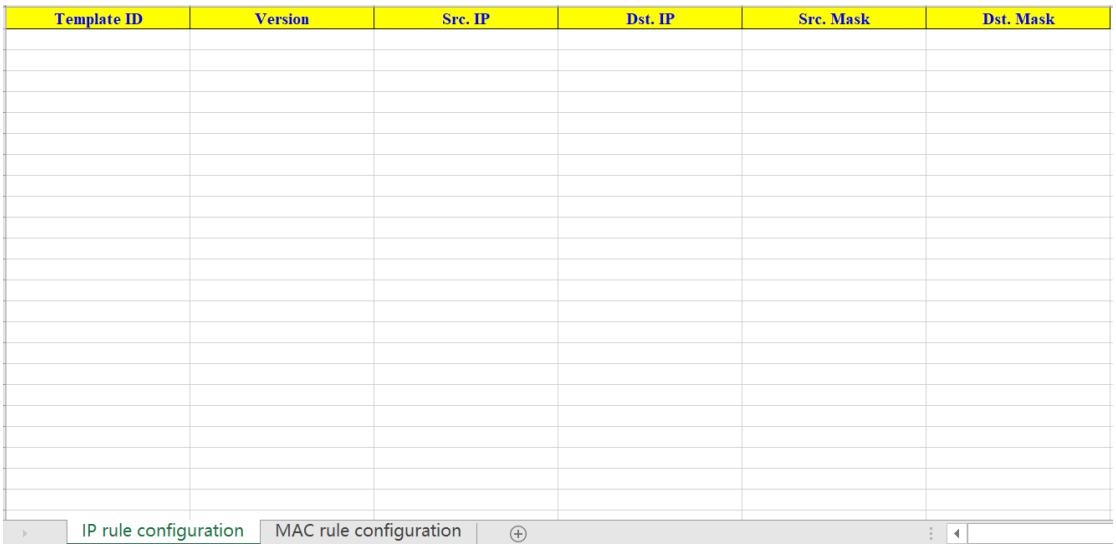


Fig.5-50 Critical Event Detection Template Export Button

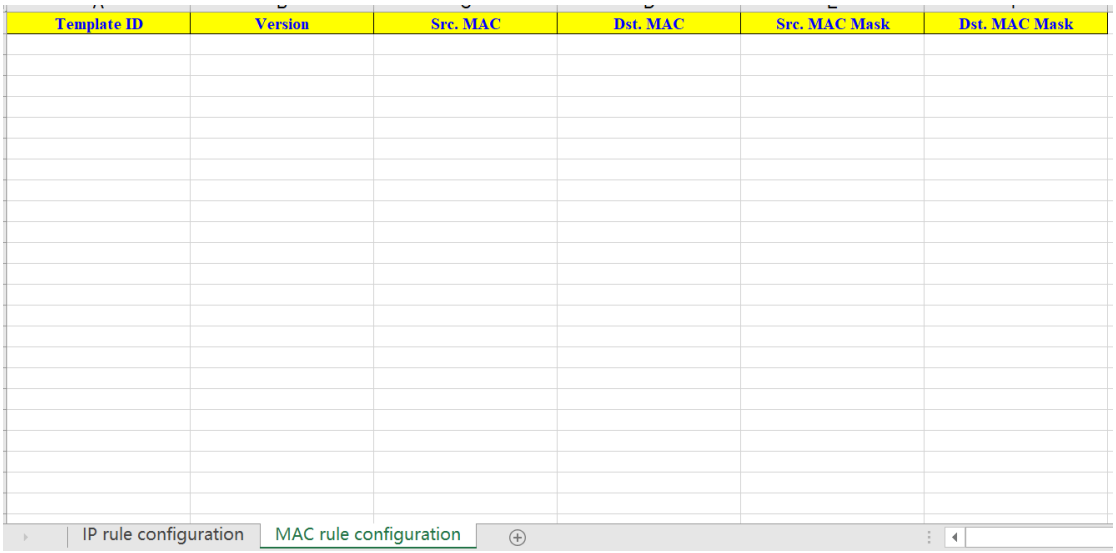
Click <Export> to export a file named "critical event detection template {template name}_{date}.xls", for example, the rule file name that is exported on November 18, 2015 and with a template name of "Test" is "critical

event detection template_test_20151118.xls". The exported excel sheet contains all the rules for the template.



Template ID	Version	Src. IP	Dst. IP	Src. Mask	Dst. Mask

IP rule configuration | MAC rule configuration



Template ID	Version	Src. MAC	Dst. MAC	Src. MAC Mask	Dst. MAC Mask

IP rule configuration | MAC rule configuration

Fig.5-51 Example of an Exported Excel File

5.4.3.5. Import a critical event detection template.

Click <Import> under the operation column in the [Critical Event Detection Template] display list of policy management (as shown in Fig.5-52), import the rules in the critical event detection template saved in excel into the template (as shown in Fig.5-53):

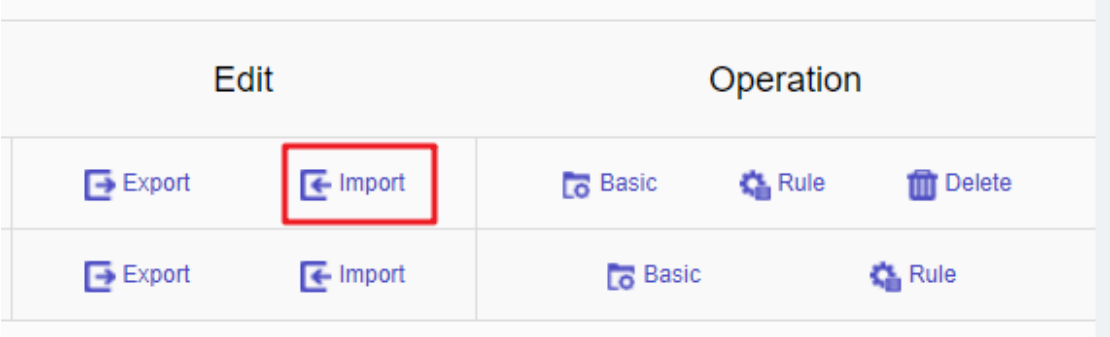


Fig.5-52 Critical Event Detection Template Import Rule Button

Click <Import>, select the file to be imported in the dialog box for selecting an excel file, and click <Import Excel> to import the rules.

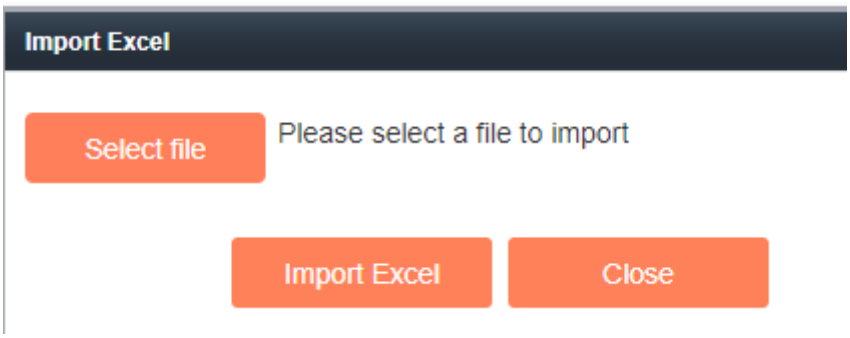


Fig.5-53 Importing the Excel Selection File Dialog Box

5.4.3.6. Critical event detection template basic configuration

Click <Basic Configuration> under the operation column in the [Critical Event Detection Template] display list of policy management (as shown in Fig.5-54), open the [Critical Event Detection Template] page, view the basic information on the critical event detection template (as shown in Fig.5-55):

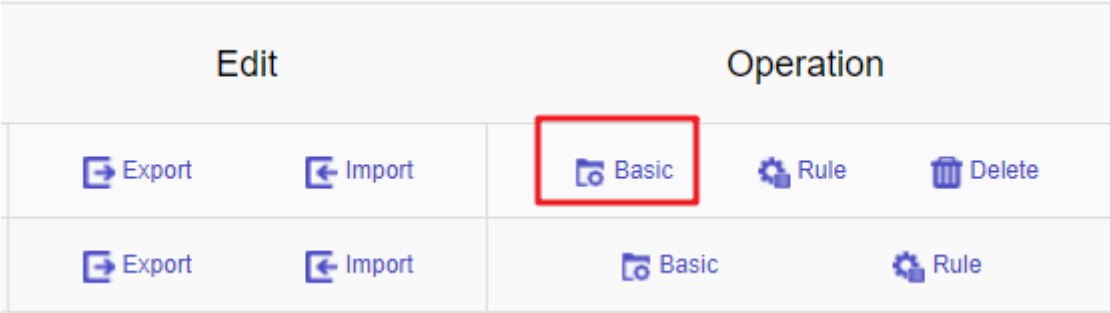


Fig.5-54 Critical Event Detection Template Basic Configuration

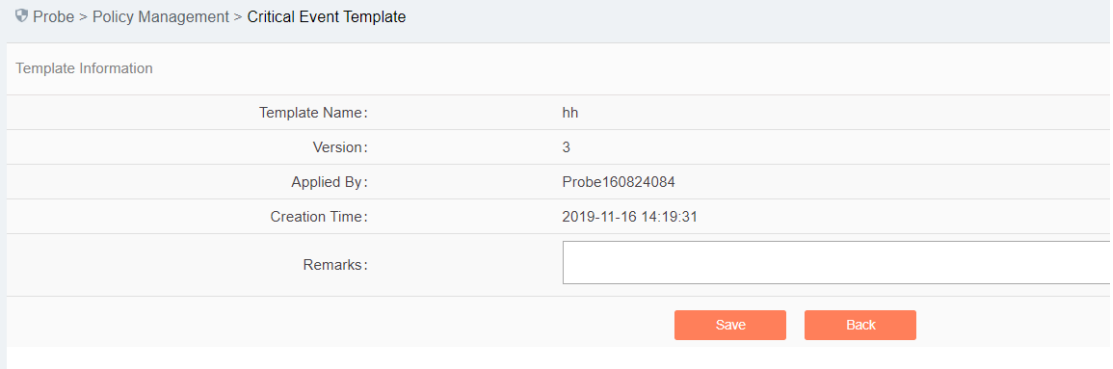


Fig.5-55 Critical Event Detection Template Basic Configuration View Page

Tab.41 Instruction to Critical Event Detection Basic Configuration Information

Column Names	**Instructions**
Template name	The name of the template
Version number	The version number of the template, which will automatically plus 1 after being modified each time
Applied By	A list of intelligent monitoring terminals using this template
Creation time	Template creation time
Remarks	To give additional information, optional

5.4.3.7. Critical event detection template rule configuration

The management of critical event detection rules is the core of critical event detection template management. All templates depend on each specific rule.

5.4.3.7.1. View the critical event detection rules.

After entering the [Rule Configuration] page, the critical event detection rules are displayed. (as shown in Fig.5-56):

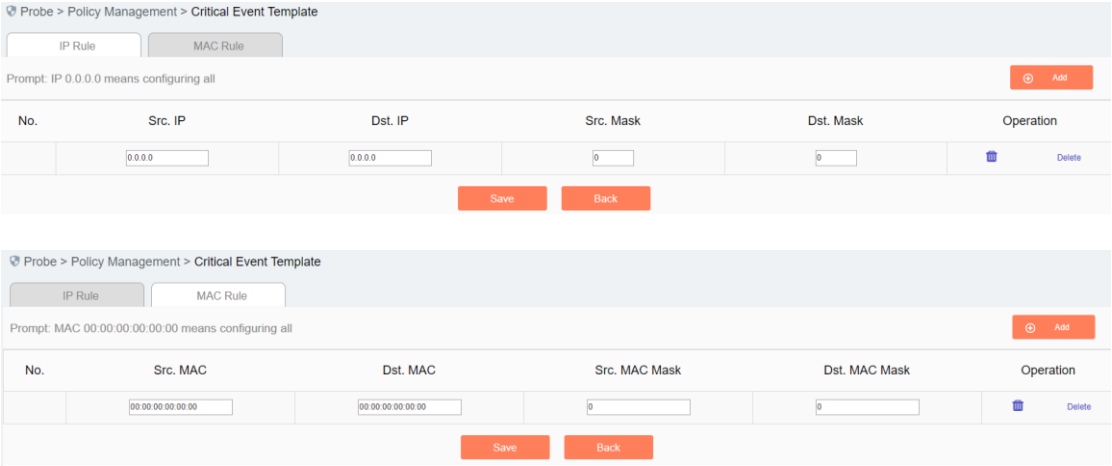


Fig.5-56 Critical Event Detection Rules View Page

Click <Back> and go back to the [Critical Event Detection Template List Display] page.

5.4.3.7.2. Add the critical event detection rules.

Enter the [Rule Configuration] page, click <Add> on the right (as shown in Fig.5-57) to automatically add a new line of critical event detection rules at the bottom of the rule (as shown in Fig.5-58):

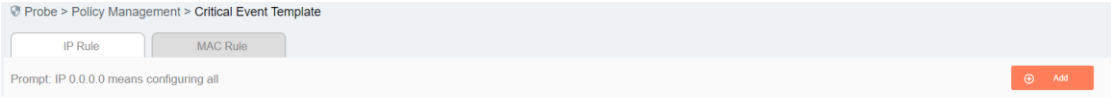


Fig.5-57 Critical Event Detection Template Add Button

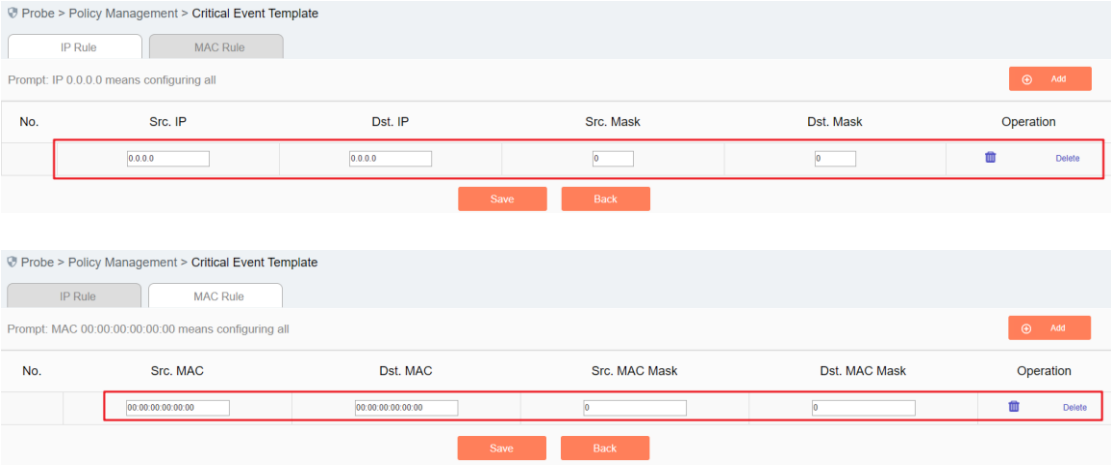


Fig.5-58 Critical Event Detection Template Add Page

Tab.45 Instruction to Critical Event Detection IP Rule Fields

Column Names	Instructions
Src. IP	The IP address initiating a critical event detection connection request, in dotted decimal format

Dst. IP	The destination IP address for critical event detection connection, in dotted decimal format	
Src. mask	The mask of the source IP address, generally ranging from 0 to 32	
Dst. mask	The mask for the destination IP address, generally ranging from 0 to 32	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the template information list display page
	Back	Ignore all modifications and go back to the template information list display page

Tab.46 Instruction to Critical Event Detection MAC Rule Fields

Column Names	**Instructions**	
Src. MAC	The MAC address initiating a critical event detection connection request	
Dst. MAC	The destination MAC address for critical event detection connection	
Src. MAC mask	A mask for the source MAC address, ranging from 0 to 48	
Dst. MAC mask	A mask for the destination MAC address, ranging from 0 to 48	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the template information list display page
	Back	Ignore all modifications and go back to the template information list display page

5.4.3.7.3. Modify the critical event detection rules.

Enter the [Critical Event Detection Template Rule Configuration] page, change the source IP, destination IP, source IP mask, destination IP mask of a rule, click <Save> after the modification.

5.4.3.7.4. Delete the critical event detection rules.

Enter the [Critical Event Detection Template Rule Configuration] page, click <Delete> on the far right of a rule to delete the corresponding rule. (As shown in Fig.5-59):

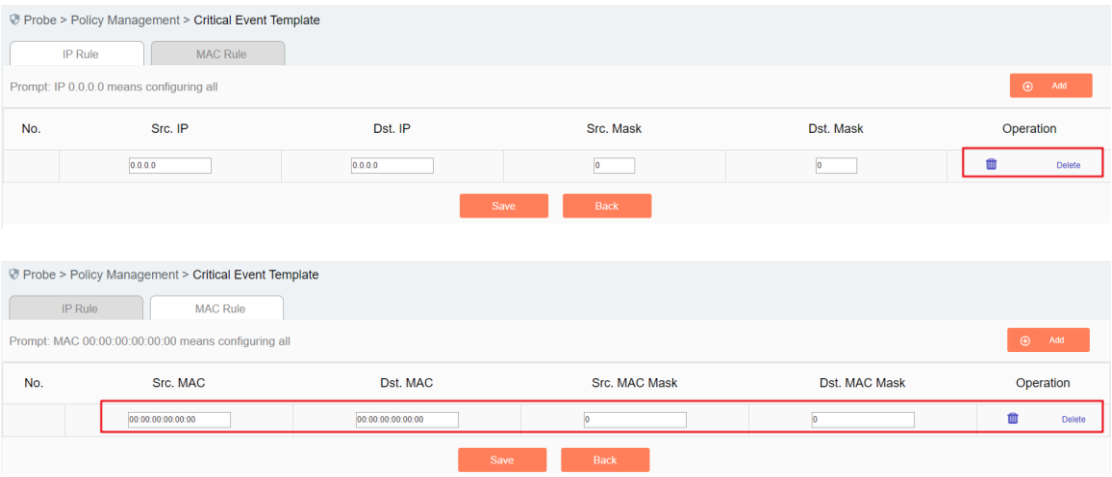


Fig.5-59 Critical Event Detection Rules Delete Button

5.4.3.8. Delete the critical event detection template.

Click <Delete> under the operation column in the [Critical Event Detection Template] information display list of policy management to delete the critical event detection templates that are no longer in use. The template being used cannot be deleted. (As shown in Fig.5-60):

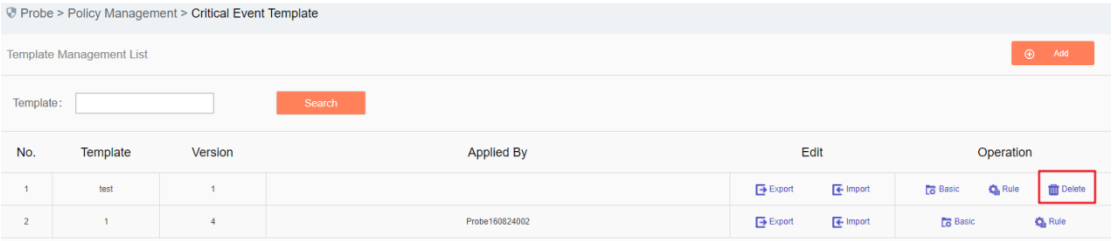


Fig.5-60 Critical Event Detection Template Delete Button

5.4.3.9. Retrieve a critical event detection template.

In the [Critical Event Detection Template] information display list page of policy management, the critical event detection template can be retrieved according to the conditions. (As shown in Fig.5-61):

Fig.5-61 Retrieve a Critical Event Detection Template

5.4.4. User-Defined Rules

5.4.4.1. Introduction to functions

In addition to the key operations built in the intelligent monitoring terminal, the intelligent monitoring terminal allows users to configure operations they care about. When a user-defined operation is detected, the intelligent monitoring terminal will give an alarm.

5.4.4.2. Rule configuration

Click [Policy Management/User-Defined Rules] in the left navigation bar (as shown in Fig.5-62) to enter the [User-Defined Rules] page (as shown in Fig.5-63):

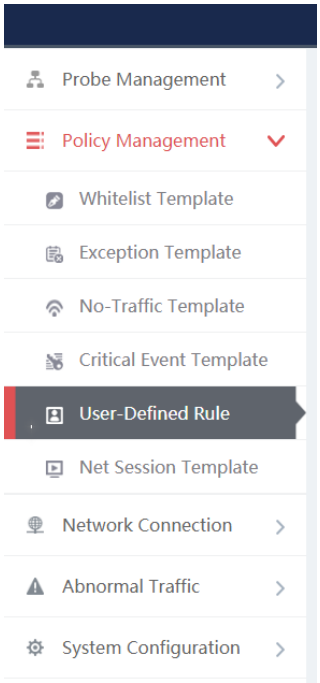


Fig.5-62 Selecting User-defined Rules.

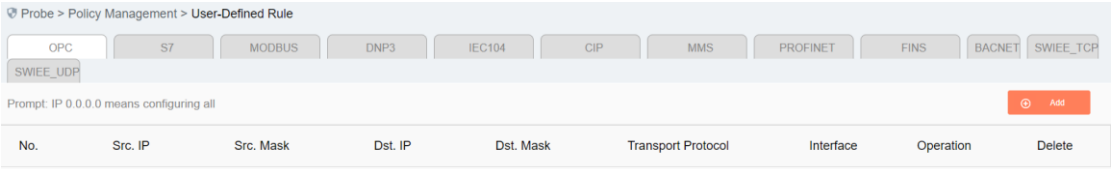


Fig.5-63 User-defined Rules

Currently, intelligent monitoring terminals support user-defined rules for five standard industrial protocols: OPC, Siemens S7, Modbus, DNP3, IEC104, CIP, MMS, PROFINET and FINS, and will support custom rules for all general industrial protocols in the future. The OPC protocol will be taken as an example below to guide how to manage user-defined rules. The case is similar for other protocols, but only with different specific fields.

5.4.4.3. OPC User-Defined Rule Configuration

5.4.4.3.1. View the OPC user-defined rules.

After entering the [User-defined Rules] page, the OPC protocol items are displayed by default. Click different tabs to display the user-defined rules of corresponding tabs. (As shown in Fig.5-64):

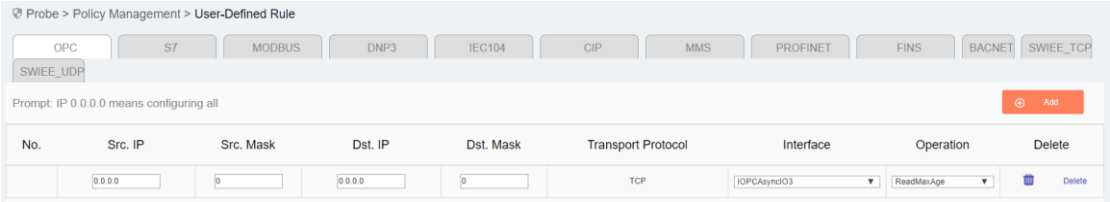


Fig.5-64 OPC User-defined Rules Information View Page

5.4.4.3.2. Add the OPC user-defined rules.

Enter the [User-defined Rules] page, click <Add> on the right (as shown in Fig.5-65) to automatically add a new line of OPC user-defined rules at the bottom of the OPC whitelist item list (as shown in Fig.5-66):

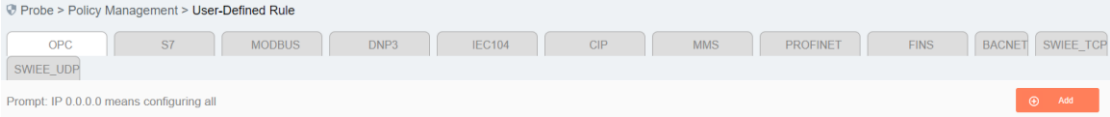


Fig.5-65 OPC User-defined Rule Add Button

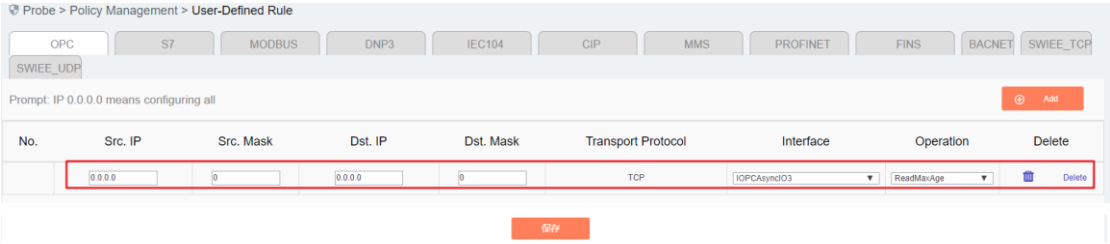


Fig.5-66 OPC User-defined Rule Add Page

Tab.47 Instruction to OPC User-defined Rule Fields

Column Names	Instructions
Src. IP	The IP address initiating an OPC data request, in dotted decimal format
Src. mask	The mask of the source IP address, generally ranging from 0 to 32
Dst. IP	The destination IP requesting OPC data, in dotted decimal format
Dst. Mask	The mask of the destination IP address, generally ranging from 0 to 32
Transport Protocol	Transport layer protocol
Interface	An interface name in the OPC protocol, built in the data dictionary

Operation	A method under an interface specified in the OPC protocol, built in a data dictionary
Delete	Delete the selected OPC user-defined rule
Save	Save all modification information to the database and make it come into effect

5.4.4.3.3. Modify the OPC user-defined rules.

Enter the [User-Defined Rules] page, change the source IP, source IP mask, destination IP, destination IP mask, interface name and method name of a user-defined rule, click <Save> after the modification.

5.4.4.3.4. Delete the OPC user-defined rules.

Enter the [User-Defined Rules] page, click <Delete> on the far right of a rule to delete the corresponding rule. (As shown in Fig.5-67):

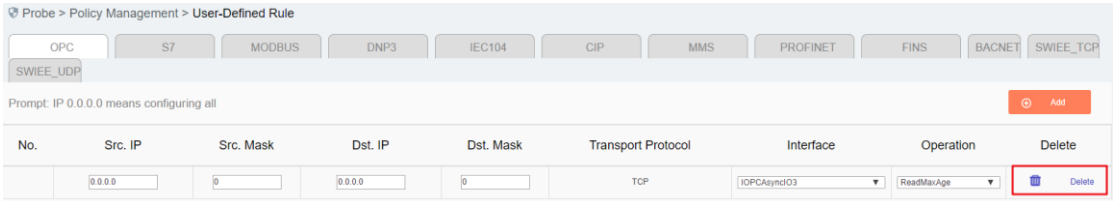


Fig.5-67 OPC User-defined Rule Delete Button

Other protocols use similar operations to add, modify and delete the user-defined rules.

5.4.5.Network Session Audit Template

5.4.5.1.Introduction to functions

The Intelligent monitoring terminal make a record on traffic flowing via it by default. When a user does not want to record all traffic, he/she may configure the traffic he/she cares about based on the network session audit template, and other traffic will not be recorded by the intelligent monitoring terminal.

5.4.5.2.Template management

Click [Policy Management/Network Session Template] in the left navigation bar (as shown in Fig.5-68) to enter the [Network Session Template] page (as shown in Fig.5-69):

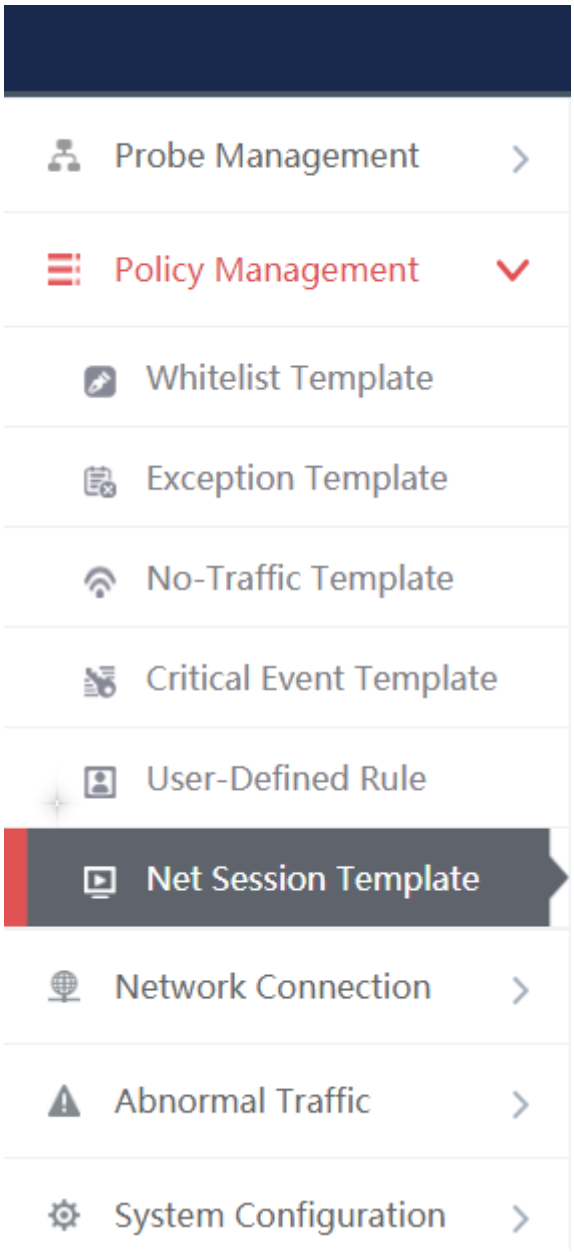


Fig.5-68 Selecting a Network Call Audit Template

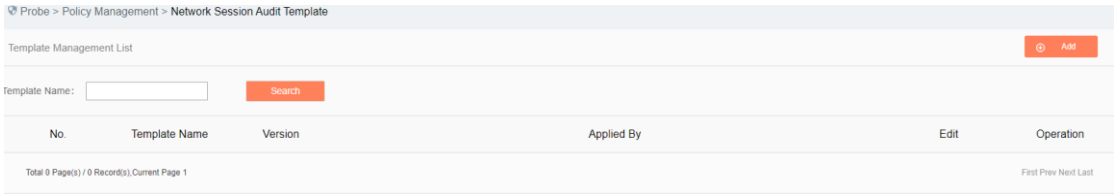


Fig.5-69 Network Session Audit Template Management

View information on all network session audit templates in the system here, with the meanings given below:

Tab.48 Instruction to Network Session Audit Template List Display

Column Names	Instructions

Template Name	A network session audit template name that is easy to remember, for example "Audit Template, Data Collection System 1"	
Version	The version of network session audit template, the version and the template ID uniquely determine a set of network session audit rules. The version number will automatically plus 1 after each time the network session audit rules are edited and saved	
Applied By	All intelligent monitoring terminals that are using this template	
Edit	Import	Network session audit rules imported to an excel sheet
	Export	Export the network session audit rules from the template to an excel sheet
Operation	Basic	View the basic information on the network session audit template
	Rule	View and modify the network session audit template rule configuration
	Delete	Delete the template. The template in use cannot be deleted

5.4.5.3. Add a network session audit template.

Click <Add> on the right side of [Network Session Audit Template] template management list tab of policy management (as shown in Fig.5-70) to pop up the network session audit template add page (as shown in Fig.5-71):

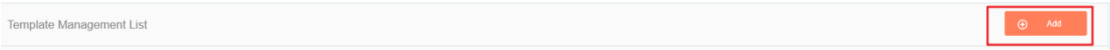


Fig.5-70 Network Session Audit Template

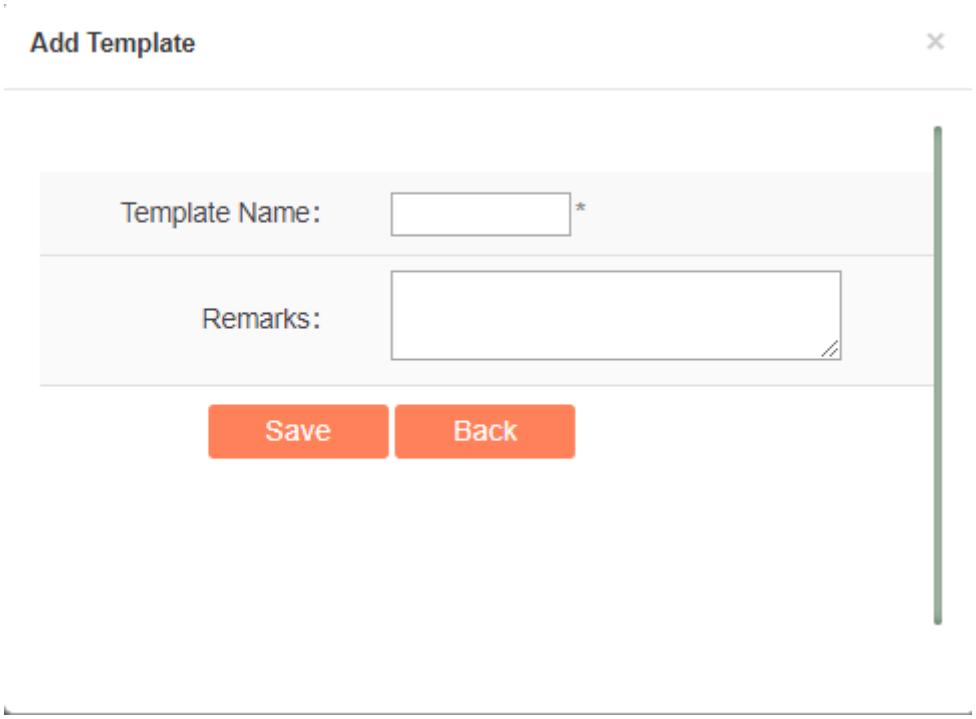


Fig.5-71 Network Session Audit Template Add Page

Tab.49 Instruction to Network Session Audit Template Add Information

Column Names	Instructions
Template Name	Define a meaningful network session audit template name that is easy to understand and remember
Remarks	Optional, additional explanatory information

5.4.5.4. Export the network session audit template.

Click <Export> (as shown in Fig.5-72) under the action column in the [Network Session Audit Template] display list of policy management, export the rules in the network session audit template in excel (as shown in Fig.5-73):

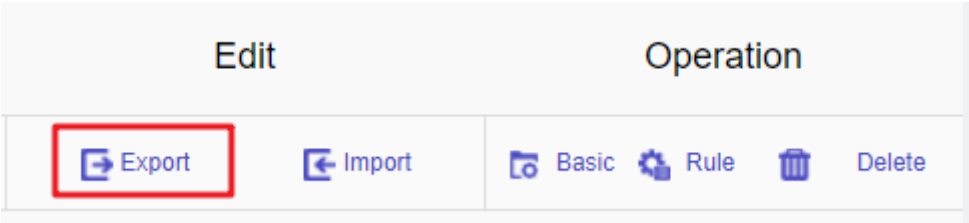
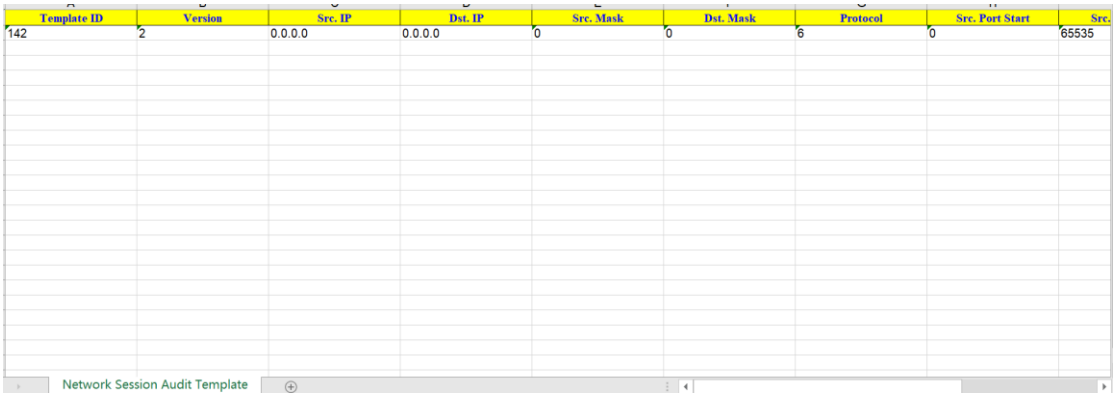


Fig.5-72 Network Session Audit Template Export Button

Click <Export> to export a file named "network session audit template_ {template name} _{date}.xls", for example, the rule file name that is exported on November 18, 2015, and with a template name of "Test" is "network session audit template_test_20151118.xls". The exported excel sheet contains all the rules for the template.



Template ID	Version	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol	Src. Port Start	Src.
142	2	0.0.0.0	0.0.0.0	0	0	6	0	65535

Network Session Audit Template

Fig.5-73 Example of an Exported Excel File

5.4.5.5. Import a network session audit template.

Click <Import> under the action column in the [Network Session Audit Template] display list of policy management (as shown in Fig.5-74), import the rules from the network session audit template saved in excel into the template (as shown in Fig.5-75):

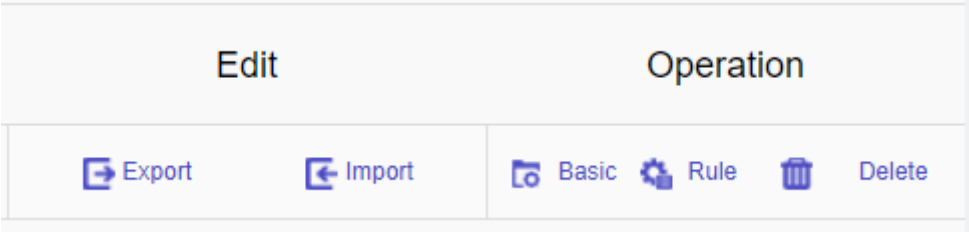


Fig.5-74 Network Session Audit Template Import Rule Button

Click <Import>, select the file to be imported in the dialog box for selecting an excel file, and click <Import Excel> to import the rules.

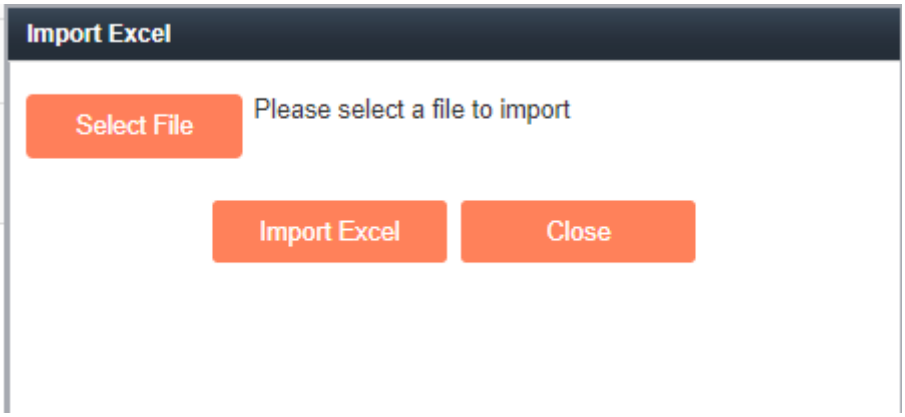


Fig.5-75 Importing the Excel Selection File Dialog Box

5.4.5.6. Network session audit template basic configuration

Click <Basic> (as shown in Fig.5-76) under the operation column in the [Network Session Audit Template] display list of policy management, open the [Network Session Audit Template] basic configuration page, view the basic information on the network session audit template (as shown in Fig.5-77):

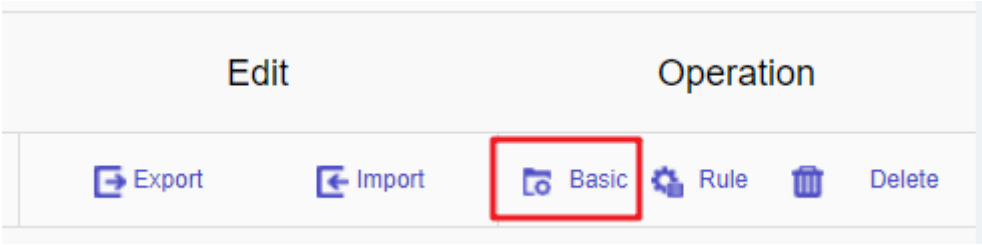


Fig.5-76 Network Session Audit Template Basic Configuration

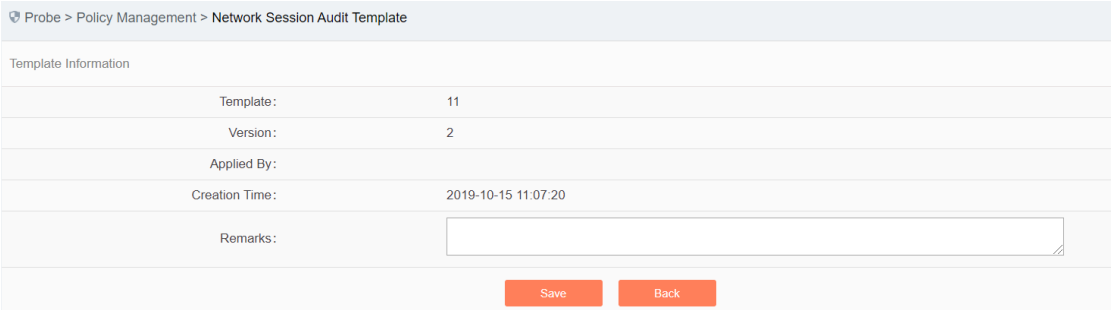


Fig.5-77 Network Session Audit Template Basic Configuration View Page

Tab.50 Instruction to Network Session Audit Template Basic Configuration Information

Column Names	Instructions
Template Name	The name of the template
Version	The version number of the template, which will automatically plus 1 after being modified each time
Applied By	A list of intelligent monitoring terminals using this template
Creation time	Template creation time
Remarks	To give additional information, optional

5.4.5.7. Network session audit template rule configuration

The management of network session audit rules is the core of network session audit template management. All templates depend on each specific rule.

5.4.5.7.1. View the network session audit rules.

After entering the [Rule Configuration] page, the network session audit rules are displayed. (As shown in Fig.5-78):

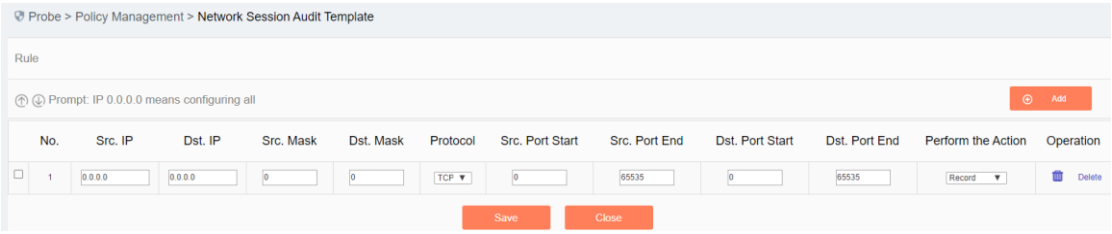


Fig.5-78 Network Session Audit Rule View Page

Click <Back> and go back to the [Network Session Audit Template List Display] page.

5.4.5.7.2. Add the network session audit rules.

Enter the [Rule Configuration] page, click <Add> on the right (as shown in Fig.5-79) to automatically add a new line of network session audit rules at the bottom of the rule (as shown in Fig.5-80):

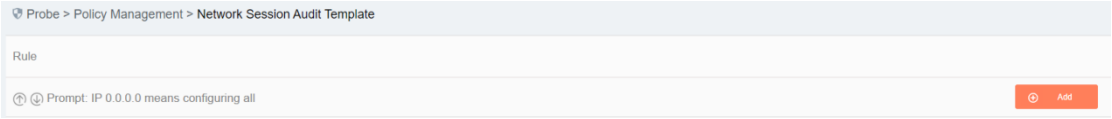


Fig.5-79 Network Session Audit Rule Add Button

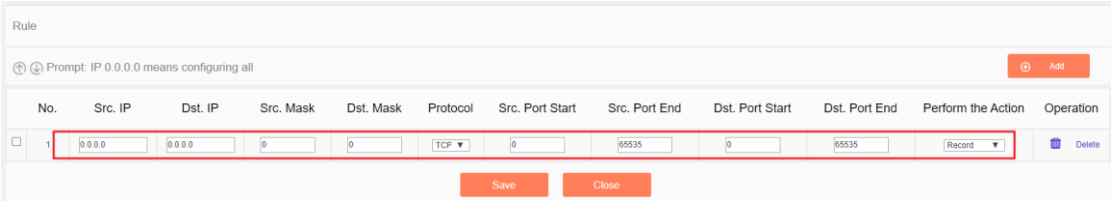


Fig.5-80 Network Session Audit Rule Add Button

Tab.51 Instruction to Network Session Audit Rule Fields

Column Names	Instructions
Src. IP	The IP address initiating a network connection request, in dotted decimal format
Dst. IP	The destination IP address for network connection, in decimal format
Src. mask	The mask of the source IP address, generally ranging from 0 to 32
Dst. mask	The mask for the destination IP address, generally ranging from 0 to 32
Protocol	Transport layer protocol, optional TCP or UDP
Src. Port Start	The starting value of the source port, ranging from 0 to 65535
Src. Port End	The end value of the source port, ranging from 0 to 65535, and the end source port must be greater than the start source port
Dst. Port Start	The starting value of the destination port, ranging from 0 to 65535
Dst. Port End	The end value of the destination port, ranging from 0 to 65535. The end destination port must be larger than the start destination port

Delete	Delete a specified rule	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the template information list display page
	Back	Ignore all modifications and go back to the template information list display page

5.4.5.7.3. Modify the network session audit rules.

Enter the [Network Session Audit Rule Configuration] page, change the source IP, destination IP, source IP mask, destination IP mask, protocol, start source port, end source port, start destination port and end destination port of a certain rule. Click <Save> after the modification.

5.4.5.7.4. Delete the network session audit rules.

Enter the [Network Session Audit Rule Configuration] page, click <Delete> on the far right of a rule to delete the corresponding rule. (As shown in Fig.5-81):

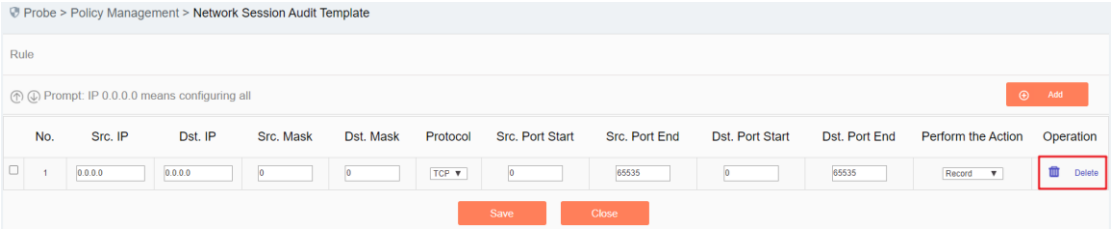


Fig.5-81 Network Session Audit Rule Delete Button

5.4.5.8. Delete a network session audit delete button.

Click <Delete> under the action column in the [Network Session Audit Template] information display list of policy management to delete the network session audit template that is no longer in use. The template being used cannot be deleted. (As shown in Fig.5-82):

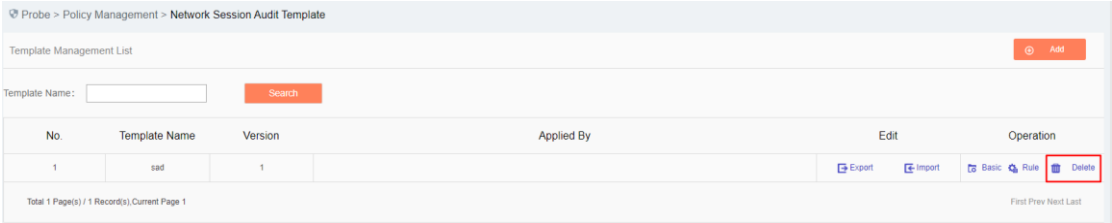


Fig.5-82 Network Session Audit Template Delete Button

5.4.5.9. Retrieve a network session audit template.

In the [Network Session Audit Template] information display column page of policy management, the network session audit template can be retrieved based on conditions. (As shown in Fig.5-83):

Fig.5-83 Retrieving a Network Session Audit Template

5.4.6. No Traffic Detection Template

5.4.6.1. Introduction to functions

The intelligent monitoring terminal can detect cases in which network connections that a user cares about has no traffic due to certain reasons and give an alarm. Users can configure the related traffic through the no-traffic template.

5.4.6.2. Template management

Click [Policy Management/No Traffic Template] in the left navigation bar (as shown in Fig.5-84), enter the [No Traffic Detection Template] page (as shown in Fig.5-85):

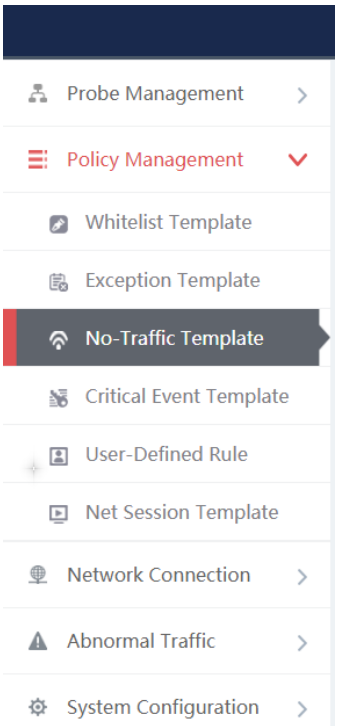


Fig.5-84 Selecting a No Traffic Detection Template

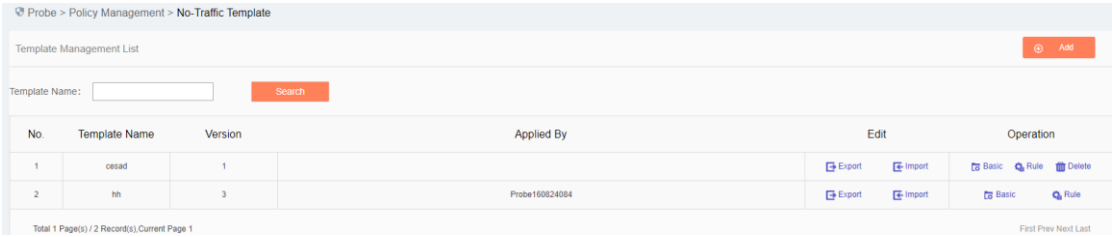


Fig.5-85 No Traffic Detection Template Management

View information on all no traffic detection templates in the system here, with the meanings given below:

Tab.52 Instruction to Network Session Audit Template List Display

Column Names	**Instructions**	
Template Name	A no traffic detection template name that is easy to remember, for example "No Traffic Detection Template, Data Collection System 1"	
Version	The version of no traffic detection template, the version and template ID uniquely determine a set of no traffic detection rules. The version number will automatically plus 1 after each time the no traffic detection rules are edited and saved	
Applied By	All intelligent monitoring terminals that are using this template	
Edit	Import	No traffic detection rules imported to an excel sheet
	Export	Export the no traffic detection rules in the template to an excel sheet
Operation	Basic	View the basic information on no traffic detection templates
	Rule	View and modify the no traffic detection template rule configuration
	Delete	Delete the template. The template in use cannot be deleted

5.4.6.3. Add a no traffic detection template.

Click <Add> (as shown in Fig.5-86) on the right side of the [No Traffic Detection Template] template management list tab of policy management to pop up the no traffic detection template add page (as shown in Fig.5-87):

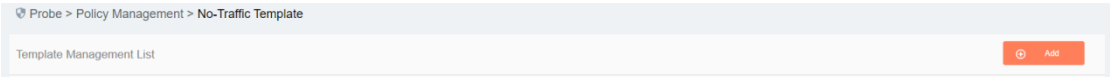


Fig.5-86 No Traffic Detection Template Add Button

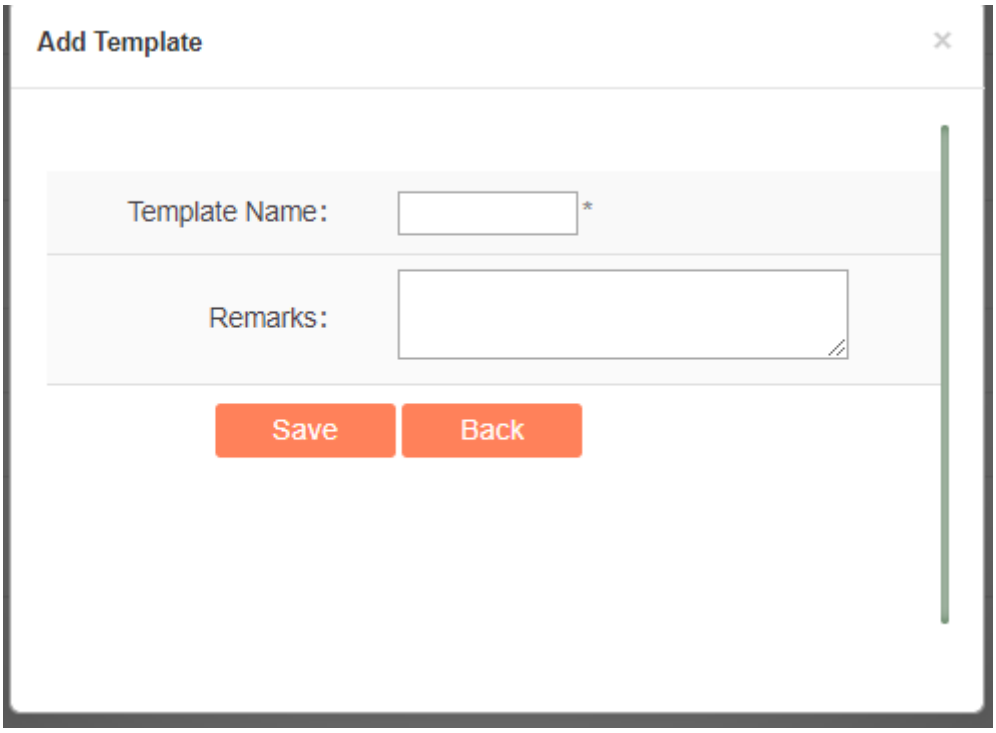


Fig.5-87 No Traffic Detection Template Add Page

Tab.53 Instruction to No Traffic Detection Template Add Information

Column Names	Instructions
Template Name	Define a meaningful no traffic detection template name that is easy to understand and remember
Remarks	Optional, additional explanatory information

5.4.6.4. Export a no traffic detection template.

Click <Export> under the operation column in the [No Traffic Detection Template] display list of policy management (as shown in Fig.5-88), export the rules in the no traffic detection template in excel (as shown in Fig.5-89):

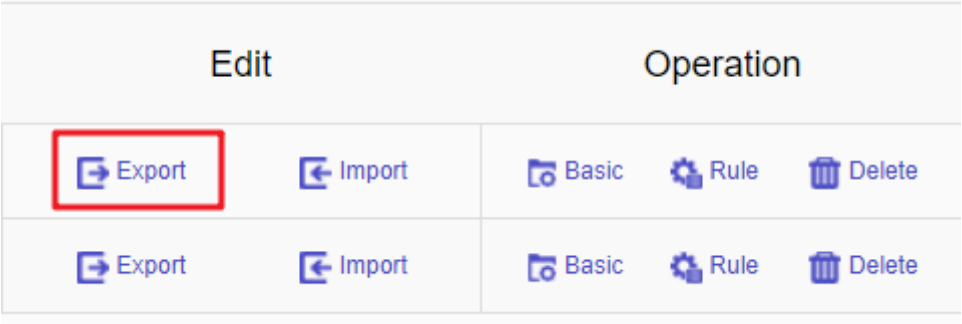
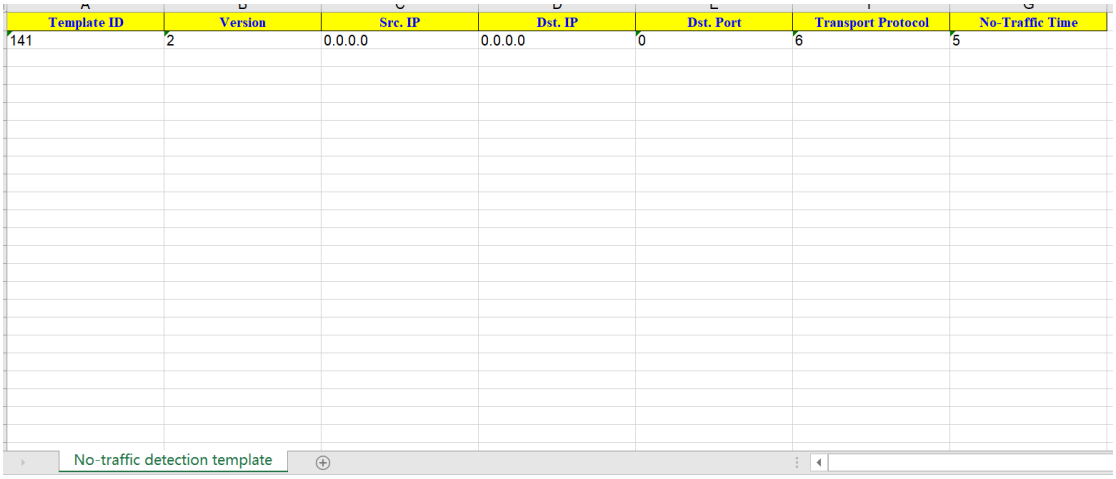


Fig.5-88 No Traffic Detection Template Export Button

Click <Export> to export a file named "no traffic detection template _ {template name}_{date}.xls", for example, the rule file name that is exported on November 18, 2015 and with a template name of "Test" is "no traffic

detection template_test_20151118.xls". The exported excel sheet contains all the rules for the template.



Template ID	Version	Src. IP	Dst. IP	Dst. Port	Transport Protocol	No-Traffic Time
141	2	0.0.0.0	0.0.0.0	0	6	5

No-traffic detection template

Fig.5-89 Example of an Exported Excel File

5.4.6.5. Import a no traffic detection template.

Click <Import> under the operation column in the [No Traffic Detection Template] display list of policy management (as shown in Fig.5-90), import the rules in the no traffic detection template saved in excel into the template (as shown in Fig.5-91):

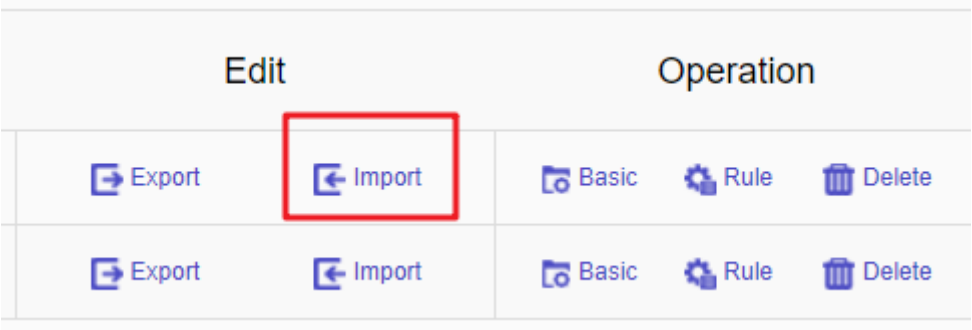


Fig.5-90 No Traffic Detection Template Import Rules

Click <Import>, select the file to be imported in the dialog box for selecting an excel file, and click <Import Excel> to import the rules.

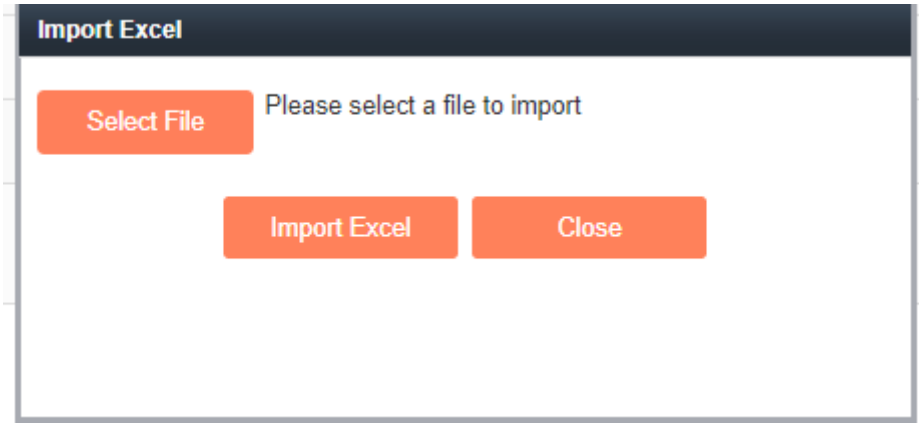


Fig.5-91 Importing the Excel Selection File Dialog Box

5.4.6.6. No traffic detection template basic configuration

Click <Basic Configuration> (as shown in Fig.5-92) under the operation column in the [No Traffic Detection Template] display list of policy management, open the [No Traffic Detection Template] basic configuration page, view the basic information on the no traffic detection template (as shown in Fig. 5-93):

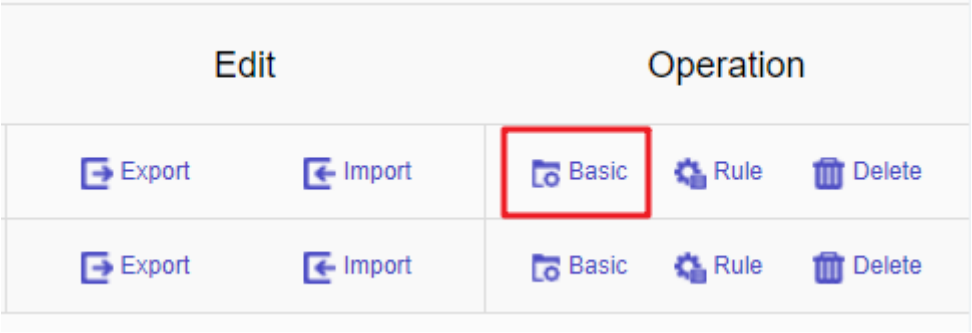


Fig.5-92 No Traffic Detection Template Basic Configuration

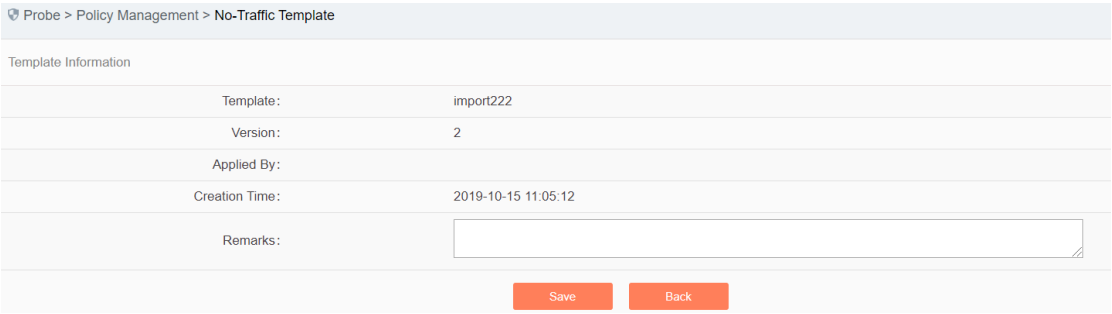


Fig.5-93 No Traffic Detection Template Basic Configuration View Page

Tab.54 Instruction to No Traffic Detection Template Basic Configuration Information

Column Names	Instructions
Template Name	The name of the template
Version	The version number of the template, which will automatically plus 1 after being modified each time
Applied By	A list of intelligent monitoring terminals using this template
Creation Time	Template creation time
Remarks	To give additional information, optional

5.4.6.7. No traffic detection template rule configuration

The management of no-traffic detection rules is the core of no-traffic detection template management. All templates depend on each specific rule.

5.4.6.7.1. View the no traffic detection rules.

After entering the [Rule Configuration] page, no traffic detection rules are displayed. (As shown in Fig.5-94):

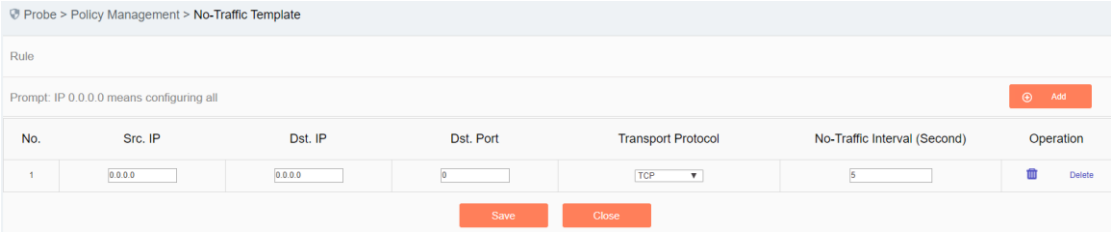


Fig.5-94 No Traffic Detection Rule View Page

Click <Close> and go back to the [No Traffic Detection Template List Display] page.

5.4.6.7.2. Add the no traffic detection rules.

Enter the [Rule Configuration] page, click <Add> on the right (as shown in Fig.5-95) to automatically add a new line of non-traffic detection rules at the bottom of the rule (as shown in Fig.5-96):

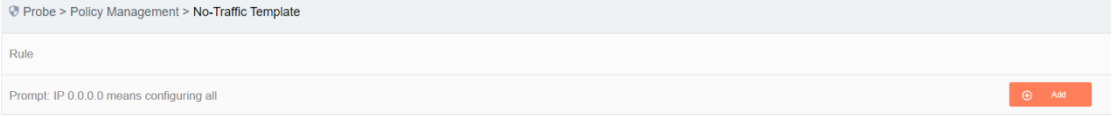


Fig.5-95 No Traffic Detection Rule Add Button

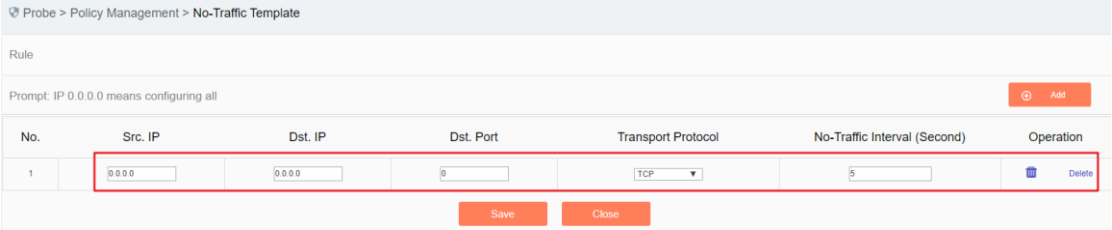


Fig.5-96 No Traffic Detection Rule Add Item

Tab.55 Instruction to No Traffic Detection Rule Fields

Column Names	**Instructions**
Src. IP	The IP address initiating a network connection request, in dotted decimal format
Dst. IP	The destination IP address for network connection, in decimal format
Dst. port	The port of server monitoring, ranging from 0 to 65535
Transport Protocol	Transport layer protocol, optional TCP or UDP
No-Traffic Interval	The no traffic time for detecting the configuration rules, ranging from 5 seconds to 86,400 seconds
Delete	Delete a specified rule

Operation	Save	Save all modification information to the database and make it come into effect, and go back to the template information list display page
	Back	Ignore all modifications and go back to the template information list display page

5.4.6.7.3. Modify no traffic detection rules.

Enter the [No Traffic Detection Rule Configuration] page, change the source IP, destination IP, destination port, transport layer protocol and no traffic time of a rule. Click <Save> after the modification.

5.4.6.7.4. Delete the no traffic detection rules.

Enter the [No Traffic Detection Rule Configuration] page, click <Delete> on the far right of a rule to delete the corresponding rule. (As shown in Fig.5-97):

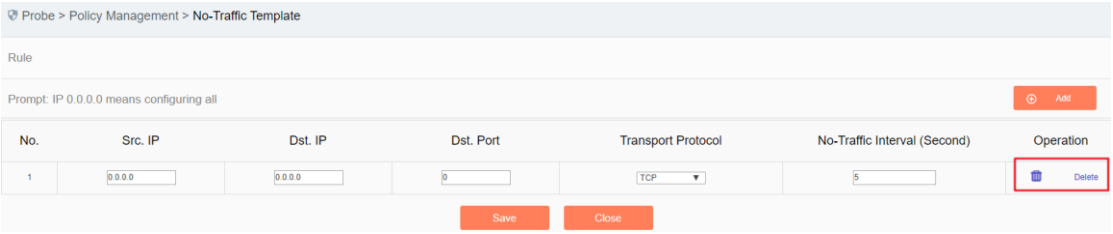


Fig.5-97 No-traffic Detection Rule Delete Button

5.4.6.8. Delete a no traffic detection template.

Click <Delete> under the operation column in the [No Traffic Detection Template] information display list of policy management to delete the no traffic detection template that is no longer in use. The template being used cannot be deleted. (As shown in Fig.5-98):

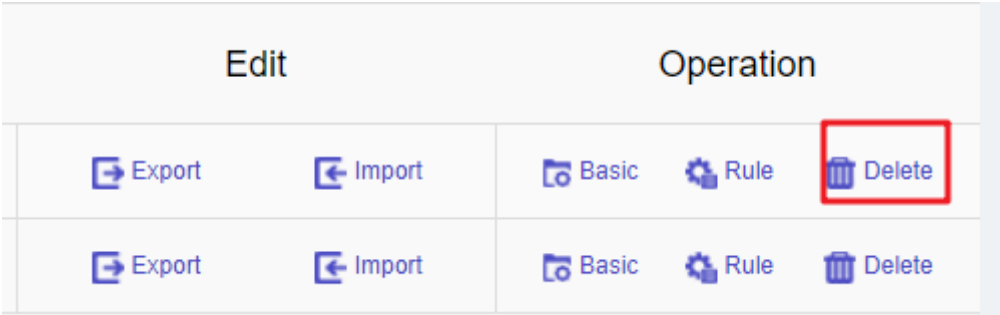


Fig.5-98 No Traffic Detection Template Delete Button

5.4.6.9. Retrieve a no-traffic detection template

In the [No Traffic Detection Template] information display list page of policy management, the no-traffic detection template can be retrieved according to the conditions. (As shown in Fig.5-99):

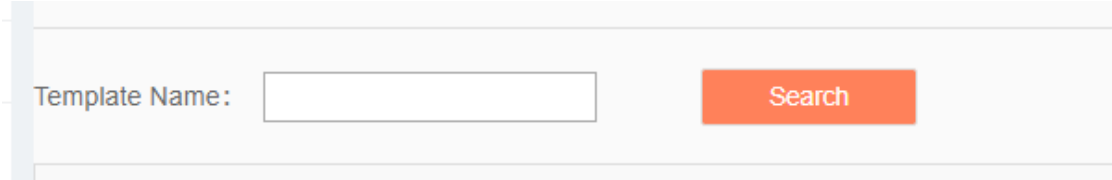


Fig.5-99 Retrieving a No Traffic Detection Template

5.5. Log Management

5.5.1. Introduction to Functions

Log management can buffer or redirect events occurred to the system or logs generated by message audit to the log receiving server. By analyzing and archiving the log contents, the administrator can check the security bugs of the network, understanding that when someone has tries to violate the security policy. In addition, real-time logging can be used to detect ongoing intrusions.

5.5.2. Industrial Protocol Whitelist Alarm

The industrial protocol whitelist alarm is generated by messages flowing through the intelligent monitoring terminal in violation of the industrial protocol whitelist rules on the intelligent monitoring terminal. Only when the intelligent monitoring terminal is in operation mode can this log be generated.

5.5.2.1. Log list

Click [Log Management/Industrial Protocol Whitelist Alarm] in the left navigation bar (as shown in Fig.5-100), enter the [Industrial Protocol Whitelist Alarm] list page (as shown in Fig.5-101):

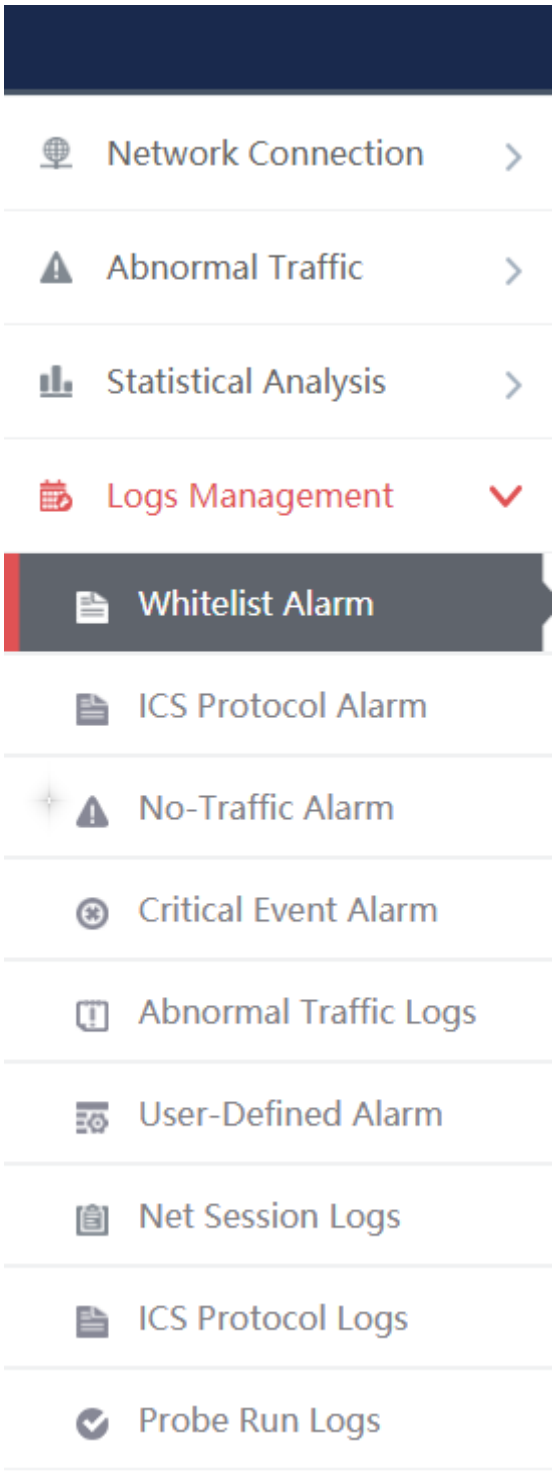


Fig.5-100 Industrial Protocol Whitelist Alarm Menu

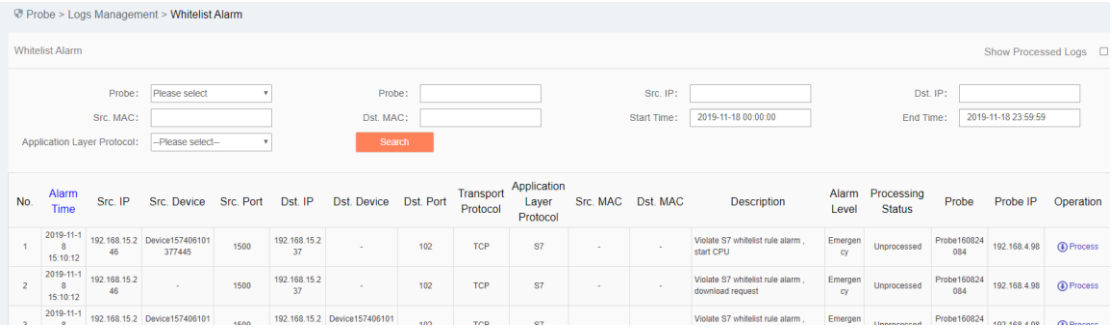


Fig.5-101 Industrial Protocol Alarm List Page

View all the log information on whitelist alarms here, with the meaning given below:

Tab.56 Instruction to Whitelist Alarm Log Display

Column Names	**Instructions**
Alarm Time	Time when an alarm occurs
Src. IP	The IP address initiating a data request, in dotted decimal format
Src. device	The system automatically generates a source device name according to the source IP, supporting custom source device name
Src. Port	The port used by the machine initiating the data request
Dst. IP	The destination IP requesting data, in dotted decimal format
Dst. device	The system automatically generates a destination device name according to destination IP, supporting custom destination device name
Dst. port	The port used by the requested destination machine
Transport Protocol	The protocol type of transport layer used by the message
Application Layer Protocol	Specific application protocol types
Src. MAC	The MAC address initiating a data request
Dst. MAC	The destination MAC address requesting the data
Description	Information on alarm description
Alarm Level	Warning of possible damage levels, refer to 5.6.2 Instruction to Alarm Levels.
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format

Operation	Process	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Show Processed Logs> on the right of the [Industrial Protocol Whitelist Alarm] whitelist alarm list tab, view the processed logs. (As shown in Fig.5-102):

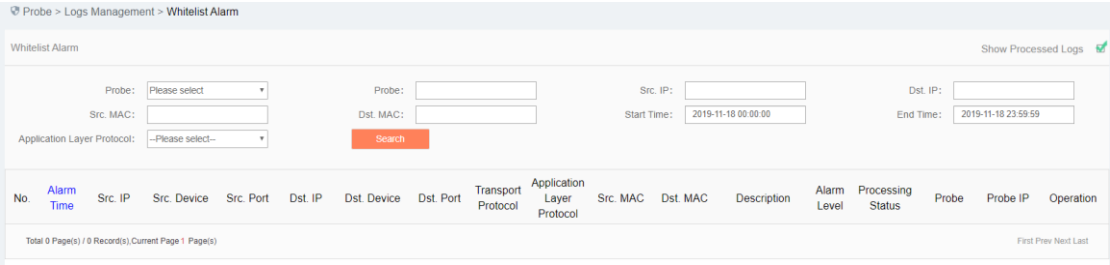


Fig.5-102 Displaying Processed Whitelist Alarm List Page

5.5.2.2. **Process a log.**

Click <Process> under the operation column of [Industrial Protocol Whitelist Alarm] display list, display the [Industrial Protocol Whitelist Alarm] processing page (as shown in Fig.5-103):

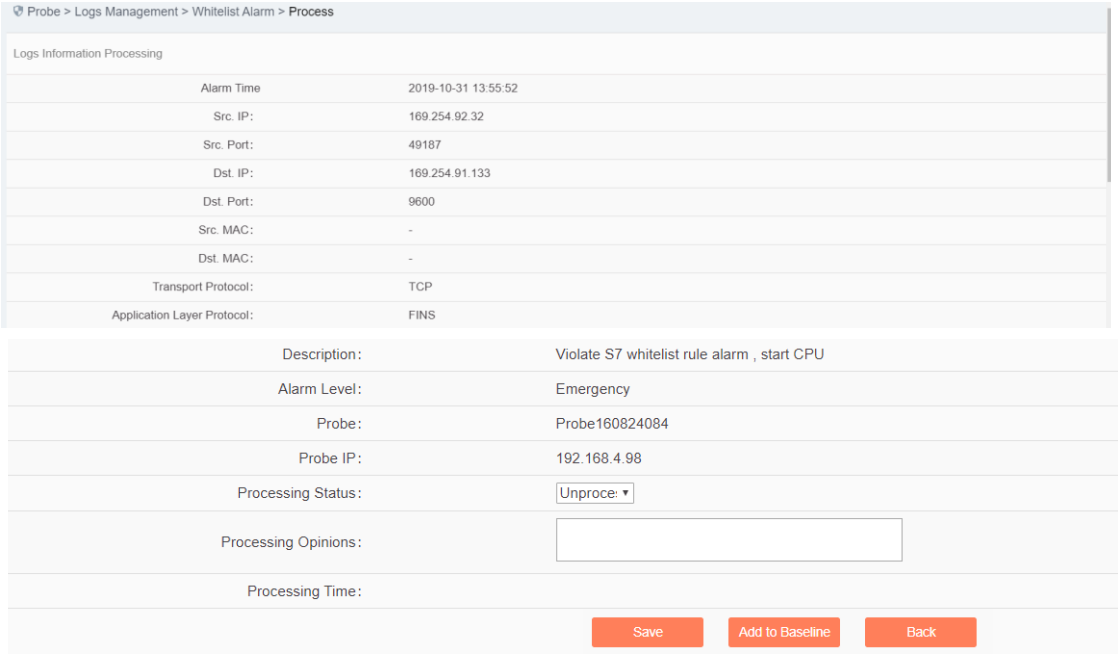


Fig.5-103 Industrial Protocol Whitelist Alarm Processing Page

5.5.2.2.1. **Close the log.**

Click the drop-down box of processing status, select "Close", fill in the relevant opinions in the processing opinions field and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the [Industrial Protocol Whitelist Alarm Logs] list page by default.

Or do not select "Close" but fill in the processing opinions instead.

5.5.2.2.2. Add a baseline.

For an industrial protocol whitelist reported mistakenly, click <Add a Baseline>, and add the alarm information to the whitelist template to generate the alarm at one click. After adding the alarm to the whitelist with one click, similar alarms will no longer be generated.

5.5.2.2.3. Export a message.

When checking to save the whitelist alarms of alarm message in the intelligent monitoring terminal configuration, the whitelist alarm message generated by such an intelligent monitoring terminal will be downloaded. Click <Export a Message> to automatically save the message to the computer executing the operation.

5.5.2.3. Retrieve a log.

In the [Industrial Protocol Whitelist Alarm] page, retrieve an alarm according to the conditions. (as shown in Fig.5-104):

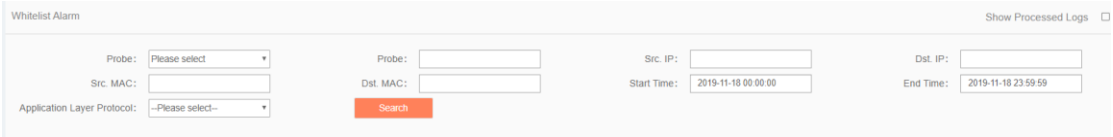


Fig.5-104 Retrieving a Whitelist Alarm

5.5.3. Industrial Protocol Detection Alarm

Industrial protocol detection alarms are generated by messages flowing through intelligent monitoring terminals that violate industrial protocol protocols.

5.5.3.1. Log list

Click [Log Management/Industrial Protocol Detection Alarm] (as shown in Fig.5-105), enter the [Industrial Protocol Detection Alarm] list page (as shown in Fig.5-106):

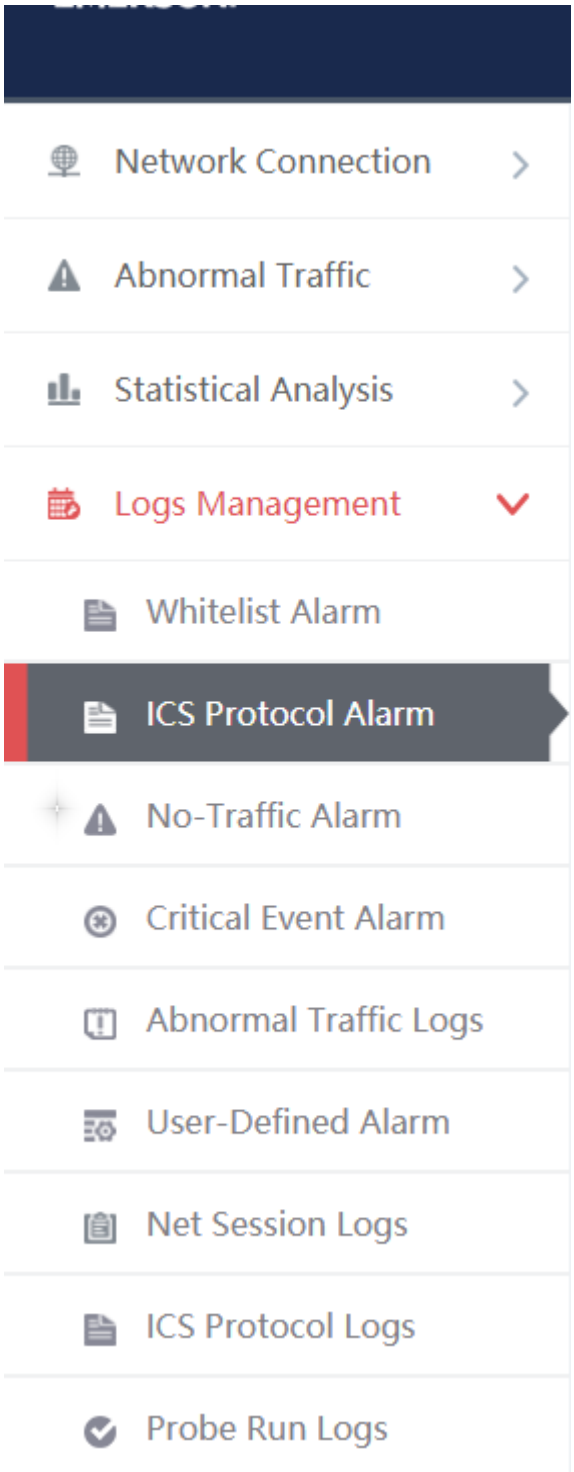


Fig.5-105 Industrial Protocol Detection Alarm Menu

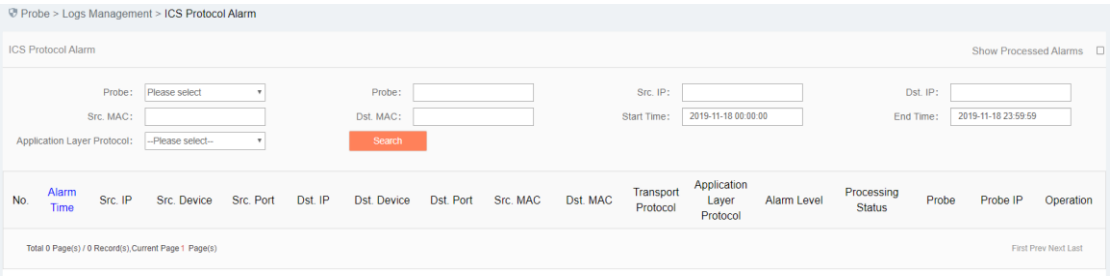


Fig.5-106 Industrial Protocol Detection Alarm List Page

View all the log information on industrial protocol alarms here, with the meaning given below:

Tab.57 Instruction to Industrial Protocol Detection Alarm Display

Column Names	**Instructions**	
Alarm Time	Time when an alarm occurs	
Src. IP	The IP address initiating a data request, in dotted decimal format	
Src. device	The system automatically generates a source device name according to the source IP, supporting custom source device name	
Src. port	The port used by the machine initiating the data request	
Dst. IP	The destination IP requesting data, in dotted decimal format	
Dst. Device	The system automatically generates a destination device name according to destination IP, supporting custom destination device name	
Dst. Port	The port used by the requested destination machine	
Src. MAC	The MAC address initiating a data request	
Dst. MAC	The destination MAC address requesting the data	
Transport Protocol	The protocol type of transport layer used by the message	
Application Layer Protocol	Specific application protocol types	
Alarm Level	Warning of possible damage levels	
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember	
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format	
Operation	Process	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed. Check <Show Processed Logs> on the right side of the [Industrial Protocol Detection Alarm] to view the

processed log. (As shown in Fig.5-107):

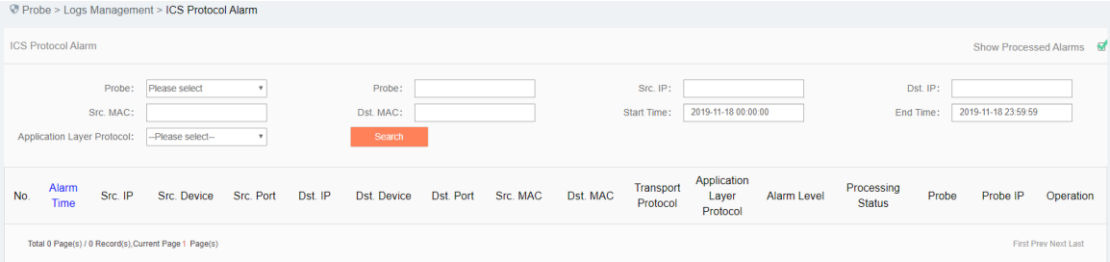


Fig.5-107 Displaying Processed Protocol Alarm List Page

5.5.3.2. **Process a log.**

Click <Process> under the operation column in the [Industrial Protocol Detection Alarm] display list, display the [Industrial Protocol Detection Alarm] processing page (as shown in Fig.5-108):

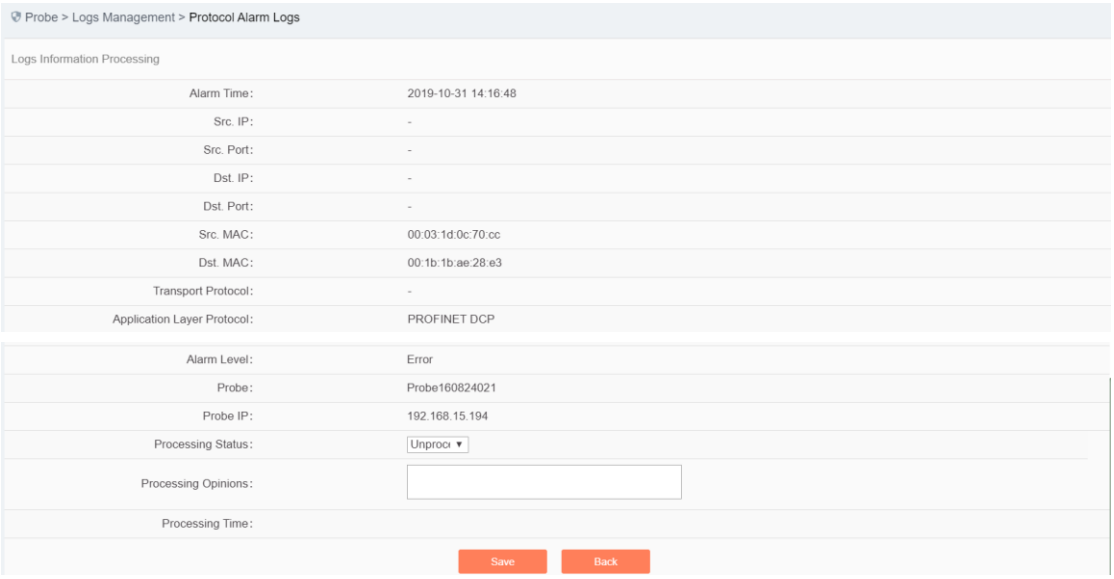


Fig.5-108 Industrial Protocol Alarm Processing Page

Click the drop-down box of processing status, select "Close", fill in the relevant opinions in the processing opinions field and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the [Industrial Protocol Detection Alarm] list page by default.

Or do not select "Close" but fill in the processing opinions instead.

5.5.3.3. **Retrieve a log.**

In the [Industrial Protocol Detection Alarm] list page, retrieve an alarm according to the conditions. (As shown in Fig.5-109):

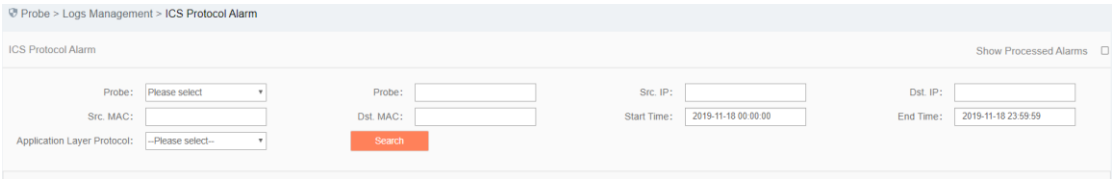


Fig.5-109 Retrieving an Industrial Protocol Detection Alarm

5.5.4.No Traffic Alarm

When from a certain moment that the traffic specified by some users is not generated, the intelligent monitoring terminal shall give an no traffic alarm.

5.5.4.1.Log list

Click [Log Management/No Traffic Alarm] in the left navigation bar (as shown in Fig.5-110), enter the [No Traffic Alarm] list page (as shown in Fig.5-111):

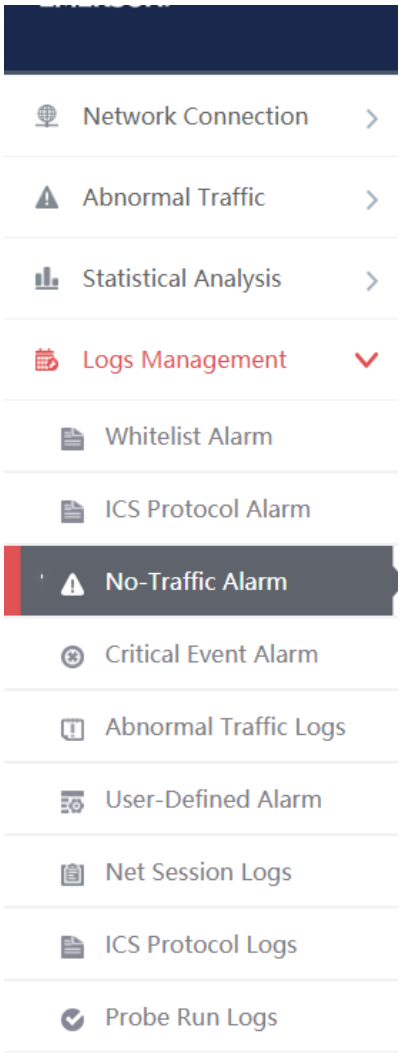


Fig.5-110 No Traffic Alarm Menu

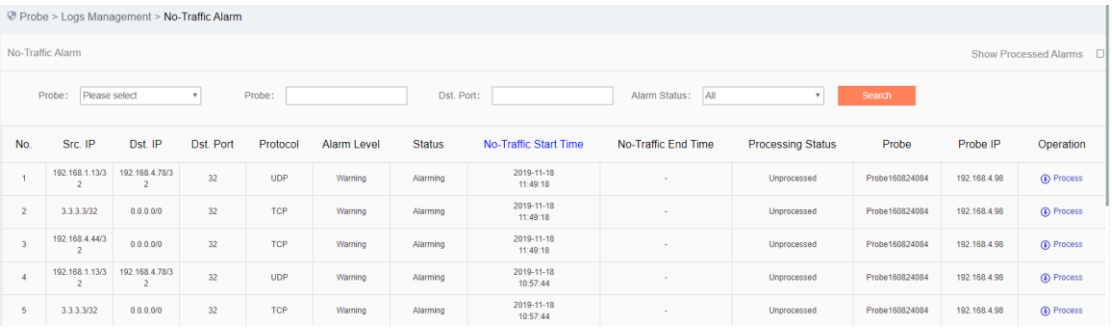


Fig.5-111 No Traffic Alarm List Page

View all the log information on no traffic alarms here, with the meaning given below:

Tab.58 Instruction to No Traffic Alarm Log Display

Column Names	**Instructions**	
Src. IP	The IP address initiating a data request, in dotted decimal format	
Dst. IP	The destination IP requesting data, in dotted decimal format	
Dst. port	The port used by the requested destination machine	
Protocol	The protocol type of transport layer used by the message	
Alarm Level	Warning of possible damage levels	
No-Traffic Start Time	From this moment, the specified rule has no traffic	
No-Traffic End Time	From this moment on, the specified rule restarts the traffic, which is displayed as "-" when there is no end time	
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember	
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format	
Operation	Process	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Show Processed Logs> on the right side of the [No Traffic Alarm] Whitelist Alarm List tab. (as shown in Fig.5-112):

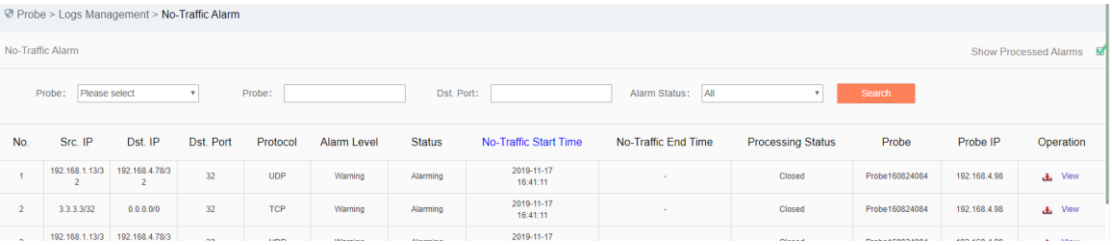


Fig.5-112 Displaying Processed No Traffic Alarm List Page

5.5.4.2. Process a log.

Click <Process> under the operation column in the [No Traffic Alarm] display list, display the [No Traffic Alarm Information] processing page (as shown in Fig.5-113):

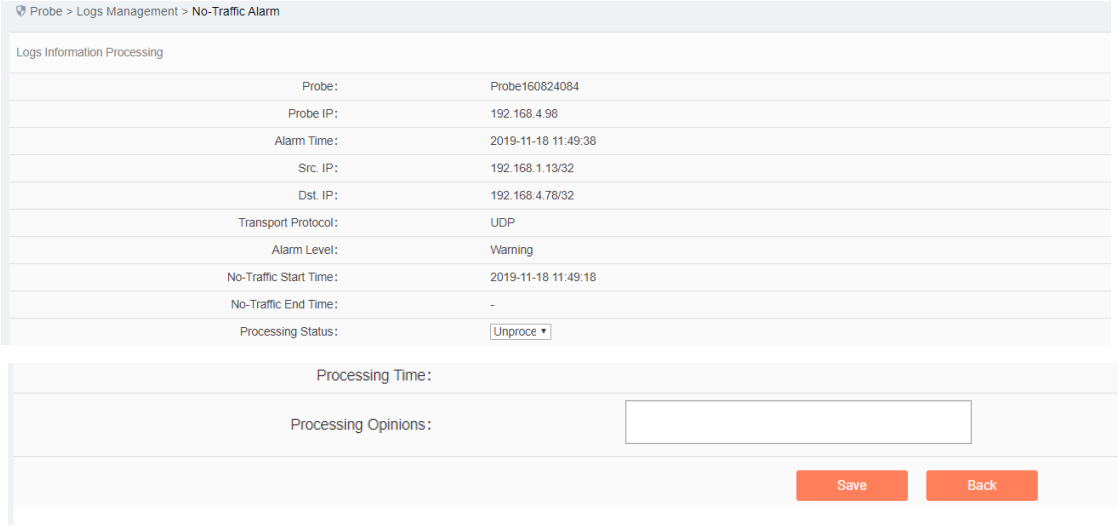


Fig.5-113 No Traffic Alarm Processing Page

Click the drop-down box of processing status, select "Close", fill in the relevant opinions in the processing opinions field and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the [No traffic Alarm] list page by default.

Or do not select "Close" but fill in the processing opinions instead.

5.5.4.3. Retrieve a log.

In the [No Traffic Alarm] list page, retrieve an alarm according to the conditions. (As shown in Fig.5-114):

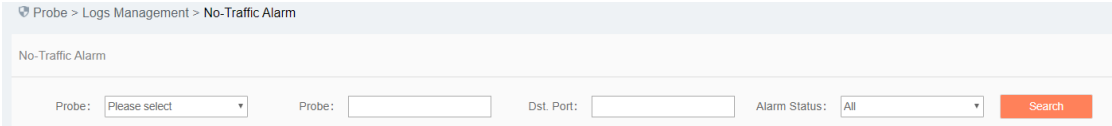


Fig.5-114

5.5.5. Critical Event Alarm

When a critical event occurs, the traffic flowing through the intelligent monitoring terminal, the intelligent monitoring terminal will generate an alarm.

Define the critical event in the system as follows:

1. Write operation of all industrial protocols:

2. Request download, start download, finish download, request upload, start upload, finish upload, CPU start, CPU stop of the S7 protocol.

5.5.5.1. Log list

Click [Log Management/Critical Event Alarm] in the left navigation bar (as shown in Fig.5-115), enter the [Critical Event Alarm] list page (as shown in Fig.5-116):

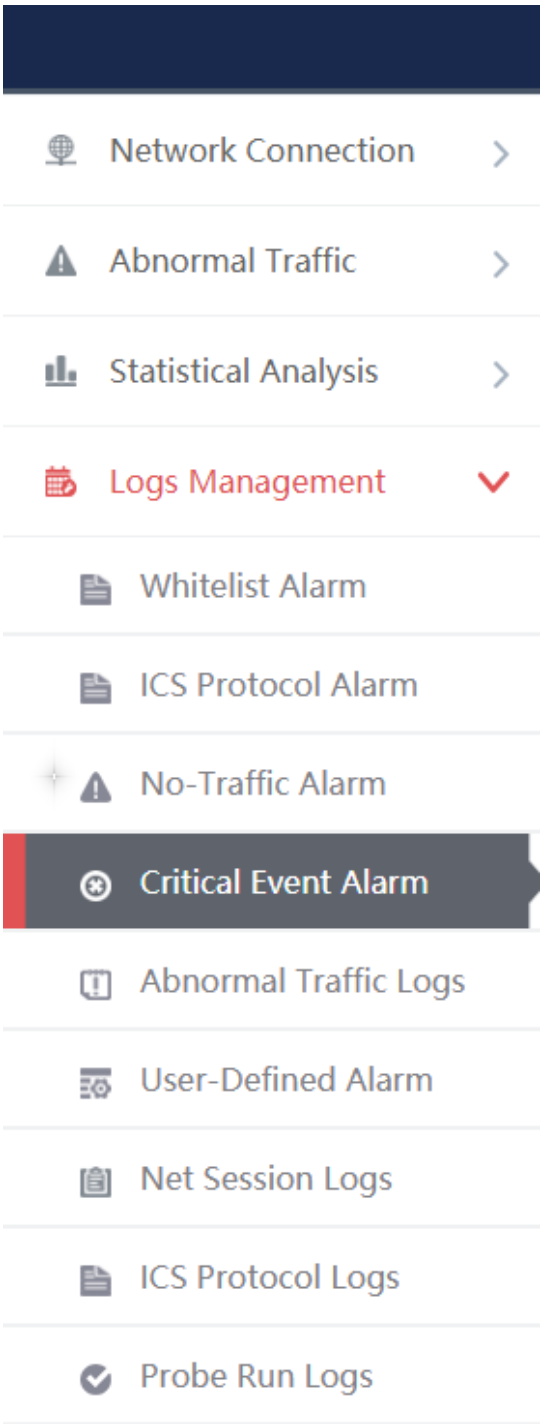


Fig.5-115 Critical Event Alarm Menu

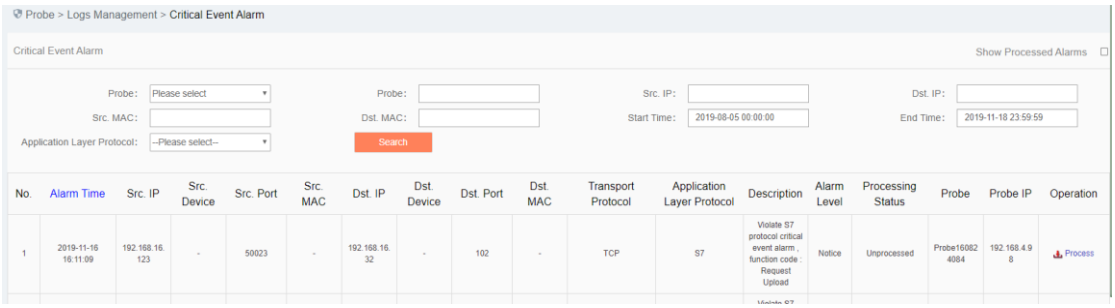


Fig.5-116 Critical Event Alarm List Page

View all the log information on critical event alarms here, with the meaning given below:

Tab.59 Instruction to Critical Event Alarm Log Display

Column Names	**Instructions**	
Alarm Time	The time to generate an alarm	
Src. IP	The IP address initiating a data request, in dotted decimal format	
Src. port	The port initiating a data request	
Src. device	The system automatically generates a source device name according to the source IP, supporting custom source device name	
Dst. IP	The destination IP requesting data, in dotted decimal format	
Dst. Device	The system automatically generates a destination device name according to destination IP, supporting custom destination device name	
Dst. port	The port used by the requested destination machine	
Transport protocol	The protocol type of transport layer used by the message	
Application Layer Protocol	The protocol used by the application layer	
Description	Alarm description	
Src. MAC	The MAC address initiating a data request	
Dst. MAC	The destination MAC address requesting the data	
Alarm Level	Warning of possible damage levels	
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember	
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format	
Operation	Processing	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Show Processed Logs> on the right side of the [Critical Event Alarm] critical event alarm list tab, view the processed log. (As shown in Fig.5-117):

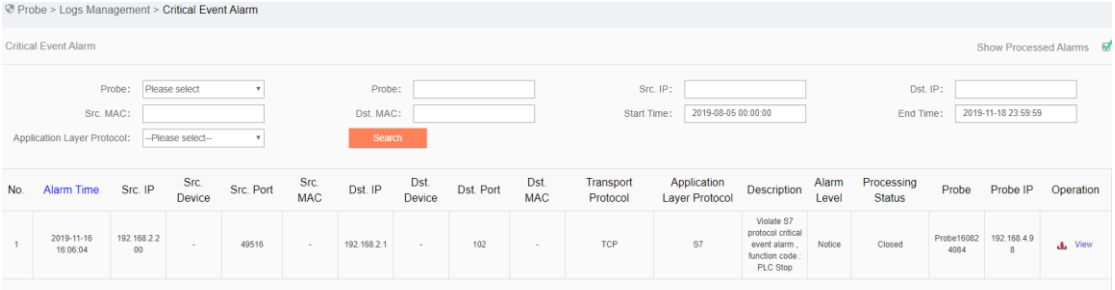


Fig.5-117 Displaying the Processed Critical Event Alarm List Page

5.5.5.2. **Process a log.**

Click <Process> under the operation column of [Critical Event Alarm] display list, display the [Critical Event Alarm Information] processing page (as shown in Fig.5-118):

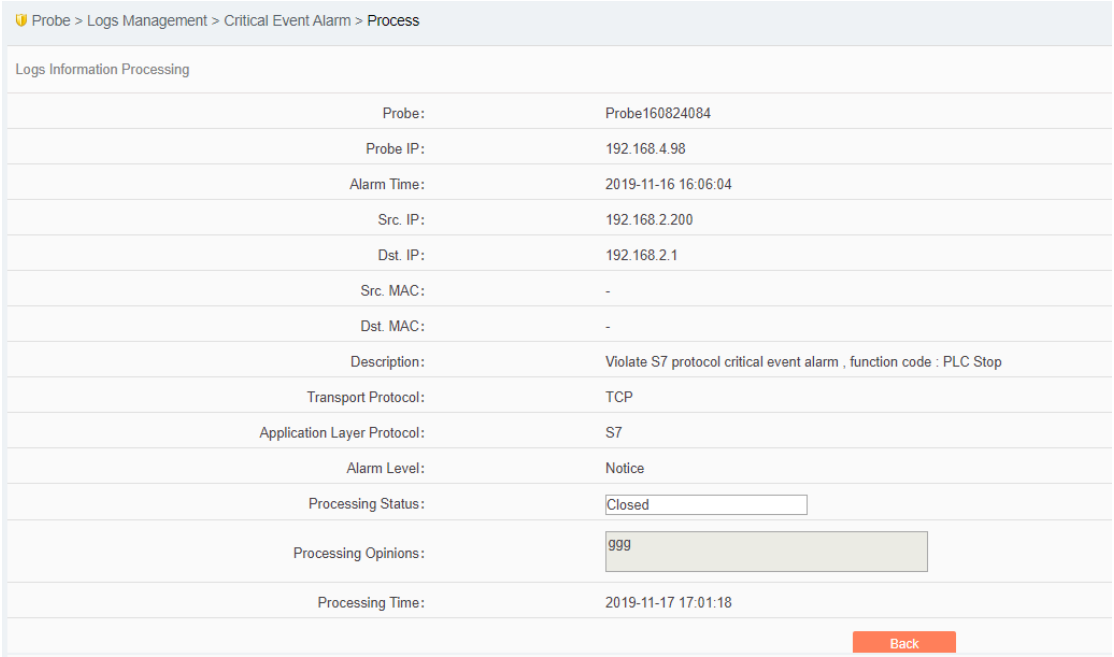


Fig.5-118 Critical Event Alarm Processing Page

Click the drop-down box of processing status, select "Close", fill in the relevant opinions in the processing opinions field and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the [Critical Event Alarm] list page by default.

Or do not select "Close" but fill in the processing opinions instead.

5.5.5.3. **Retrieve a log.**

In the [Critical Event Alarm] list page, retrieve an alarm according to the conditions. (As shown in Fig.5-119):

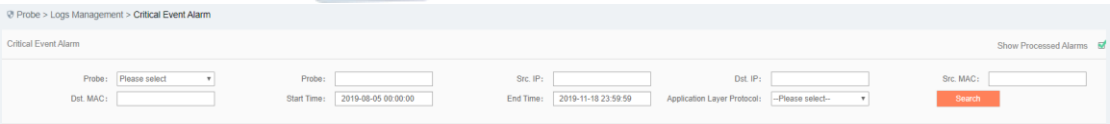


Fig.5-119 Retrieving a Critical Event Alarm

5.5.6. User-Defined Alarm

User-defined alarms are generated by messages flowing through intelligent monitoring terminals in accordance with user-configured rules.

5.5.6.1. Log list

Click [Log Management/User-defined Alarm] in the left navigation bar (as shown in Fig.5-120), enter the [User-defined Alarm] list page (as shown in Fig.5-121):

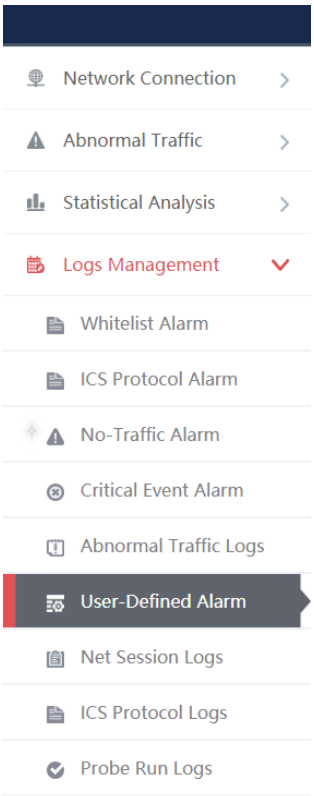


Fig.5-120 User-defined Menu

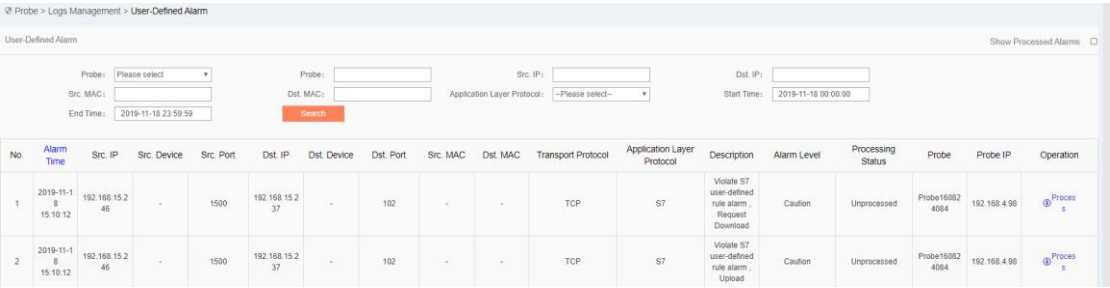


Fig.5-121 User-defined Alarm List Page

View all the log information on user-defined alarms here, with the meaning given below:

Tab. 60 Instruction to User-defined Alarm Log Display

Column Names	**Instructions**	
Alarm Time	Time when an alarm occurs	
Src. IP	The IP address initiating a data request, in dotted decimal format	
Src. Port	The port used by the machine initiating the data request	
Src. Device	The system automatically generates a source device name according to the source IP, supporting custom source device name	
Dst. IP	The destination IP requesting data, in dotted decimal format	
Dst. Device	The system automatically generates a destination device name according to destination IP, supporting custom destination device name	
Dst. Port	The port used by the requested destination machine	
Transport Protocol	The protocol type of transport layer used by the message	
Application Layer Protocol	Specific application types	
Src.Mac	The destination MAC address requesting the data	
Dst. MAC	The destination MAC address requesting the data	
Alarm Level	Warning of possible damage levels	
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember	
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format	
Operation	Process	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Show Processed Logs> on the right side of the [User-defined Alarm] user-defined alarm list tab, view the processed log. (As shown in Fig.5-122):

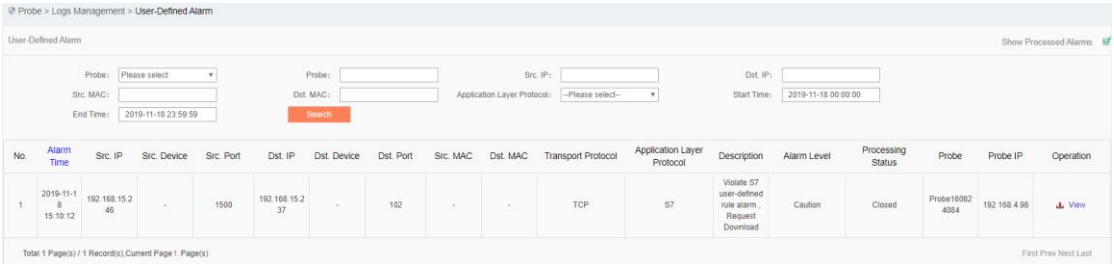


Fig.5-122 Displaying Processed User-defined Alarm List Page

5.5.6.2. Process a log.

Click <Process> under the operation column of [User-defined Alarm] display list, display the [User-defined Alarm Information] processing page (as shown in Fig.5-123):

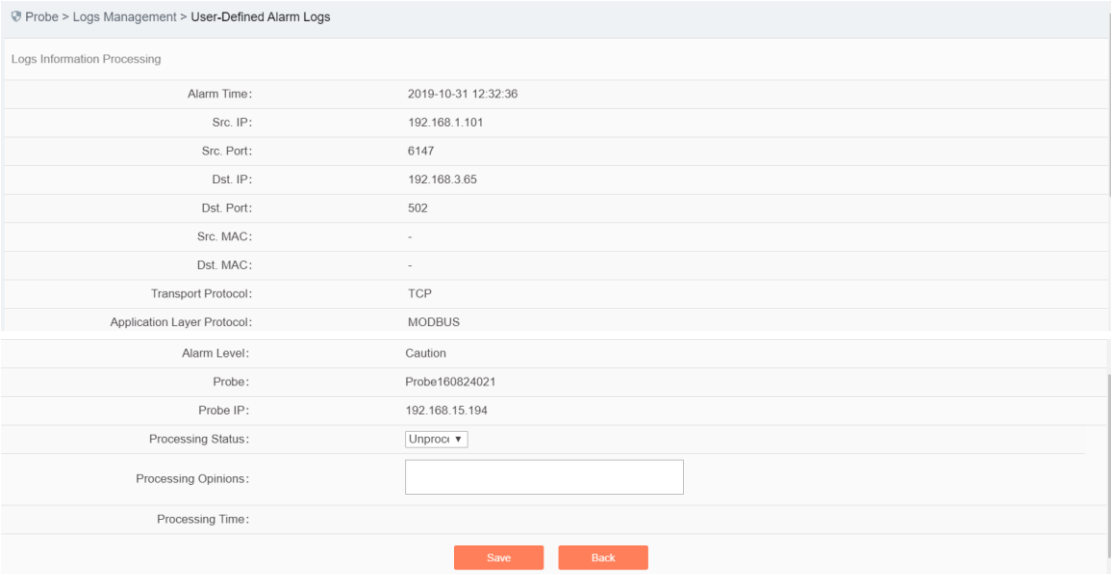


Fig.5 -123 User-defined Alarm Processing Page

5.5.6.2.1. Close the log.

Click the drop-down box of processing status, select "Close", fill in the relevant opinions in the processing opinions field and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the list of [User-defined Alarm Logs] page by default.

Or do not select "Close" but fill in the processing opinions instead.

5.5.6.2.2. Export a message.

When checking to save the user-defined alarms of alarm messages in the intelligent monitoring terminal configuration, the user-defined alarm message generated by such an intelligent monitoring terminal can be downloaded. Click <Export a Message> to automatically save the message to the computer executing the operation.

5.5.6.3. Retrieve a log.

In the [User-defined Alarm] list page, retrieve an alarm according to the conditions. (As shown in Fig.5-124):

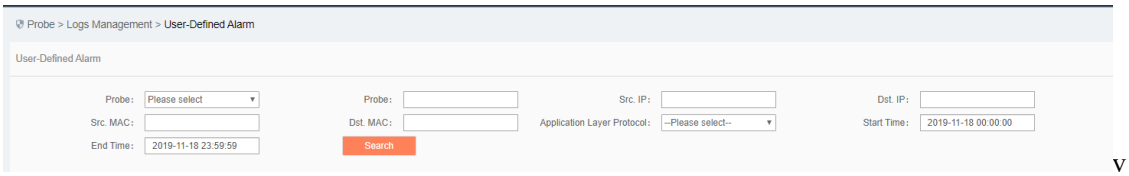


Fig.5 -124 Retrieving a User-defined Alarm.

5.5.7. Industrial Protocol Audit Log

All industrial protocols flowing through the intelligent monitoring terminal will generate an industrial protocol audit log.

5.5.7.1. Log list

Click [Log Management/Industrial Protocol Audit Logs] in the left navigation bar (as shown in Fig.5-125), enter the [Industrial Protocol Audit Logs] list page (as shown in Fig.5-126):

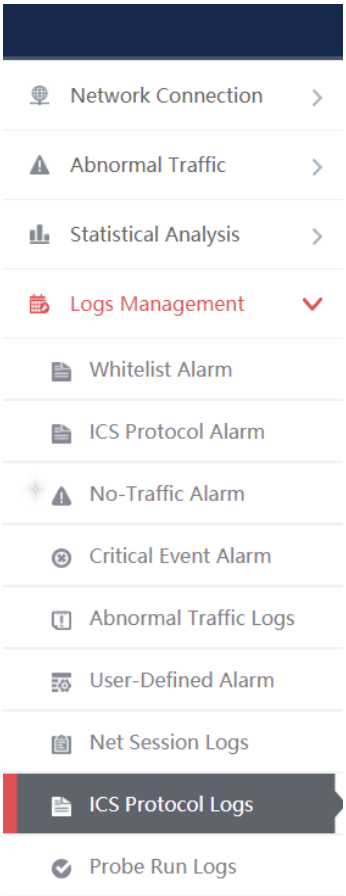


Fig.5 -125 Industrial Protocol Audit Log Menu

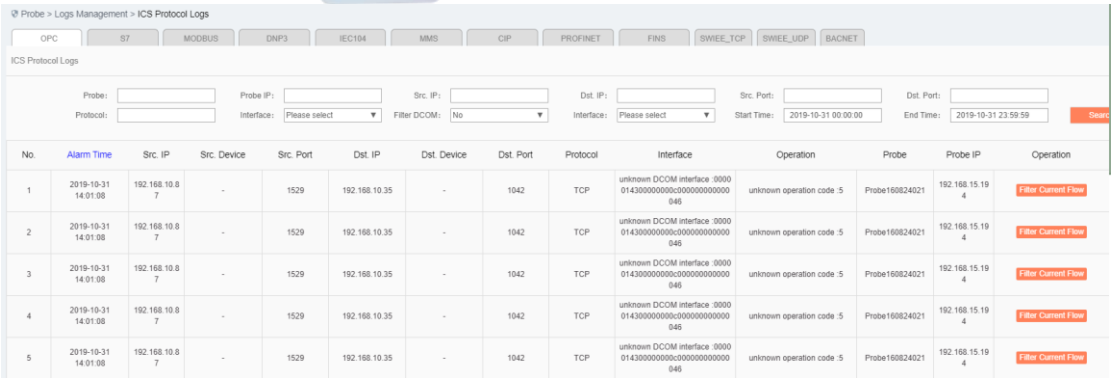


Fig.5 -126 Industrial Protocol Audit Log List Page

The industrial protocol audit logs can be divided into OPC, Modbus, S7, DNP3 and IEC104 protocols. OPC will be taken as an example here, with other two protocols similar. View all the log information on OPC industrial protocol audit logs, with the meaning given below:

Tab.61 Instruction to Industrial Protocol Audit Log Display

Column Names	**Instructions**	
Alarm Time	The time to generate a log	
Src. IP	The IP address initiating a data request, in dotted decimal format	
Src. port	The port initiating a data request	
Src. device	The system automatically generates a source device name according to the source IP, supporting custom source device name	
Dst. IP	The destination IP requesting data, in dotted decimal format	
Dst. Device	The system automatically generates a destination device name according to destination IP, supporting custom destination device name	
Dst. port	The port used by the requested destination machine	
Protocol	The protocol type of transport layer used by the message	
Interface	The operation interface used by OPC	
Operation	The operation method used by OPC	
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember	
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format	
Operation	Filter Current Flow	Filter the logs, only display all logs on flows to which the logs belong to
	Export Logs	Export a log to the local computer

5.5.7.2. Retrieve a log.

In the [Industrial Protocol Audit Logs] list page, retrieve a log according to the conditions. (As shown in Fig.5-127):

Fig.5 -127 Retrieving an Industrial Protocol Audit Log

5.5.8. Network Session Audit Log

All traffic flowing through the intelligent monitoring terminal will generate a network session audit log.

5.5.8.1. Log list

Click [Log management/Network Session Audit Logs] in the left navigation bar (as shown in Fig.5-128), enter the [Network Session Audit Logs] list page (as shown in Fig.5-129):

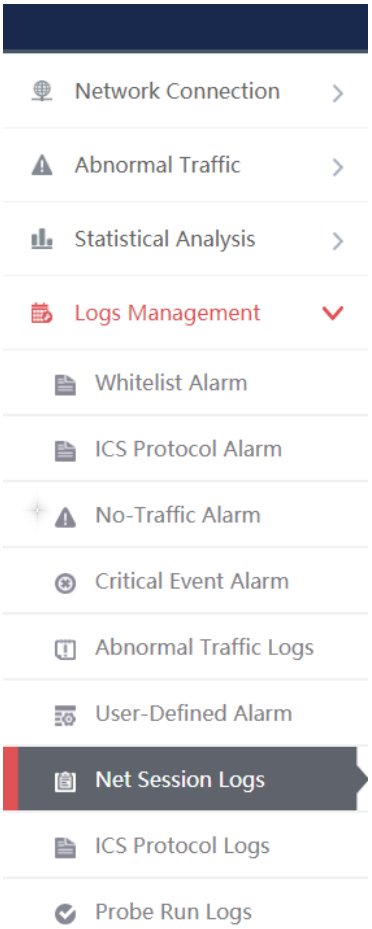


Fig.5 -128 Network Session Audit Log Menu

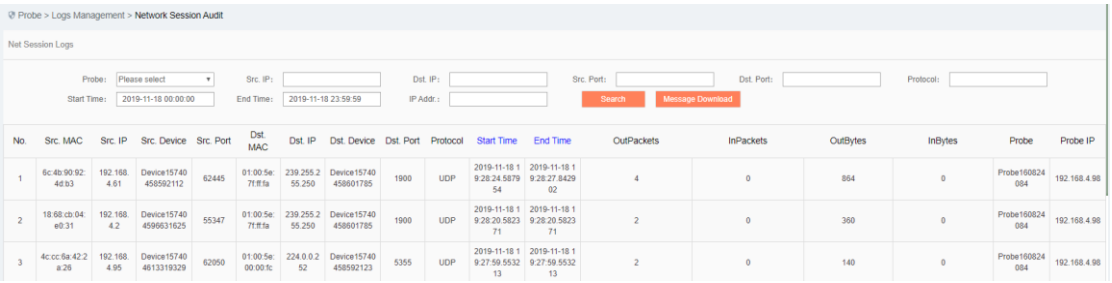


Fig.5 -129 Network Session Audit Log List Page

View all the log information on network session audit logs, with the meaning given below:

Tab.62 Instruction to Industrial Protocol Audit Log Display

Column Names	**Instructions**
Src. MAC	The MAC address initiating a data request, taking ":" as the delimiter
Src. IP	The IP address initiating a data request, in dotted decimal format
Src. Device	The system automatically generates a source device name according to the source IP, supporting custom source device name
Src. Port	The port initiating a data request
Dst. MAC	The destination MAC address requesting data, taking ":" as the delimiter
Dst. IP	The destination IP requesting data, in dotted decimal format
Dst. Device	The system automatically generates a destination device name according to destination IP, supporting custom destination device name
Dst. Port	The port used by the requested destination machine
Protocol	The protocol type of transport layer used by the message
Start Time	The time starting to generate a network session
End Time	The time ending a network session
OutPackets	Number of messages transmitted from the client to the server
InPackets	Number of messages transmitted from the server to the client
OutBytes	Number of bytes transmitted from the client to the server
InBytes	Number of bytes transmitted from the server to the client
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format

Operation	Export Logs	Export a log to the local computer

5.5.8.2. Retrieve a log.

In the [Network Session Audit Logs] list page, retrieve a log according to the conditions. (As shown in Fig.5-130):

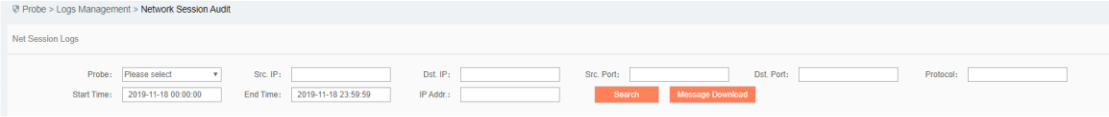


Fig.5 -130 Retrieving a Network Session Audit Log

5.5.8.3. Original message download

In the [Network Session Audit Logs] list page, download messages that are retained at the intelligent terminal and flow through it. (As shown in Fig.5-131):

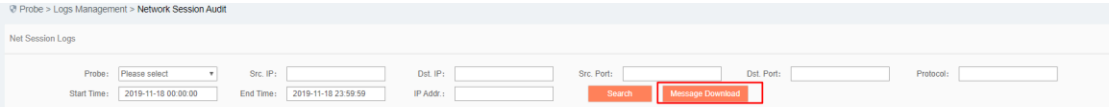


Fig.5 -131 Original Message Download Button

Click <Message Download> and enter the message download page, as shown in Fig.5-132. Click <Download> to download the corresponding message to the local computer.

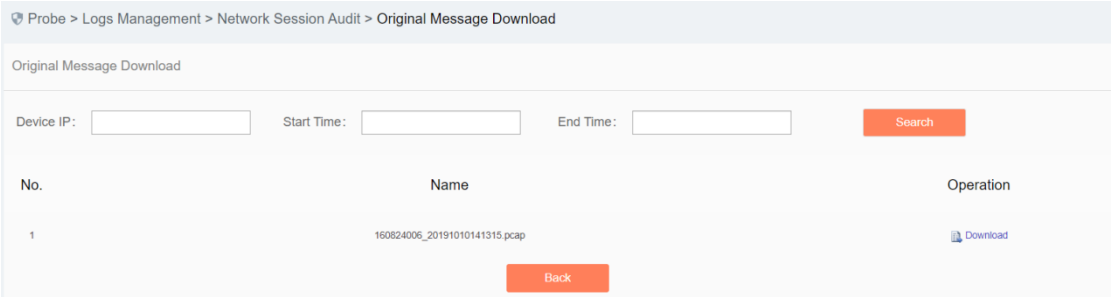


Fig.5 -132 Original Message Download Page

5.5.9. Intelligent Monitoring Terminal Run Log

The intelligent monitoring terminal run log is a log recording the running status of the intelligent monitoring terminal.

5.5.9.1. Log list

Click [Log Management/Intelligent Monitoring Terminal Run Logs] in the left navigation bar (as shown in Fig.5-133), enter the [Intelligent Monitoring Terminal Run Logs] list page (as shown in Fig.5-134):

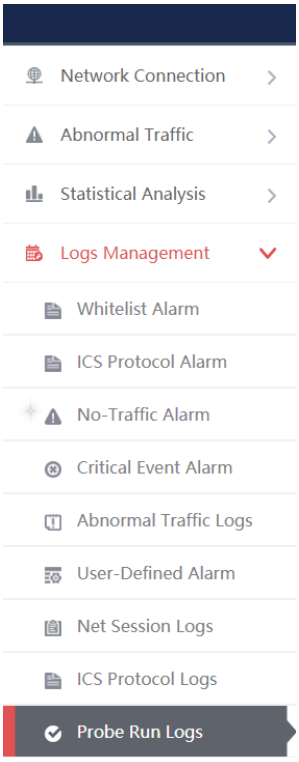


Fig.5 -133 Intelligent Monitoring Terminal Run Log Menu

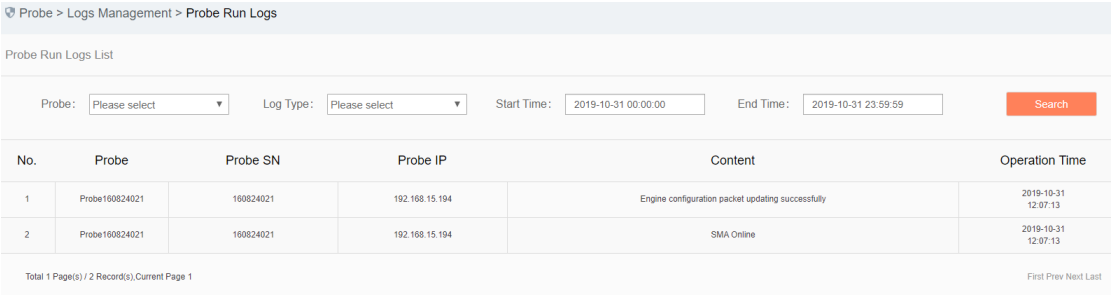


Fig.5 -134 Intelligent Monitoring Terminal Run Log List Page

View the information on all intelligent monitoring terminal run logs, with the meanings given below:

Tab.63 Instruction to Intelligent Monitoring Terminal Run Log Display

Column Names	**Instructions**
Probe	An intelligent monitoring terminal name that is generated by the system or named by users, which is easy to remember
Probe SN	The intelligent monitoring terminal ID generated by the system
Probe IP	The IP address assigned by the intelligent monitoring terminal, in dotted decimal format
Content	Detailed descriptive information on logs
Operation time	Log generation time

5.5.9.2. Retrieve a log.

In the [Intelligent Monitoring Terminal Run Logs] list page, retrieve a log according to the conditions. (As shown in Fig.5-135):

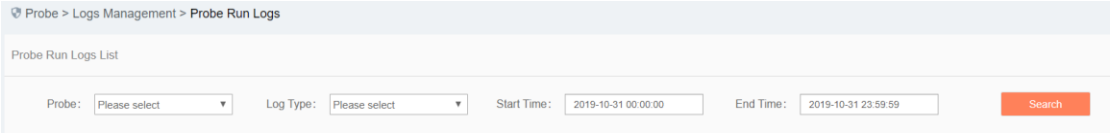


Fig.5-135 Retrieving an Intelligent Monitoring Terminal Run Log

5.5.10. Abnormal Traffic Log

An abnormal traffic log will be generated whenever abnormal traffic occurs.

5.5.10.1. Log list

Click [Log Management/Abnormal Traffic Logs] (as shown in Fig.5-136) to open the abnormal traffic log page. (As shown in Fig.5-137):

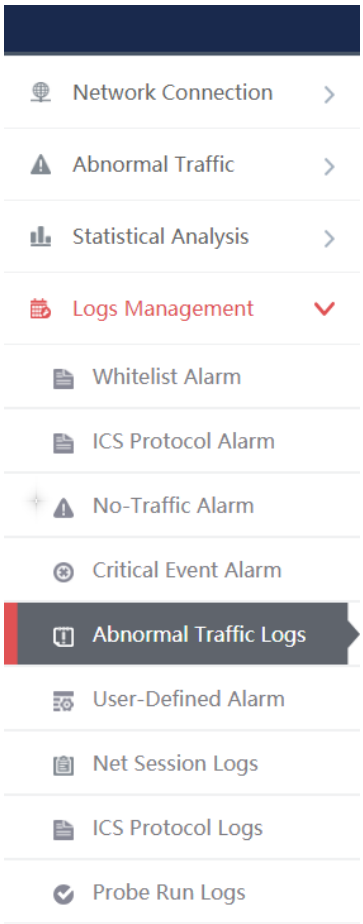


Fig.5 -136 Abnormal Traffic Log Menu

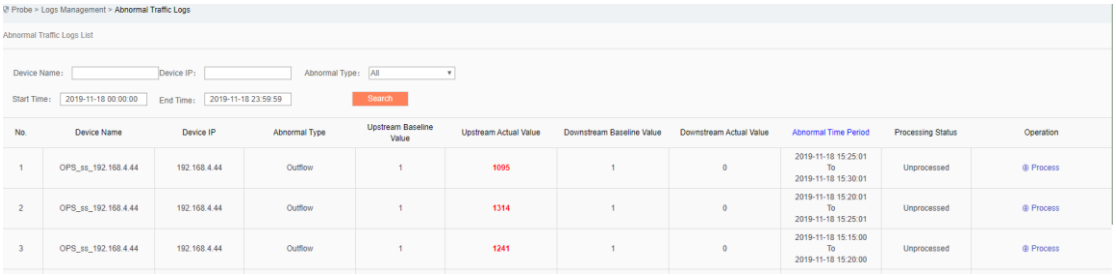


Fig.5 -137 Abnormal Traffic Log Page

View all the log information on abnormal traffic alarms here, with the meaning given below:

Tab.64 Instruction to Whitelist Alarm Log Display

Column Names	**Instructions**	
Device Name	The name of devices abnormal in traffic	
Device IP	The IP of devices abnormal in traffic	
Abnormal Type	The outflow or inflow traffic	
Upstream Baseline Value	The amount of upstream traffic in the abnormal traffic baseline configuration	
Upstream Actual Value	The amount of upstream traffic actually occurred to the device	
Downstream Baseline Value	The amount of downstream traffic in the abnormal traffic baseline configuration	
Downstream Actual Value	The amount of downstream traffic actually occurred to the device	
Abnormal Time Period	The time of generating abnormal traffic	
Confirmed	Confirm whether abnormal traffic has been processed	
Operation	Process	Further process abnormal traffic

5.5.10.2. **Process a log.**

Click <Process> under the operation column in the [Abnormal Traffic] display list, display the [Abnormal Traffic] processing page (as shown in Fig.5-138):

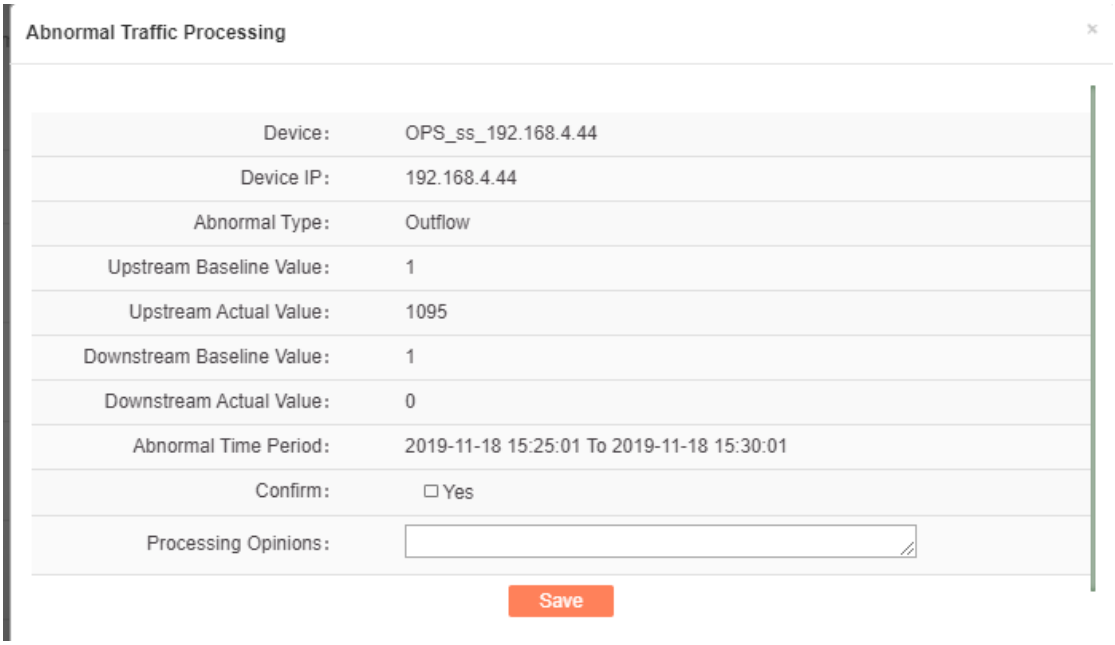


Fig.5 -138 Processing Abnormal Traffic

Check to confirm the check box on the right, confirm the log operation. (As shown in Fig.5-139):

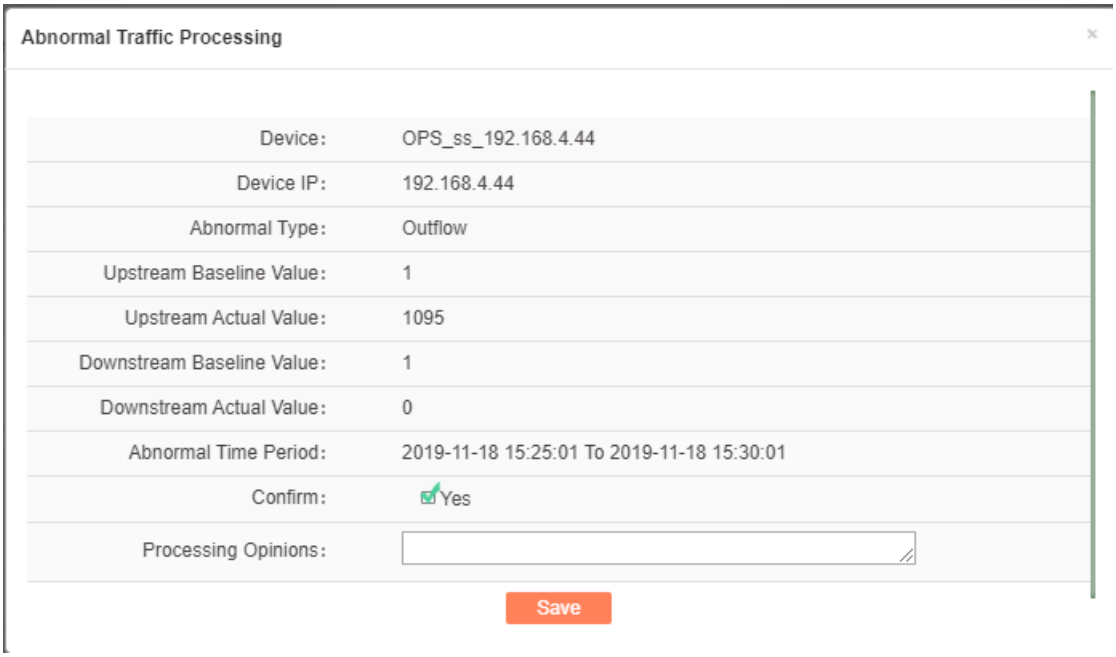


Fig.5 -139 Confirming Abnormal Traffic

5.6. System Configuration

5.6.1.Alarm Level Settings

Log in the management platform, click [System Settings/Alarm Level Settings] (as shown in Fig.5-140) to open the alarm level settings page. (As shown in Fig.5-141):

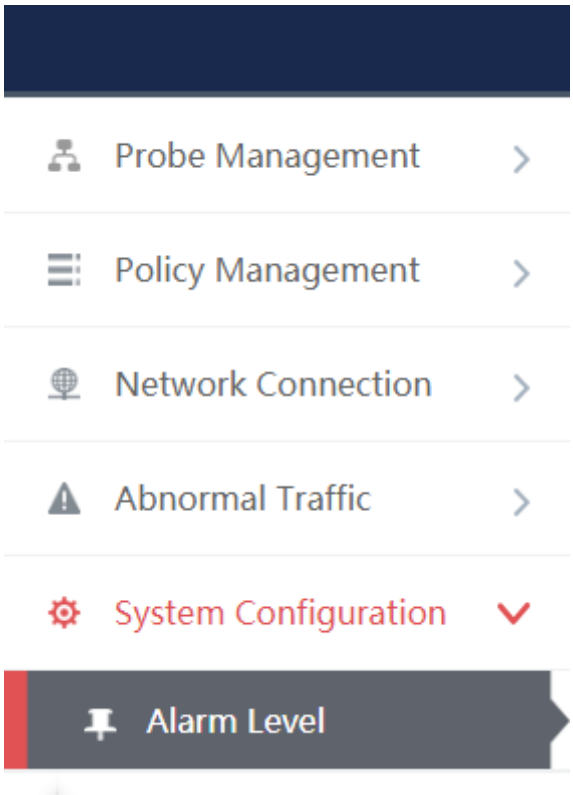


Fig.5-140 Selecting Alarm Level Settings

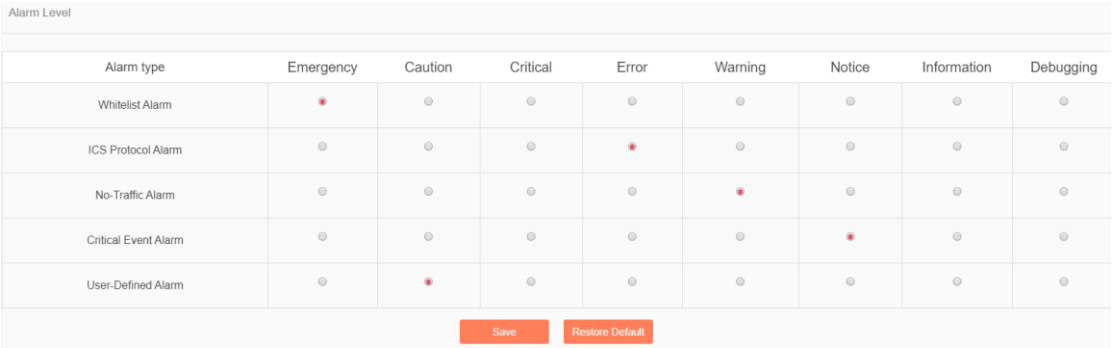


Fig.5-141 Selecting Alarm Level to be Set

5.6.2.Instruction to Alarm Levels

Tab.65 Alarm Level List

Sequence number	Levels	Instruction to Levels
1	Emergency	Having made the system inoperable
2	Warning	Messages to which the administrator shall pay immediate attention
3	Critical	Messages that may have affected the use of device functions

4	Error	Messages that may have caused the device functions unavailable, such as failed illegal operation
5	Warning	Messages that may affect the normal use of device functions normal
6	Notice	Event messages normally generated by the device, including messages such as configuration change as triggered by the administrator
7	Information	Common messages about system operations
8	Debugging	Detailed information used for system debugging

5.7. Network Connection

5.7.1. Introduction to Functions

Real-time and historical display of network traffic through the terminal device.

5.7.2. Network Connection Baseline Configuration

5.7.2.1. Introduction to functions

Network connection through the terminal device conform to the network connections baseline configuration rules. The network connection diagram shall be drafted with green lines, otherwise with red lines if incompatible.

5.7.2.2. Rule configuration

Click [Network Connection/Network Connection Baseline Configuration] (as shown in Fig.5-142), open the network connection baseline configuration page. (As shown in Fig.5-143):

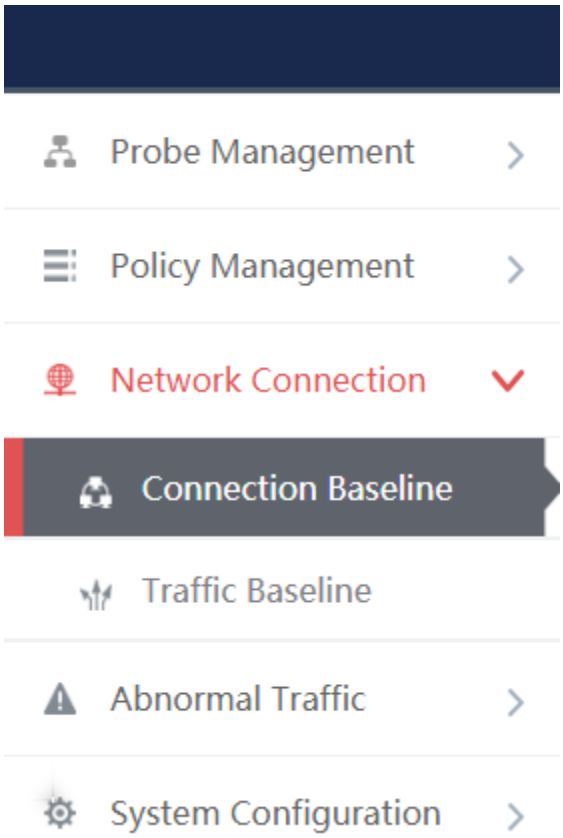


Fig.5-142 Network Connection Baseline Configuration Menu

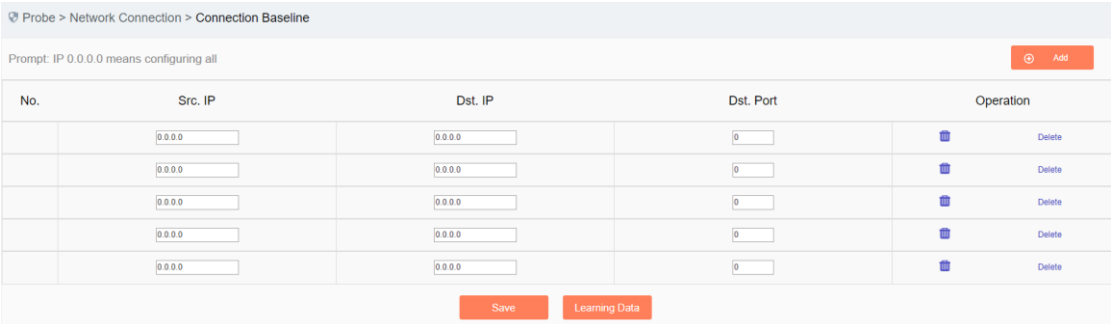


Fig.5-143 Network Connection Baseline Configuration Page

Enter the [Network Connection Baseline Configuration] page, click <Add> on the right (as shown in Fig.5-144) to add a new line of rules automatically at the bottom of the list (as shown in Fig.5-145):

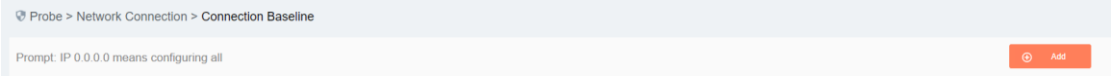


Fig.5-144 Rule Add Button

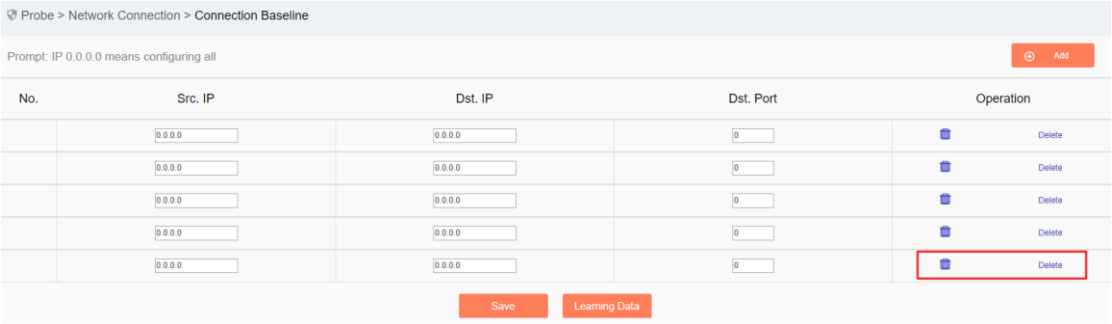


Fig.5-145 Rule Add Page

Tab.66 Instruction to Rule Fields

Column Names	Instructions
Src. IP	The IP address initiating a data request, in dotted decimal format
Dst. IP	The destination IP requesting data, in dotted decimal format
Dst. Port	Destination port, ranging from 0 to 65535
Delete	Delete the selected rule
Save	Save all modification information to the database and make it come into effect

5.7.2.3. Learning Data

Enter the [Network Connection Baseline Configuration] page (as shown in Fig.5-146), click <Learning Data> to skip to the learning data page. (As shown in Fig.5-147):

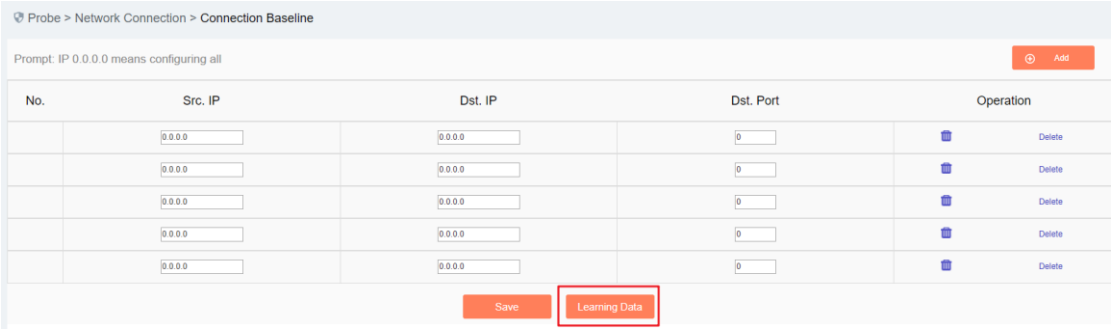


Fig.5-146 Learning Data Button

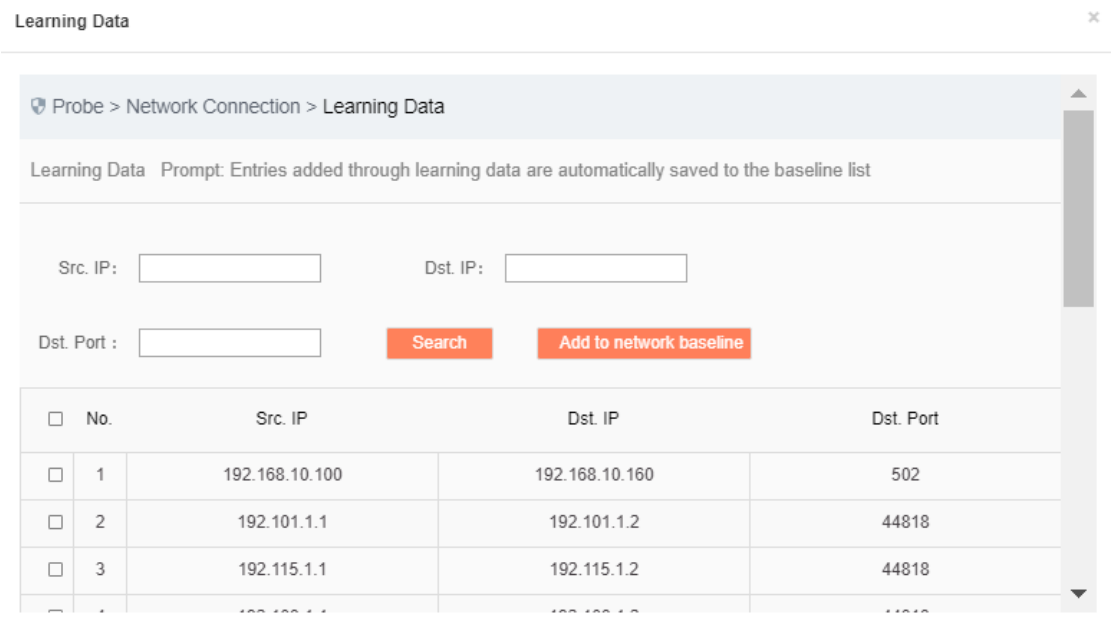


Fig.5-147 Learning Data Page

Filter learning data by query criteria. (As shown in Fig.5-148):

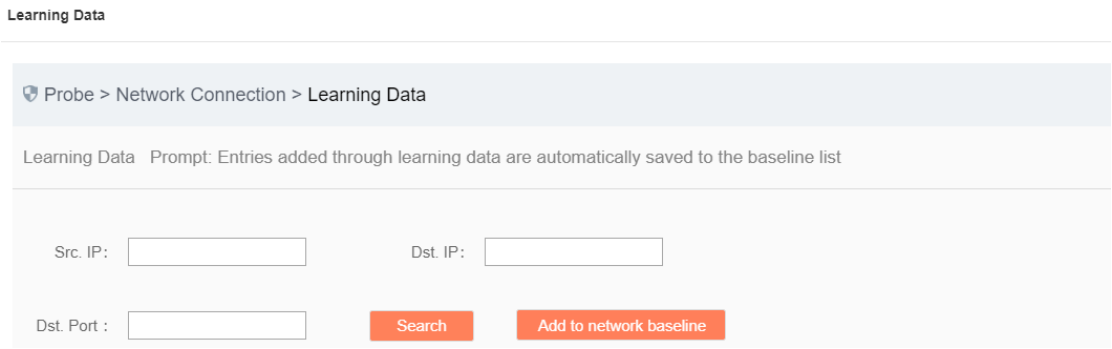


Fig.5-148 Learning Data Search

After selecting the data, click <Add to Network Baseline> to add the learning data to the rule configuration page. (As shown in Fig.5-149):

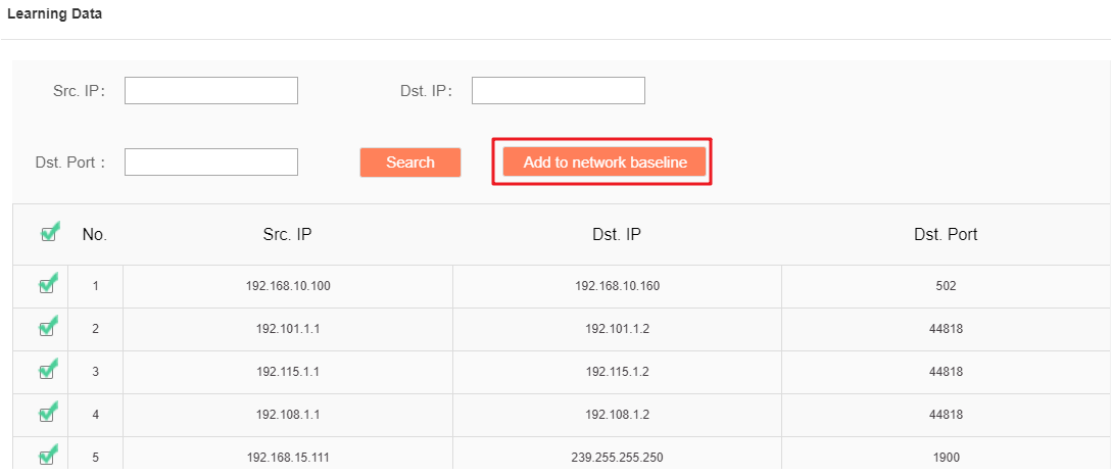


Fig.5-149 Adding the Learning Data

After selecting the data, click <Delete> to delete the learning data. (As shown in Fig.5-150):

	No.	Src. IP	Dst. IP	Dst. Port
	1	192.168.10.100	192.168.10.160	502
	2	192.101.1.1	192.101.1.2	44818
	3	192.115.1.1	192.115.1.2	44818
	4	192.108.1.1	192.108.1.2	44818
	5	192.168.15.111	239.255.255.250	1900

Fig.5-150 Deleting the Learning Data

5.7.3.Network Traffic Baseline Configuration

5.7.3.1.Introduction to functions

Network connection through the terminal device conform to the network connections baseline configuration rules. The networking diagram shall be drafted with green lines, otherwise with red lines if incompatible.

5.7.3.2.Rule configuration

Click [Network Connection/Network Traffic Baseline Configuration] (as shown in Fig.5-151), open the network traffic baseline configuration page. (As shown in Fig.5-152):

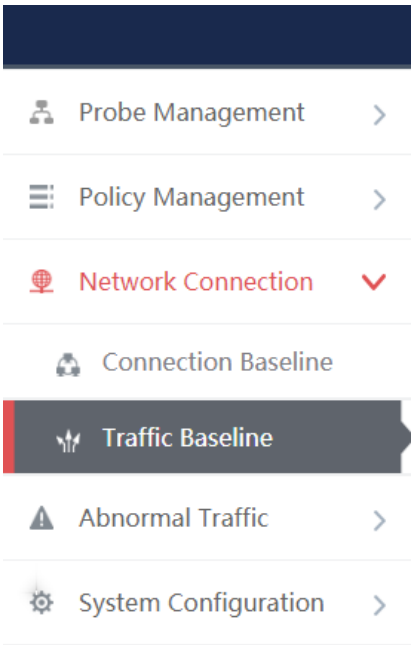


Fig.5-151 Network Traffic Baseline Configuration Menu

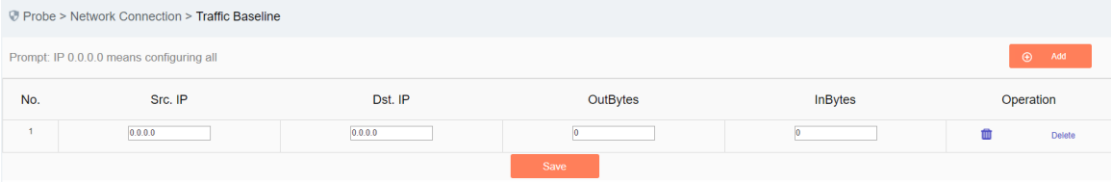


Fig.5-152 Network Traffic Baseline Configuration Page

Enter the [Network Traffic Baseline Configuration] page, click <Add> on the right (as shown in Fig.5-153) to add a new line of rules automatically at the bottom of the list (as shown in Fig.5-154):

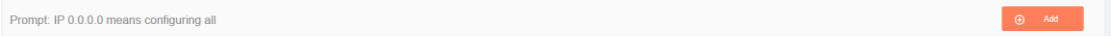


Fig.5-153 Rule Add Button

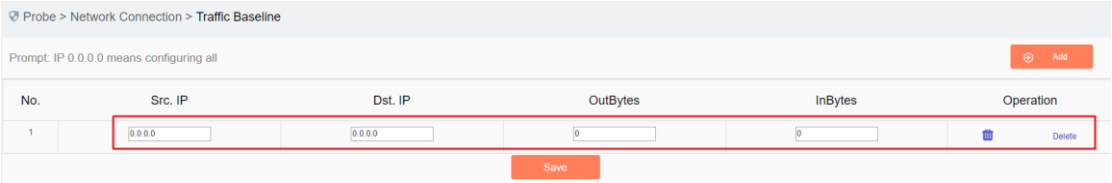


Fig.5-154 Rule Add Page

Table 67 Instruction to Rule Fields

Column Names	Instructions
Src. IP	The IP address initiating a data request, in dotted decimal format
Dst. IP	The destination IP requesting data, in dotted decimal format
OutBytes	The amount of upstream traffic through the terminal device.
InBytes	The amount of downstream traffic through the terminal device.
Delete	Delete the selected rule
Save	Save all modification information to the database and make it come into effect

5.7.4.Network Connection Diagram

5.7.4.1.Introduction to functions

Draft all network connections through the terminal device in real time, with the data conforming to rule configuration drafted with a green line, otherwise with a red line. Query the historical network connections, Based on rules same to those for real time.

5.7.4.2.Real-Time network connection diagram

Click [Network Connection/Network Connection Diagram] (as shown in Fig.5-155), open the network connection diagram page. (As shown in Fig.5-156):

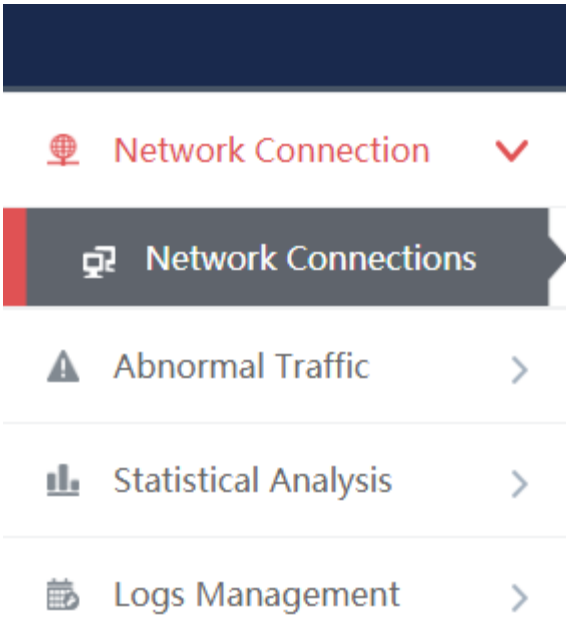


Fig.5-155 Network Connection Diagram Menu

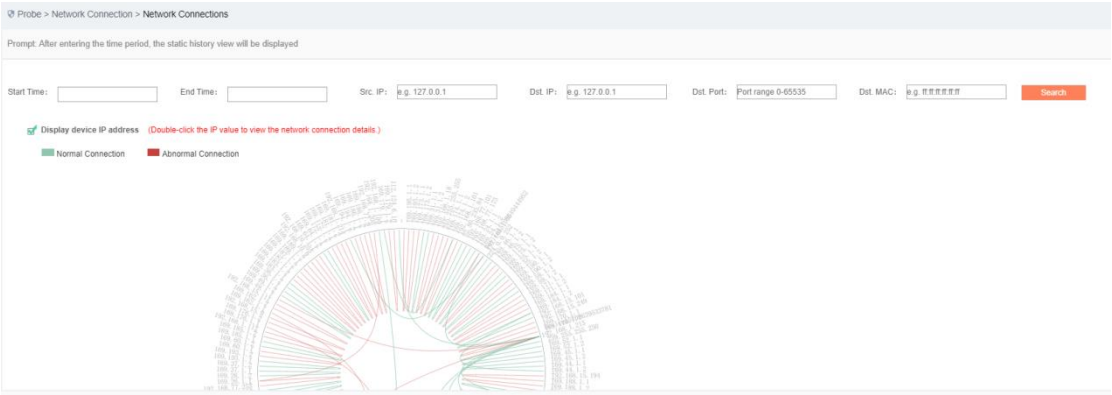


Fig.5-156 Network Connection Diagram Page

When the start time and end time are blank, the network connection diagram drafted in this case is a real-time one, which can be filtered and searched by other conditions. (As shown in Fig.5-157):

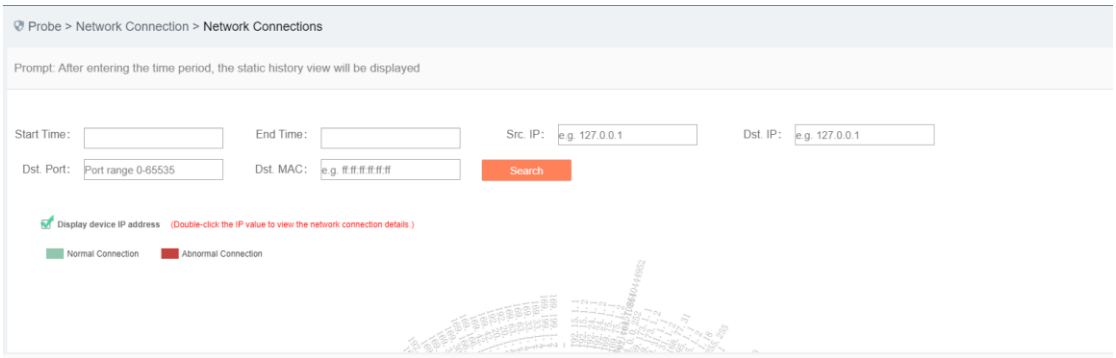


Fig.5-157 Real Time Network Connection Diagram

5.7.4.3. Historical network connection diagram

When the start and end time are not blank, the network connection diagram displayed is a historical one, which can be filtered by other conditions. (As shown in Fig.5-158):

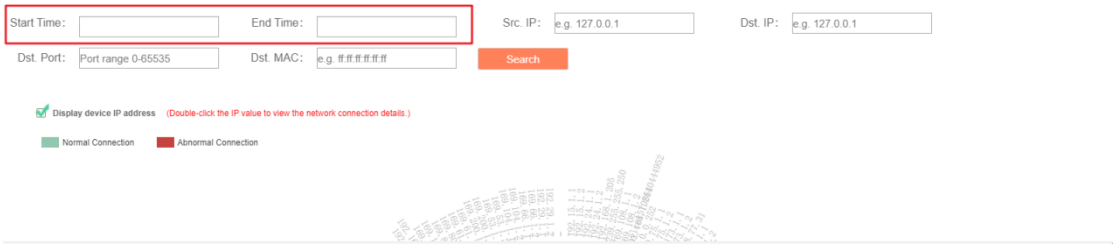


Fig.5-158 Historical Network Connection Diagram

5.8. Abnormal Traffic

5.8.1. Introduction to Functions

Graphically display whether the network traffic of all devices is normal, with three states in total: (as shown in Fig.5-159)

1.Normal status: the traffic during the current inspection cycle is normal, with all abnormal traffic alarms confirmed.

2.Flashing in red: the traffic during the current inspection cycle is abnormal, whether the abnormal traffic alarm is confirmed or not.

3.Red box: the traffic during the current inspection cycle is normal, not with all abnormal traffic alarms confirmed.

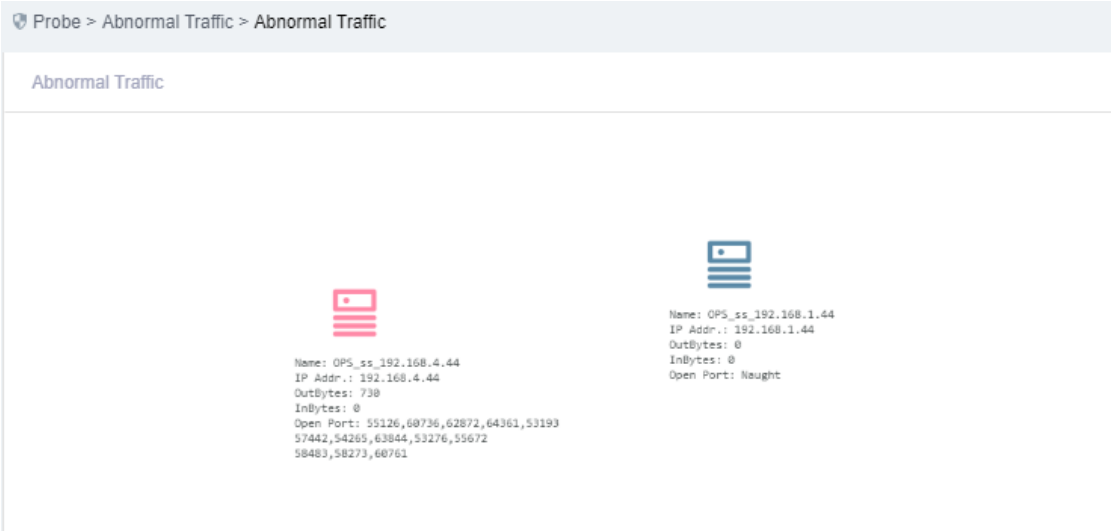


Fig.5-159 Three Graphical Displays

5.8.2. Baseline Configuration

5.8.2.1. Introduction to functions

Configure the extent to which the traffic through the device goes beyond in 5 minutes as abnormal traffic.

5.8.2.2. Rule configuration

Click [Abnormal Traffic/Baseline Configuration] (as shown in Fig.5-160), open the baseline configuration page. (As shown in Fig.5-161):

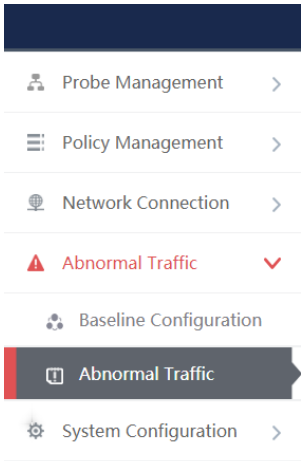


Fig.5-160 Baseline Configuration Menu

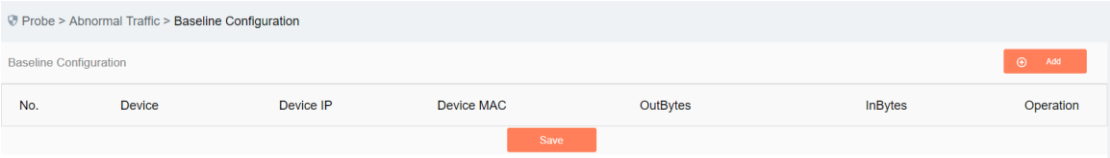


Fig.5-161 Baseline Configuration Page

Enter the [Baseline Configuration] page, click < Add> on the right (as shown in Fig.5-162) to add a new line of rules automatically at the bottom of the list (as shown in Fig.5-163):

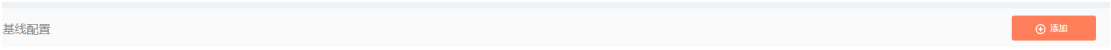


Fig.5-162 Rule Add Button

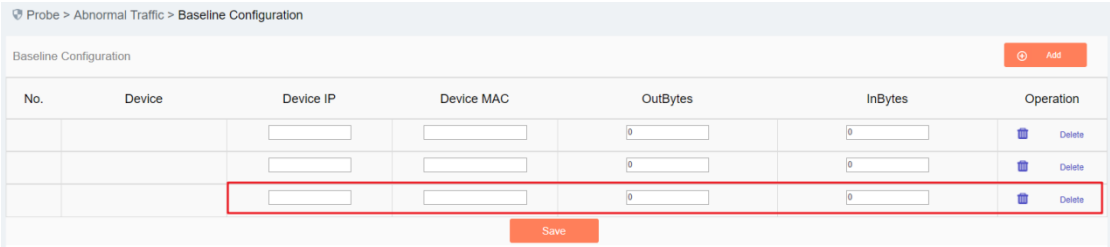


Fig.5-163 Rule Add Page

Tab.68 Instruction to Rule Fields

Column Names	Instructions
Device	Automatically display the corresponding device name through the input device IP
Device IP	Device IP address
OutBytes	The amount of upstream traffic through the terminal device
InBytes	The amount of downstream traffic through the terminal device
Delete	Delete the selected rule
Save	Save all modification information to the database and make it come into effect

5.8.3. Abnormal Traffic Monitoring

5.8.3.1. Introduction to functions

The user can select the device to be displayed. The device dragged to the main interface displays the status information. For devices not included in the main interface, traffic anomaly is not checked.

5.8.3.2. Traffic monitoring

Click [Abnormal Traffic/Abnormal Traffic Monitoring], as shown in Fig.5-164, open the abnormal traffic monitoring page. (As shown in Fig.5-165):

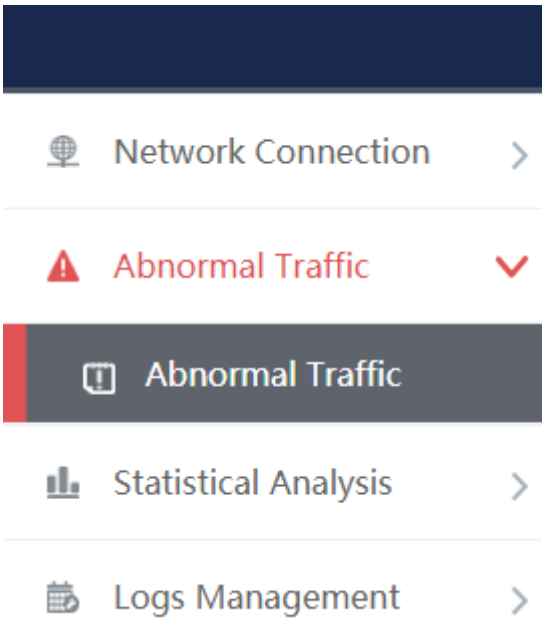


Fig.5-164 Abnormal Traffic Monitoring Menu

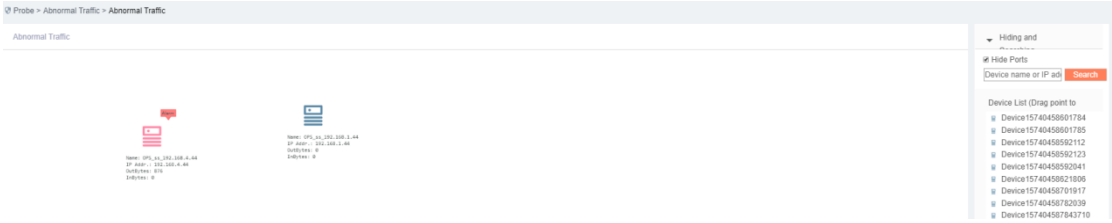


Fig.5-165 Abnormal Traffic Monitoring Page

Filter device lists by device name or IP address. (As shown in Fig.5-166):

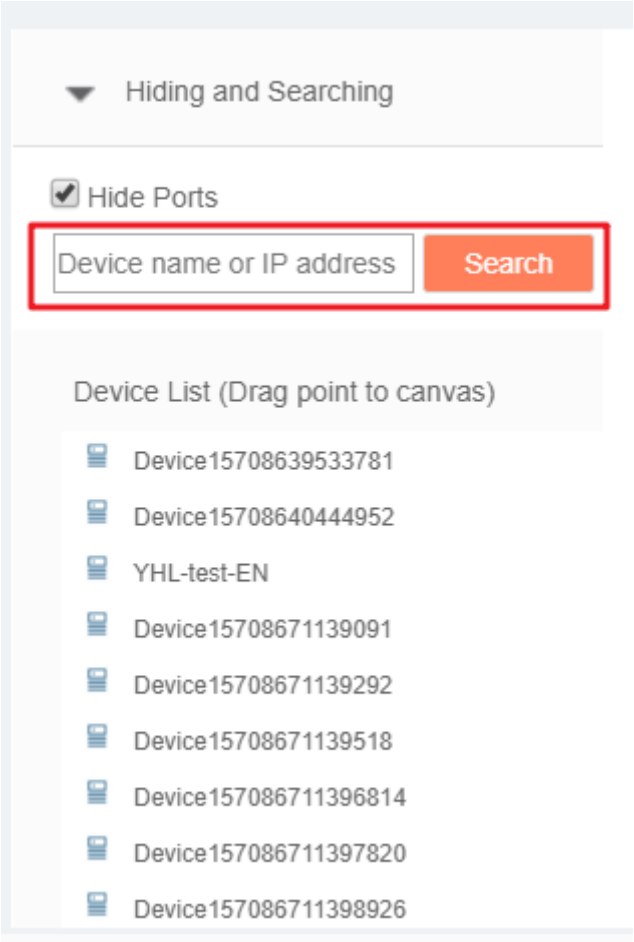


Fig.5-166 Filtering Function

Drag the device onto the canvas, start to monitor the device traffic. (As shown in Fig.5-167):

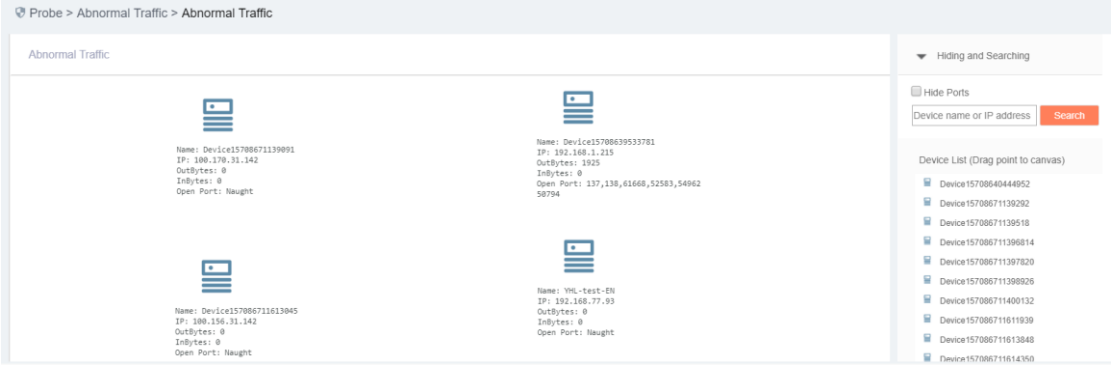


Fig.5-167 Monitoring Page

5.9. Statistical Analysis

5.9.1. Historical Statistics of Network Traffic Messages

5.9.1.1. Introduction to functions

Compare the network traffic and number of messages of the two devices by hour and day respectively.

5.9.1.2. Statistical query

Click [Statistical Analysis/Historical Statistics of Network Traffic Messages] (as shown in Fig.5-168), open the historical statistics of network traffic messages page. (As shown in Fig.5-169):

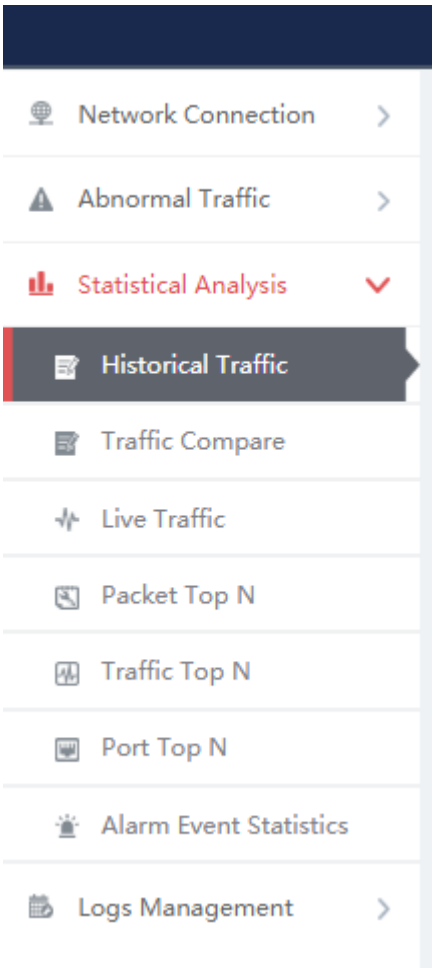


Fig.5-168 Menu of Historical Statistics of Network Traffic Messages

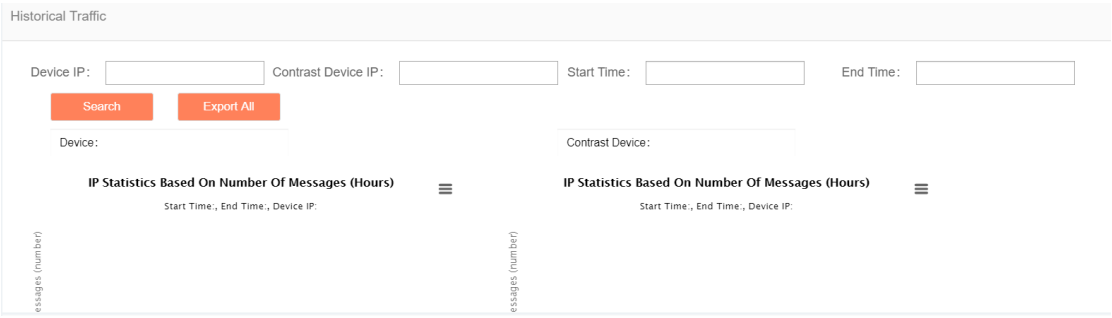


Fig.5-169 Page of Historical Statistics of Network Traffic Messages

Input the IP of the device and the compared device, click Search the Query Results, which refer to the statistical data of that day based on hours (as shown in Fig.5-170), input the start time and the end time to make statistics of the data during the selected time period by day. (As shown in Fig.5-171):

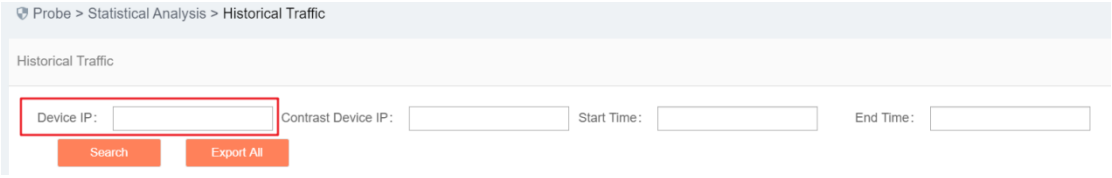


Fig.5-170 Data Statistics of that Day

Fig.5-171 Data Statistics Based on days.

5.9.1.3. Export a statistical graph.

Click the Export icon, export the current statistical graph (as shown in Fig. 5-172), click <Export All> to export all statistical graphs in the page. (As shown in Fig.5-173):

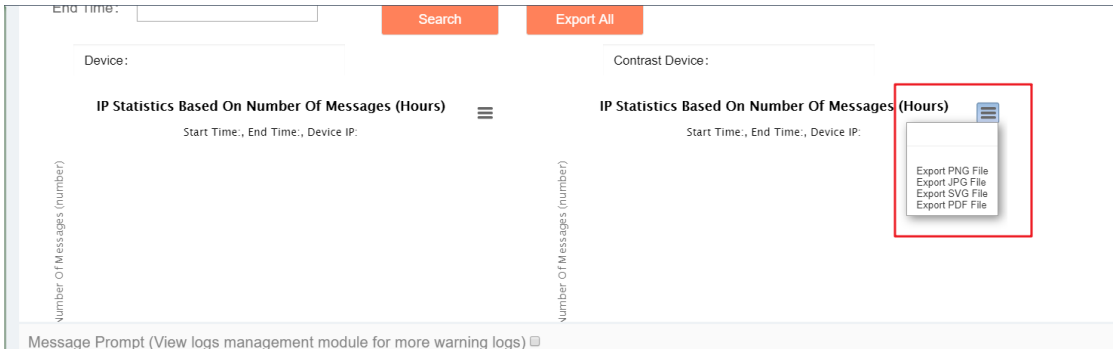


Fig.5-172 Export to a Single Statistical Graph

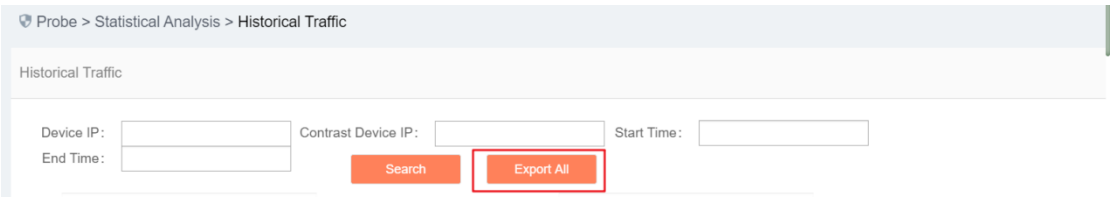


Fig.5-173 Export All Statistical Graphs

5.9.2.Network Real-Time Traffic

5.9.2.1.Introduction to functions

Press 5 minutes, 2 hours, display the real-time traffic currently flowing through the system for a node every day.

5.9.2.2.Real-time traffic

Click [Statistical Analysis/Network Real-time Traffic] (as shown in Fig.5-174), open the network real-time traffic page. (As shown in Fig.5-175):

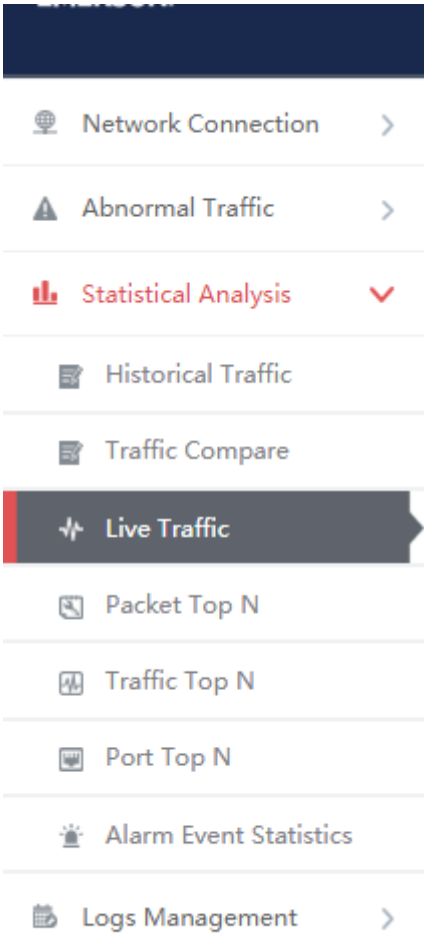


Fig.5-174 Network Real-time Traffic Menu

Fig.5-175 Network Real-time Traffic Page

Enter the page, refresh the minute-based diagram every 5 minutes, the hour-based diagram every 2 hours and the day-based diagram every 24 hours.

5.9.3.Statistics of Number of Messages

5.9.3.1.Introduction to functions

IP statistics corresponding to the number of messages passing through.

5.9.3.2.Query the number of messages.

Click [Statistical Analysis/Statistics of Number of Messages] (as shown in Fig.5-176), open the statistics of number of messages page. (As shown in Fig.5-177):

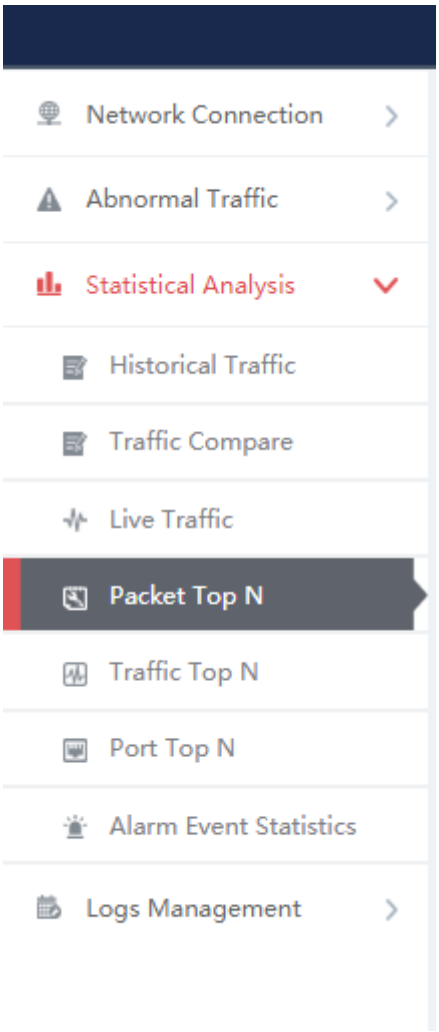


Fig.5-176 Menu of Statistics of Number of Messages

Fig.5-177 Page of Statistics of Number of Messages

Query the number of messages in a specified time by query conditions, which can be filtered by receiving and sending. (As shown in Fig.5-178):

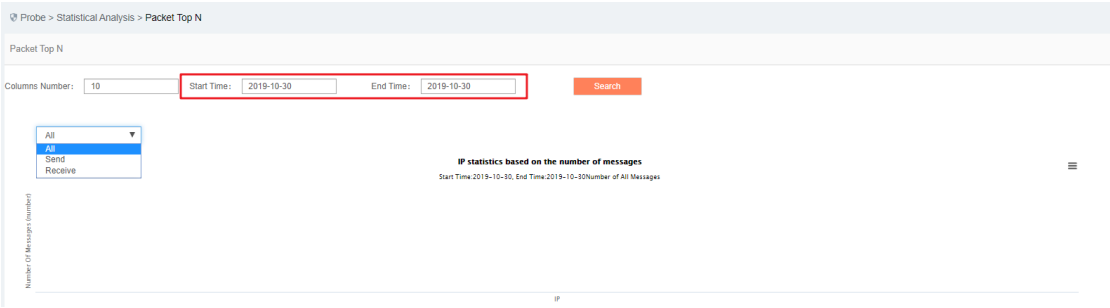


Fig.5-178 Query the Number of Messages

5.9.3.3. Export a statistical graph.

Click the Export icon, export the current statistical graph. (As shown in Fig.5-179):

Fig.5-179 Export a Statistical Graph

5.9.4. Traffic Statistics

5.9.4.1. Introduction to functions

The corresponding traffic based on IP statistics.

5.9.4.2. Query traffic

Click [Statistical Analysis/Traffic Statistics] (as shown in Fig.5-180), open the traffic statistics page. (As shown in Fig.5-181):

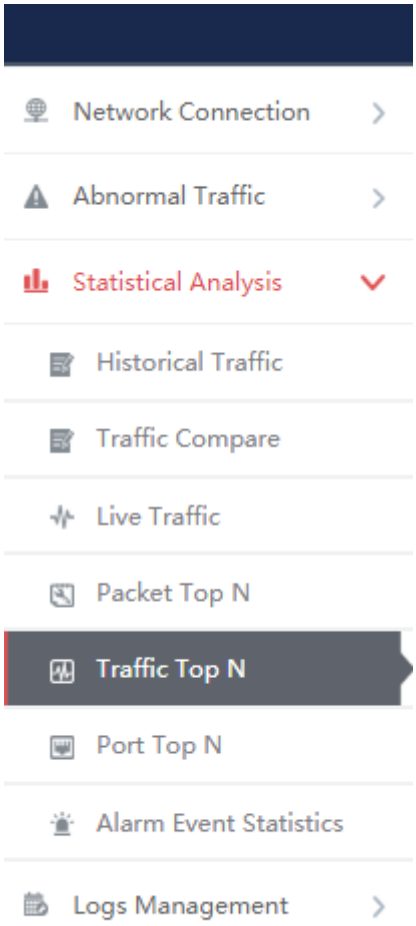


Fig.5-180 Traffic Statistics Menu

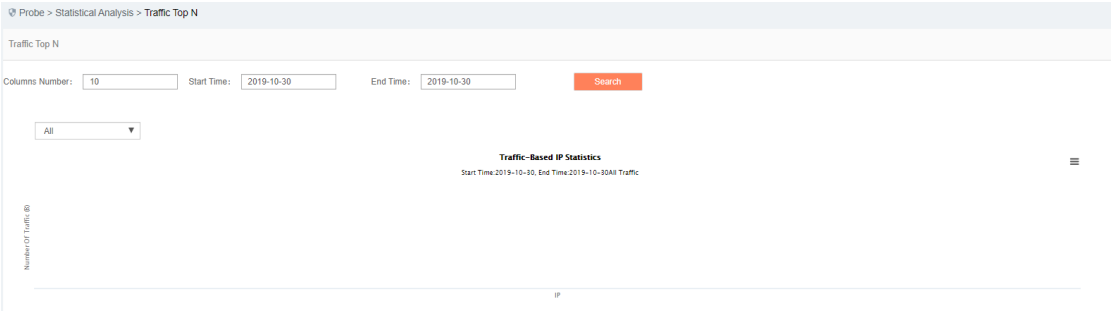


Fig.5-181 Traffic Statistics Page

Query the traffic in a specified time by query conditions, which can be filtered by receiving and sending. (As shown in Fig.5-182):

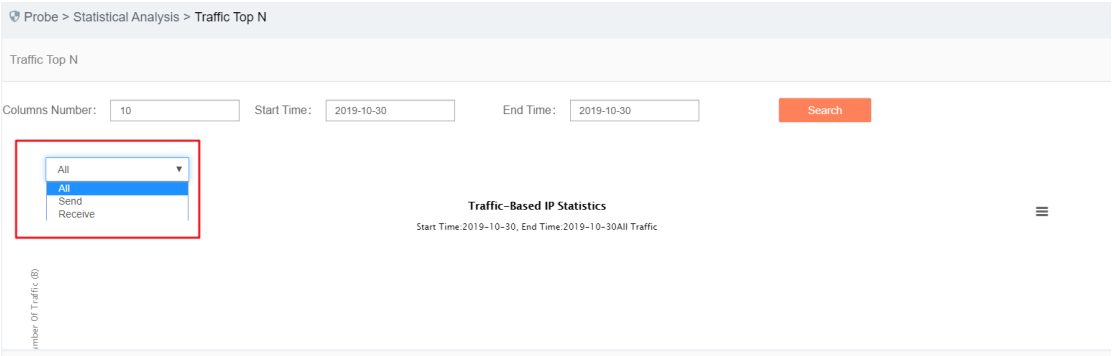


Fig.5-182 Query Traffic

5.9.4.3. Export a statistical graph.

Click the Export icon, export the current statistical graph. (As shown in Fig.5-183):

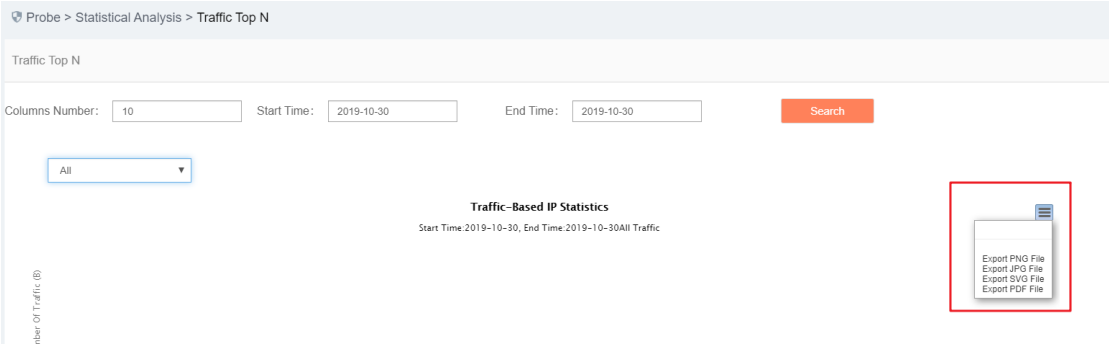


Fig.5-183 Exporting the Current Statistical Graph

5.9.5. Port Statistics

5.9.5.1. Introduction to functions

The corresponding traffic based on IP statistics; the corresponding traffic based on port statistics.

5.9.5.2. Query port

Click [Statistical Analysis/Port Statistics] (as shown in Fig.5-184), open the port statistics page, as shown in the figure below: (as shown in Fig.5-185):

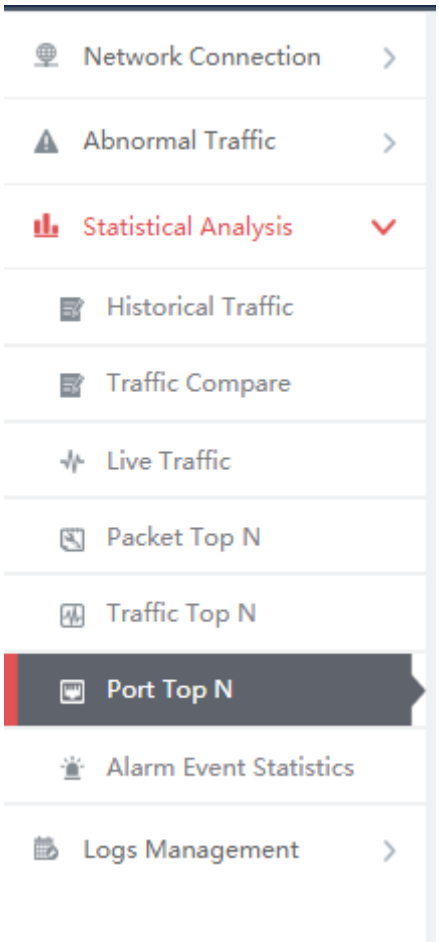


Fig.5-184 Port Statistics Menu

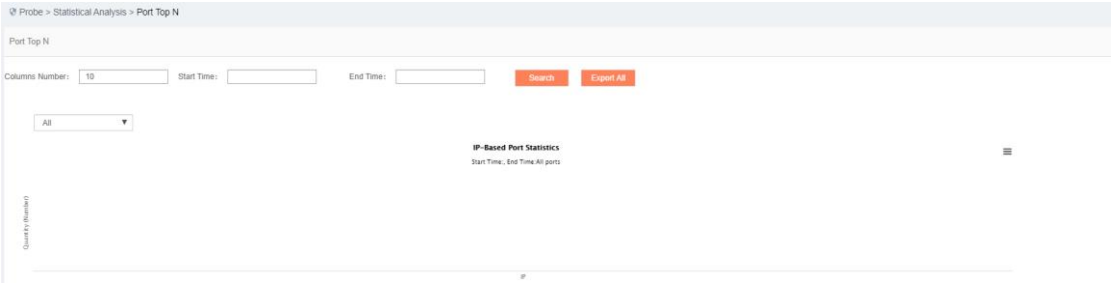
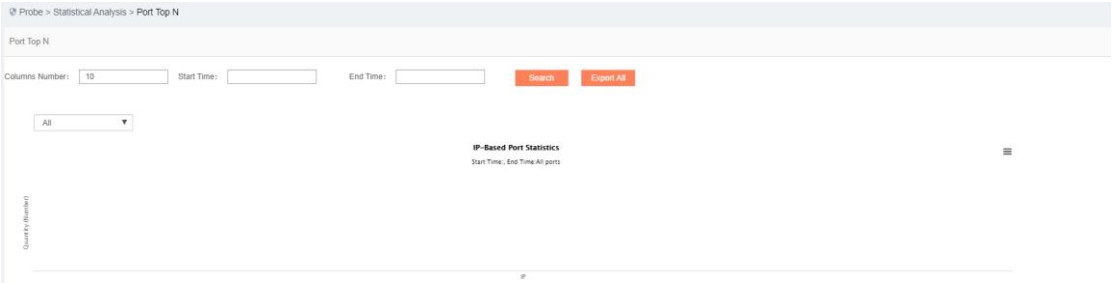


Fig.5-185 Port Statistics Page

Query the traffic in a specified time by query conditions, which can be filtered by receiving and sending. (As shown in Fig.5-186):



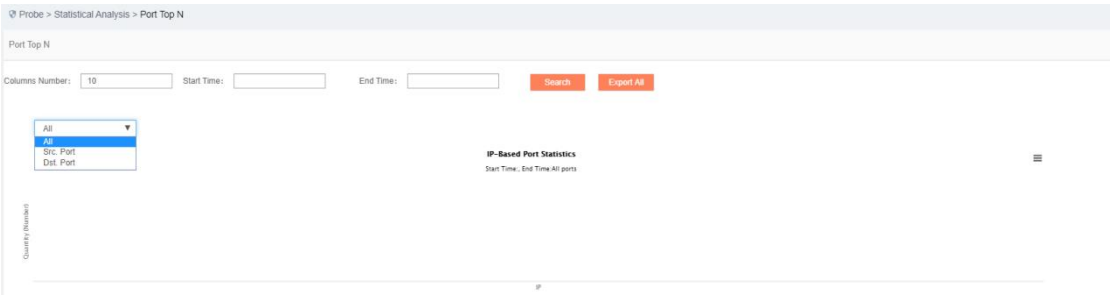


Fig.5-186 Query Traffic

5.9.5.3. Export a statistical graph.

Click the Export icon, export the current statistical graph (as shown in Fig.5-187), click <Export All> to export all statistical graphs in the page. (As shown in Fig.5-188):

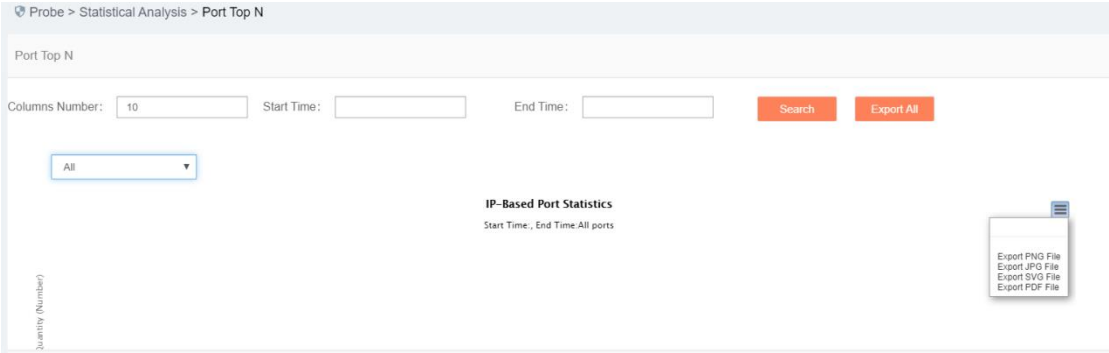


Fig.5-187 Exporting a Statistical Graph

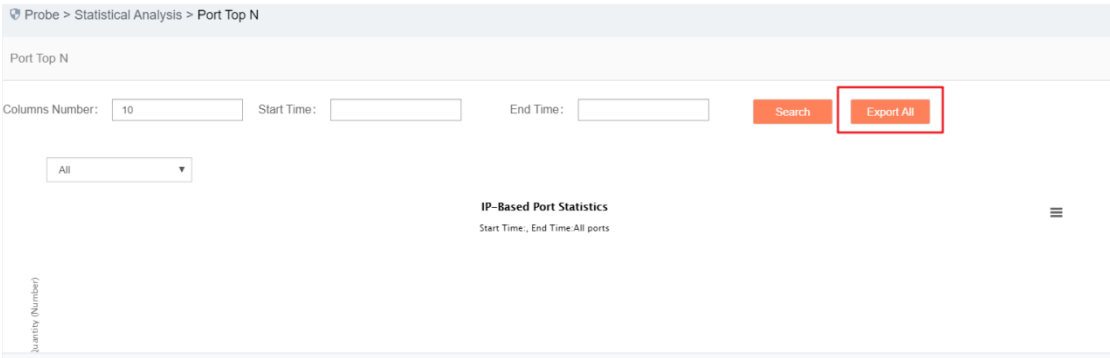


Fig.5-188 Exporting All Statistical Graphs

5.9.6. Alarm Event Statistics

5.9.6.1. Introduction to functions

Generate direct-viewing images according to the number of alarm events, for the auditor to make an analysis. (As shown in Fig.5-189):

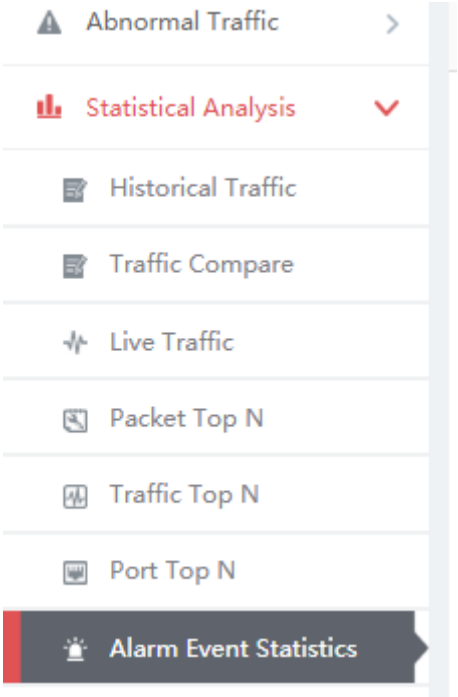


Fig.5-189 Menu

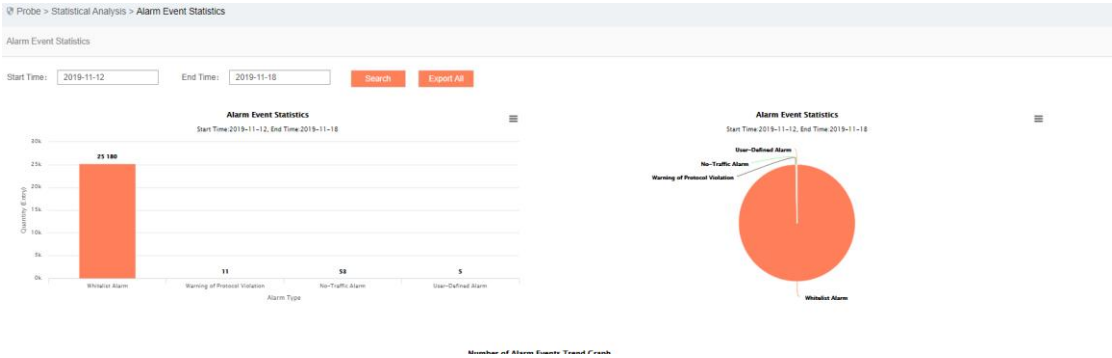


Fig.5-190 Statistics Page

5.9.6.2. Query data

Query the data in a specified time by query conditions. (As shown in Fig.5-191):

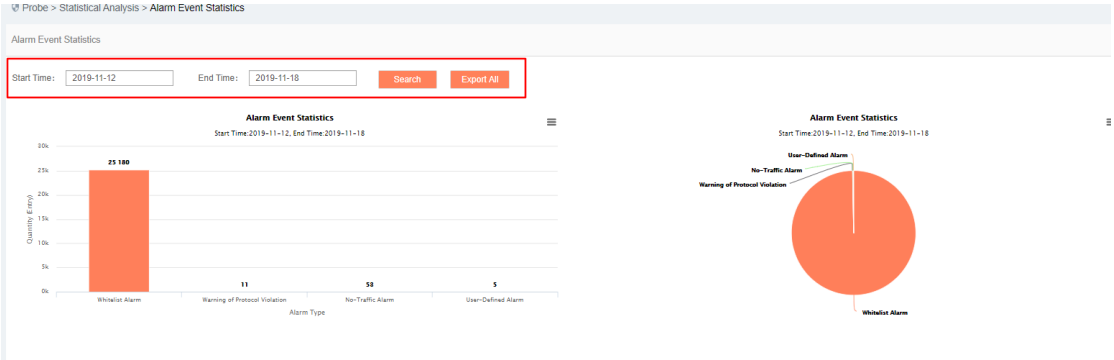


Fig.5-191 Query Data

5.9.6.3. Export a statistical graph.

Click the Export icon, export the current statistical graph (as shown in Fig.5-192), click <Export All> to export all statistical graphs in the page. (As shown in Fig.5-193):

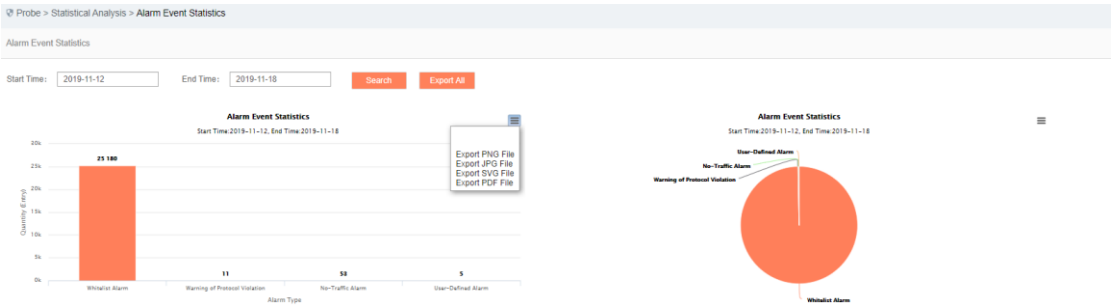


Fig.5-192 Exporting a Statistical Graph

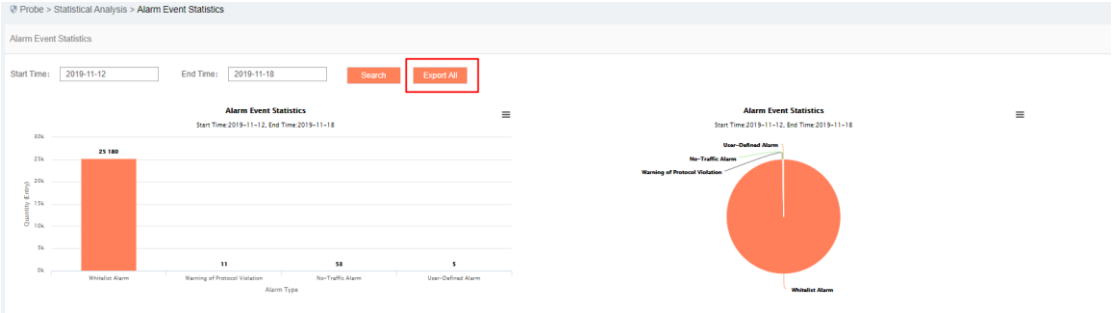


Fig.5-193 Exporting All Statistical Graphs

6. System Configuration

6.1. System Overview

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [System Overview/System Overview] in the left navigation bar, click Menu (as shown in Fig.6-1), display the system operation log page on the right (as shown in Fig.6-2):

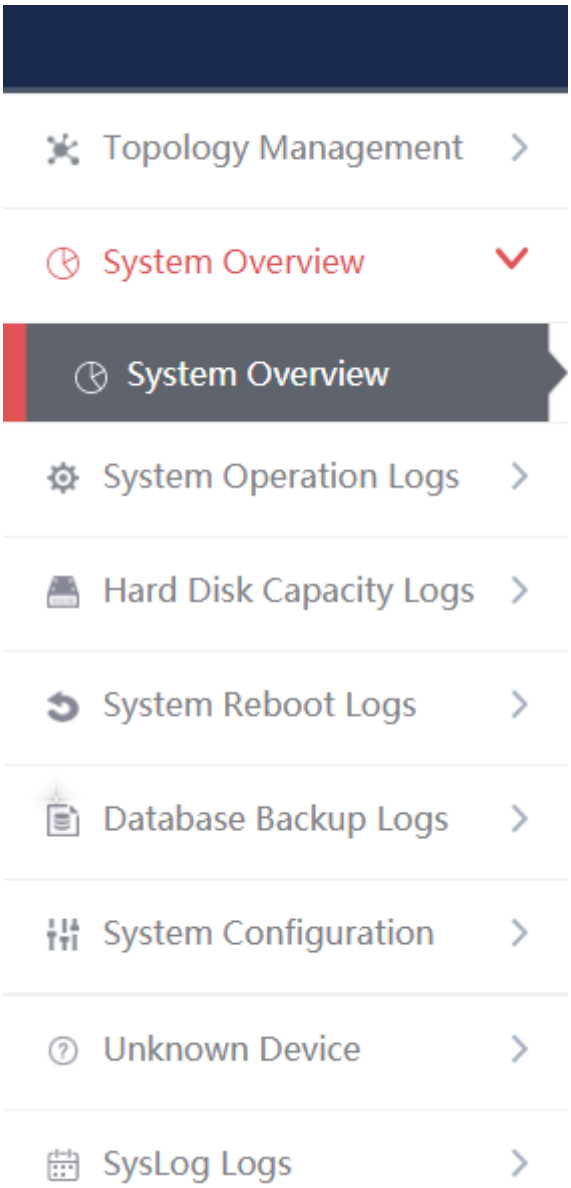


Fig.6-1 System Overview Menu Bar

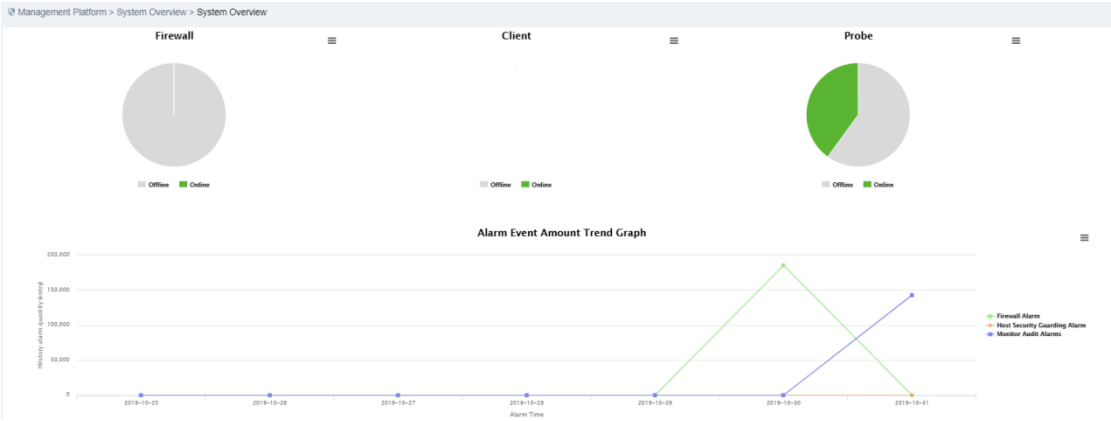


Fig.6-2 System Overview Page

6.1.1.System Overview Display

System overview can view the online status of industrial firewall, IEG client and monitoring audit terminal device (as shown in Fig.6-3), as well as number of alarms (as shown in Fig.6-4) and alarm trendy (as shown in Fig.6-5) in real time.

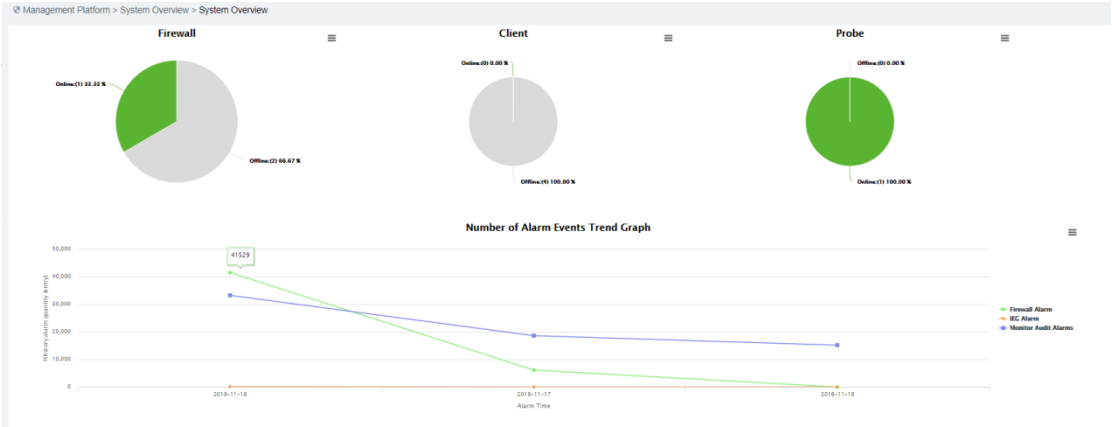


Fig.6-3 Online Status of Device

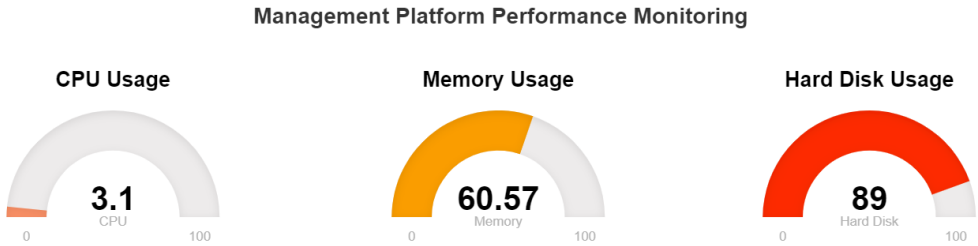
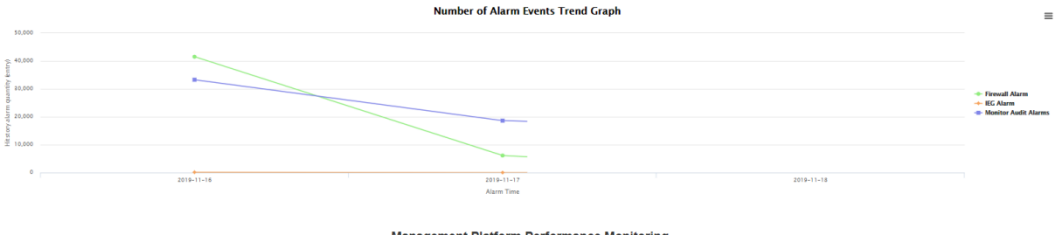


Fig.6-4 Management Platform Performance Monitoring



2

Fig.6-5 Alarm Trend

6.2. System Operation Log

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [System Operation Logs/System Operation Logs] in the left navigation bar, click Menu (as shown in Fig.6-6), display the system operation log page on the right (as shown in Fig.6-7):

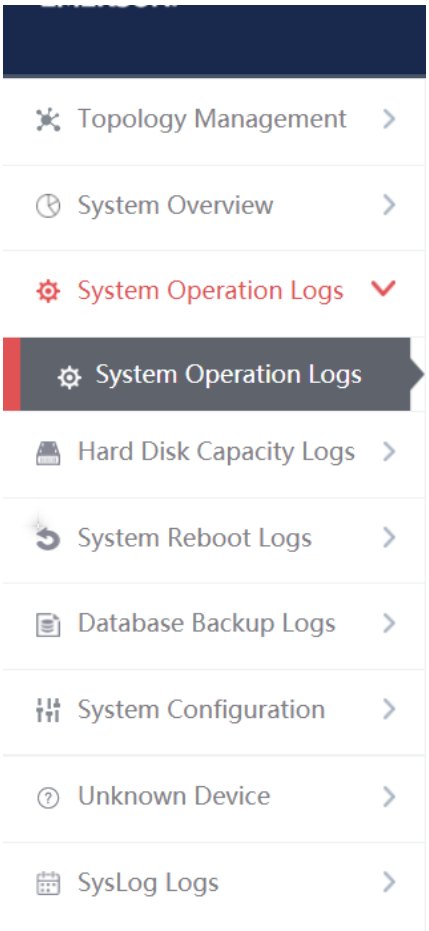
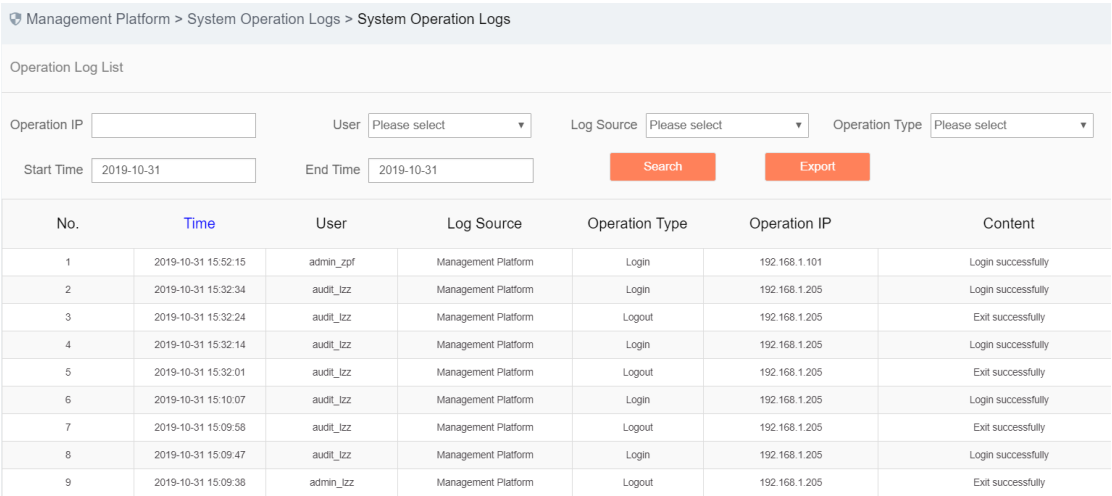


Fig.6-6 System Operation Log Menu Bar



No.	Time	User	Log Source	Operation Type	Operation IP	Content
1	2019-10-31 15:52:15	admin_zpf	Management Platform	Login	192.168.1.101	Login successfully
2	2019-10-31 15:32:34	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
3	2019-10-31 15:32:24	audit_lzz	Management Platform	Logout	192.168.1.205	Exit successfully
4	2019-10-31 15:32:14	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
5	2019-10-31 15:32:01	audit_lzz	Management Platform	Logout	192.168.1.205	Exit successfully
6	2019-10-31 15:10:07	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
7	2019-10-31 15:09:58	audit_lzz	Management Platform	Logout	192.168.1.205	Exit successfully
8	2019-10-31 15:09:47	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
9	2019-10-31 15:09:38	admin_lzz	Management Platform	Logout	192.168.1.205	Exit successfully

Fig.6-7 System Operation Log Page

6.2.1.**Retrieve a Log**

In the [System Operation Logs] list page, retrieve a log according to the conditions. (As shown in Fig.6-8):

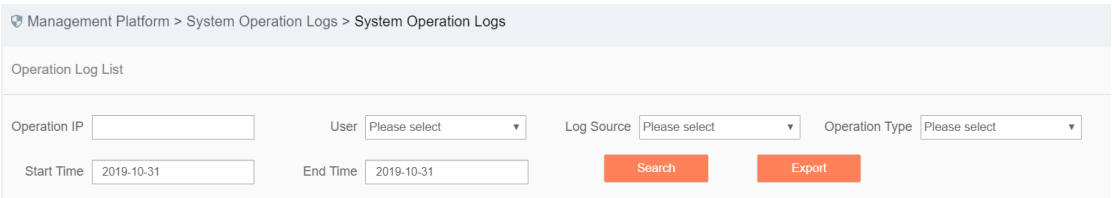


Fig.6-8 Query Conditions

6.3. **Hard Disk Utilization Logs**

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [Hard Disk Utilization Logs/Hard Disk Utilization Logs] in the left navigation bar, click Menu (as shown in Fig.6-9), display the hard disk utilization logs page on the right (as shown in Fig.6-10):

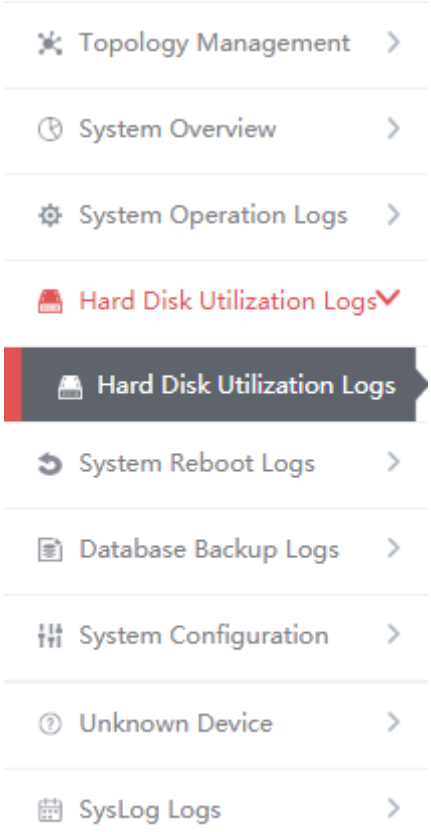


Fig.6-9 Hard Disk Utilization Logs Menu Bar

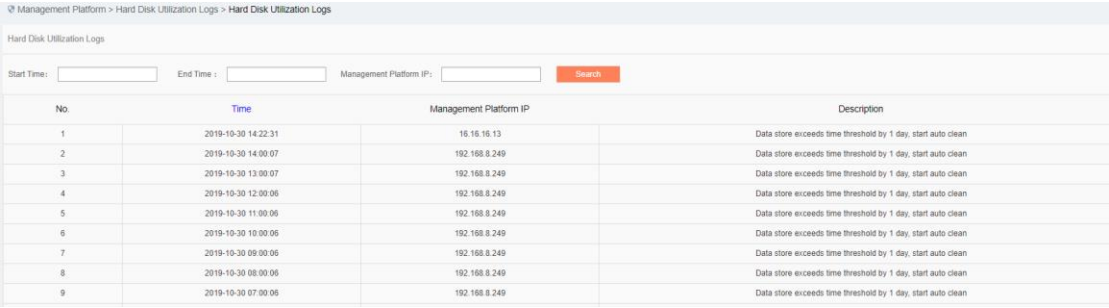


Fig.6-10 Hard Disk Utilization Logs Page

6.3.1.**Retrieve a Log**

In the [Hard Disk Utilization Logs] list page, retrieve a log according to the conditions. (As shown in Fig.6-11):

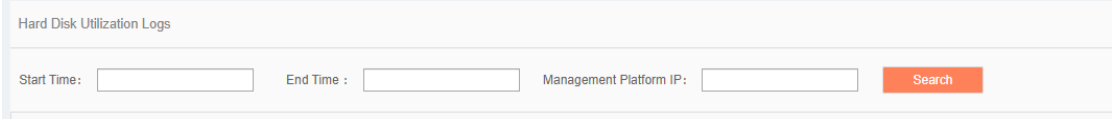


Fig.6-11 Retrieve Conditions

6.4. **System Restart Log**

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [System Restart Logs/Hard Disk Utilization Logs] in the left navigation bar, click Menu (as shown in Fig.6-12), display the system restart log page on the right (as shown in Fig.6-13):

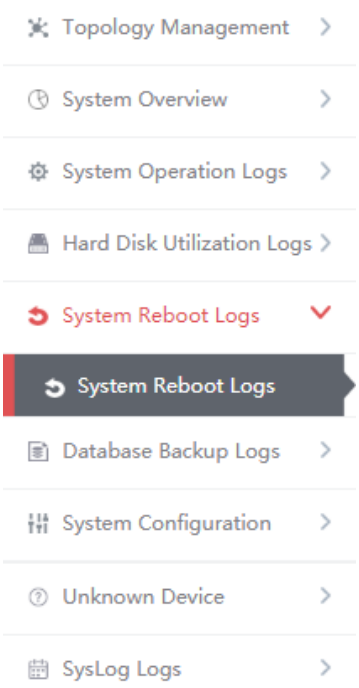


Fig.6-12 System Restart Log Menu Bar

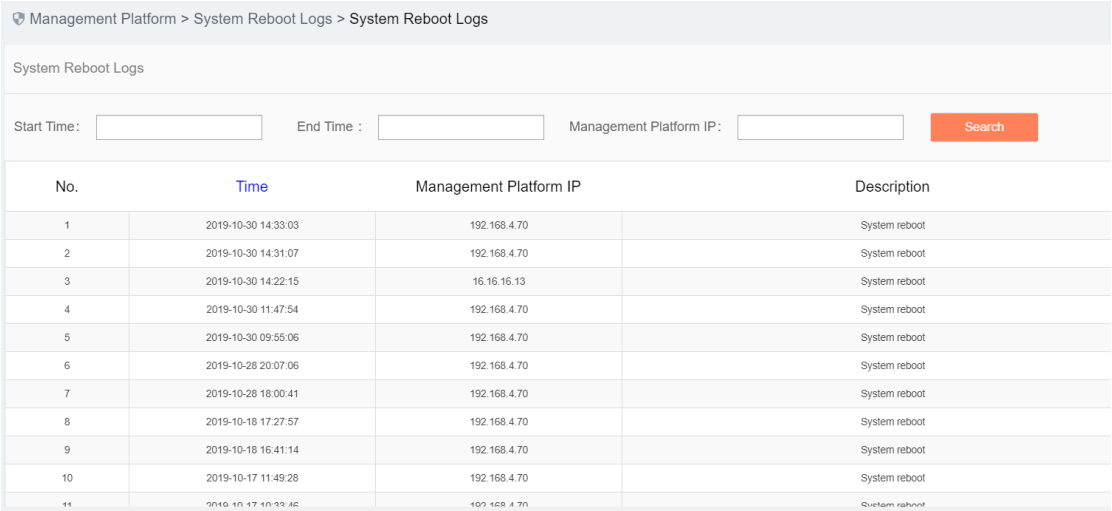


Fig.6-13 System Restart Log Page

6.4.1.Retrieve a Log

In the list page of system restart logs, the logs can be retrieved based on the conditions. (As shown in Fig.6-14):

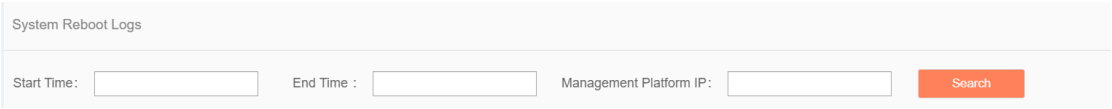


Fig.6-14 Retrieve Conditions

6.5. **Database Backup Log**

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [Database Backup Logs/Database Backup Logs] in the left navigation bar, click Menu (as shown in Fig.6-15), display the database backup log page on the right (as shown in Fig.6-16):

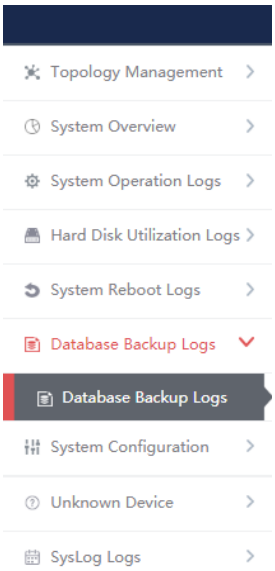


Fig.6-15 Database Backup Log Menu Bar

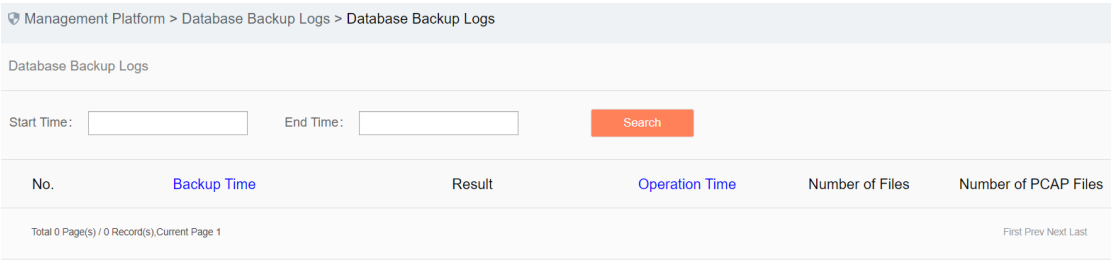


Fig.6-16 Database Backup Log Page

6.5.1.**Retrieve a Log**

In the [Database Backup Logs] list page, retrieve the log according to the conditions. (As shown in Fig.6-17):

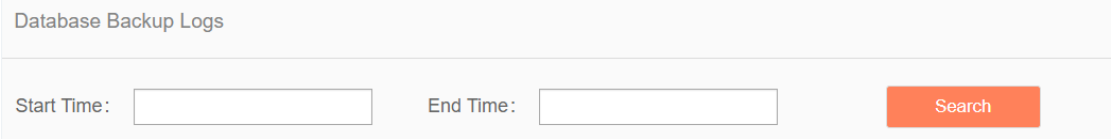


Fig.6-17 Retrieve Conditions

6.6. System Configuration

6.6.1.Password Management

Log in as the configuration administrator, find [System Configuration/Password Management] in the left navigation bar (as shown in Fig.6-18):

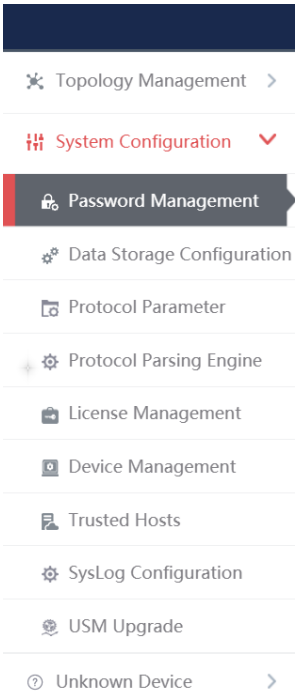


Fig.6-18 Password Management Menu Bar

Log in as auditor, find [System Configuration/Password Management] in the left navigation bar (as shown in Fig.6-19):

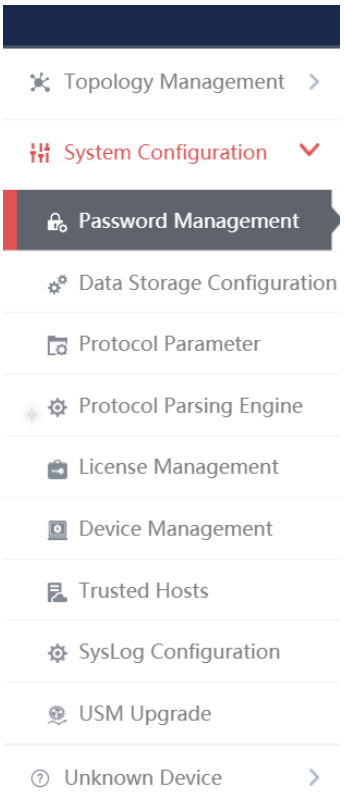


Fig.6-19 Password Management Menu Bar

Log in as the system operator, find [System Configuration/Password Management] in the left navigation bar (as shown in Fig.6-20):

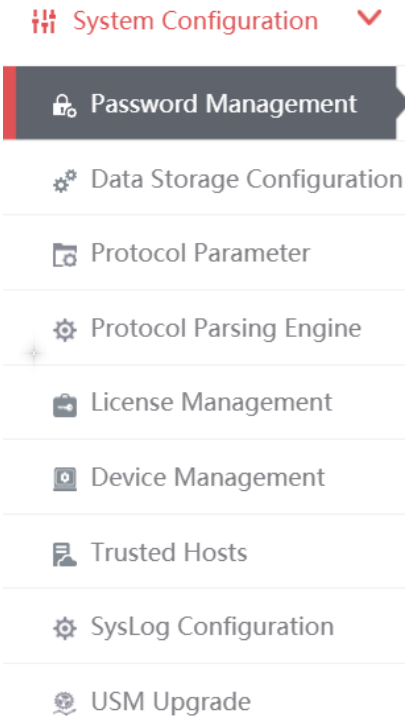


Fig.6-20 Password Management Menu Bar

Click Menu to see the password management page on the right (as shown in Fig.6-22):

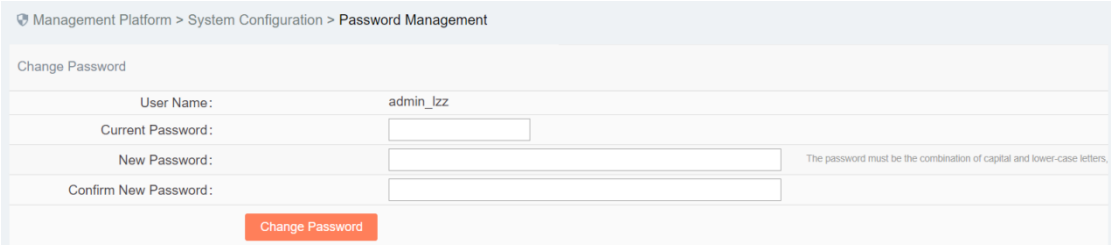


Fig.6-22 Password Management Page

6.6.1.1. Reset a password.

Reset the password for the user having currently logged in, fill in the password and click <Save>.

6.6.1.2. Modify the PIN

Modifying the PIN code allows the user to modify the PIN code of the USBKey already associated with the user. This feature is only available to users who have correctly installed the USBKey plug-in and are associated with the USBKey.

To modify the PIN code, download and install the USBKey plug-in. See Fig.6-23 for the download link url:

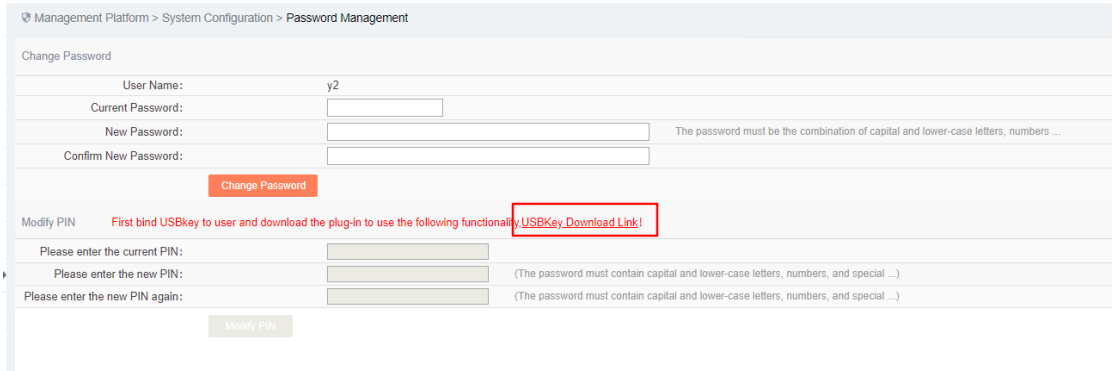


Fig.6-23 Modify a PIN Code Page

To modify the PIN code, please enter the correct old PIN code. The new PIN code and the repeated new PIN code must be the same. The PIN code must meet the following conditions: the password must contain upper- and lower-case letters, numbers and special characters, with a length of less than 8 characters and up to 16 characters. Click <Modify a PIN Code> to complete the operation of modifying a PIN code.

6.6.2. User Management

The management platform supports decentralized and hierarchical management, currently supporting users of four levels: system operator, configuration administrator and audit administrator. The system operator can create different users and assign different roles. The configuration administrator can manage configurations, and auditor can view all logs.

6.6.2.1. Information view

System operator logs in, click system configuration/user management in the left navigation bar (as shown in Fig.6-24), and enter the page of user management (as shown in Fig.6-25):

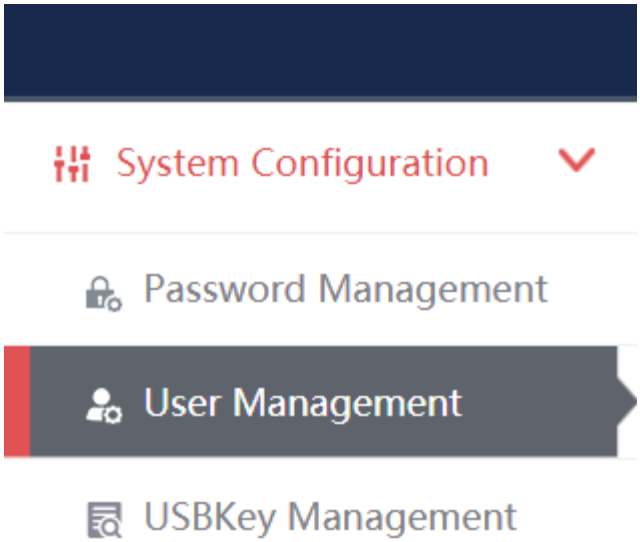


Fig.6-24 user administration menu

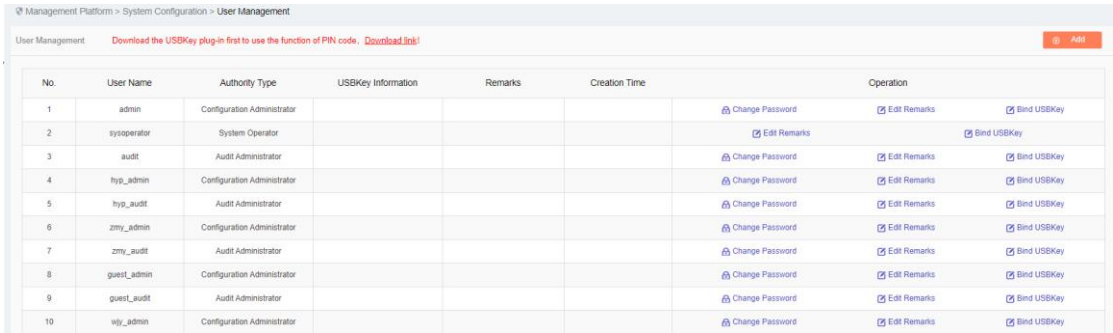


Fig.6-25 user managed list page

6.6.2.2. Add user.

Log in as the system operator, click <Add> on the right side of the [System Configuration/User Management] user list tab (as shown in Fig.6-26) to pop up the user add page (as shown in Fig. 6-27):

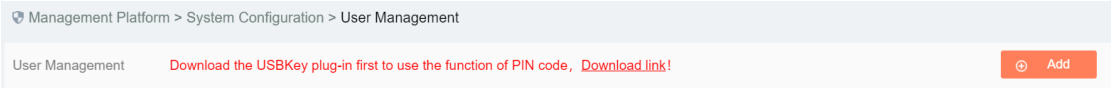


Fig.6-26 User Add Button

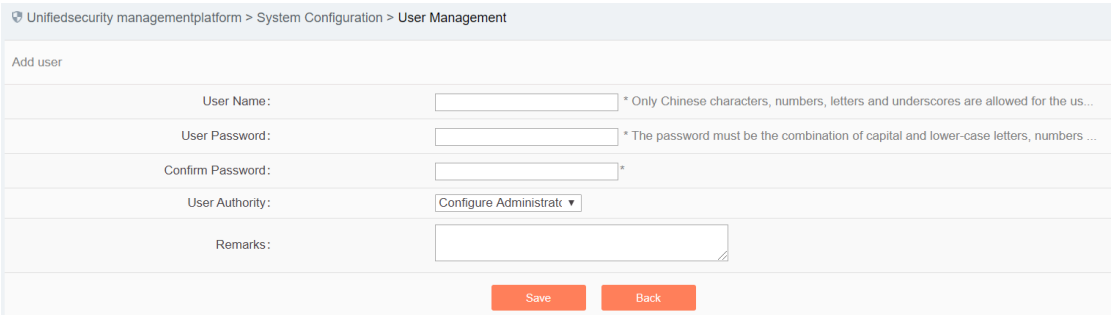


Fig.6-27 User Add Page

Table 64 Instruction to User Add Information

Column Names	Instructions	
Username	Define a meaningful name for the user that is easy to understand and remember	
User Password	The user login password must be upper and lower case letters, numbers and special characters (#@! ~%^&*), with a length not less than 8 characters and up to 16 characters	
Confirm Password	Enter the user's login password again	
User Authority	User access level; choose between the configuration administrator and auditor	
Remarks	Optional, additional explanatory information	
Operation	Save	Submit all information and go back to the user list display page
	Back	Ignore all modifications and go back to the user list display page

6.6.2.3. Modify a password.

Log in as the system operator, click <Modify a Password> under the operation column in the [User Management] user list, open the [User Management] user basic information modify page, modify the basic information on the user (as shown in Fig.6-28):

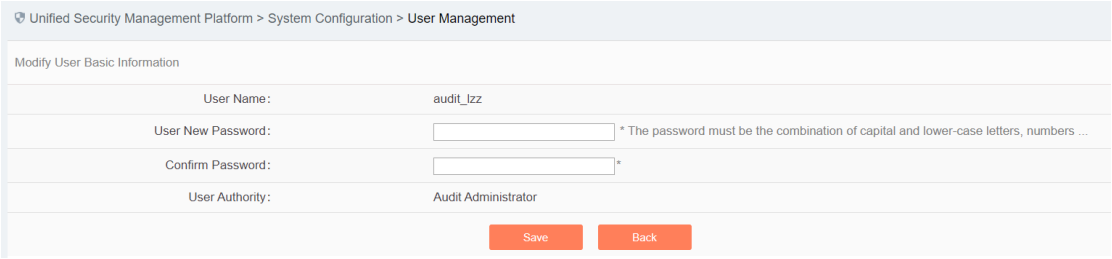


Fig.6-28 Modify a Password Page

6.6.2.4. Modify a remark.

Log in as the system operator, click <Modify a Remark> under the operation column in the [User Management] user list, open the [User Management] user basic information modify page, modify the basic information on the user (as shown in Fig.6-29):

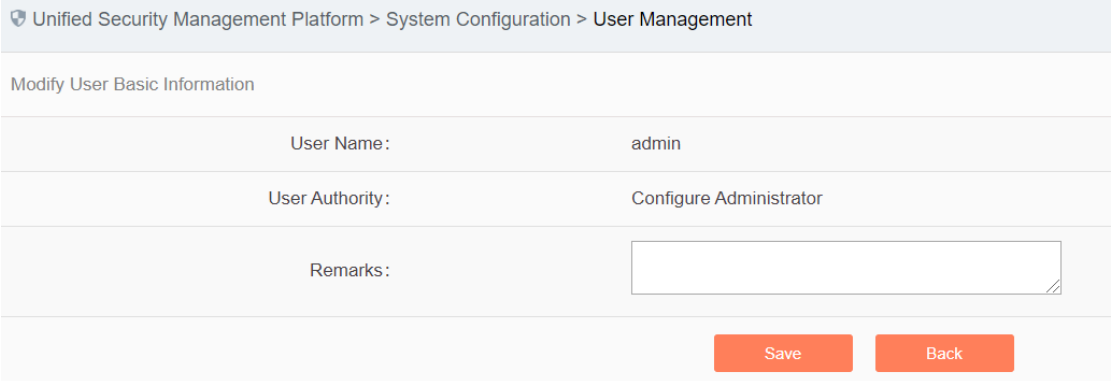


Fig.6-29 Modify a Remark Page

6.6.2.5. Delete a user.

Log in as the system operator, click <Delete> under the operation column in the [User Management] user list, click <Save> to delete the user that is no longer in use.

6.6.2.6. Bind a USBKey

To bind the USBKey, please download and properly install the USBKey plug-in first, and insert the USBKey to be bound before it can be used properly.

Log in as the system operator, click <Bind a USBKey> under the operation list to be bound with the USBKey under [User Management] (as shown in Fig.6-30), enter the bind a USBKey page (as shown in Fig.6-31):

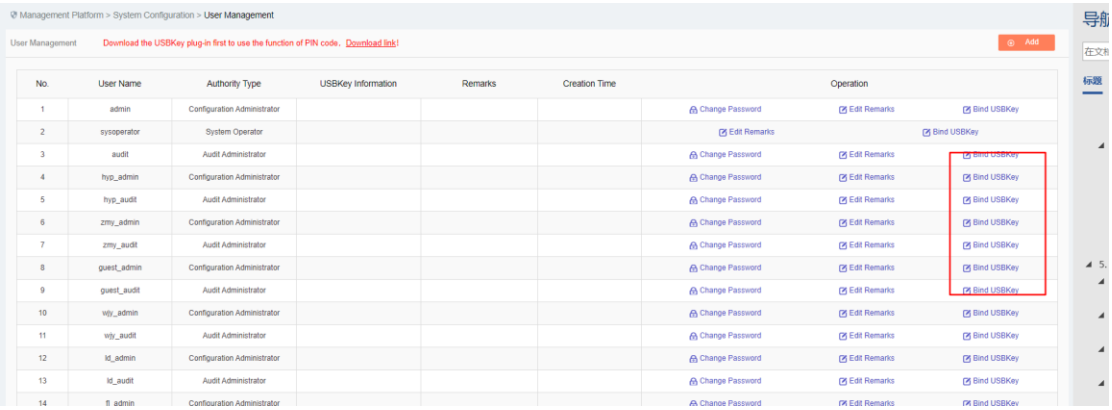


Fig.6-30 Bind a USBKey Button

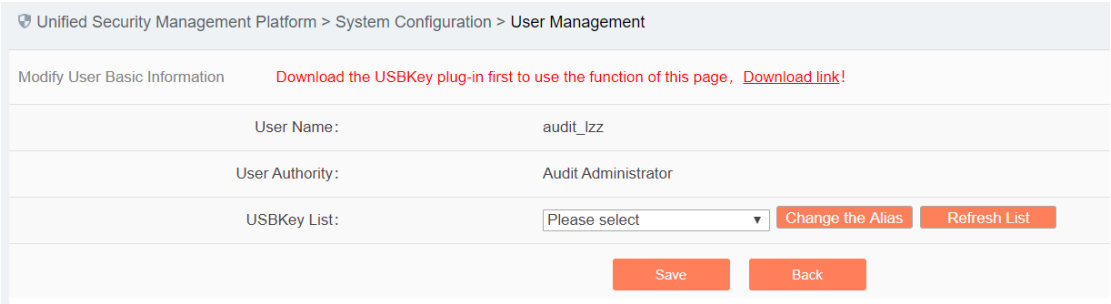


Fig.6-31 Bind a USBKey Page

Select the USBKey to be bound in the drop-down USBKey list, click <Save> to successfully associate the selected USBKey with the user. The user needs to insert the associated USBKey and enter the correct PIN code to log in the USM again.

After selecting a USBKey in the USBKey list, click <Change an Alias> to enter the USBKey alias modification page, (as shown in Fig.6-32):

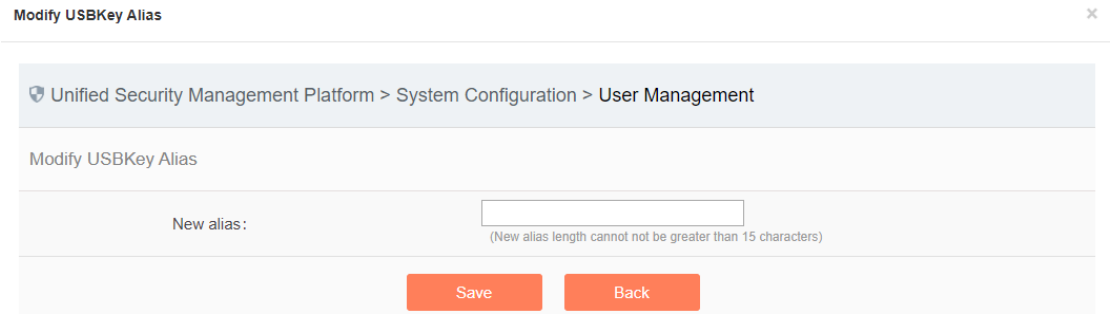


Fig.6-32 USBKey Alias Modification Page

Enter the new alias, click <Save> and make it come into effect, go back to the bind a USBKey page; click <Back> and go back to the bind a USBKey page.

6.6.2.7. Unbind a USBKey

To unbind a USBKey, only operate for a user bound with a USBKey.

Log in as the system operator, click <Unbind a USBKey> under the user operation list with the USBKey to be unbound under [User Management] (as shown in Fig.6-33):

Fig.6-33 Unbind a USBKey Button

Click <Confirm> to unbind the USBKey. Click <Cancel> to cancel the operation, (as shown in Fig.6-34):

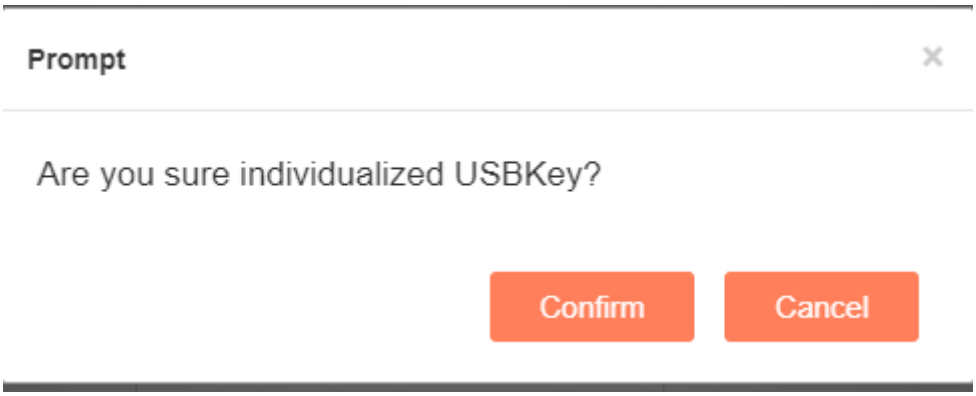


Fig.6-34 Unbind a USBKey Confirm Page

6.6.2.8. Reset a PIN code.

To reset a PIN code, please download and properly install the USBKey plug-in first. Insert the USBKey with the user to be reset before it can be used properly.

Log in as the system operator, click <Reset a PIN Code> under the user operation list with the PIN code to be unbound under [User Management] (as shown in Fig.6-35):

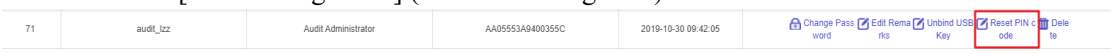


Fig.6-35 Reset a PIN Code Button

Click to display the page as shown in Fig.6-36, click <Confirm>, reset the PIN code of the user's USBKey to the initial password, click <Cancel> to cancel the operation.

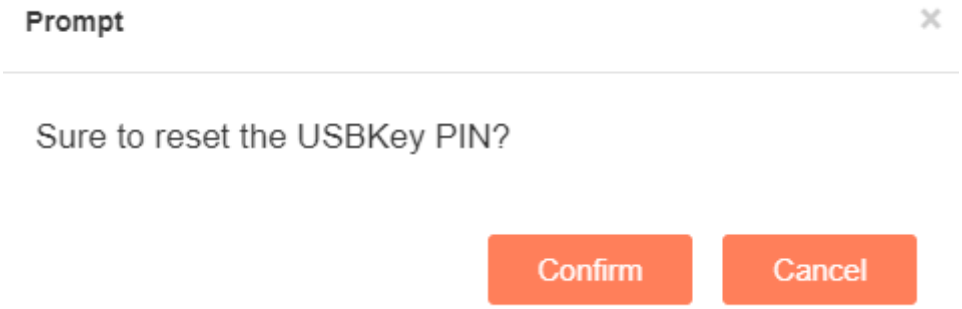


Fig.6-36 Unbind a USBKey Confirm Page

6.6.3. USBKey Management

The operation page is used to change an alias and reset a PIN code for USBKey. To use the functions, download and professionally install the USBKey plug-in. Log in as the system operator, click [System Configuration/USBKey Management] in the left navigation bar (as shown in Fig.6-37), enter the [USBKey Management] page (as shown in Fig.6-38):

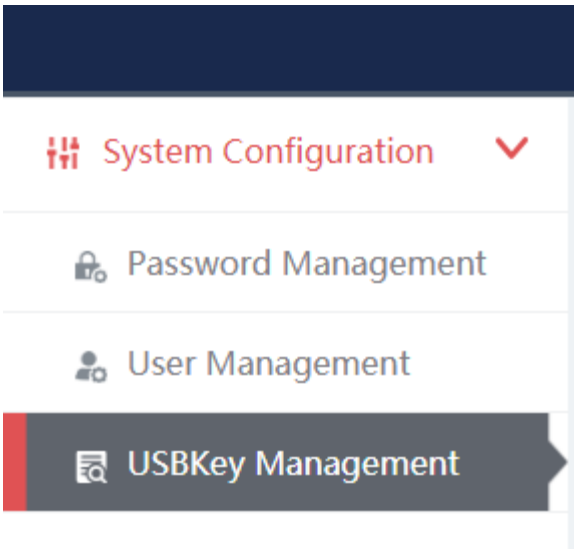


Fig.6-37 USBKey Management Navigation

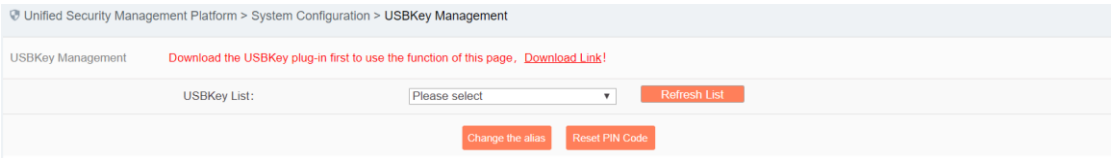


Fig.6-38 USBKey Management Page

6.6.3.1. Change an alias.

After selecting a USBKey in the USBKey list, click <Change an Alias>, enter the USBKey alias modification page, (as shown in Fig.6-39):

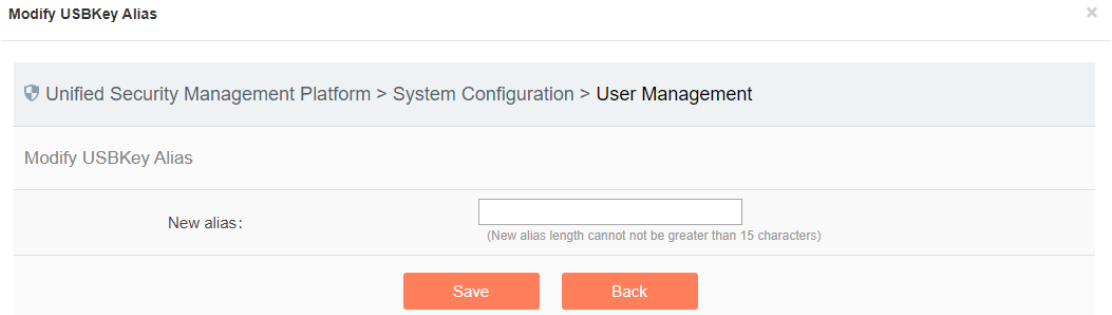


Fig.6-39 USBKey Alias Modification Page

Enter the new alias, click <Save> and make it come into effect, go back to the USBKey management page; click <Back> and go back to the USBKey management page.

6.6.3.2. Reset a PIN code.

After selecting a USBKey in the USBKey list, click <Reset a PIN Code>, click <Reset a PIN Code> to pop up the reset PIN code confirmation box, (as shown in Fig.6-40):

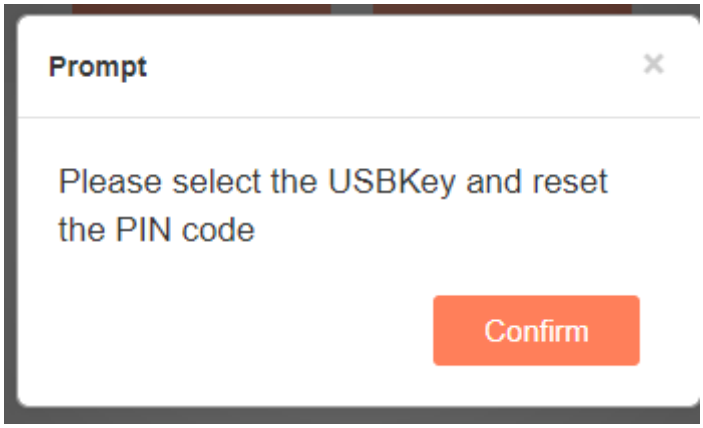


Fig.6-40 Reset a PIN Code Confirmation Box

Click <Confirm>, reset the PIN code of the user's USBKey to the initial password, click <Cancel> to abandon the operation.

6.6.4.Database Storage Cycle Configuration

It is used to configure the management platform database storage and backup cycle. Log in as the configuration administrator, click [System Configuration/Database Storage Cycle Configuration] in the left navigation bar (as shown in Fig.6-41), enter the [Database Storage Cycle Configuration] page (as shown in Fig.6-42):

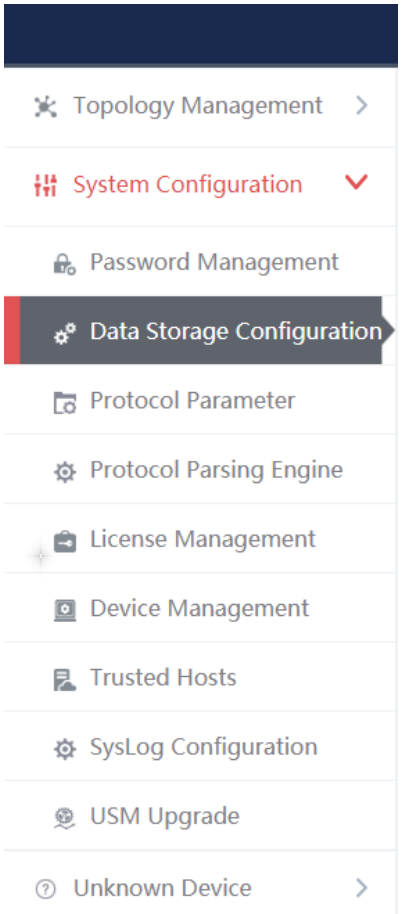


Fig.6-41 Database Storage Cycle Configuration

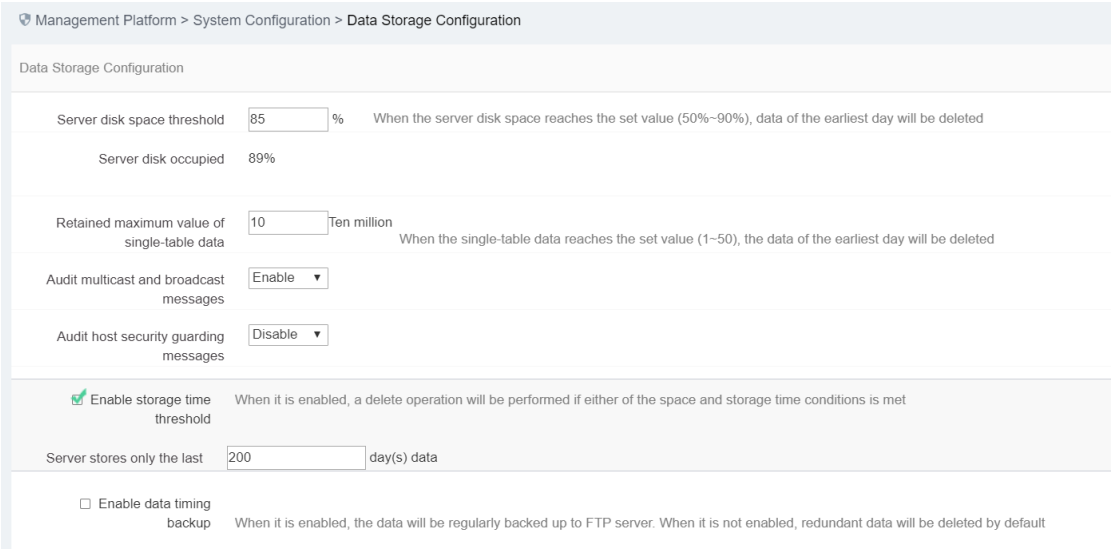


Fig.6-42 Database Storage Cycle Configuration Page

6.6.4.1. Save

Fill in the information according to the prompts. Click <Modify> first, then click <Save> to distribute the configuration. (As shown in Fig.6-43):

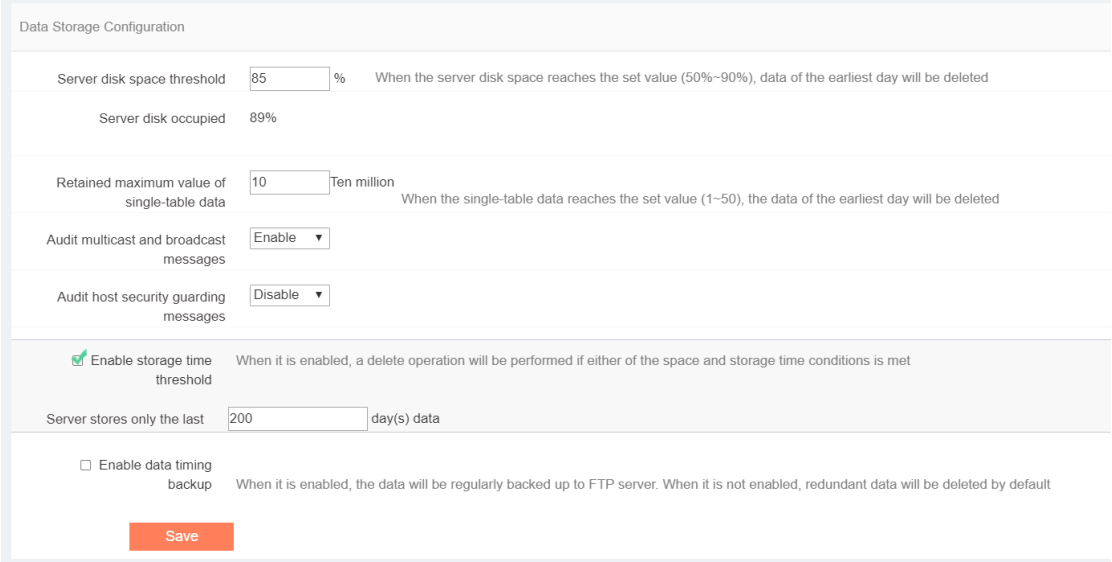


Fig.6-43 save the configuration.

6.6.5. Protocol Parameter Configuration

6.6.5.1. Introduction to functions

The whitelist configuration template often needs to use custom function codes and other addable fields. At present, the CIP drop-down menu can add such fields through custom items, but only support adding. In the

industrial firewall learning process, new custom fields used by users may be learnt. In this case, it is necessary to re-modify the field description and delete user-defined fields. To this end, the industrial firewall, through a dedicated protocol parameter configuration page, facilitates users to manage the specific features of some industrial protocols.

6.6.5.2. Protocol parameter configuration

Log in as the configuration administrator, click [Whitelist Management/Protocol Parameter Configuration] in the left navigation bar (as shown in Fig.6-44), enter the [Protocol Parameter Configuration] page (as shown in Fig.6-45):

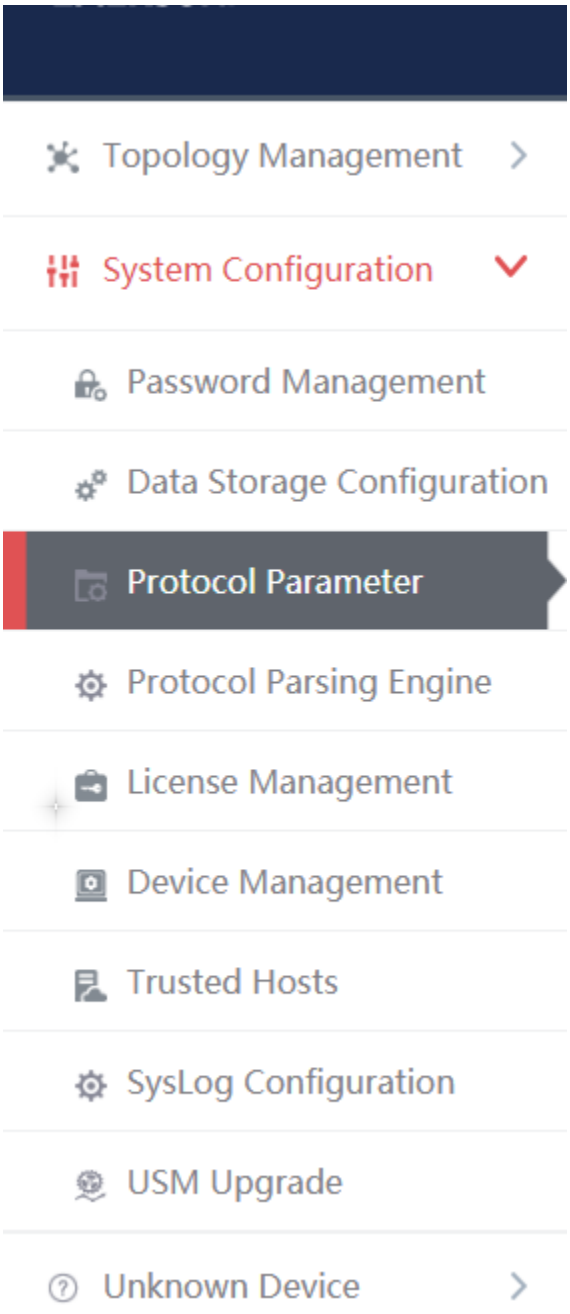


Fig.6-44 Selecting Protocol Parameter Configuration

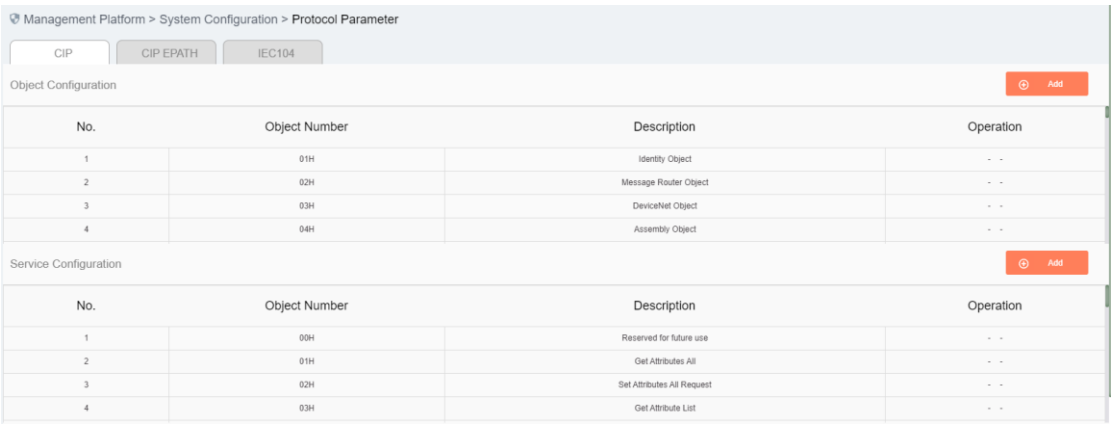


Fig.6-45 Protocol Parameter Configuration Page

Users can configure the following three parameters in view of the CIP protocol here:

- Object configuration
- Service configuration
- PCCC configuration

The meaning of each field of these three configurations is stated below.

Tab.65 Instruction to CIP Protocol Object Configuration Fields

Column Names	**Instructions**	
The object number	Standard objects defined under the CIP protocol and user-defined objects in the industrial field are displayed in hexadecimal values	
Description	The specific meaning of the object	
Operation	Modify	Modify the descriptive information on the user-defined object, but the descriptive information on the CIP standard object cannot be modified
	Delete	Delete the user-defined object, unable to delete the CIP standard objects

Tab.66 Instruction to CIP Protocol Service Configuration Fields

Column Names	**Instructions**	
Service no.	The standard services provided under the CIP Protocol and custom services in the industrial field are displayed in hexadecimal values	
Description	Specific meaning of service	
Operation	Modify	Modify the descriptive information on user-defined CIP service, unable to modify the descriptive information on CIP standard service

	Delete	Delete user-defined CIP service, unable to delete CIP standard service

Tab.67 Instruction to CIP Protocol PCCCC Configuration Fields

Column Names	**Instructions**	
CMD	The CMD number in a PCCC message embedded in the CIP protocol, displayed in hexadecimal values	
FNC	The FNC number in a PCCC message embedded in the CIP protocol, displayed in hexadecimal values	
Description	The method description uniquely determined by the CMD and FNC combination in PCCC	
Operation	Modify	Redefine the method uniquely determined by the CMD and FNC combination, unable to modify the standard method defined by PCCC
	Delete	Delete the user-defined method uniquely determined by the CMD and FNC combination, unable to delete the standard method defined by PCCC

6.6.5.3. CIP configuration addition

Click <Add> on the right of each configuration list, <Add> in object configuration of (as shown in Fig.6-46), open the object configuration addition page (as shown in Fig.6-47):

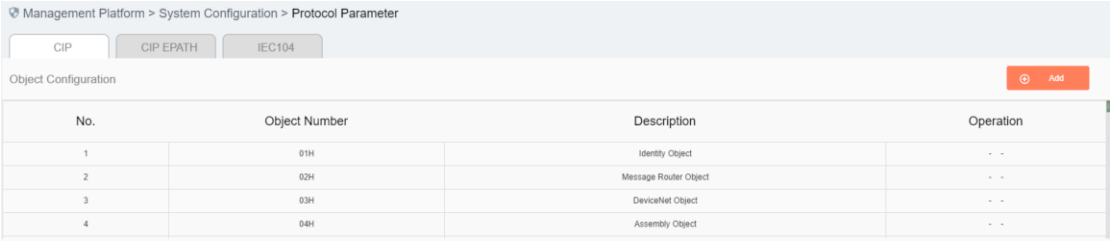


Fig.6-46 CIP Protocol Object Configuration Addition Button

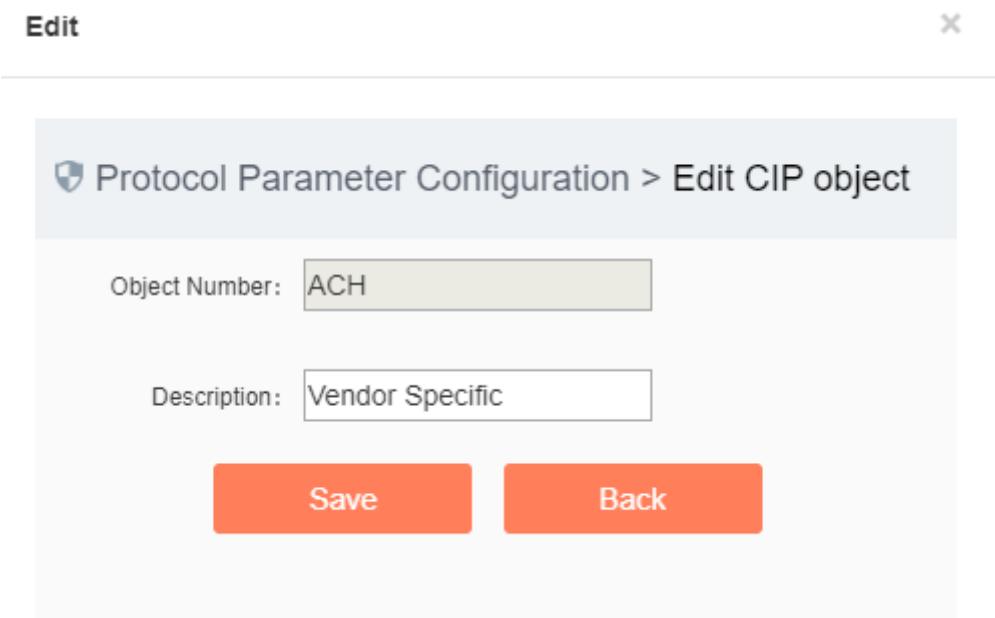


Fig.6-47 CIP Protocol Object Configuration Addition Page

Please refer to 6.6.5.2 Protocol Parameter Configuration for the meaning of object number and description.

Click <Save> to save the added custom object to the backstage, and then skip to the protocol parameter configuration page.

Click <Back> to go back to the protocol parameter configuration page without saving the edited custom object.

6.6.5.4. CIP Configuration modification

Please refer to the modification instructions under 6.6.5.2 Protocol Parameter Configuration Operation Column.

6.6.5.5. CIP Configuration deletion

Please refer to the modification instructions under 6.6.5.2 Protocol Parameter Configuration Operation Column.

6.6.5.6. CIP EPATH Configuration addition

Click the tab and skip to the CIP EPATH configuration page (as shown in Fig.6-48), click <Add> to add a rule.

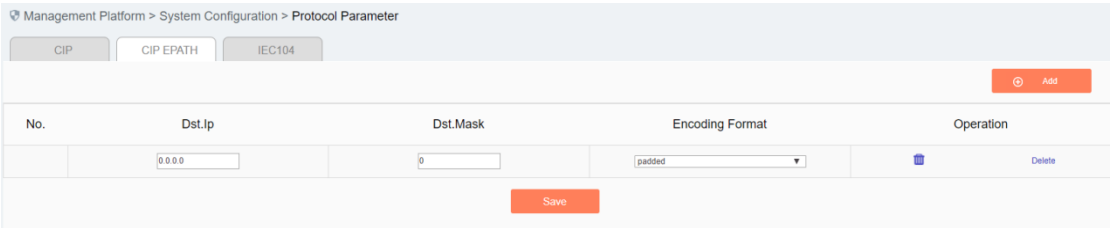


Fig.6-48 CIP EPATH Configuration Page

6.6.5.7. CIP EPATH Configuration deletion

Click <Delete> to delete a rule (Fig.6-49).

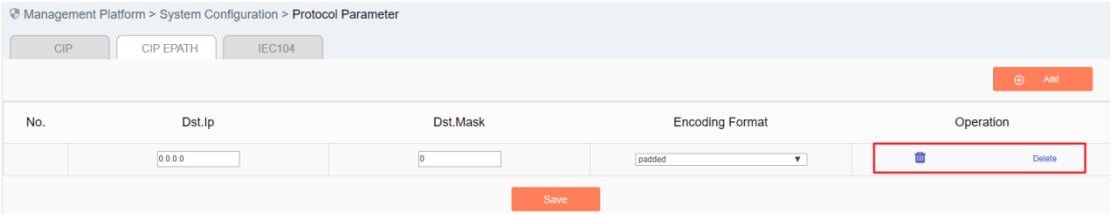


Fig.6-49 CIP EPATH Deletion Operation

6.6.5.8. CIP EPATH Configuration saving

Click <Save> to save all rules and distribute them to the device (as shown in Fig.6-50):

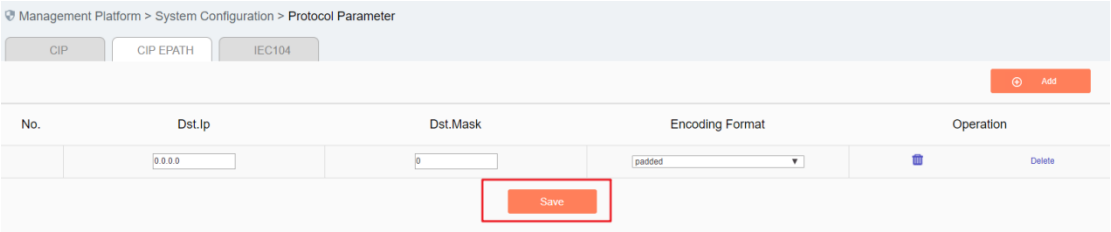


Fig.6-50 CIP EPATH Saving operation.

6.6.5.9. IEC104 Configuration

Click the tab and skip to the IEC104 configuration page (Fig.6-51):

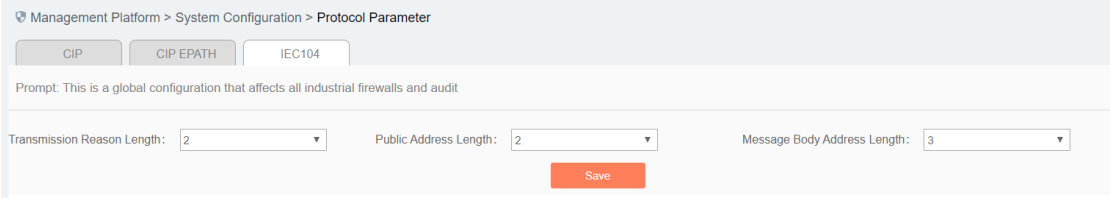


Fig.6-51 IEC104 Configuration Page

6.6.5.10. IEC104 Configuration saving

Click <Save> to save and distribute the page configuration (as shown in Fig.6-52):

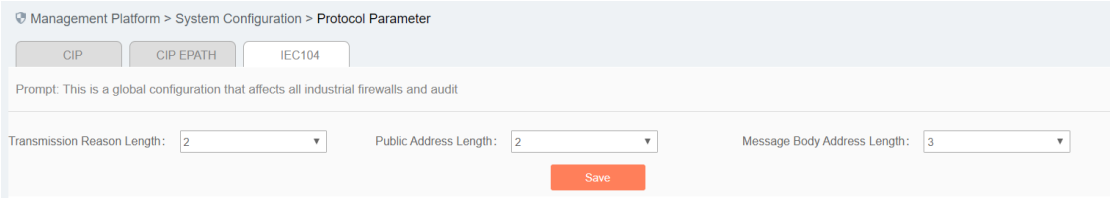


Fig.6-52 IEC104 Saving

6.6.6.Decoding Engine Configuration

The configuration of the decoding engine allows users to conveniently and quickly define the supported private protocols, realize in-depth protocol resolving by uploading the engine configuration files, automatically generate the rule configuration interface and give an alarm.

Click [System Configuration/Decoding Engine Configuration] in the left navigation bar (as shown in Fig.6-53), enter the [Decoding Engine Configuration] page (as shown in Fig.6-54):

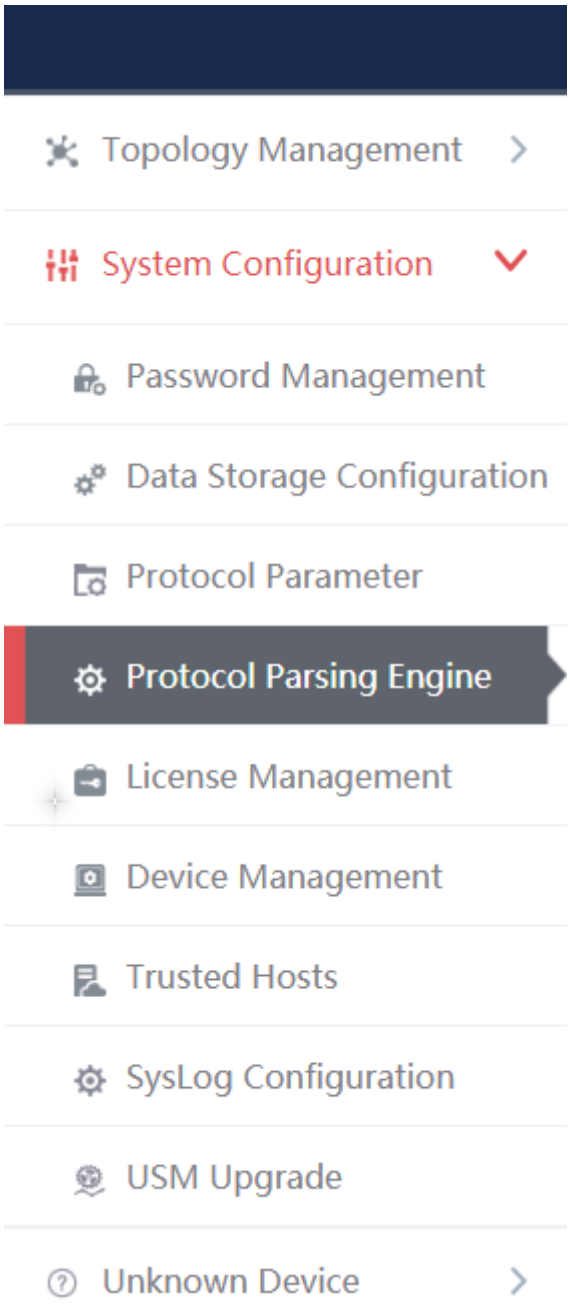


Fig.6-53 Decoding Engine Configuration Menu

Fig.6-54 Decoding Engine Configuration Page

6.6.6.1. Upload a decoding engine configuration file.

Click "Select a File" to select the preset decoding engine configuration file, click "Upload" to complete the configuration of private protocol (as shown in Fig.6-55):

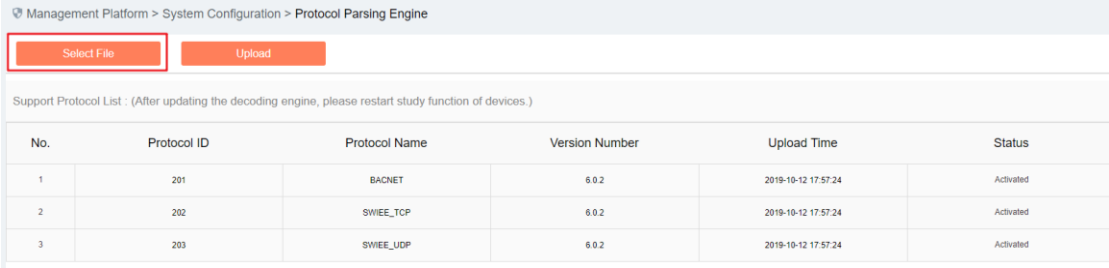


Fig.6-55 Protocol Decoding Engine Upload Configuration File

6.6.6.2. Protocol parsing information display.

After successful resolving, the management platform displays the resolved private protocol information (as shown in Fig.6-56). Display fields, including protocol ID, protocol name, version number, upload time and usage status.

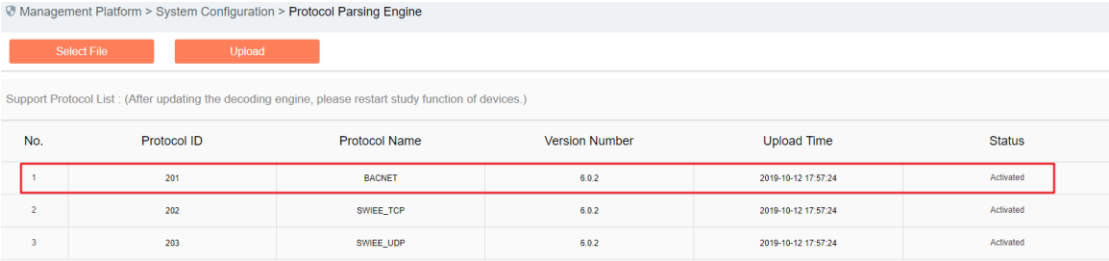


Fig.6-56 Protocol Resolving Information Display

6.6.7. Authorization Management

To authorize functions such as [Industrial Firewall], [Host Reinforcement] and [Monitoring Audit], click [System Configuration/Authorization Management] in the left navigation bar (as shown in Fig.6-57), enter the [Authorization Management] page (as shown in Fig.6- 58):

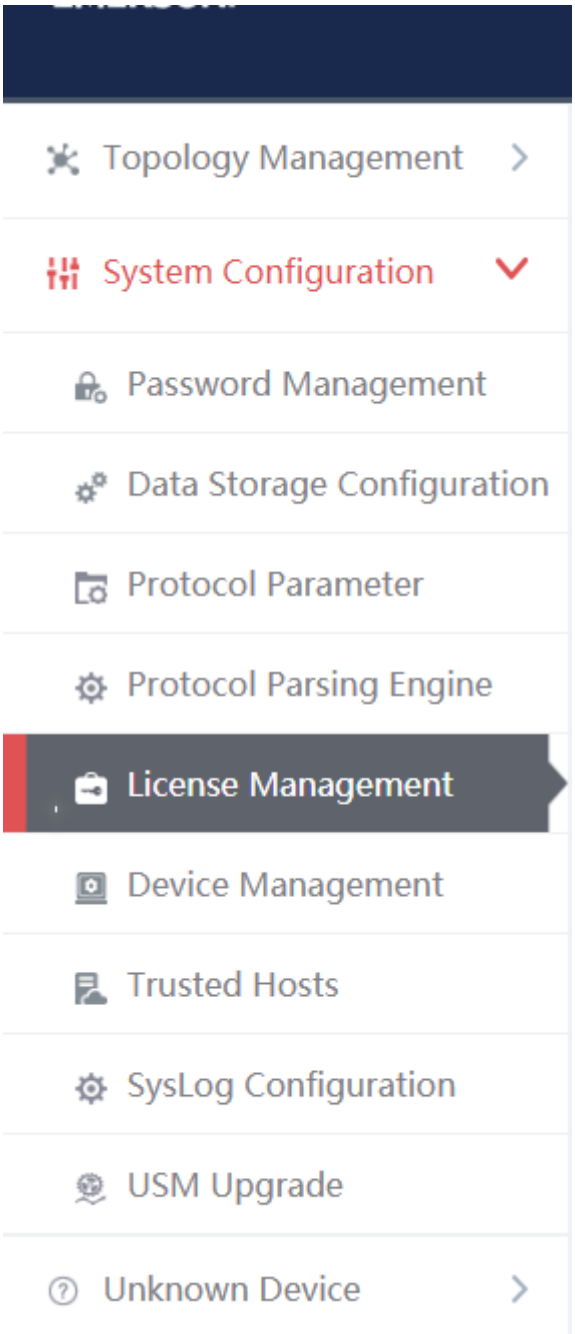


Fig.6-57 Authorization Management Menu Bar

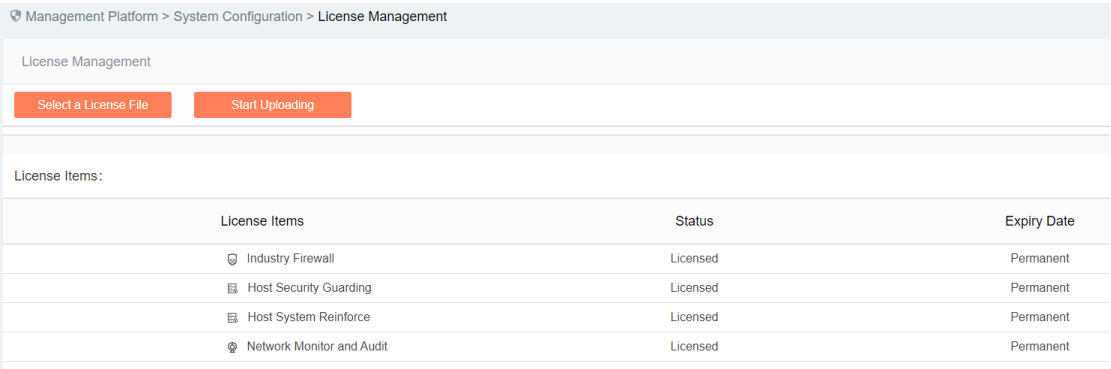


Fig.6-58 Authorization Management Page

6.6.7.1. Start upload.

Click <Please Select an Authorization File>, select the authorization file, click <Start Uploading> and execute the authorization.

6.6.8. Device Management

Device management is one of the important functions of the management platform, which provides a friendly interface to help users manage devices.

Log in as the configuration administrator, click [System Configuration/Device Management] in the left navigation bar (as shown in Fig.6-59), enter the [Device Management] page (as shown in Fig.6-60):

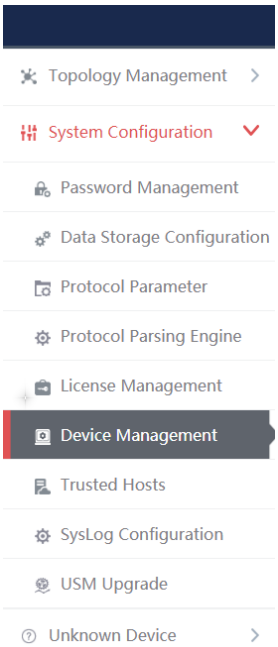


Fig.6-59 Device Management Menu

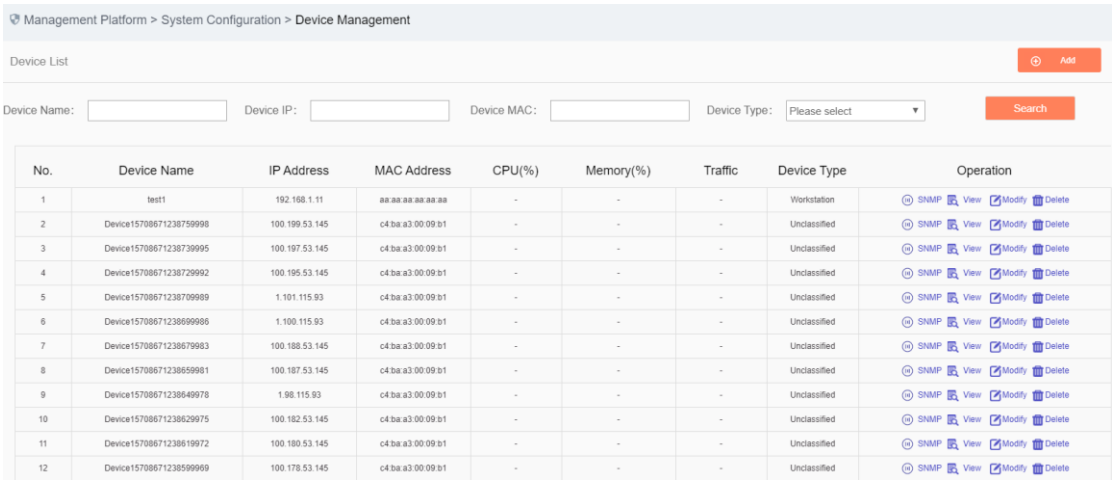


Fig.6-60 Device Management Page

View all the device information in the system here, with the following meanings given:

Tab.68 Instruction to Device List Display

Column Names	**Instructions**	
Device name	A device name that is easy to remember	
IP address MAC address CPU (%) Memory (%) traffic	The IP address assigned by the device, in dotted decimal format. The MAC address assigned by the device The SNMP protocol obtains the device CPU utilization ratio information on the current IP address The SNMP protocol obtains the device memory utilization ratio information on the current IP address The SNMP protocol obtains the total traffic generated by the device in view of the current IP address	
Device type	The purpose classification of the device, such as workstation and controller, etc. SNMP configuration configures the SNMP protocol information	
Operation	View	View more detailed information on the device
	Modify	Modify and set the device information
	Delete	Delete a device

6.6.8.1. SNMP Configuration

Click <SNMP Configuration> under the operation column in the [Device Management], display the detailed

information on SNMP configuration as shown in the following figure. (As shown in Fig.6-61):

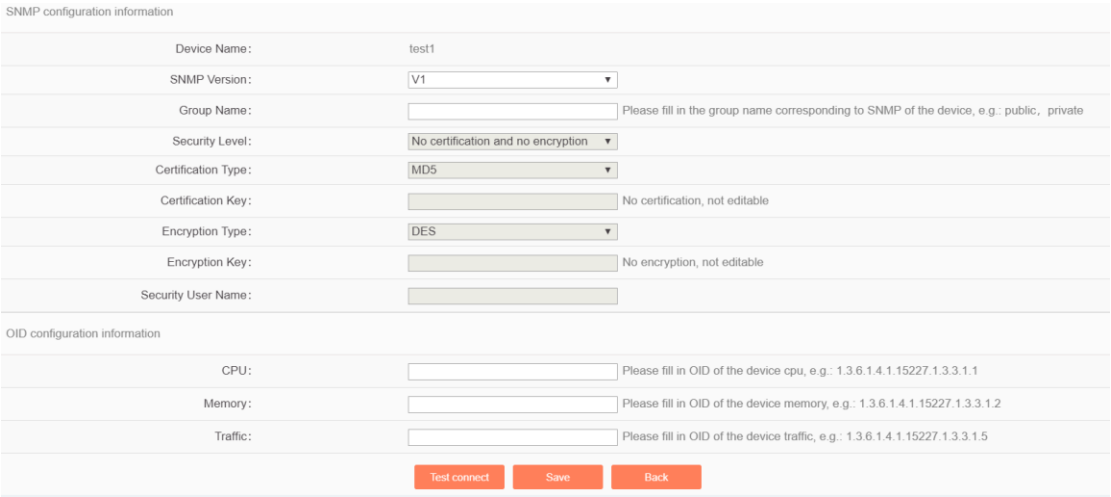


Fig.6-61 SNMP Configuration

6.6.8.2. Check a device.

Click <View> under the operation column of [device management] display list, display the detailed information on the device as shown in the following figure. (As shown in Fig.6-62):

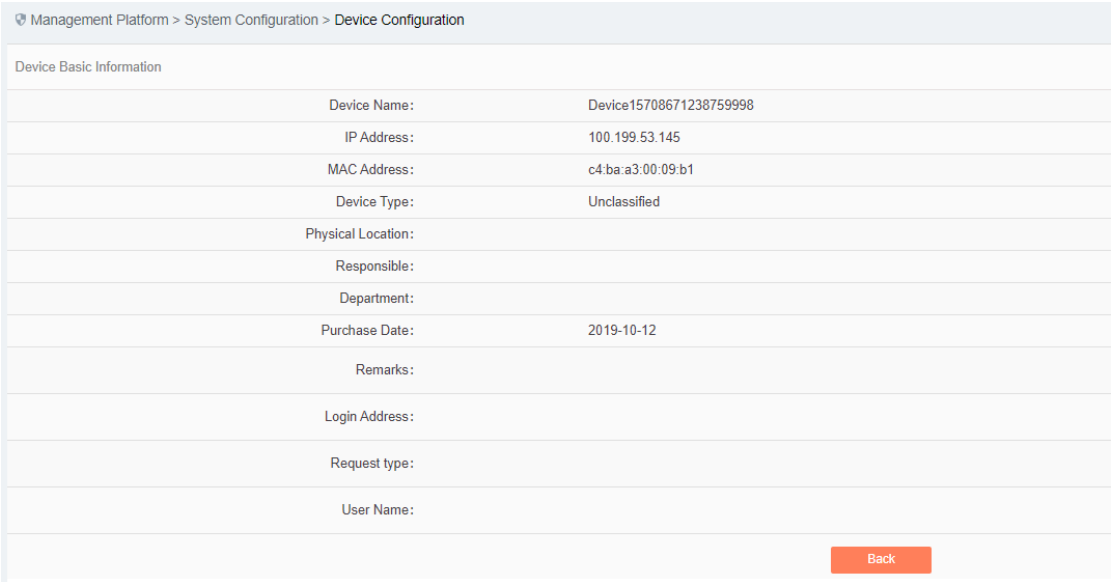


Fig.6-62 Device Information View Page

Click <Back> and go back to the [Device Management] page.

6.6.8.3. Add a device.

Click <Add> on the right side of the [Device Management] device list tab to pop up the device add page. (As shown in Fig.6-63):

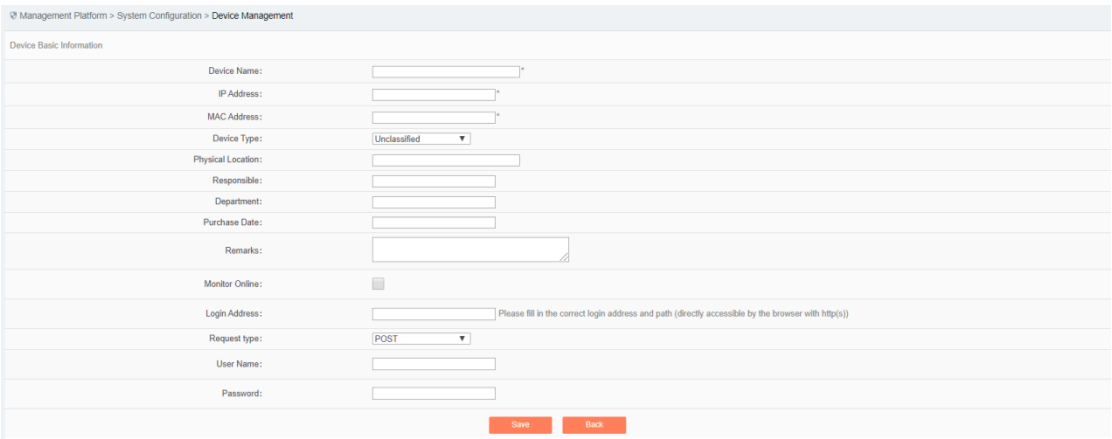


Fig.6-63 Device Add Page

Tab.69 Instruction to Device Add Information

Column Names	Instructions
Device name	A device name that is easy to remember
IP address	The IP address assigned by the device, in dotted decimal format
Device type	The purpose classification of the device, such as workstation and controller, etc.
Remarks	Optional, additional explanatory information

6.6.8.4. Modify a device.

Click <Modify> under the operation column in the [Device Management] device list, open the [Device Basic Information] to modify the basic information on the device (as shown in Fig.6-64):

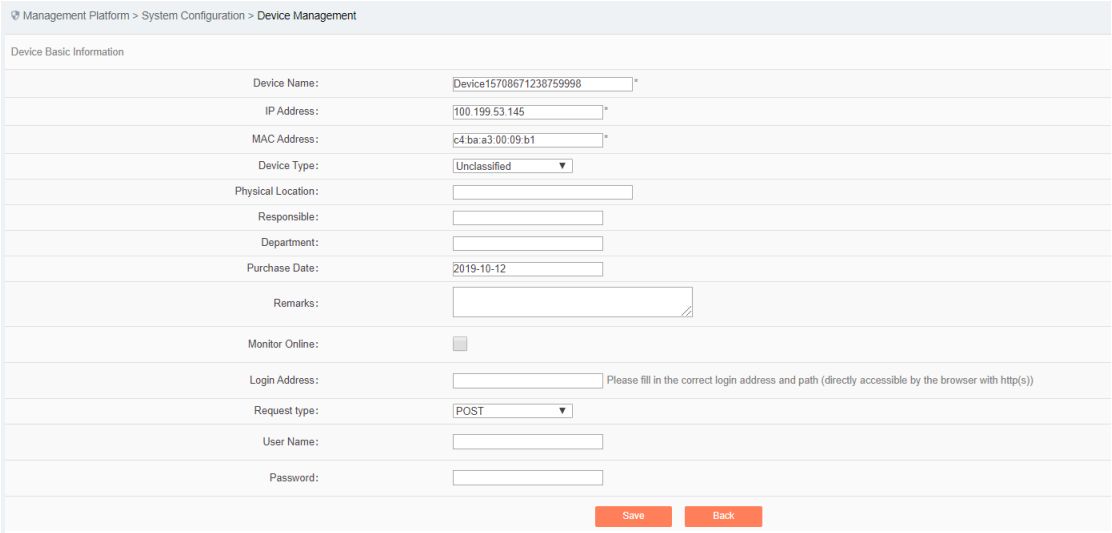


Fig.6-64 Device Basic Information Modification Page

6.6.8.5. Delete a device.

Click <Delete> under the [Device Management] device list operation column, delete devices that are no longer in use.

6.6.8.6. Retrieve a device.

In the [Device Management] device display list page, retrieve a device according to the conditions. (As shown in Fig.6-65):

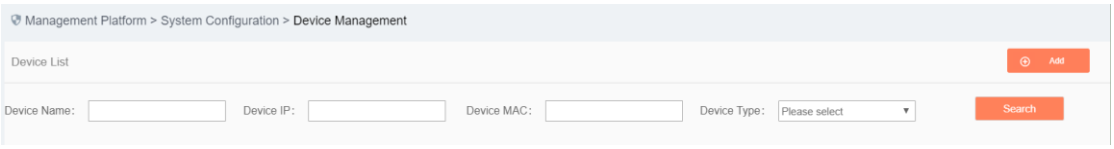


Fig.6-65 Retrieve a Device

6.6.9. Trusted Host

The host accessing to the management platform is limited. In the initial case, any machine can access to the management platform only if it can be connected to the management platform server. Once a trusted host is configured, only machines that are added to the trusted host can access the management platform. The host where the management platform server is located can access to the management platform in any case.

6.6.9.1. Information view

Log in as the configuration administrator, click [System Configuration/Trusted Host] in the left navigation bar (as shown in Fig.6-66), enter the [Trusted Host] page (as shown in Fig.6-67):

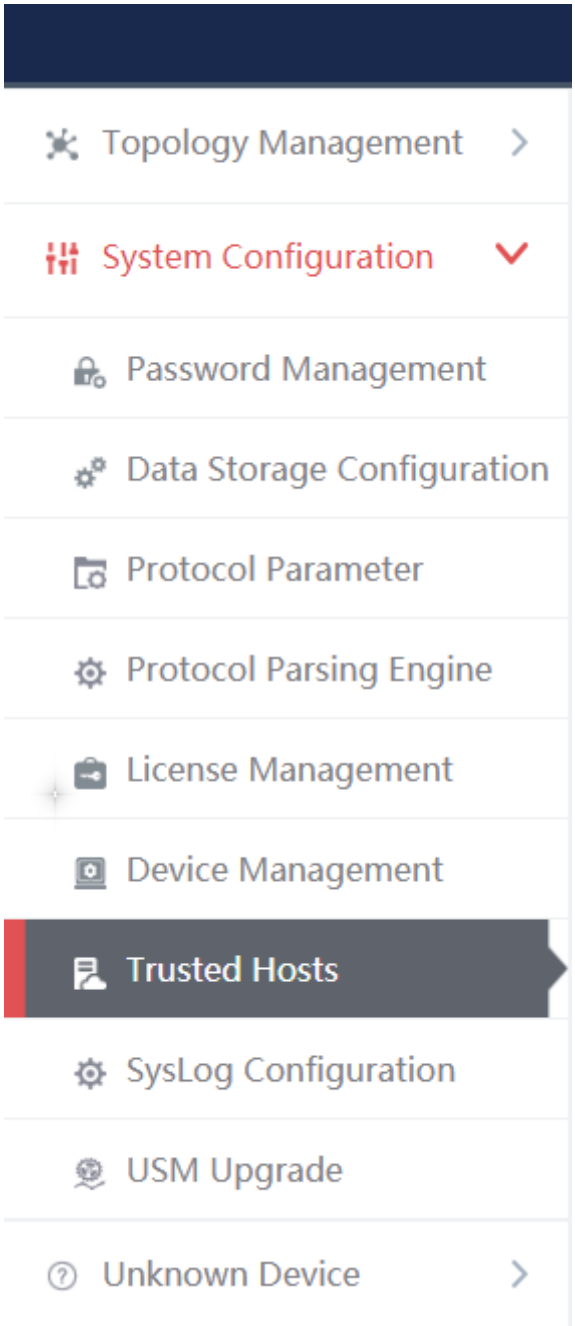


Fig.6-66 Trusted Host Menu

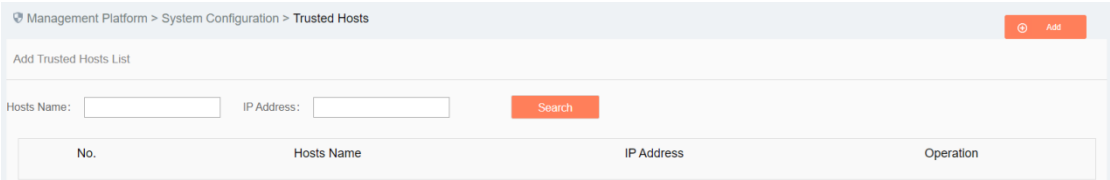


Fig.6-67 Trusted Host List Page

View all the trusted host information of the system here, with the following meanings given:

Table 70 Instruction to Trusted Host List Display

Column Names	Instructions

The host name	A name that is defined by users and easy to remember when being added	
IP address	The IP address of a trusted host, in dotted decimal format	
Operation	View	View more detailed information on the trusted host
	Modify	Modify or reset the trusted host information
	Delete	Delete a trusted host

Click <View> under the operation column in this page, display the detailed information on the trusted host details as shown in the figure below. (As shown in Fig.6-68):

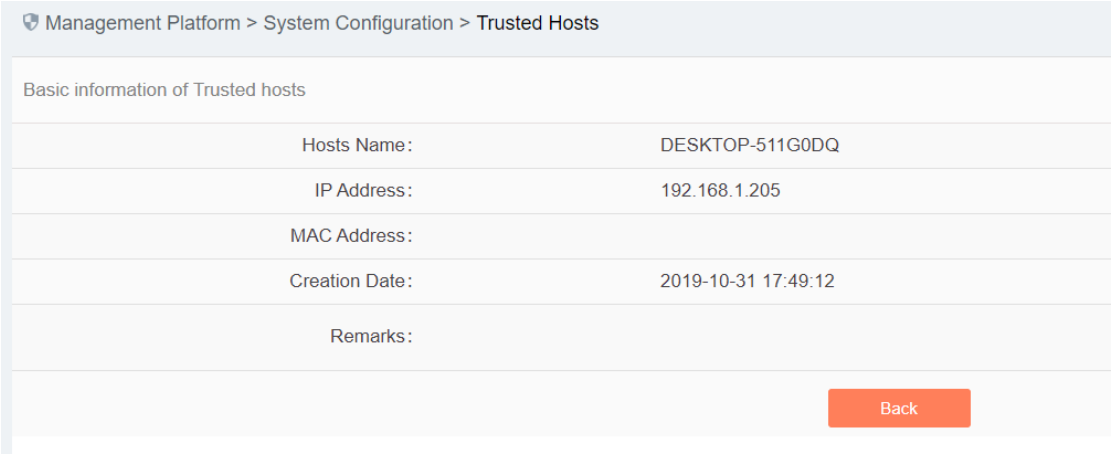


Fig.6-68 Trusted Host Information View Page

Click <Back> and go back to the [Trusted Host] page.

6.6.9.2. Add a host.

Click <Add> on the right side of [System Settings/Trusted Host] trusted host list tab (as shown in Fig.6-69) to pop up the trusted host add page (as shown in Fig.6-70):

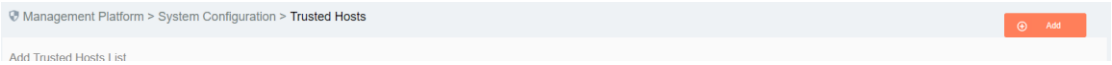


Fig.6-69 Trusted Host Add Button

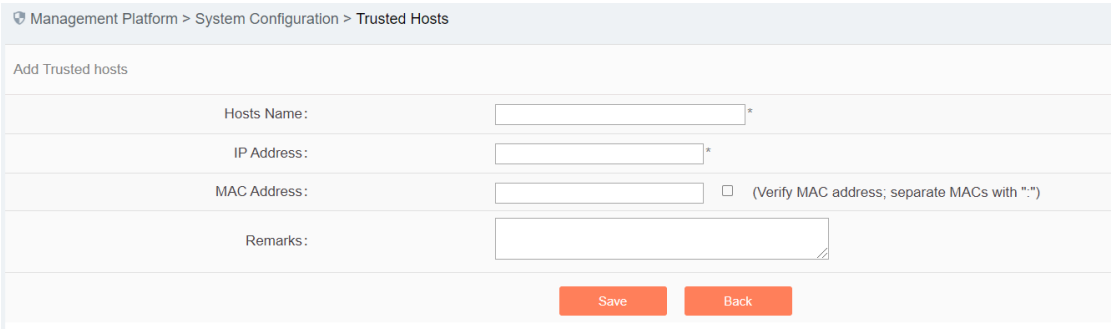


Fig.6-70 Trusted Host Add Page

Tab.71 Instruction to Trusted Host Add Information

Column Names	**Instructions**

The host name	Define a meaningful trusted host name that is easy to understand and remember	
IP address	The IP address assigned by the trusted host, in dotted decimal format	
Remarks	Optional, additional explanatory information	
Operation	Save	Save all modification information to the database and make it come into effect, and go back to the trusted host list display page
	Back	Ignore all modifications and go back to the trusted host list display page

6.6.9.3. Modify trusted host information.

Click <Modify> under the operation column in the [Trusted Host] trusted host list, open the [Trusted Host Basic Information] to modify the basic information on the trusted host (as shown in Fig.6-71):

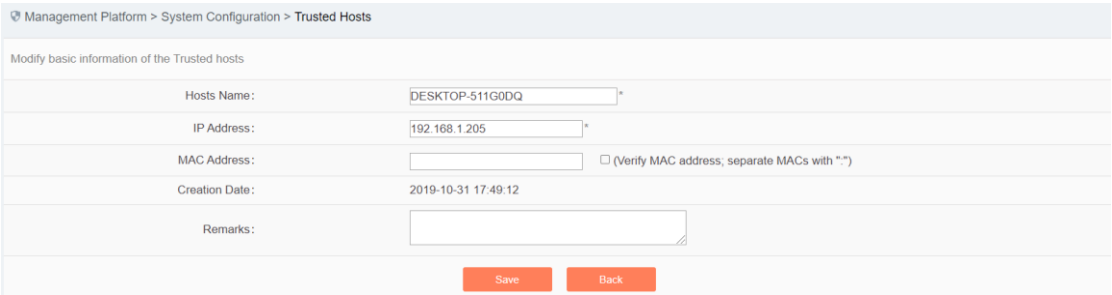


Fig.6-71 Trusted Host Basic Information Modification Page

6.6.9.4. Delete a host.

Click <Delete> under the operation column of [Trusted Host] trusted host list to delete the trusted host that is no longer in use.

6.6.9.5. Retrieve a host.

In the [Trusted Host] trusted host list page, retrieve a trusted host according to the conditions. (As shown in Fig.6-72):

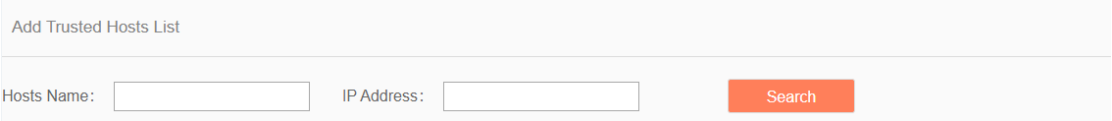


Fig.6-72 Retrieving a Trusted Host

6.6.10. Syslog Configuration

6.6.10.1. Introduction to functions

Configure the IP address and port of syslog server, send the firewall alarm log and the whitelist alarm log that are generated by the industrial firewall device to the syslog server, which are divided into a common type and a grid type.

6.6.10.2. Save and enable the syslog service configuration.

Log in as the configuration administrator, click [System Configuration/syslog Configuration] (as shown in Fig.6-73), enter the syslog configuration page. (As shown in Fig.6-74):

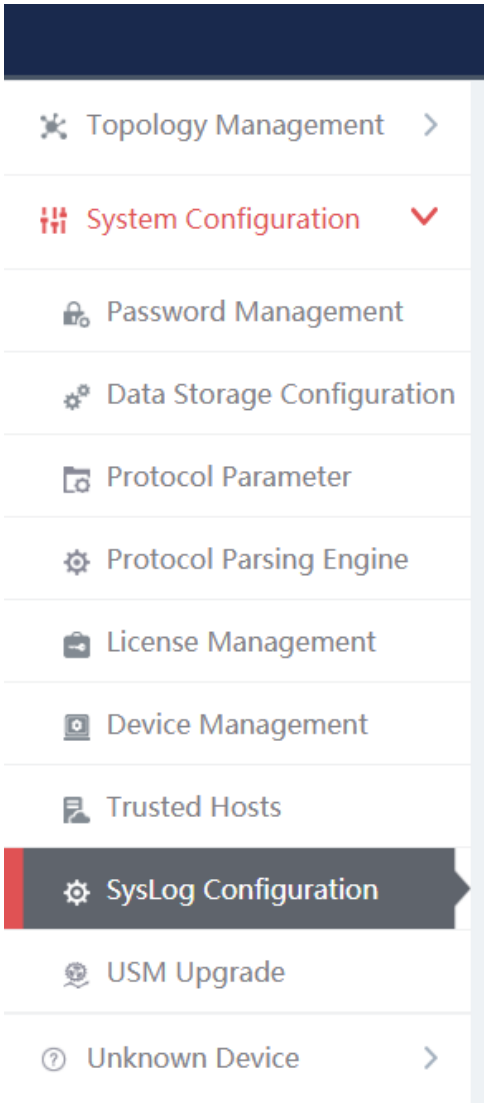


Fig.6-73 Menu

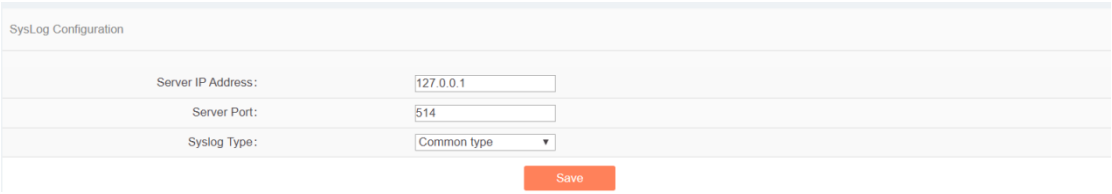


Fig.6-74 syslog Configuration Page

Fill in the IP address and port number, click <Save> to save and enable the syslog service. (As shown in Fig.6-75):

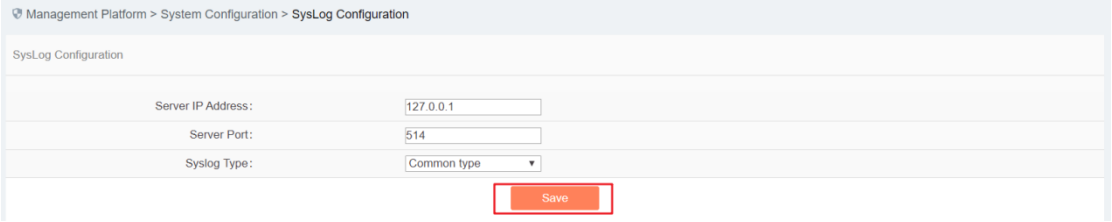


Fig.6-75 Saving the syslog Configuration.

6.6.10.3. Save and enable the grid type syslog service configuration.

Select the grid type through syslog type, which requires a specified elect network card, select the network card and click <Save> to save and enable the syslog service. (As shown in Fig.6-76):

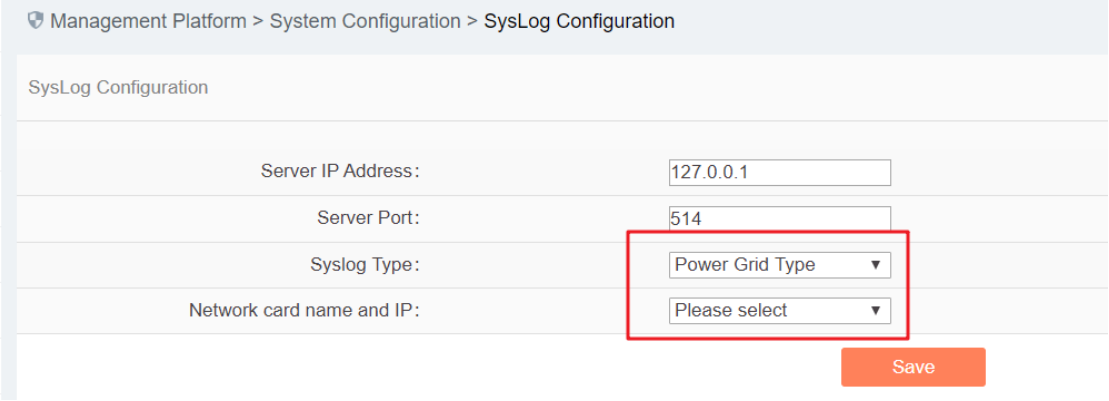


Fig.6-76 Grid Type

6.6.11. Management Platform Upgrade

The management platform upgrades to a new version of management platform functions, skip to the upgrade server for upgrade operation.

6.6.11.1. Management platform upgrade

Log in as the configuration administrator, click [System Configuration/Management Platform Configuration] (as shown in Fig.6-77), enter the management platform upgrade page. (As shown in Fig.6-78):

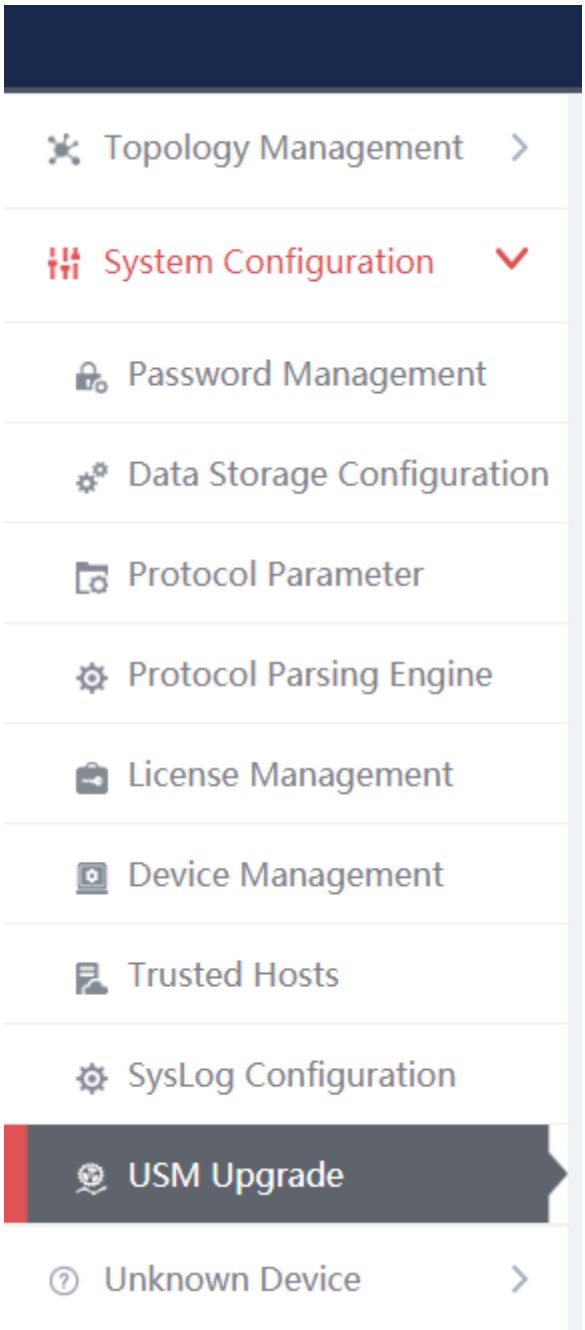


Fig.6-77 Management Platform Upgrade Menu Bar

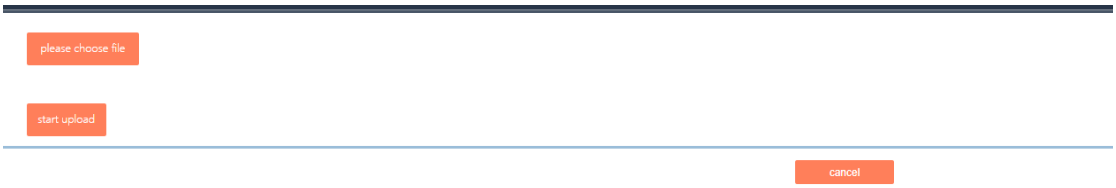


Fig.6-88 Management Platform Upgrade Page

6.6.11.2. **Start upgrade.**

After selecting the upgrade file, click <Start Upload>, check the progress of the progress bar. After successful

upgrade, access to the management platform.
(As shown in Fig.6-89):

Fig.6-89 Start Upgrade

6.7. Topology Management

6.7.1.Introduction to Functions

Network topology management is a basis for the security management of the target system. To clarify the network topology of the customer system can not only find the existing security problems and hidden dangers of the customer system, but also have a very positive and important significance for subsequent security protection.

The management platform provides more professional device management tools and network topology management tools, which can help customers to carry out digital management of the existing device, and also allow customers to create and modify the current network topology of the system very easily.

6.7.2.Topology

The management platform provides a network topology management tool, which can easily form network topology diagram according to the current situation of the user system. Log in as the configuration administrator, display the network topology of the user system by default, click [Topology Management/Topology Management] in the left navigation bar (as shown in Fig.6-90), enter the [Topology Management] page (as shown in Fig.6-91):

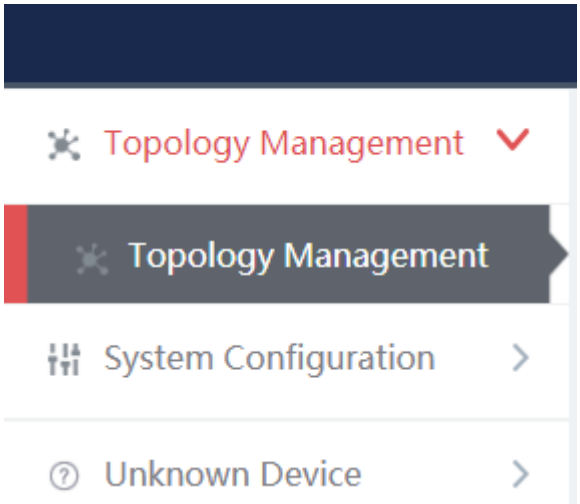


Fig.6-90 Device Management Menu

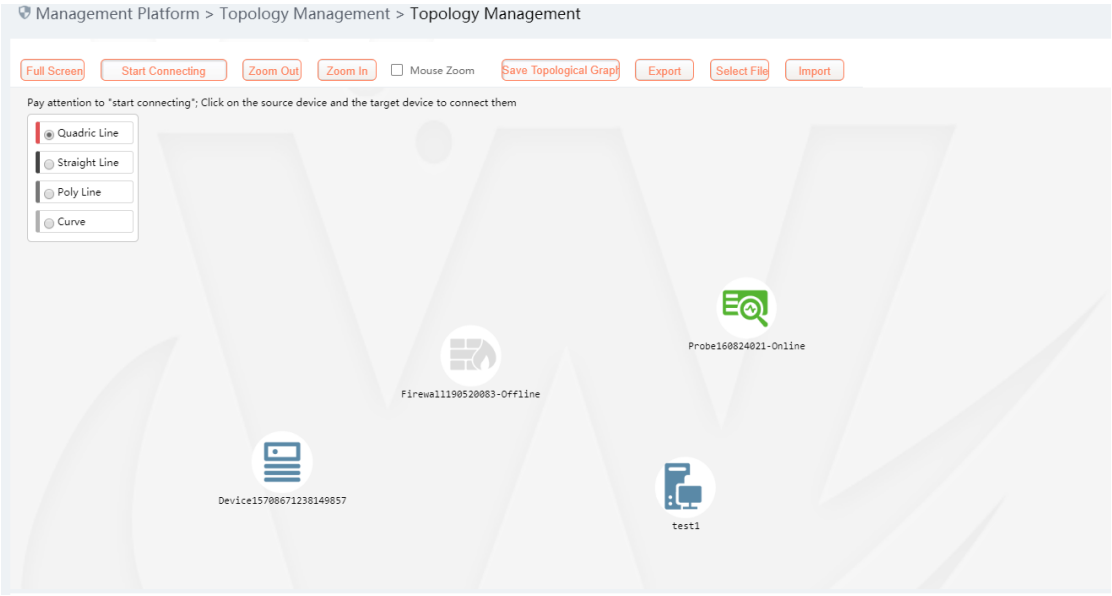


Fig.6-91 Device Management Page

Log in as auditor, display the network topology of the user system by default, click [Topology Management/Topology Management] in the left navigation bar (as shown in Fig.6-92), enter the [Topology Management] page (as shown in Fig.6-93):

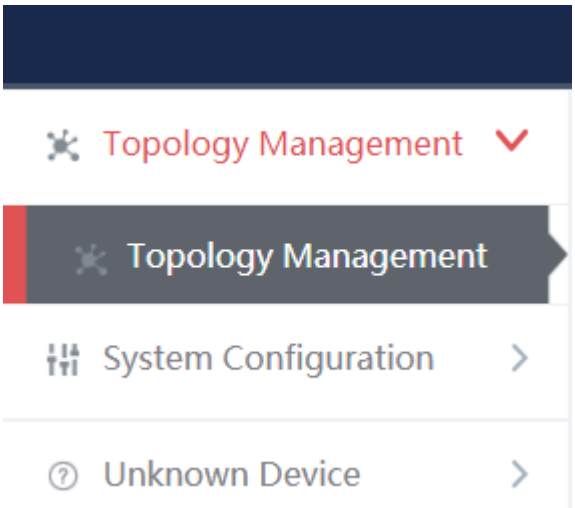


Fig.6-92 Device Management Menu

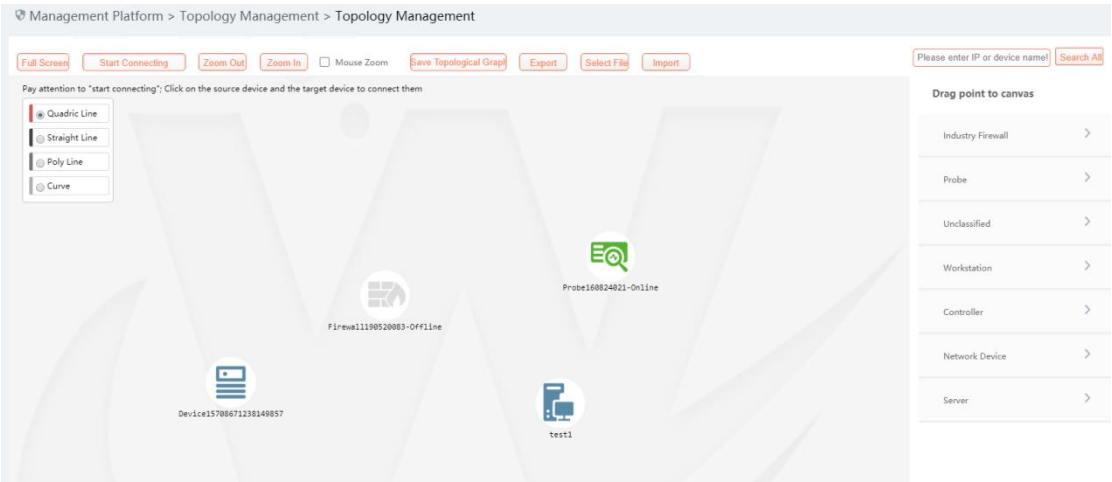


Fig.6-93 Device Management Page

6.7.2.1. Composition of network topology

The network topology of the management platform is mainly composed of devices and lines, with the devices including the following:

- Industrial firewall
- Intelligent monitoring terminal
- Workstation (including IEG)
- Controller
- Network device
- Server
- Unclassified

(As shown in Fig.6-94):

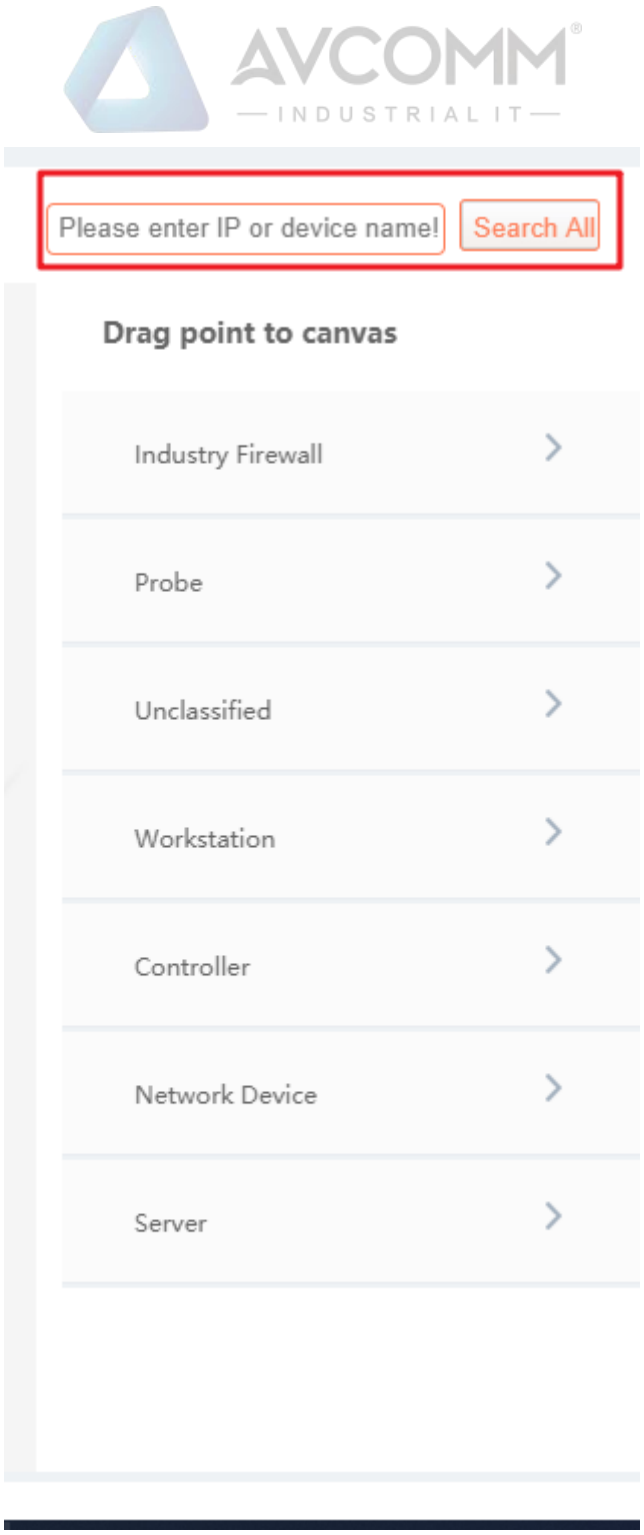


Fig.6-94 Topology Device List

6.7.2.2. Network topology device query

Query the device that meets the requirements according to the conditions, click <Search All> to execute the query (as shown in Fig.6-95):

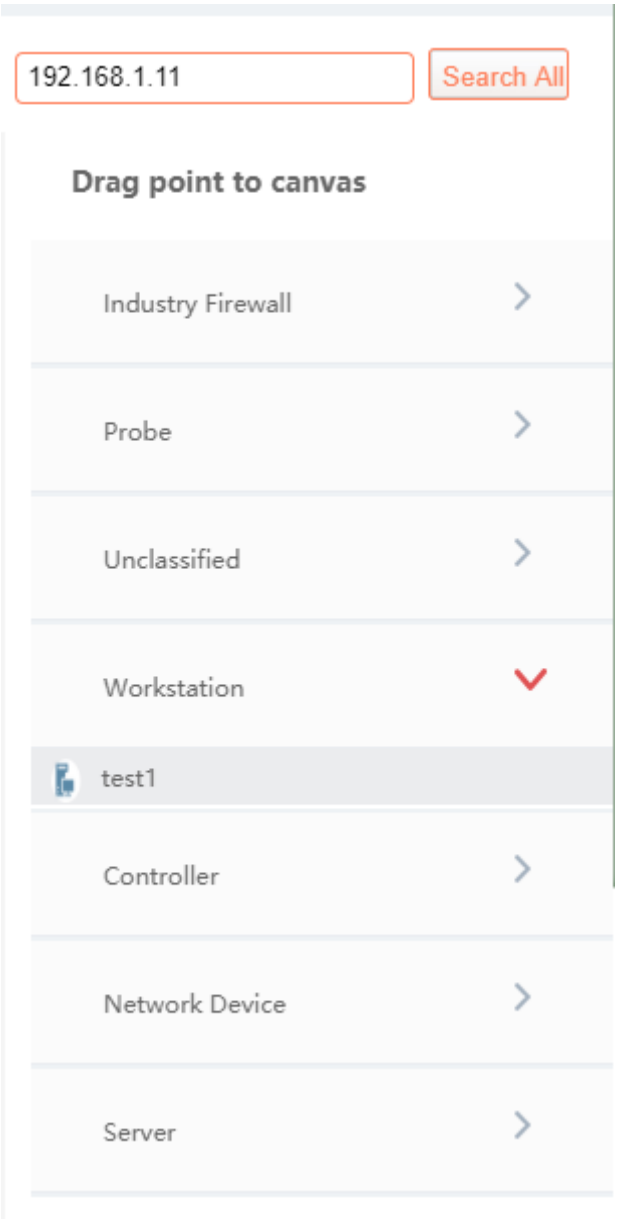


Fig.6-95 Query Results

6.7.2.3. Edit a network topology.

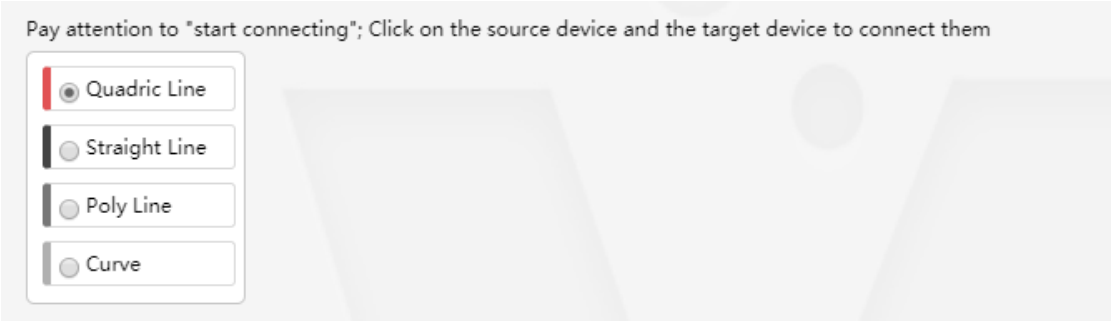
It is very convenient to edit the topology.

- **For the device**

The user only needs to find the device to be added into the topology on the right device tree, click the small icon on the left of the device and drag it into the canvas to complete the addition of the device.

- **For the connector**

The user first selects the type of lines. Currently, there are the following types of connection lines:



Select the type of connecting wire, click < Start Connection> above the topology as shown in: Start Connecting , then move to the canvas, click the mouse successively on the two devices to be wired to complete the addition of the line.

The topology also supports zoom in and zoom out, not only support zoom by clicking, as shown in: Zoom Out Zoom In , but also supports zoom by mouse wheel: Mouse Zoom .

After editing the topology, the user clicks <Save Topology>, as shown: Save Topological Graph to complete the saving of the topology. The topology information can be normally viewed when logging in next time.

6.7.2.4. Topology linkage

Topology management can not only view the network topology of the user system, but also view the number of alarms currently generated on the industrial firewall. Right-click and select View in the pop-up menu to view the detailed information on the device.

Right click on any device in the topology and click <Delete> in the pop-up menu to delete the device from the topology, with the corresponding connecting line deleted at the same time. Or right click on the connecting line, select <Delete> to delete the corresponding connecting line.

6.8. Unknown Device Detection

6.8.1. Unknown Device Detection Configuration

Log in as the configuration administrator, click [Unknown Device Detection/Unknown Device Detection Configuration] in the left navigation bar (as shown in Fig.6-96), enter the [Unknown Device Configuration] page (as shown in Fig.6-97):

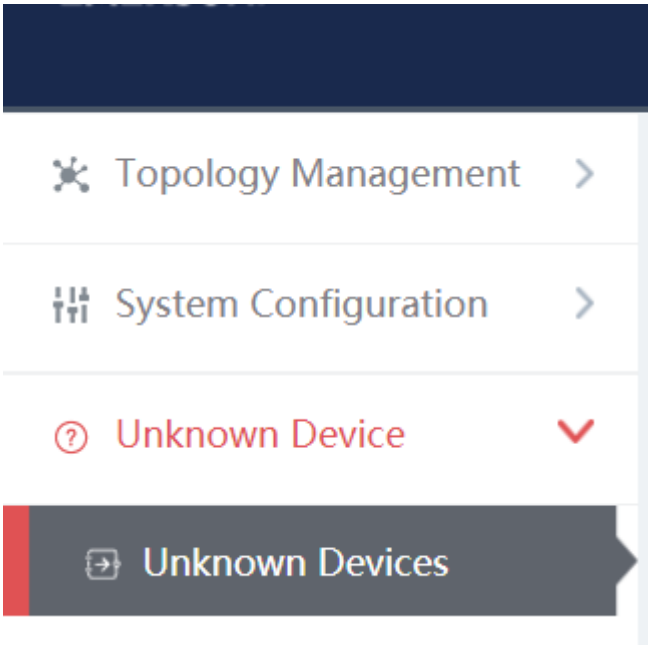
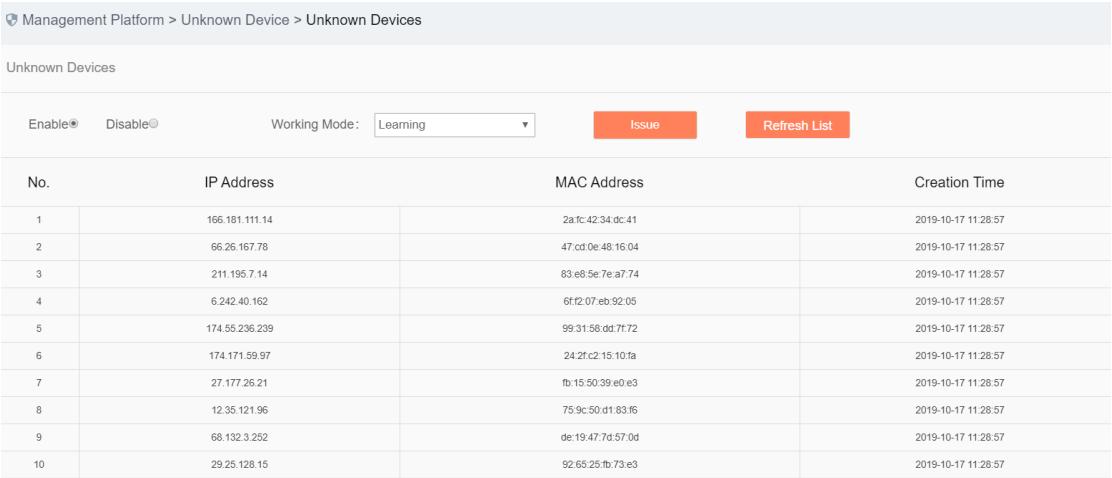


Fig.6-96 Unknown Device Detection Configuration Menu Bar



No.	IP Address	MAC Address	Creation Time
1	166.181.111.14	2a:fc:42:34:dc:41	2019-10-17 11:28:57
2	66.26.167.78	47:cd:0e:48:16:04	2019-10-17 11:28:57
3	211.195.7.14	83:e8:5e:7e:a7:74	2019-10-17 11:28:57
4	6.242.40.162	6f:f2:07:eb:92:05	2019-10-17 11:28:57
5	174.55.236.239	99:31:58:dd:7f:72	2019-10-17 11:28:57
6	174.171.59.97	24:2f:c2:15:10:fa	2019-10-17 11:28:57
7	27.177.26.21	fb:15:50:39:e0:e3	2019-10-17 11:28:57
8	12.35.121.96	75:9c:50:d1:83:f6	2019-10-17 11:28:57
9	68.132.3.252	de:19:47:7d:57:0d	2019-10-17 11:28:57
10	29.25.128.15	92:65:25:fb:73:e3	2019-10-17 11:28:57

Fig.6-97 Unknown Device Detection Configuration Page

6.8.1.1. **Distribute the configuration.**

Unknown device detection can be enabled or disabled. The working status must be selected after being enabled, which includes Learning, Detecting.

When selecting Learning, click <Distribute the Configuration> to generate the learning data, click <Refresh a List> to view the learned learning data. (As shown in Fig.6-98):

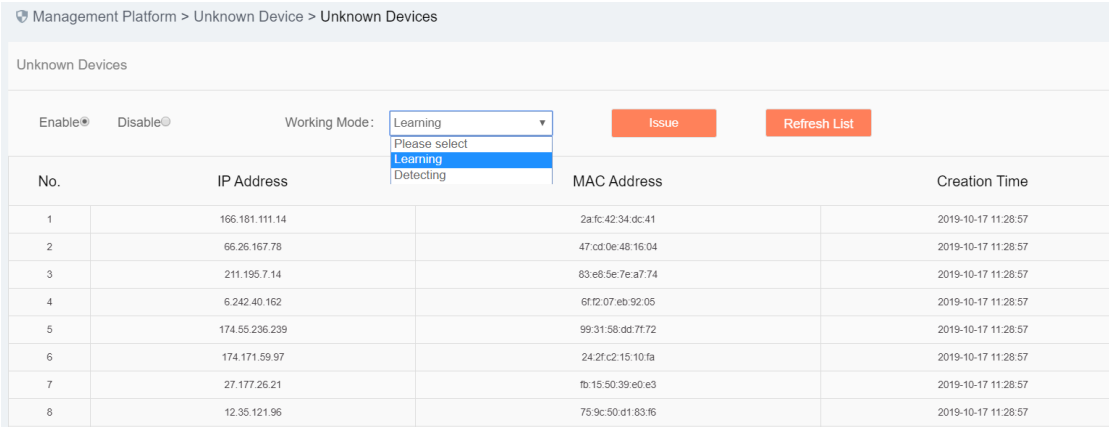


Fig.6-98 Learning

Switch Learning to Detecting, click <Distribute the Configuration>, add the learnt data to the rule table. (As shown in Fig.6-99):

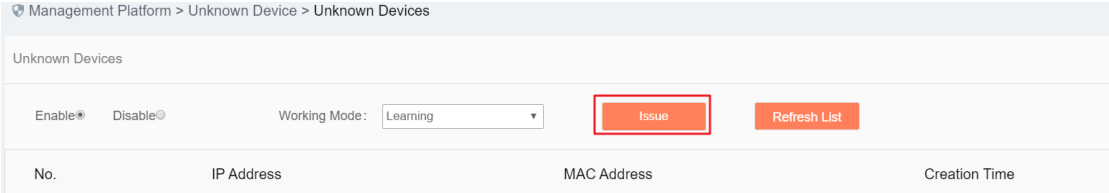


Fig.6-99 Detecting

Rule Edit

Click <Edit a Rule> and skip to the rule edit page. (As shown in Fig.6-100):

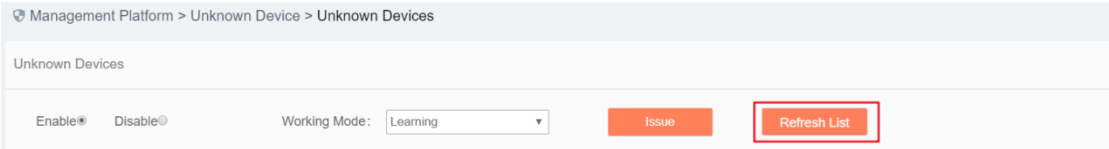


Fig.6-100 Rule Editing

Edit the rules in the rule page, click <Save> to save the edited results. (As shown in Fig.6-101):

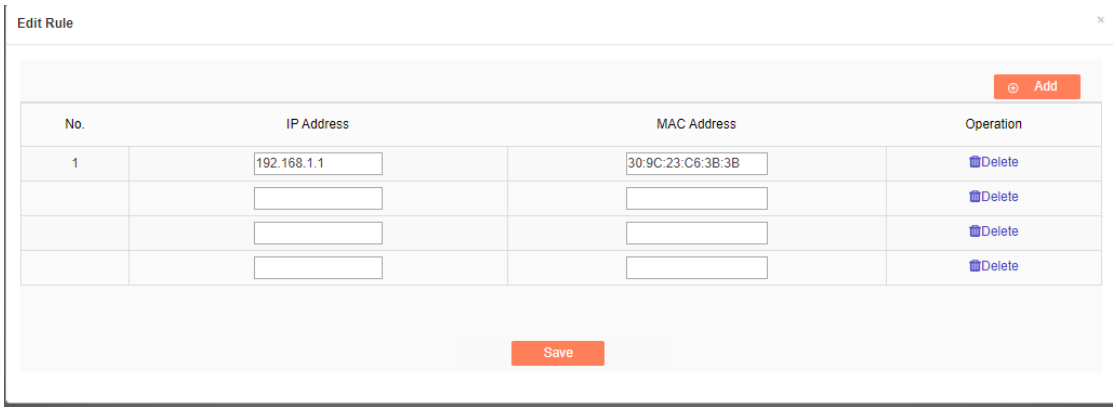


Fig.6-101 Saving a Rule

Unknown device detection log

Log in as auditor, click [Unknown Device Detection/Unknown Device Detection Logs] in the left navigation bar (as shown in Fig.6-102), enter the [Unknown Device Detection Logs] page (as shown in Fig.6-103):

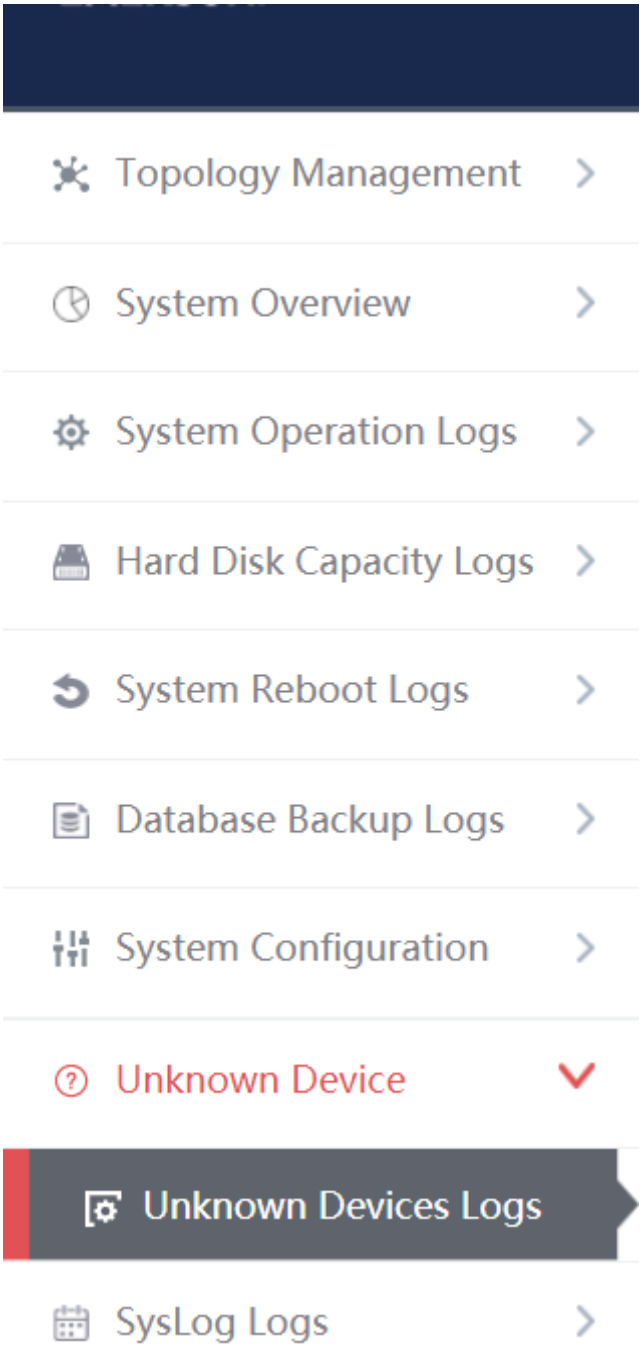


Fig.6-102 Unknown Device Detection Log Menu Bar

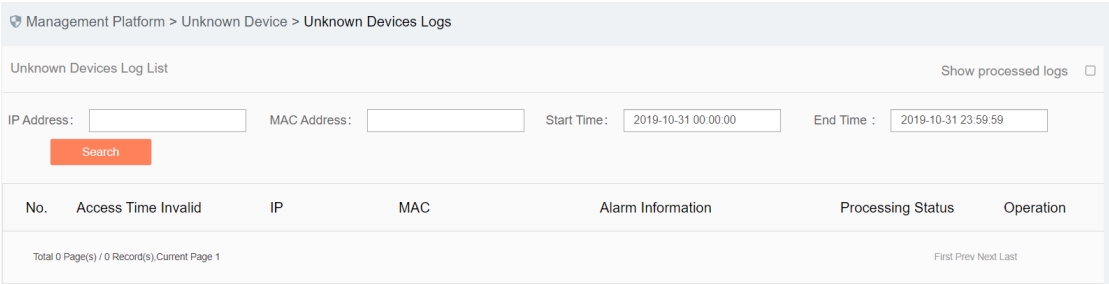


Fig.6-103 Unknown Device Detection Log Page

Log list

View all the log information on unknown device detection alarms here, with the meaning given below:

Tab.72 Instruction to Industrial Protocol Detection Alarm Display

Column Names	Instructions	
IP	The IP address of the device generating an alarm	
MAC	The MAC address of the device generating an alarm	
Alarm information	Alarm details	
Processing status	Whether to process an alarm	
Illegal access time	Log generation time	
Operation	Processing	Further processing of alarm information

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed.

Check <Show Processed Logs> on the right side of the [Unknown Device Detection Logs] protocol detection alarm list tab, view the processed log. (As shown in Fig.6-104):

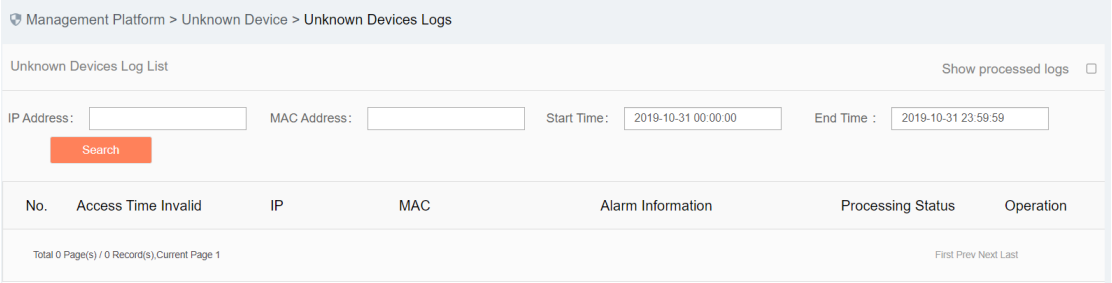


Fig.6-104 Show Processed Unknown Device Detection Log List Page

6.8.1.2. **Process a log.**

Click <Process> under the operation column in the [Unknown Device Detection Logs] display list, display (as shown in Fig.6-105) the [Unknown Device Detection Logs] processing page:

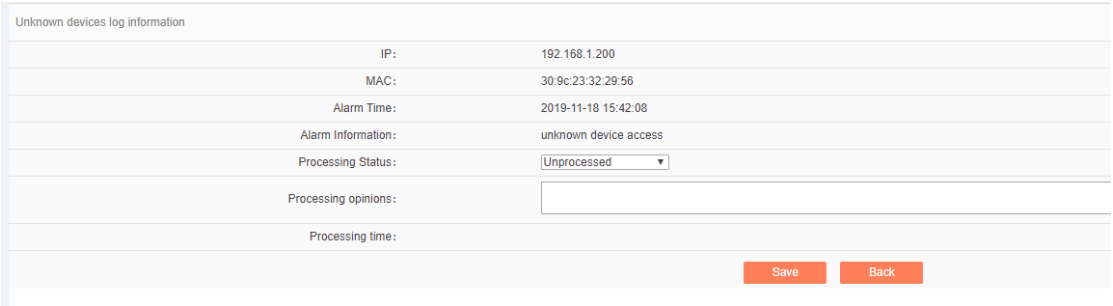


Fig.6-105 Unknown Device Detection Log Processing Page

Click the drop-down box of processing status, select "Close", fill in the relevant opinions in the processing opinions and click "Save" to complete the processing of alarm information. In this case, such a log will no longer be seen in the list of the [Unknown Device Detection Logs] page by default.

Or do not select "Close" but fill in the processing opinions instead.

6.8.1.3. **Retrieve a log.**

On the [Unknown Device Detection Logs] list page, retrieve an alarm based on the conditions. (As shown in Fig.6-106):

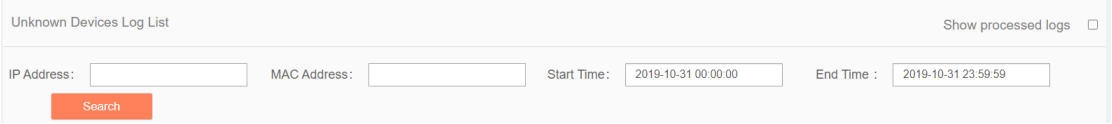


Fig.6-106 Retrieving an Unknown Device Detection Log

6.9. **Syslog Log**

Receive the syslog logs reported from other devices, click [Syslog Logs/Syslog Logs] in the left navigation bar (as shown in Fig.6-107), enter the [Syslog Logs] page (as shown in Fig.6-108):

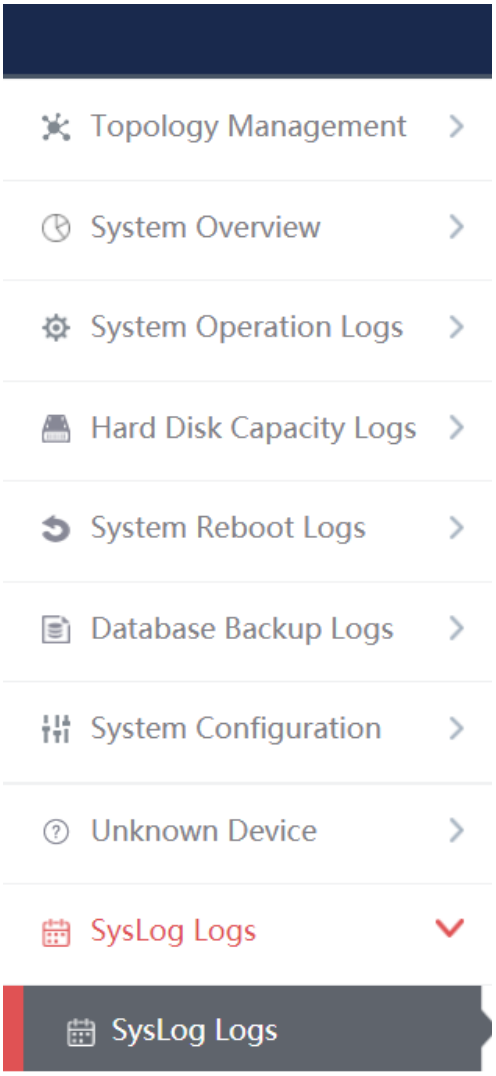


Fig.6-107 syslog Log Menu

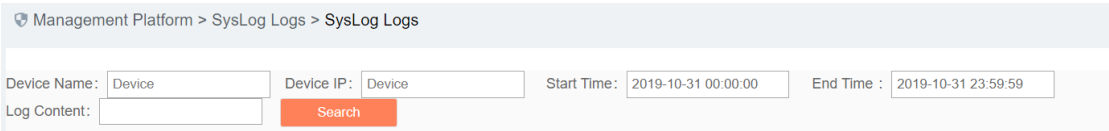


Fig.6-108 syslog Log

6.9.1.**Retrieve a Log**

In the [Syslog Logs] list page, retrieve the log according to the conditions. (As shown in Fig.6-109):

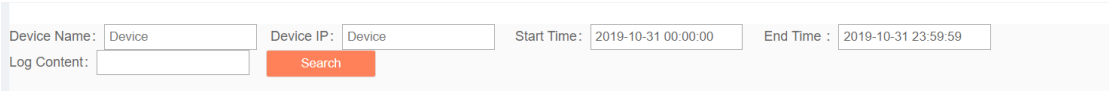


Fig.6-109 Log Query