AVCOMM Firewall S2100

User Manual

AVCOMM Technologies Inc.

Firewall S2100

User Manual

Copyright Notice

About This Manual

This user manual is intended to guide a professional installer to install and configure the Firewall. 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 firewall.

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.

Table of Contents

1. Overview of Firewall

1.1. Product Description

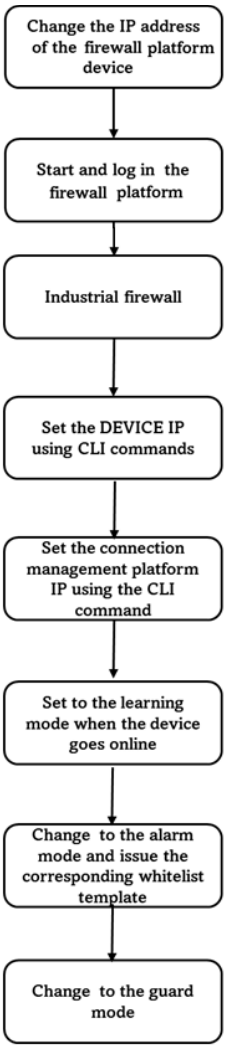
The Avcomm firewall platform can carry out management of industrial firewalls, able to provide Web management to the outside.

The administrator can manage Avcomm firewall via the Web management interface, including to:

- View the current working status of the installed industrial firewall.
- 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.
- Configure system-related database backup policy, trusted host and management users.

1.2. Operating Steps

The process flow chart for the firewall, briefly introduces the basic operating steps for the industrial firewall.


Change the IP address of the firewall platform device
Start and log in the firewall platform
Industrial firewall
Set the DEVICE IP using CLI commands
Set the connection management platform IP using the CLI command
Set to the learning mode when the device goes online
Change to the alarm mode and issue the corresponding whitelist template
Change to the guard mode

1.3. 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 and system configuration. During configuration, you can seek the online help from www.avcomm.us. 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, as well as system configuration & management, please read the Manual carefully.

1.4. How to Use the Manual

The Manual mainly give a detailed description of industrial firewalls and system configuration as much as possible.

For more information, please visit: www.avcomm.us.

1.5. 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 Firewall Platform

2.1. Start the Firewall Platform

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

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

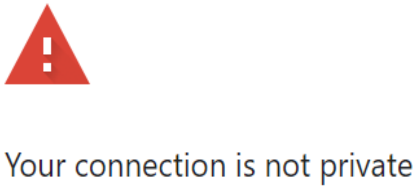
https://192.168.8.8:8440 (new version) or

http://192.168.8.8:8080 (old version)

to access to the firewall 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) ".



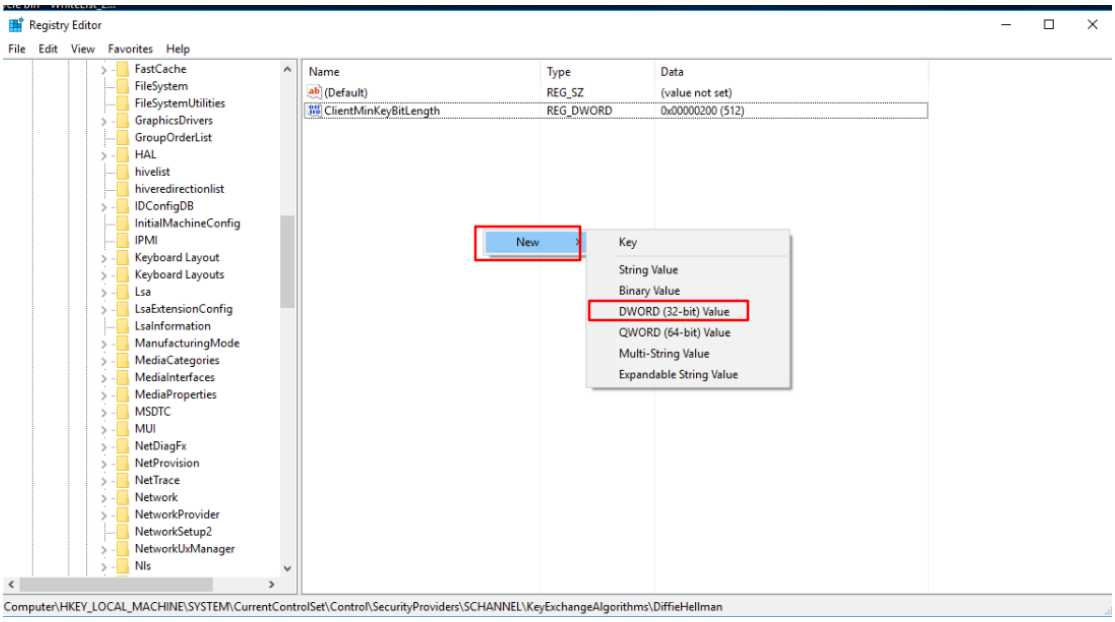
Your connection is not private

🕮 **Description:**

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

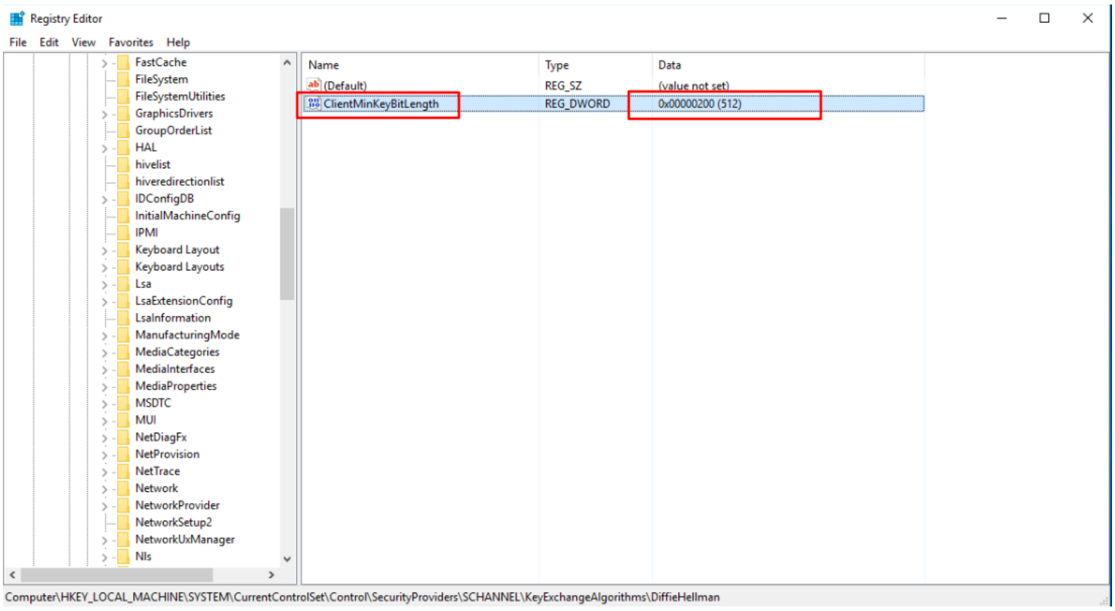
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
ClientMinKeyBitLength	REG_DWORD	0x00000200 (512)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\DiffieHellman



FastCache
FileSystem
FileSystemUtilities
GraphicsDrivers
GroupOrderList
HAL
hivelist
hiveredirectionlist
IDConfigDB
InitialMachineConfig
IPMI
Keyboard Layout
Keyboard Layouts
Lsa
LsaExtensionConfig
LsaInformation
ManufacturingMode
MediaCategories
MediaInterfaces
MediaProperties
MSDTC
MUI
NetDiagFx
NetProvision
NetTrace
Network
NetworkProvider
NetworkSetup2
NetworkUxManager
Nls

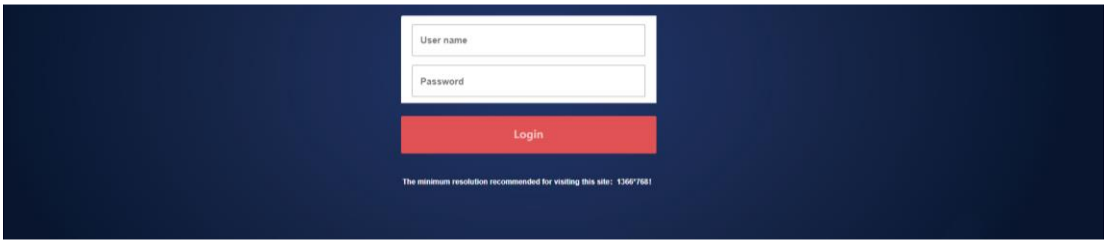
Name	Type	Data
(Default)	REG_SZ	(value not set)
ClientMinKeyBitLength	REG_DWORD	0x00000200 (512)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\DiffieHellman

2.2. Log in the Firewall Platform

2.2.1. Normal Login

After the startup of the firewall platform, enter the correct page address of the firewall 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.



The minimum resolution recommended for visiting this site: 1366*768!

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

Currently, the firewall platform supports users with three roles. If it is the first time to log in the 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.

2.2.2. Two-Factor Authentication Login

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

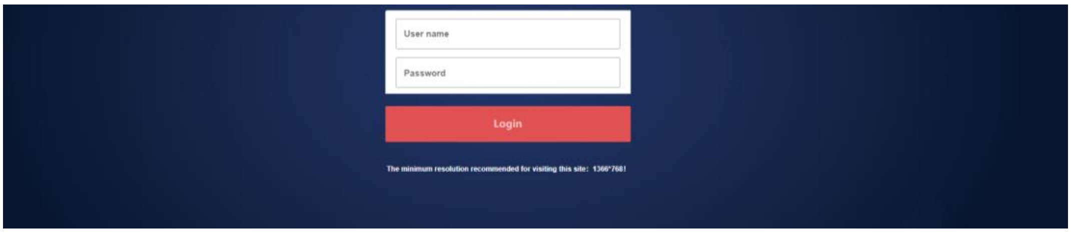

User name
Password
Login
The minimum resolution recommended for visiting this site: 1366*768!

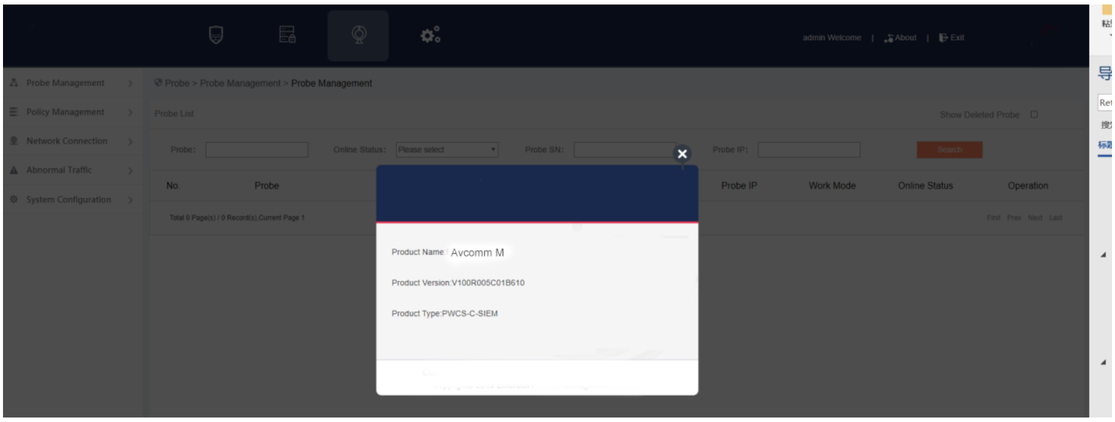
Fig.2-2 Page after the Startup of the Firewall Platform after Having Connected the USBKey

If the user hasn't 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 Firewall Platform Version

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



Product Name: Avcomm M

Product Version:V100R005C01B610

Product Type:PWCS-C-SIEM

Fig.2-3 Version Information on firewall Platform

2.4. Exit the Firewall Platform

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

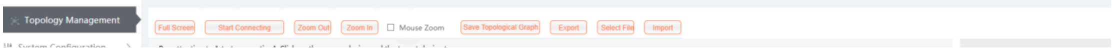


Fig.2-4 Firewall platform exit

3. Industrial Firewall

3.1. Introduction to Products

3.1.1. Product Overview

Designed for industrial systems, Avcomm Industrial Firewall S2100 provides efficient security solutions for industrial control networks, with comprehensive security functions such as industrial Ethernet protocol depth analysis, instruction access control, and log auditing. S2100 uses high-performance, high-stability multi-core hardware architecture to provide users with efficient and stable security guarantees. S2100 can intelligently identify all external attacks in industrial communication, and warn and block it at the first time, protecting industrial information networks against various network attack methods such as source address spoofing, DOS attacks, address scanning, viruses, and Trojans. This product has a sales license.

3.1.2. Appearance and Description

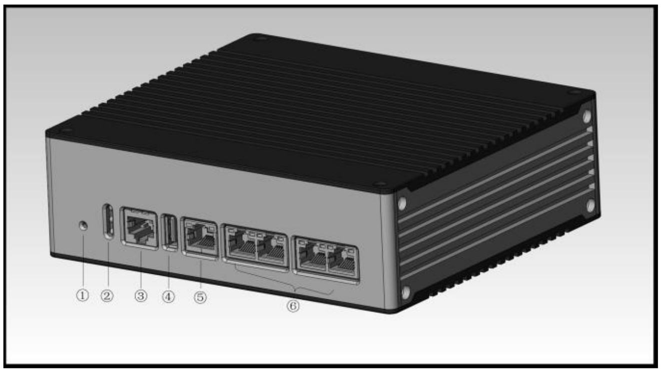


Fig.3-1 Appearance of S2100

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

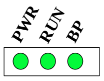


Fig.3-2 Indicator Lights

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	**S2100**
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, 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

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
Memory	DDR3 1G
Log storage	4G
Business port	4 ports, RJ45 10/100/1000 Mbps adaptive
Bypass	2 pairs
Management port	1 port 10/100/1000 Mbps adaptive
Serial interface	RJ45 debugging port
USB interface	1 port, USB 2.0
Dimensions/power supply/operating environment	
Working environment	Temperature: -40 ~ 75℃ Humidity: 5%-95%, no condensation
Storage environment	Temperature: -40 ~ 85℃ Humidity: 5%-95%, no condensation
MTBF	250,000 hours
Power supply	12-36V DC 1+1 redundant power supply
Peak power	<7W
Dimensions (WxDxH) mm	168 x 118 x 58
Installation method	35mm standard DIN rail clamping
Protection grade	IP40
Authentication	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.

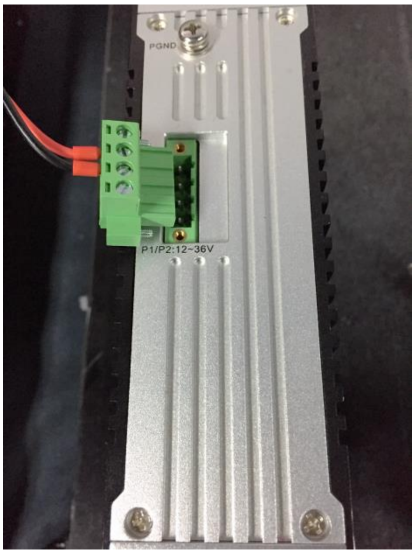


Fig.3-3 Powering on Industrial Firewall by Using Power Cord Supplied

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.

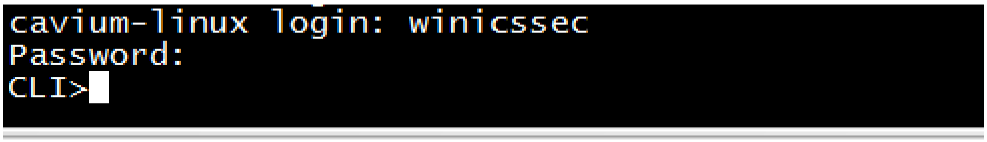
The industrial firewall shall be connected to the firewall platform to go online normally before it can be configured. Please insert the network cable into the MGMT port when connecting the firewall platform. The default IP address of all industrial firewalls is set to 192.168.8.6 when leaving the factory, which can be changed to the MGMT port address of the industrial firewall before or after connecting to the network for the firewall platform. Before the firewall 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 firewall 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 Firewall Platform Address when setting the firewall 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, 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 firewall 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.



```
cavium-linux login: winicssec
Password:
CLI>
```

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 firewall platform

CLI>show serverip

Check the IP address of the firewall platform as configured in the industrial firewall

CLI#set serverip <IPV4ADDR: serverip>

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

For example: the address of the firewall 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 firewall 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 firewall 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 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):

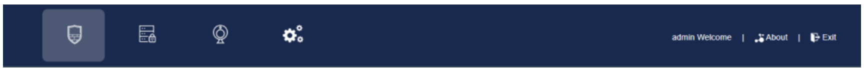


Fig.3-5 Industrial Firewall in Upper Menu Bar

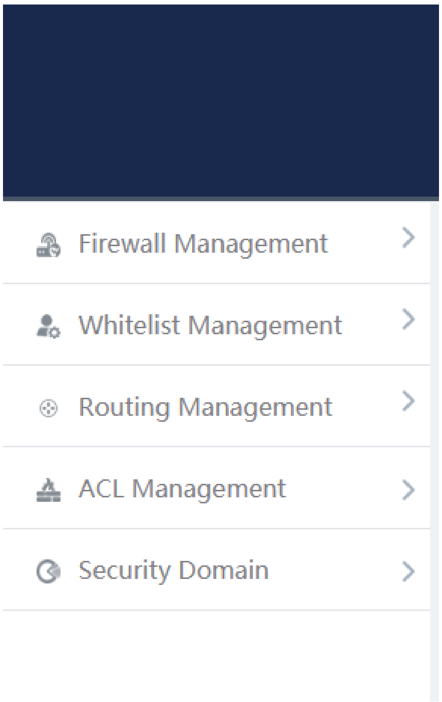
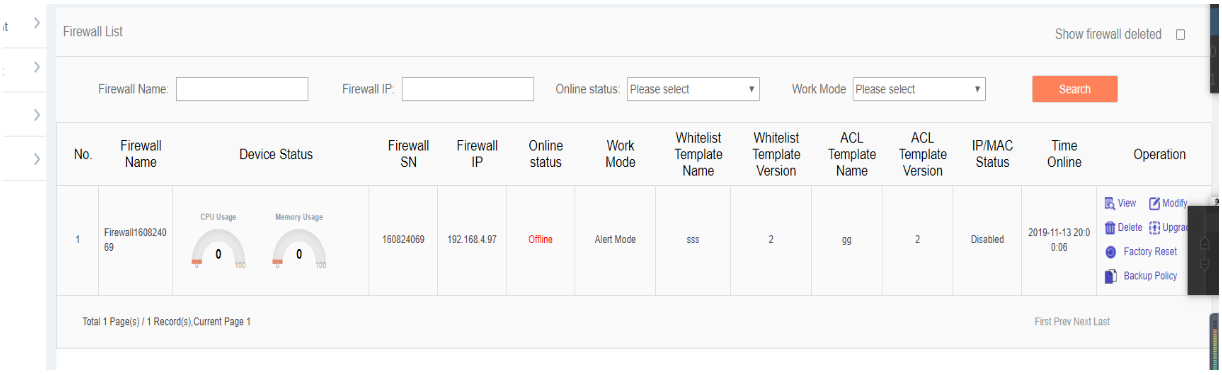


Fig.3-6 Firewall Management in Navigation Bar



Firewall List

Show firewall deleted □

Firewall Name: Firewall IP: Online status: Please select ▾ Work Mode Please select ▾ Search

No.	Firewall Name	Device Status	Firewall SN	Firewall IP	Online status	Work Mode	Whitelist Template Name	Whitelist Template Version	ACL Template Name	ACL Template Version	IP/MAC Status	Time Online	Operation
1	Firewall160824069	CPU Usage 0 Memory Usage 0	160824069	192.168.4.97	Offline	Alert Mode	sss	2	gg	2	Disabled	2019-11-13 20:00:06	View Modify Delete Upgra Factory Reset Backup Policy

Total 1 Page(s) / 1 Record(s),Current Page 1

First Prev Next Last

Fig.3-7 Firewall Management Display Page

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

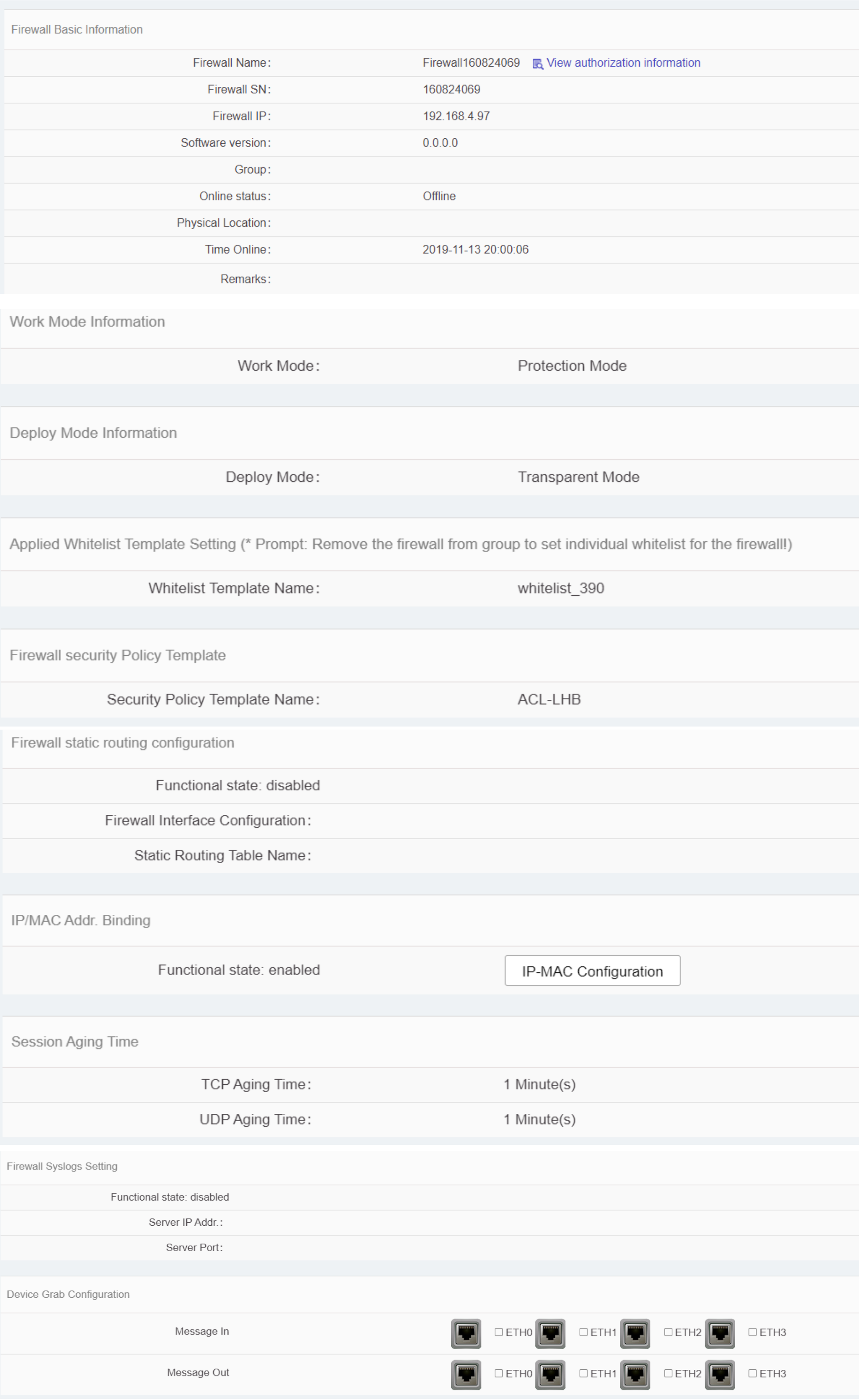
Tab.3 Instruction to Firewall Management List Display

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 firewall 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 ACL Template Name	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 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	View more detailed information on industrial firewalls, view the authorized function of each industrial firewall under the sub-page
	Modify Modify	Modify and set the information, operation mode, whitelist template and security policy rules, etc. of industrial firewall
	Delete 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	Upgrade the software running on the industrial firewall online. Only when the industrial firewall is online can this operation be carried out, refer to Section 3.3.4 Firewall Upgrade
	Restore the factory settings Factory Res	One-key reset the factory settings of fire walls devices
	Back up all policy applications Backup F	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 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)

Firewall Syslogs Setting

Functional state: disabled

Server IP Addr.:

Server Port:

Device Grab Configuration

Message In	□ ETH0 □ ETH1 □ ETH2 □ ETH3
Message Out	□ ETH0 □ ETH1 □ ETH2 □ ETH3

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):

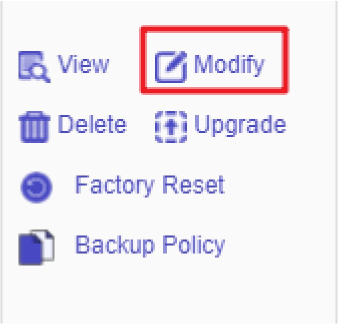
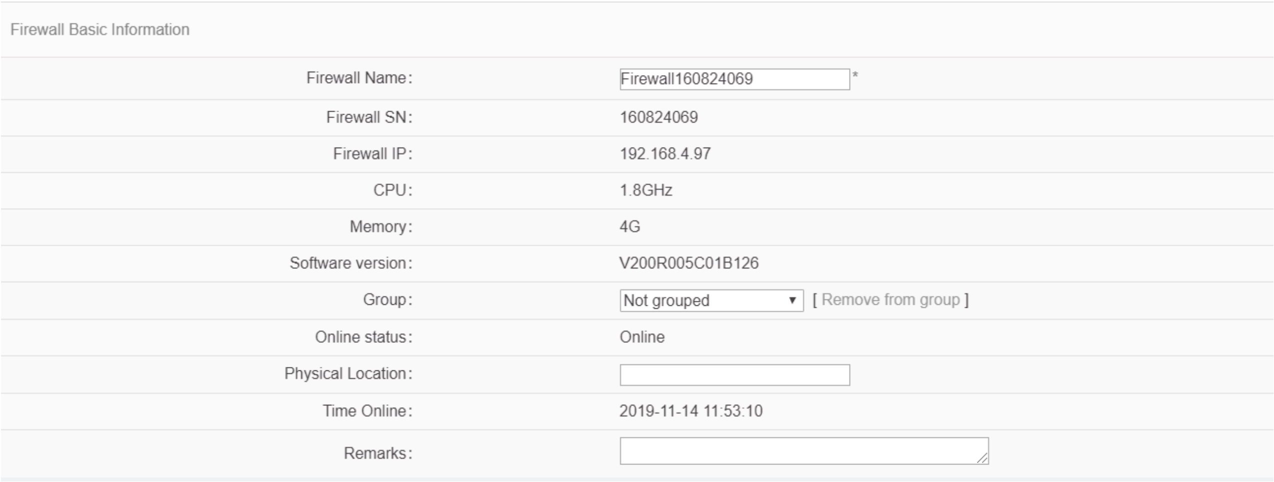
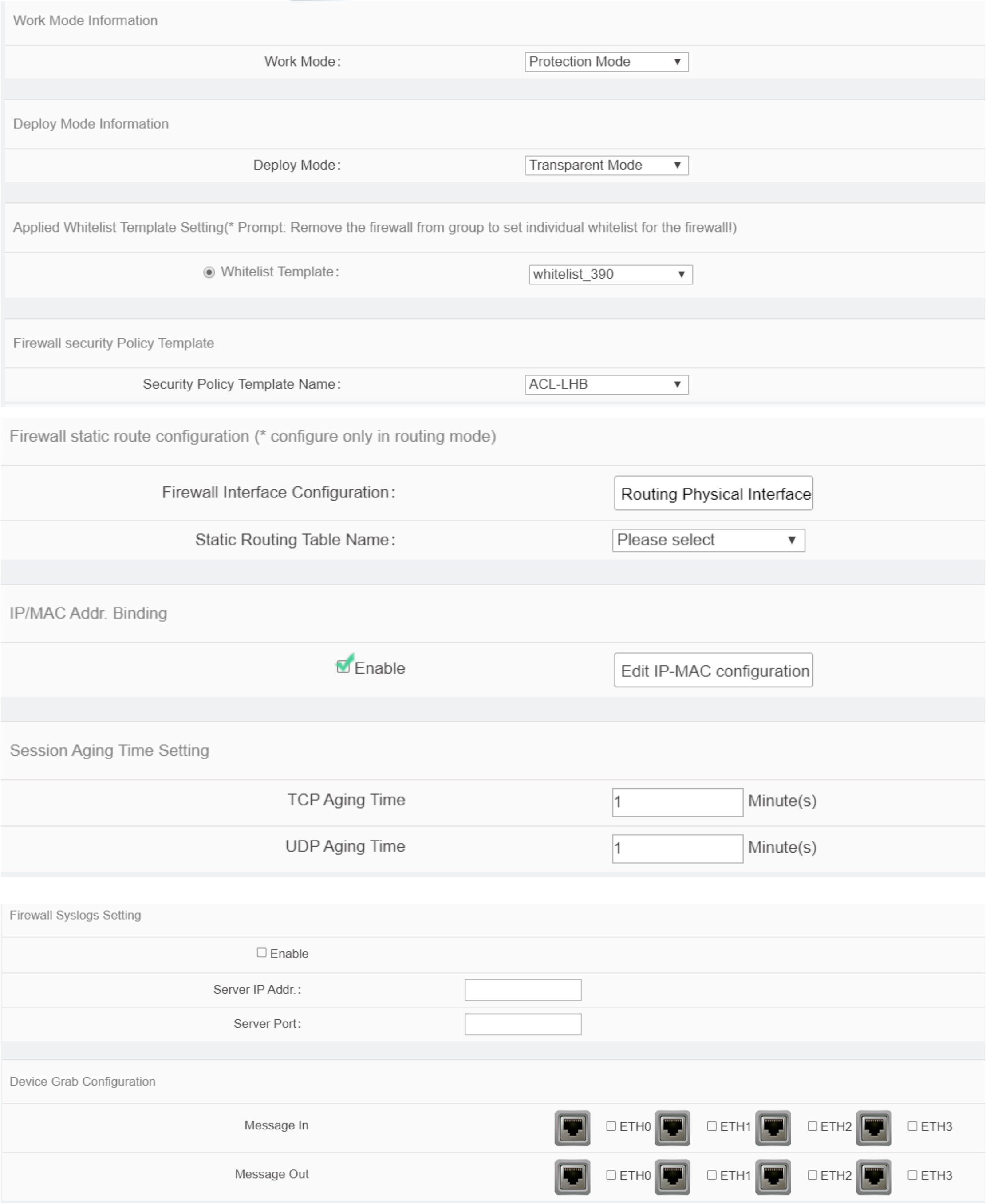


Fig.3-9 Modify Button


Firewall Basic Information

Firewall Name:	Firewall160824069 *
Firewall SN:	160824069
Firewall IP:	192.168.4.97
CPU:	1.8GHz
Memory:	4G
Software version:	V200R005C01B126
Group:	Not grouped ▾ [Remove from group]
Online status:	Online
Physical Location:	
Time Online:	2019-11-14 11:53:10
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: whitelist_390 ▼

Firewall security Policy Template

Security Policy Template Name: ACL-LHB ▼

Firewall static route configuration (* configure only in routing mode)

Firewall Interface Configuration: Routing Physical Interface

Static Routing Table Name: Please select ▼

IP/MAC Addr. Binding

☑ Enable Edit IP-MAC configuration

Session Aging Time Setting

TCP Aging Time 1 Minute(s)

UDP Aging Time 1 Minute(s)

Firewall Syslogs Setting

☐ Enable

Server IP Addr.:

Server Port:

Device Grab Configuration

Message In ☐ ETH0 ☐ ETH1 ☐ ETH2 ☐ ETH3

Message Out ☐ ETH0 ☐ ETH1 ☐ ETH2 ☐ ETH3

Fig.3-10 Industrial Firewall Modification Page

Tab.4 Instruction to Industrial Firewall Modification Information

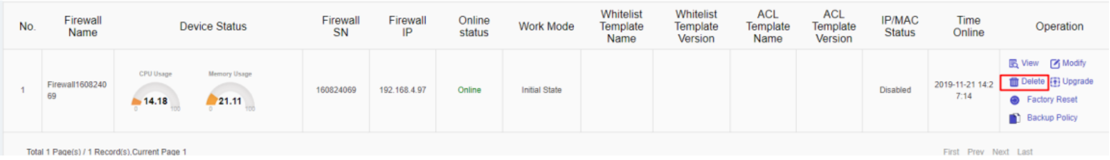
Column Names	**Instructions**
Firewall Name	Define a meaningful name for an industrial firewall that is easy to understand and remember. Modify this when configuring an industrial firewall
Physical Location	The physical location of the department or where an industrial firewall belongs to, for example, "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 firewall 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):



No.	Firewall Name	Device Status	Firewall SN	Firewall IP	Online status	Work Mode	Whitelist Template Name	Whitelist Template Version	ACL Template Name	ACL Template Version	IP/MAC Status	Time Online	Operation
1	Firewall160824069	CPU Usage 14.18 Memory Usage 21.11	160824069	192.168.4.97	Online	Initial State					Disabled	2019-11-21 14:27:14	View Modify Delete Upgrade Factory Reset Backup Policy

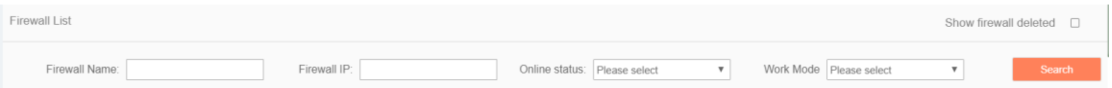
Total 1 Page(s) / 1 Record(s),Current Page 1

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):



Firewall List

Show firewall deleted □

Firewall Name:

Firewall IP:

Online status: Please select

Work Mode Please select

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:

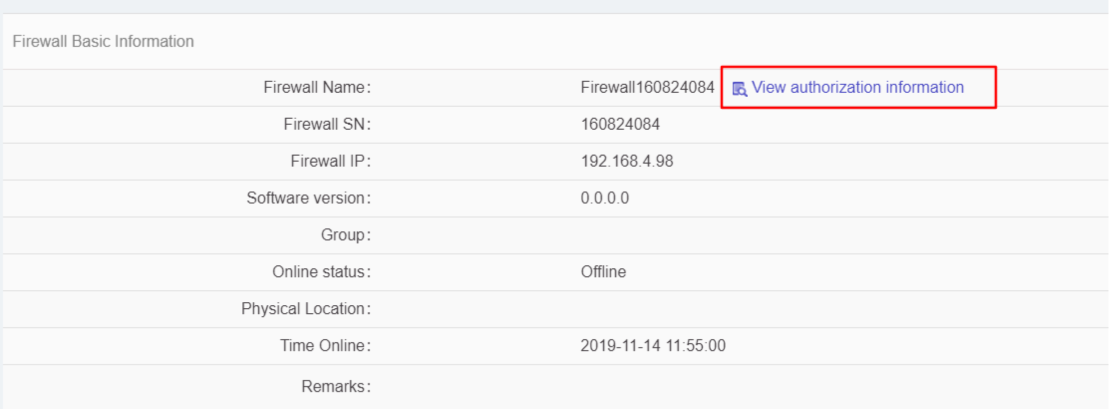
- Manually activate it through the firewall platform

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 firewall platform.

Industrial firewall authorization management consists of three components: the authorization tool, the industrial firewall and the firewall 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:



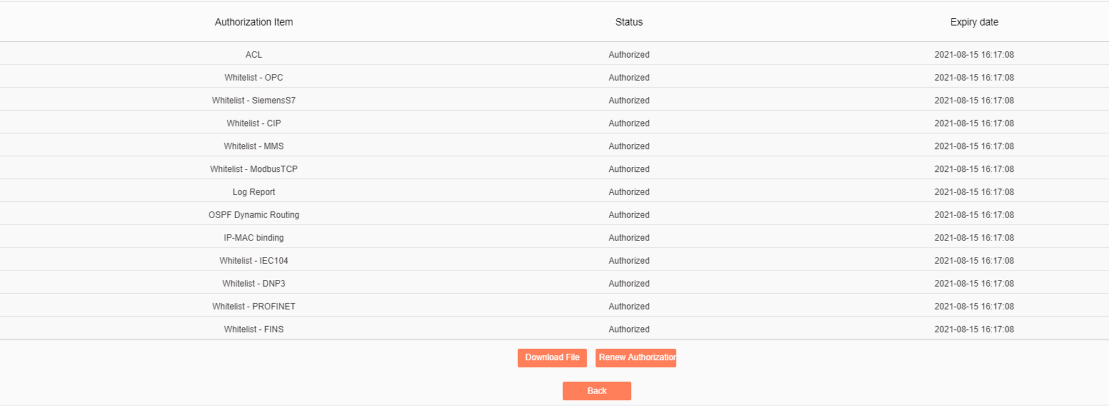
Firewall Basic Information

Firewall Name:	Firewall160824084	View authorization information
Firewall SN:	160824084	
Firewall IP:	192.168.4.98	
Software version:	0.0.0.0	
Group:		
Online status:	Offline	
Physical Location:		
Time Online:	2019-11-14 11:55:00	
Remarks:		

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

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

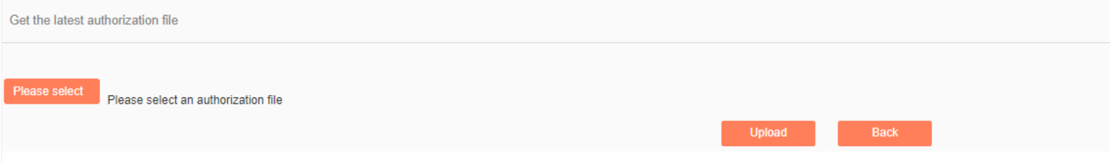
Update the authorization information on the current industrial firewall.

- ➢ 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):


Get the latest authorization file

Please select an authorization file

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 firewall 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.

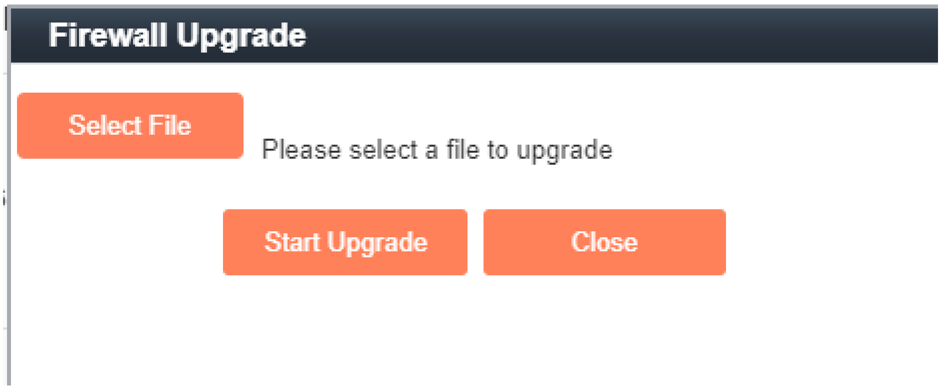
- Back

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 firewall 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):


Firewall Upgrade

Please select a file to upgrade

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

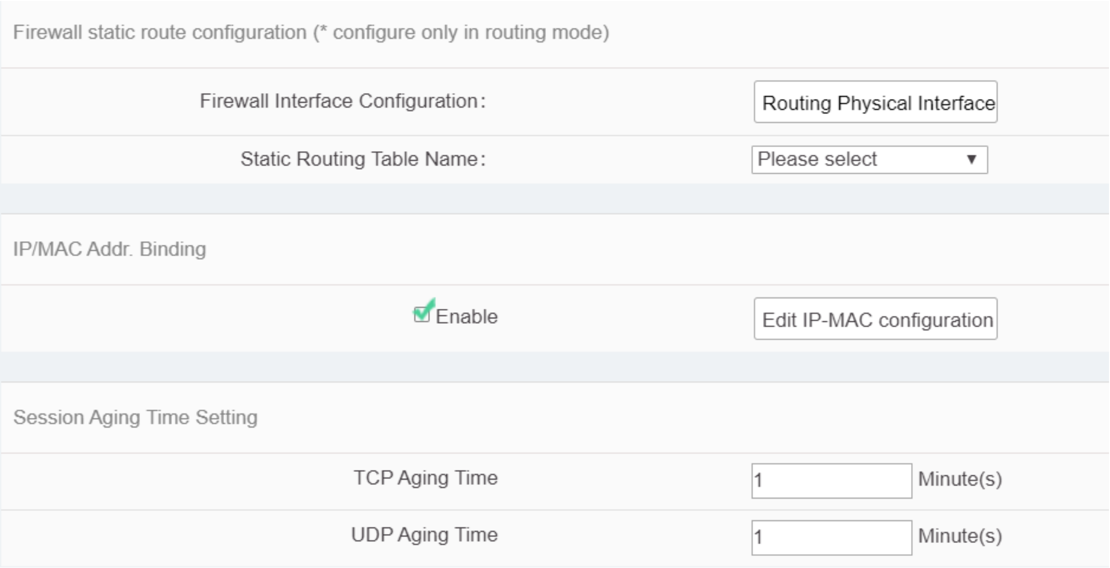
Upon clicking this button, the browser will firstly upload the upgrade file to the server where the firewall platform is located, and then notify and distribute the upgrade file to the industrial firewall, which will execute specific upgrade operation.

➢ 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):



Firewall static route configuration (* configure only in routing mode)

Firewall Interface Configuration: Routing Physical Interface

Static Routing Table Name: Please select ▾

IP/MAC Addr. Binding

☑ Enable

Session Aging Time Setting

TCP Aging Time 1 Minute(s)

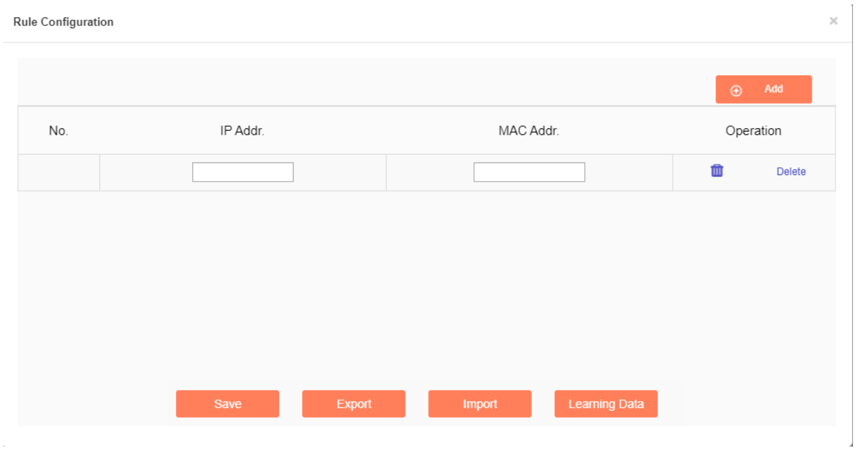
UDP Aging Time 1 Minute(s)

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):



Rule Configuration

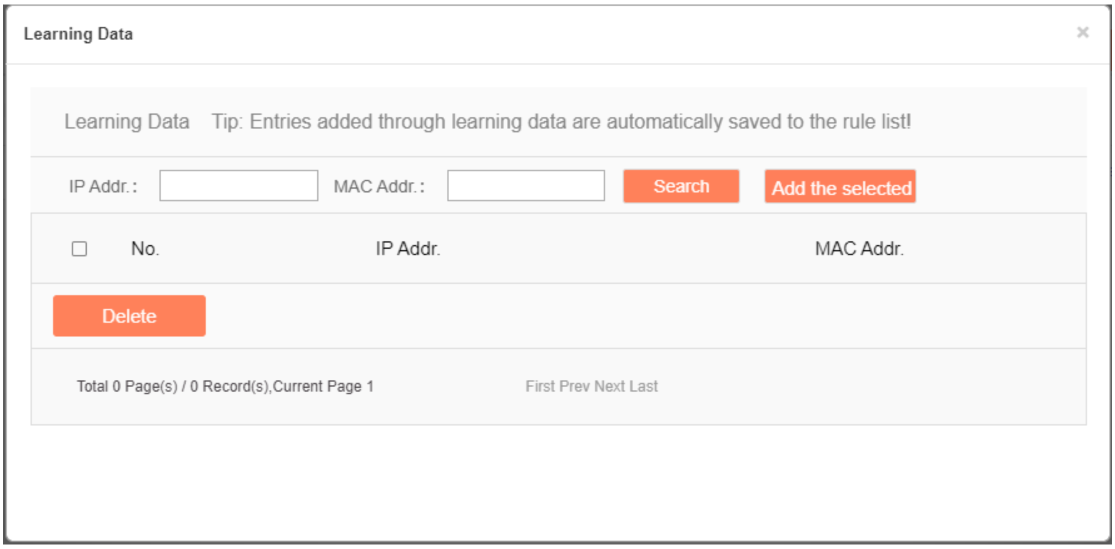
No.	IP Addr.	MAC Addr.	Operation
			Delete

Fig.3-18 Rule Configuration Page

Click <Add> to add rules, click 🗑 Delete 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):



Learning Data ×

Learning Data Tip: Entries added through learning data are automatically saved to the rule list!

IP Addr.: [ ] MAC Addr.: [ ] Search | Add the selected

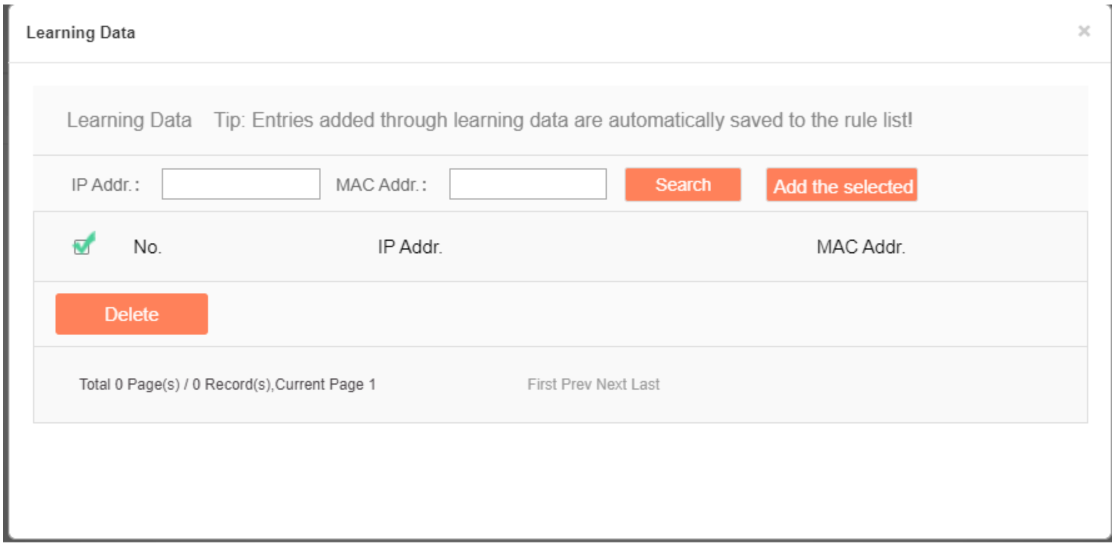
□	No.	IP Addr.	MAC Addr.

Delete

Total 0 Page(s) / 0 Record(s),Current Page 1 First Prev Next Last

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):



Learning Data ×

Learning Data Tip: Entries added through learning data are automatically saved to the rule list!

IP Addr.: [ ] MAC Addr.: [ ] Search | Add the selected

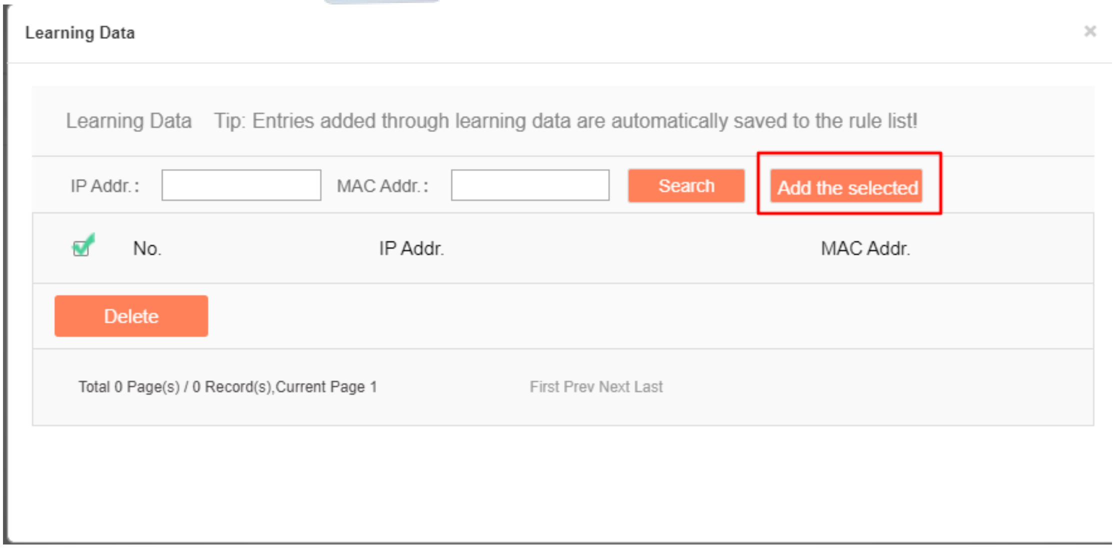
☑	No.	IP Addr.	MAC Addr.

Delete

Total 0 Page(s) / 0 Record(s),Current Page 1 First Prev Next Last

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):


Learning Data ×

Learning Data Tip: Entries added through learning data are automatically saved to the rule list!

IP Addr.: MAC Addr.: Search Add the selected

☑ No.	IP Addr.	MAC Addr.

Delete

Total 0 Page(s) / 0 Record(s),Current Page 1 First Prev Next Last

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):

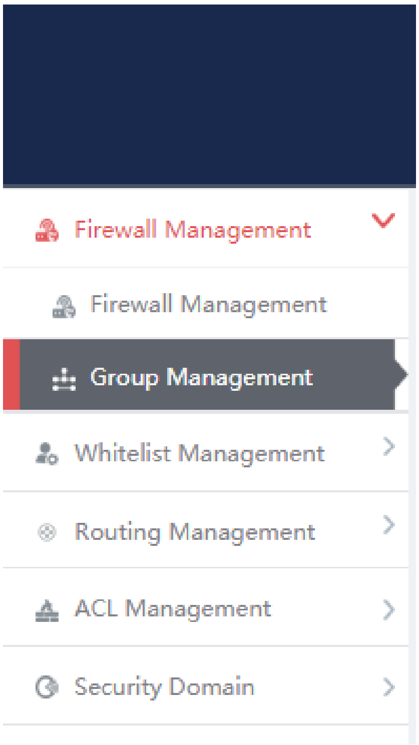
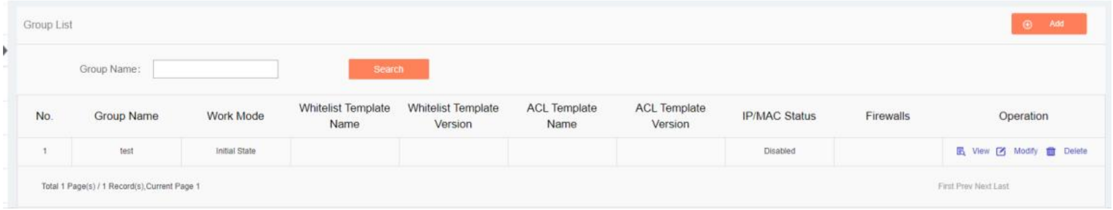


Fig.3-22 Group Management in Navigation Bar



No.	Group Name	Work Mode	Whitelist Template Name	Whitelist Template Version	ACL Template Name	ACL Template Version	IP/MAC Status	Firewalls	Operation
1	test	Initial State					Disabled		View Modify Delete

Total 1 Page(s) / 1 Record(s),Current Page 1

Fig.3-23 Group List Display Page

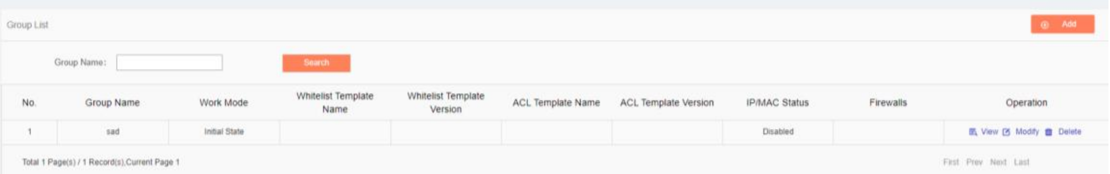
View the information on all industrial firewall groups in the system here, with the meaning as follows:

Tab.5 Instruction to Group Management List Display

Column Names	**Instructions**	
Group Name	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, Disable 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):

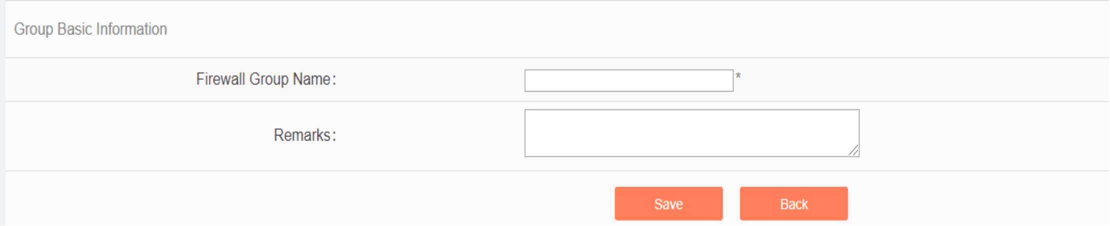


Group Name:

No.	Group Name	Work Mode	Whitelist Template Name	Whitelist Template Version	ACL Template Name	ACL Template Version	IP/MAC Status	Firewalls	Operation
1	sad	Initial State					Disabled		View Modify Delete

Total 1 Page(s) / 1 Record(s),Current Page 1

Fig.3-24 Firewall Group Add Buttons



Firewall Group Name: *

Remarks:

Fig.3-25 Firewall Group Add Page

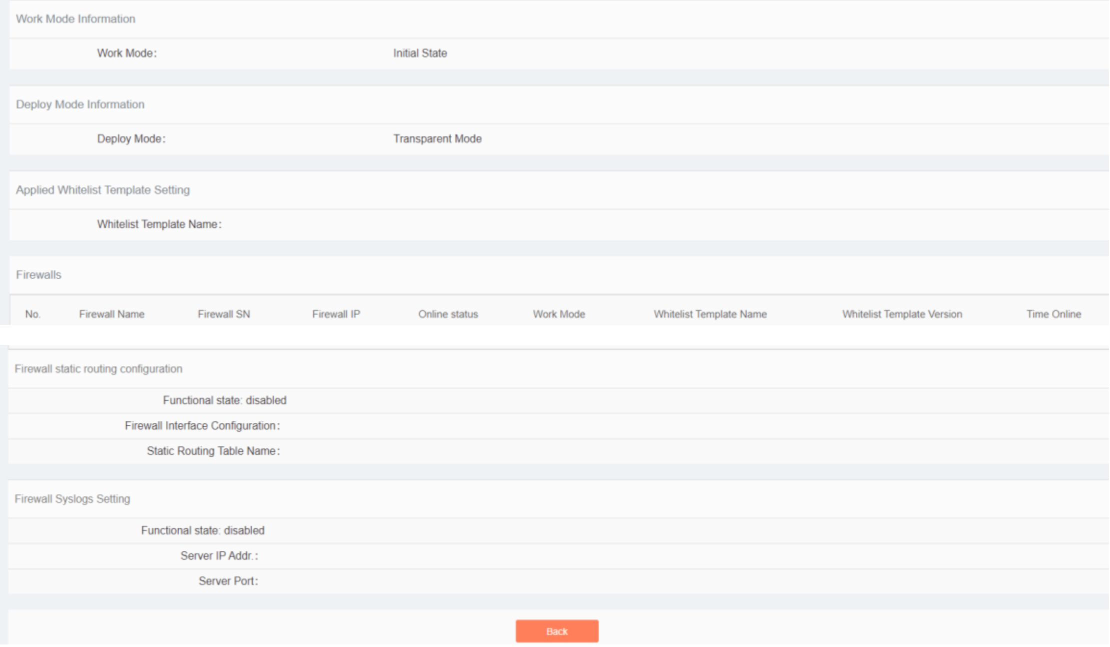
Tab.6 Instruction to Firewall Group Add Information

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):



Work Mode: Initial State

Deploy Mode: Transparent Mode

Whitelist Template Name:

No.	Firewall Name	Firewall SN	Firewall IP	Online status	Work Mode	Whitelist Template Name	Whitelist Template Version	Time Online

Functional state: disabled

Firewall Interface Configuration:

Static Routing Table Name:

Functional state: disabled

Server IP Addr.:

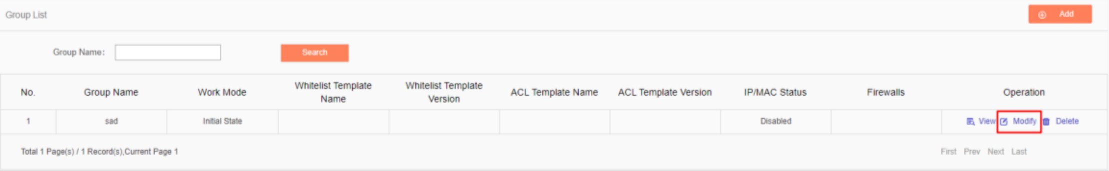
Server Port:

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):

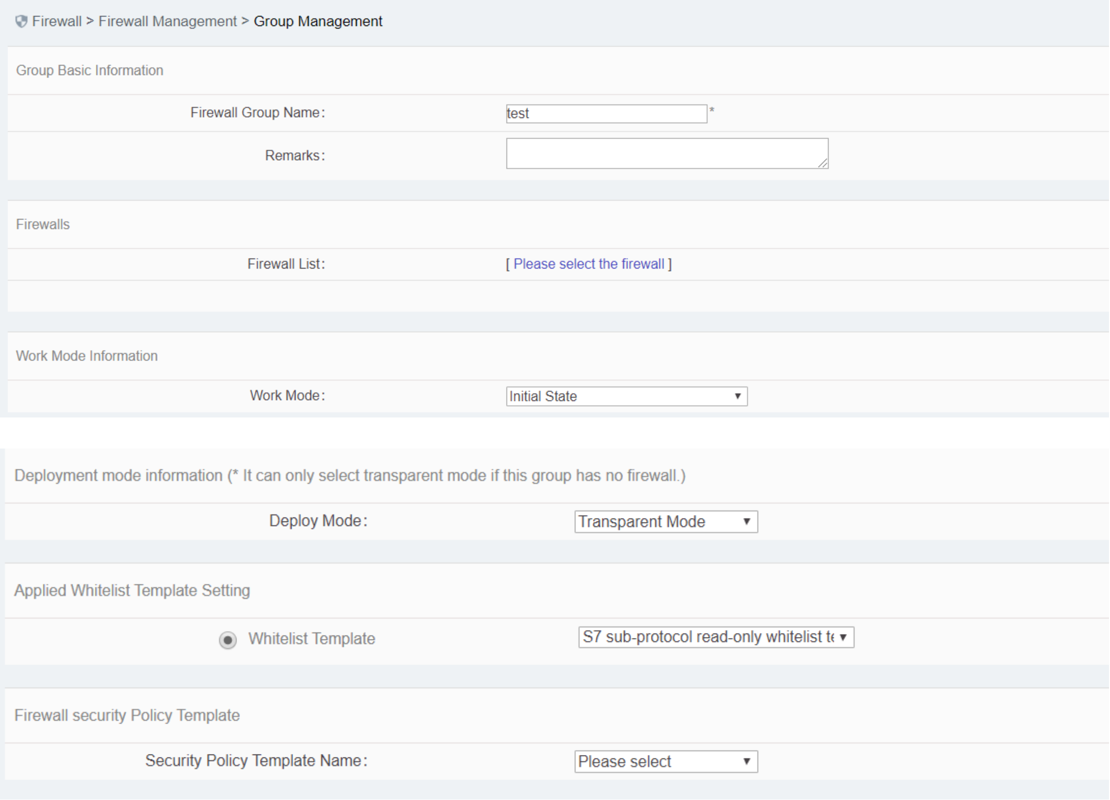


Group Name:

No.	Group Name	Work Mode	Whitelist Template Name	Whitelist Template Version	ACL Template Name	ACL Template Version	IP/MAC Status	Firewalls	Operation
1	sad	Initial State					Disabled		View Modify Delete

Total 1 Page(s) / 1 Record(s),Current Page 1

Fig.3-27 Modify Button



Group Basic Information

Firewall Group Name: test *

Remarks:

Firewalls

Firewall List: [Please select the firewall]

Work Mode Information

Work Mode: Initial State

Deployment mode information (* It can only select transparent mode if this group has no firewall.)

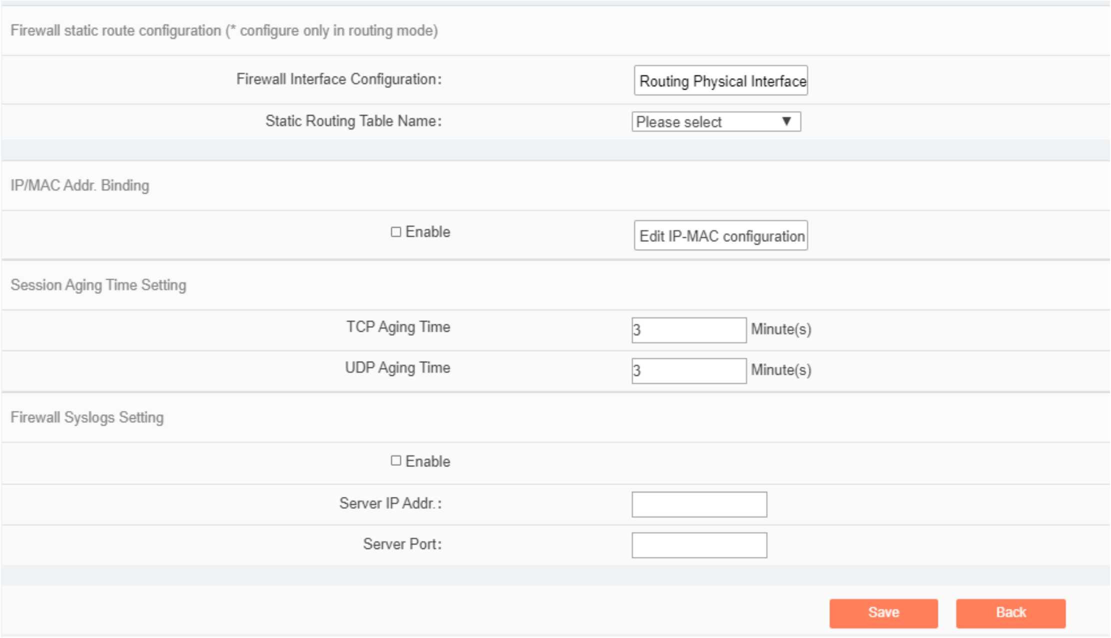
Deploy Mode: Transparent Mode

Applied Whitelist Template Setting

● Whitelist Template S7 sub-protocol read-only whitelist te

Firewall security Policy Template

Security Policy Template Name: Please select



Firewall static route configuration (* configure only in routing mode)

Firewall Interface Configuration:	Routing Physical Interface
Static Routing Table Name:	Please select ▼

IP/MAC Addr. Binding

□ Enable	Edit IP-MAC configuration

Session Aging Time Setting

TCP Aging Time	3 Minute(s)
UDP Aging Time	3 Minute(s)

Firewall Syslogs Setting

□ Enable	
Server IP Addr.:	
Server Port:	

Fig.3-28 Group Information Modification

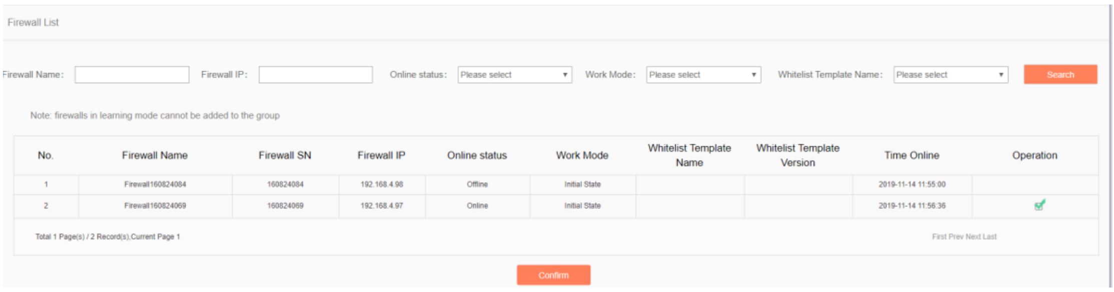
Tab.7 Instruction to Firewall Group Modification Information

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):



Firewall List

Firewall Name:
Firewall IP:
Online status: Please select
Work Mode: Please select
Whitelist Template Name: Please select

Note: firewalls in learning mode cannot be added to the group

No.	Firewall Name	Firewall SN	Firewall IP	Online status	Work Mode	Whitelist Template Name	Whitelist Template Version	Time Online	Operation
1	Firewall160824084	160824084	192.168.4.98	Offline	Initial State			2019-11-14 11:55:00	
2	Firewall160824069	160824069	192.168.4.97	Online	Initial State			2019-11-14 11:56:36	✓

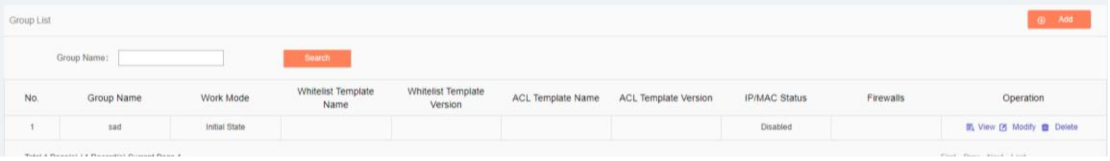
Total 1 Page(s) / 2 Record(s),Current Page 1

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):



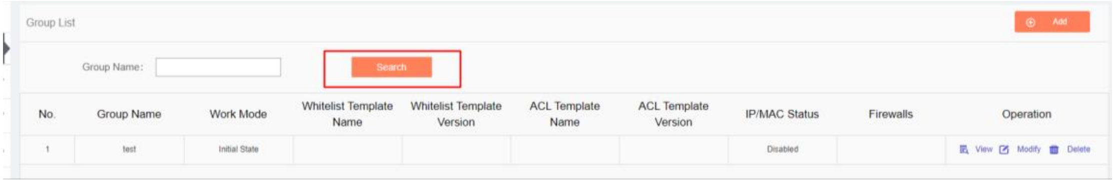
No.	Group Name	Work Mode	Whitelist Template Name	Whitelist Template Version	ACL Template Name	ACL Template Version	IP/MAC Status	Firewalls	Operation
1	sad	Initial State					Disabled		View Modify Delete

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):



No.	Group Name	Work Mode	Whitelist Template Name	Whitelist Template Version	ACL Template Name	ACL Template Version	IP/MAC Status	Firewalls	Operation
1	test	Initial State					Disabled		View Modify Delete

Fig.3-31 Retrieve a Group

3.3.7. Firewall Syslog Configuration

3.3.7.1. Function description

Report the specified information and security events that are specified in view of industrial firewalls.

3.3.7.2. Configuration process

After logging in the firewall 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".

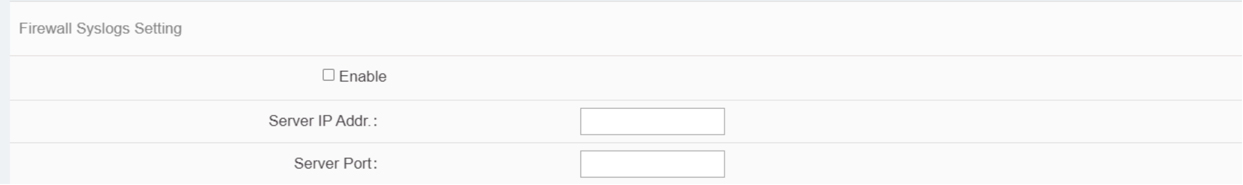
After clicking <Enable>, the page sets the relevant controls for Syslog service configuration to editable. See the following table for the contents that can be set:

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 port used for sending Syslog in range 1-65535	

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

See the diagram below:



Firewall Syslogs Setting

□ Enable

Server IP Addr.:

Server Port:

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 totally 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 a 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 firewall 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):

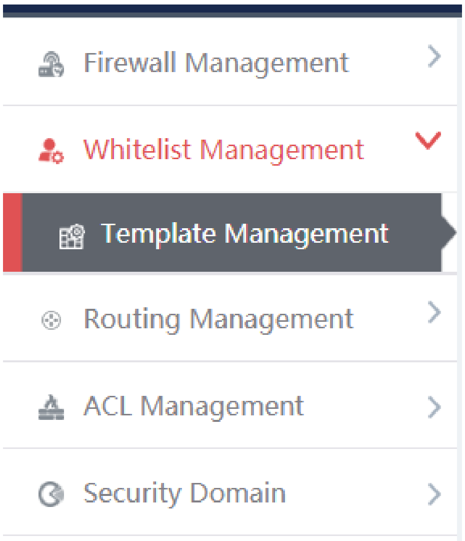
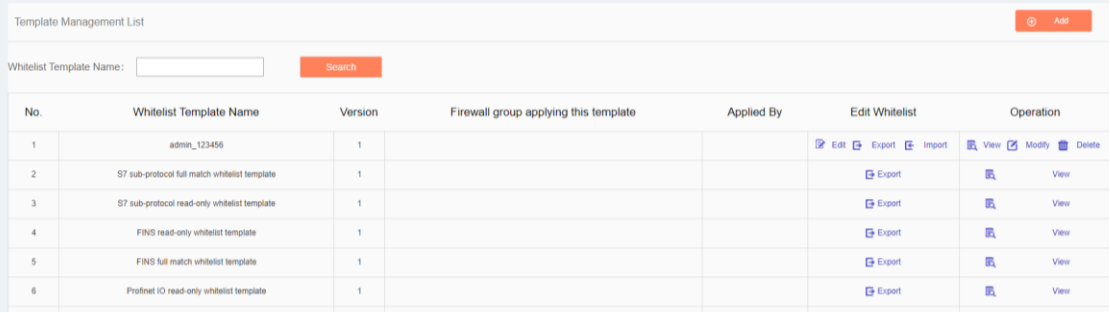


Fig.3-33 Select Whitelist Template Management



Template Management List

Add

Whitelist Template Name:

Search

No.	Whitelist Template Name	Version	Firewall group applying this template	Applied By	Edit Whitelist	Operation
1	admin_123456	1			Edit Export Import	View Modify Delete
2	S7 sub-protocol full match whitelist template	1			Export	View
3	S7 sub-protocol read-only whitelist template	1			Export	View
4	FINS read-only whitelist template	1			Export	View
5	FINS full match whitelist template	1			Export	View
6	Profinet IO read-only whitelist template	1			Export	View

Fig.3-34 Whitelist Template Management

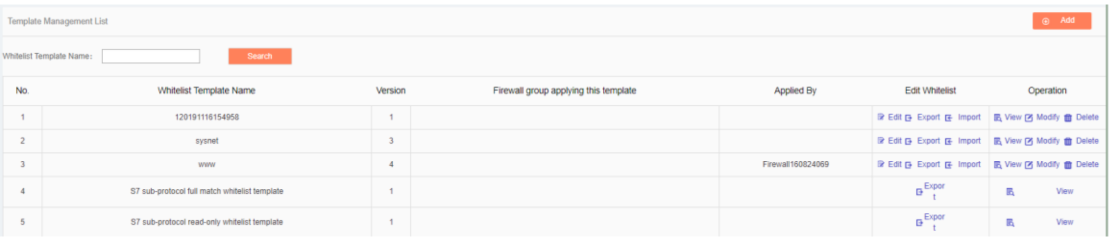
View information on all whitelist templates in the system here, with the meanings given below:

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):

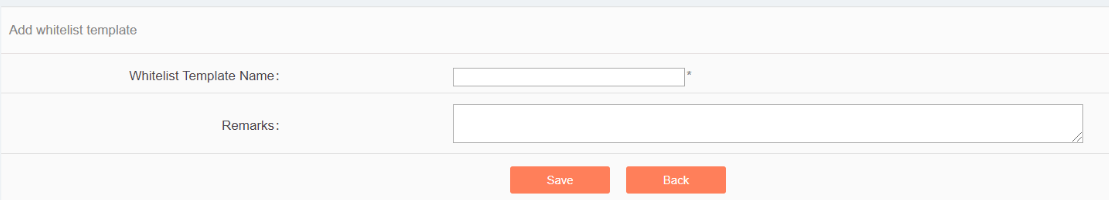


Template Management List

Whitelist Template Name:

No.	Whitelist Template Name	Version	Firewall group applying this template	Applied By	Edit Whitelist	Operation
1	120191116154958	1			Edit Export Import	View Modify Delete
2	sysnet	3			Edit Export Import	View Modify Delete
3	www	4		Firewall160824069	Edit Export Import	View Modify Delete
4	S7 sub-protocol full match whitelist template	1			Export	View
5	S7 sub-protocol read-only whitelist template	1			Export	View

Fig.3-35 Whitelist Template Add Button



Add whitelist template

Whitelist Template Name: *

Remarks:

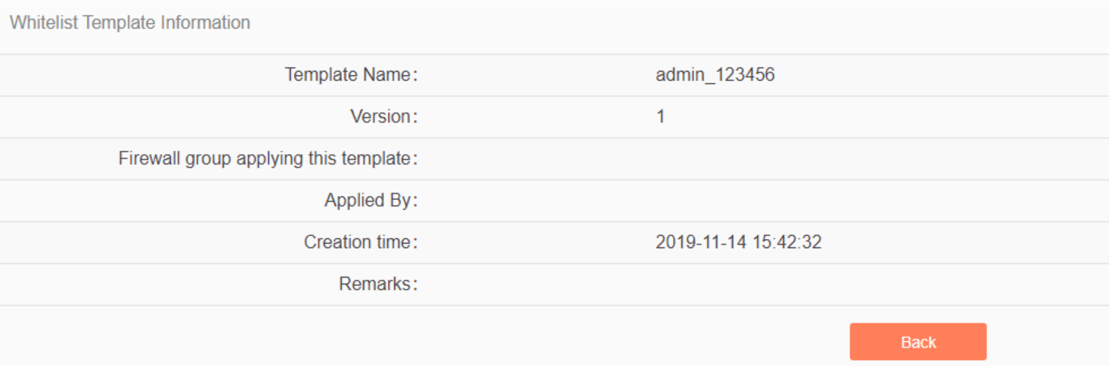
Fig.3-36 Whitelist Template Add Page

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):



Whitelist Template Information

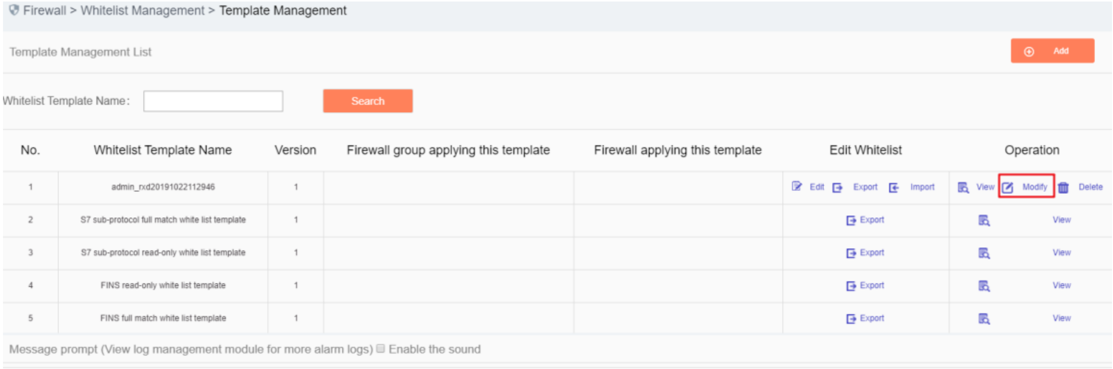
Template Name:	admin_123456
Version:	1
Firewall group applying this template:	
Applied By:	
Creation time:	2019-11-14 15:42:32
Remarks:	

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):



Firewall > Whitelist Management > Template Management

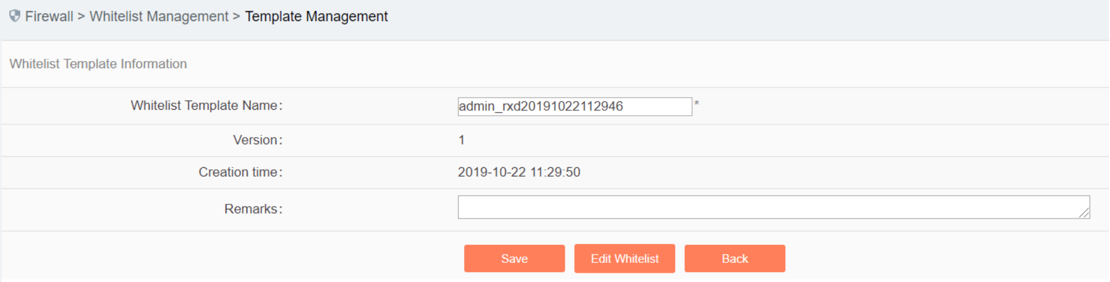
Template Management List

Whitelist Template Name:

No.	Whitelist Template Name	Version	Firewall group applying this template	Firewall applying this template	Edit Whitelist	Operation
1	admin_rxd20191022112946	1			Edit Export Import	View Modify Delete
2	S7 sub-protocol full match white list template	1			Export	View
3	S7 sub-protocol read-only white list template	1			Export	View
4	FINS read-only white list template	1			Export	View
5	FINS full match white list template	1			Export	View

Message prompt (View log management module for more alarm logs) □ Enable the sound

Fig.3-38 Whitelist Template Modification Buttons



Firewall > Whitelist Management > Template Management

Whitelist Template Information

Whitelist Template Name:	admin_rxd20191022112946 *
Version:	1
Creation time:	2019-10-22 11:29:50
Remarks:	

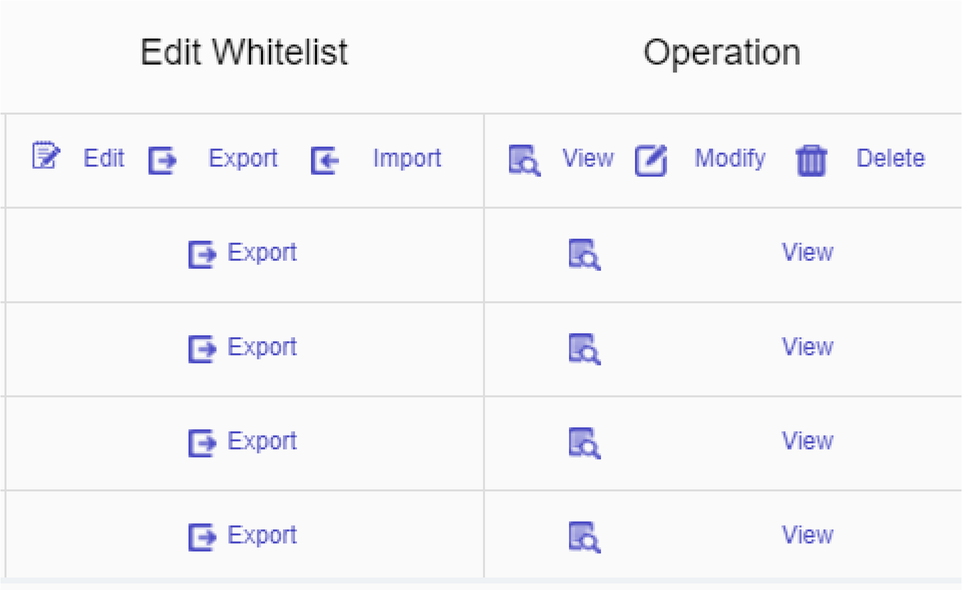
Fig.3-39 Whitelist Template Modification Page

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):

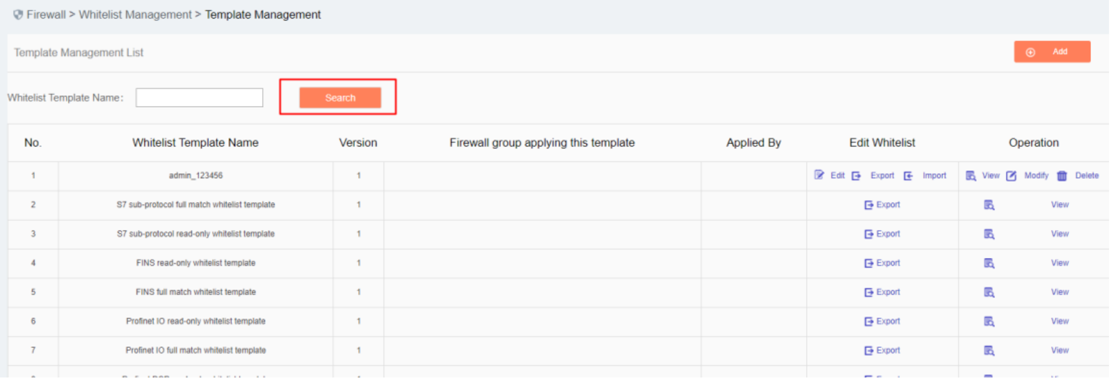


Edit Whitelist	Operation
Edit Export Import	View Modify Delete
Export	View
Export	View
Export	View
Export	View

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):



Firewall > Whitelist Management > Template Management

Template Management List

Whitelist Template Name:

No.	Whitelist Template Name	Version	Firewall group applying this template	Applied By	Edit Whitelist	Operation
1	admin_123456	1			Edit Export Import	View Modify Delete
2	S7 sub-protocol full match whitelist template	1			Export	View
3	S7 sub-protocol read-only whitelist template	1			Export	View
4	FINS read-only whitelist template	1			Export	View
5	FINS full match whitelist template	1			Export	View
6	Profinet IO read-only whitelist template	1			Export	View
7	Profinet IO full match whitelist template	1			Export	View

Fig.3-41 Retrieves a Whitelist Template

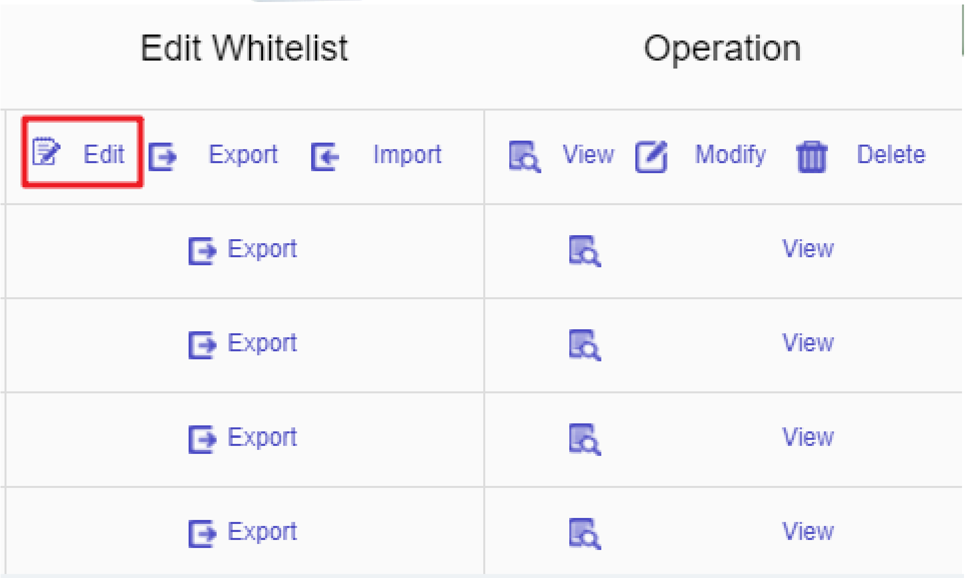
3.4.3. Whitelist Template Rule Management

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 soon.

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

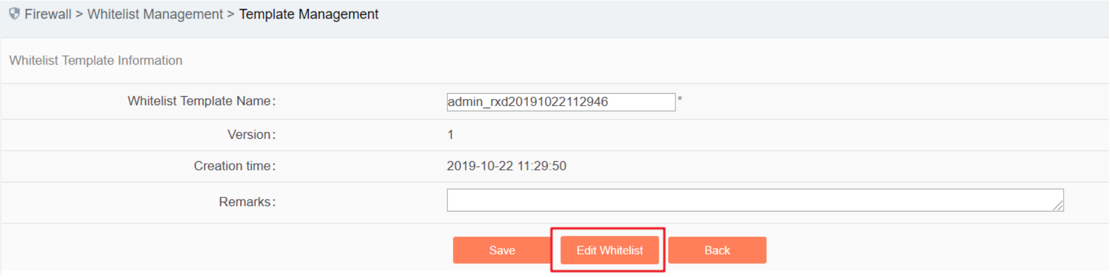
The first path: click <Edit> in the [Whitelist Management]-[Template Management]-[Edit Whitelist] column;

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):



Edit Whitelist	Operation
Edit Export Import	View Modify Delete
Export	View
Export	View
Export	View
Export	View

Fig.3-42 Edit Button



Firewall > Whitelist Management > Template Management

Whitelist Template Information

Whitelist Template Name: admin_rxd20191022112946 *

Version: 1

Creation time: 2019-10-22 11:29:50

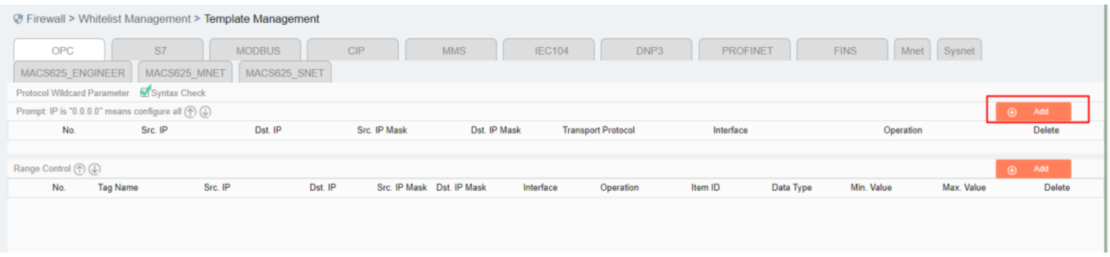
Remarks:

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):



Firewall > Whitelist Management > Template Management

Protocol Wildcard Parameter ☑ Syntax Check

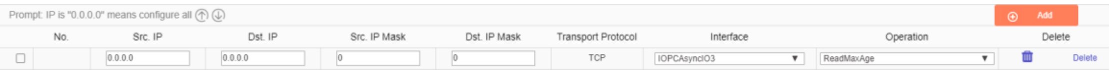
Prompt: IP is "0.0.0.0" means configure all

No.	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Transport Protocol	Interface	Operation	Delete

Range Control

No.	Tag Name	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Interface	Operation	Item ID	Data Type	Min. Value	Max. Value	Delete

Fig.3-44 Whitelist Template Add Button



Prompt: IP is "0.0.0.0" means configure all

	No.	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Transport Protocol	Interface	Operation	Delete	
□		0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsyncIO3 ▼	ReadMaxAge ▼	🗑	Delete

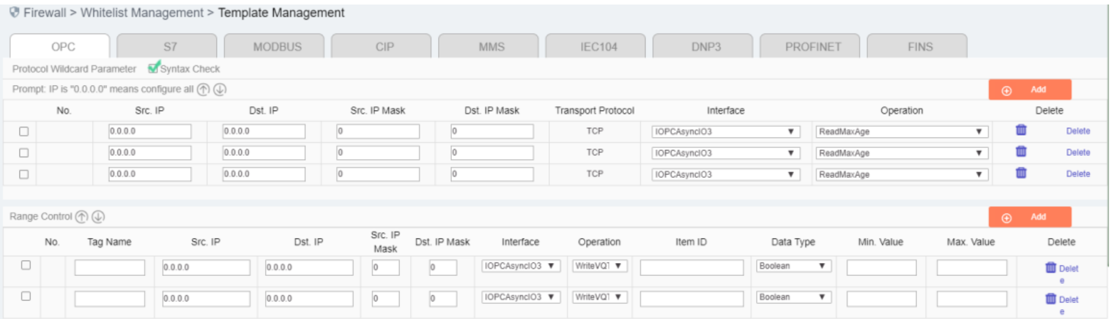
Fig.3-45 Whitelist Template Added Successfully

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):



Firewall > Whitelist Management > Template Management

Protocol Wildcard Parameter ☑ Syntax Check

Prompt: IP is "0.0.0.0" means configure all

	No.	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Transport Protocol	Interface	Operation	Delete
□		0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsyncIO3	ReadMaxAge	Delete
□		0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsyncIO3	ReadMaxAge	Delete
□		0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsyncIO3	ReadMaxAge	Delete

Range Control

	No.	Tag Name	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Interface	Operation	Item ID	Data Type	Min. Value	Max. Value	Delete
□			0.0.0.0	0.0.0.0	0	0	IOPCAsyncIO3	WriteVQT		Boolean			Delete
□			0.0.0.0	0.0.0.0	0	0	IOPCAsyncIO3	WriteVQT		Boolean			Delete

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

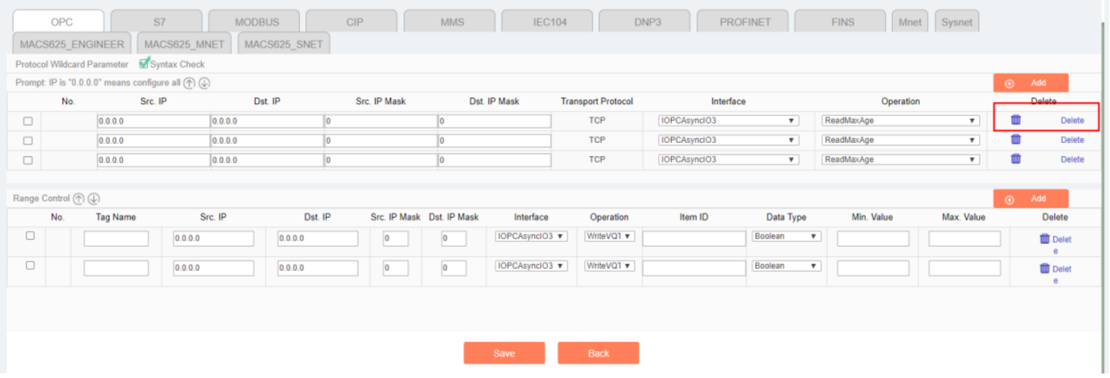
After entering the [Whitelist Template Rule Management] page, click the edit box under a whitelist item to change the source IP, destination IP, source IP mask, destination IP mask, interface name and method name of a whitelist item, click <Save> after the modification.

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, Item ID, 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):



Protocol Wildcard Parameter ☑ Syntax Check

Prompt: IP is "0.0.0.0" means configure all

	No.	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Transport Protocol	Interface	Operation	Delete
□		0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsyncIO3 ▼	ReadMaxAge ▼	Delete
□		0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsyncIO3 ▼	ReadMaxAge ▼	Delete
□		0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsyncIO3 ▼	ReadMaxAge ▼	Delete

Range Control

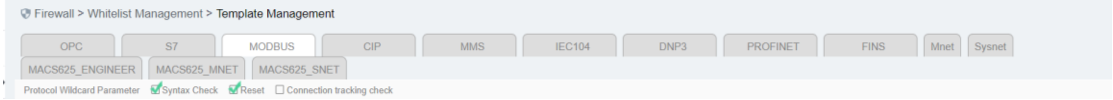
	No.	Tag Name	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Interface	Operation	Item ID	Data Type	Min. Value	Max. Value	Delete
□			0.0.0.0	0.0.0.0	0	0	IOPCAsyncIO3 ▼	WriteVQ1 ▼		Boolean ▼			Delete
□			0.0.0.0	0.0.0.0	0	0	IOPCAsyncIO3 ▼	WriteVQ1 ▼		Boolean ▼			Delete

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:



Protocol Wildcard Parameter ☑ Syntax Check ☑ Reset □ Connection tracking check

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

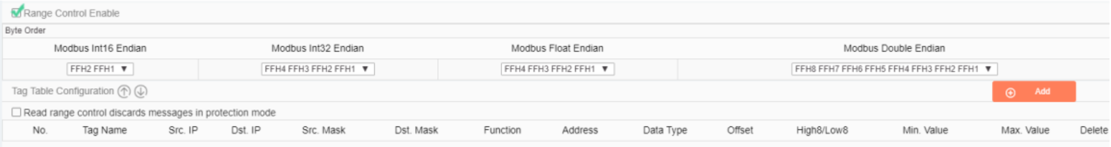
  With this option enabled, messages will be discarded and alarmed by default if the connection status is abnormal in the protection mode. Other operation modes will not lose packets, but corresponding alarm information will be available in the alarm mode.

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):



☑ Range Control Enable

Byte Order

Modbus Int16 Endian	Modbus Int32 Endian	Modbus Float Endian	Modbus Double Endian
FFH2 FFH1 ▼	FFH4 FFH3 FFH2 FFH1 ▼	FFH4 FFH3 FFH2 FFH1 ▼	FFH8 FFH7 FFH6 FFH5 FFH4 FFH3 FFH2 FFH1 ▼

Tag Table Configuration

□ Read range control discards messages in protection mode

No.	Tag Name	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Function	Address	Data Type	Offset	High8/Low8	Min. Value	Max. Value	Delete

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

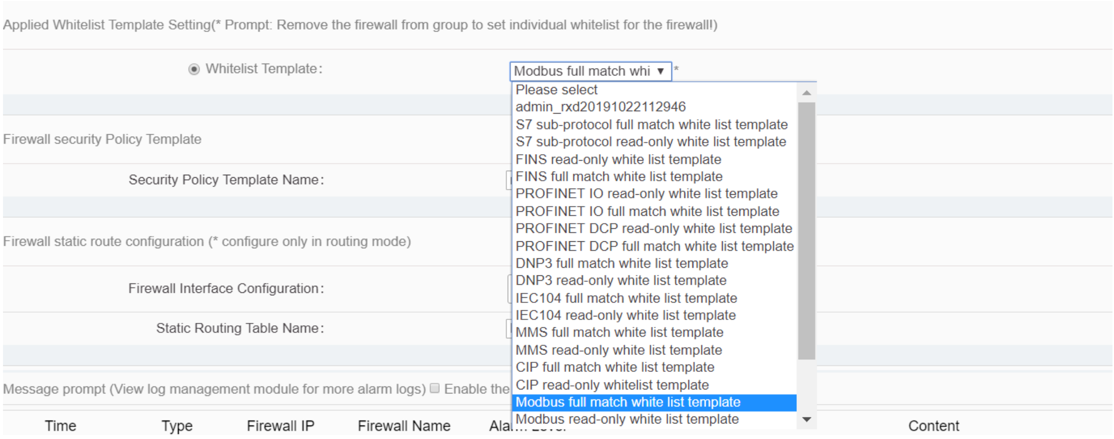
For adding, modifying, editing, and deleting a range rule item, please refer to the basic Modbus item operation.

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):



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

● Whitelist Template: Modbus full match whi ▾ *

- Please select
- admin_rxd20191022112946
- S7 sub-protocol full match white list template
- S7 sub-protocol read-only white list template
- FINS read-only white list template
- FINS full match white list template
- PROFINET IO read-only white list template
- PROFINET IO full match white list template
- PROFINET DCP read-only white list template
- PROFINET DCP full match white list template
- DNP3 full match white list template
- DNP3 read-only white list template
- IEC104 full match white list template
- IEC104 read-only white list template
- MMS full match white list template
- MMS read-only white list template
- CIP full match white list template
- CIP read-only whitelist template
- Modbus full match white list template
- Modbus read-only white list template

Firewall security Policy Template

Security Policy Template Name:

Firewall static route configuration (* configure only in routing mode)

Firewall Interface Configuration:

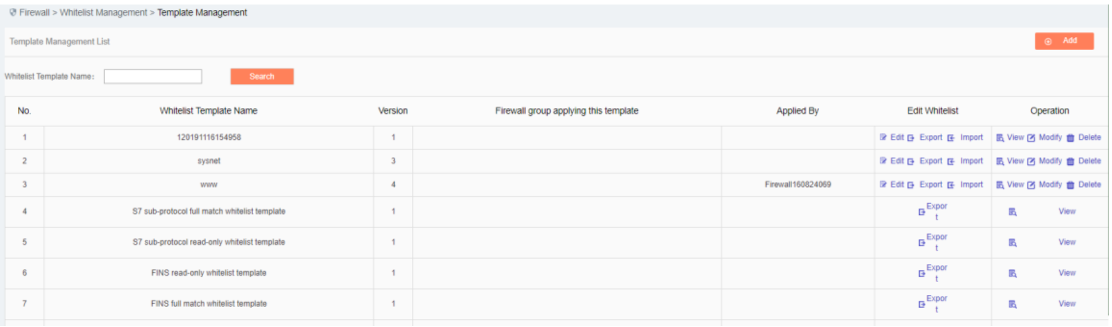
Static Routing Table Name:

Message prompt (View log management module for more alarm logs) □ Enable the

Time Type Firewall IP Firewall Name Ala... Content

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.



Firewall > Whitelist Management > Template Management

Template Management List

Whitelist Template Name:

No.	Whitelist Template Name	Version	Firewall group applying this template	Applied By	Edit Whitelist	Operation
1	120191116154958	1			Edit Export Import	View Modify Delete
2	sysnet	3			Edit Export Import	View Modify Delete
3	www	4		Firewall160824069	Edit Export Import	View Modify Delete
4	S7 sub-protocol full match whitelist template	1			Export	View
5	S7 sub-protocol read-only whitelist template	1			Export	View
6	FINS read-only whitelist template	1			Export	View
7	FINS full match whitelist template	1			Export	View

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

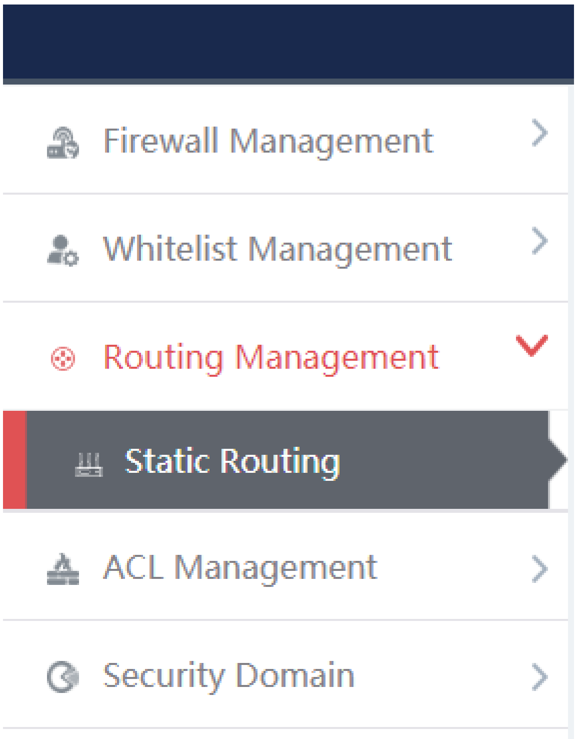
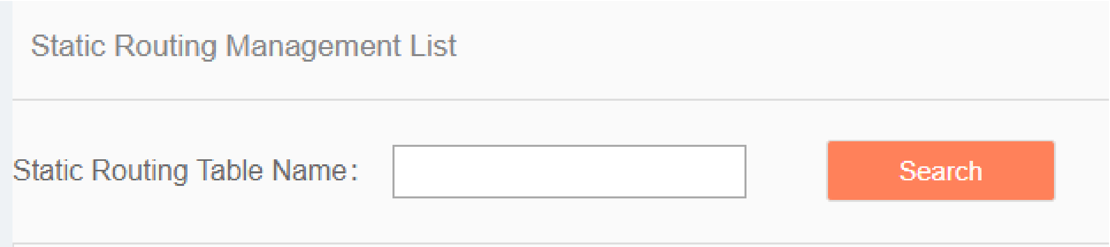


Fig.3-52 Static Route Navigation

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

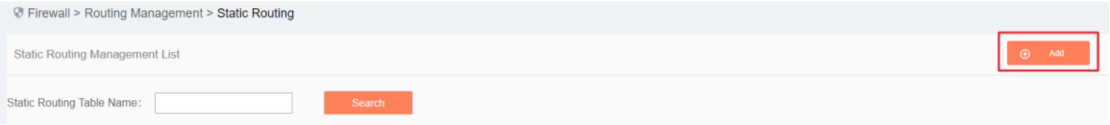

Static Routing Management List

Static Routing Table Name:

Fig.3-53 Screening Conditions for Static Route Table

3.5.2.3. Add the static route management list

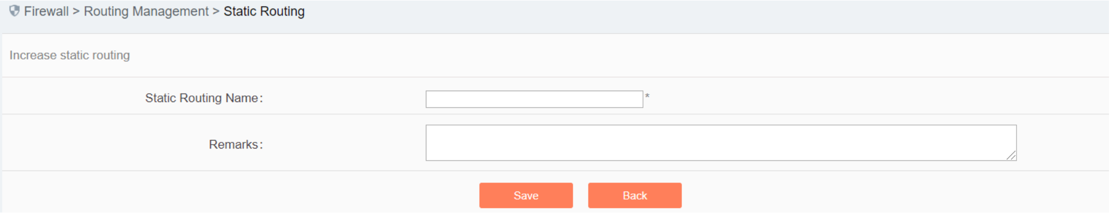
In the [Static Route Management List] display list page, click [Add] to add a new static route table template, as shown in the figure



Static Routing Management List

Static Routing Table Name:

Fig.3-54 Add the Static Route Management Template



Firewall > Routing Management > Static Routing

Increase static routing

Static Routing Name: ______ *

Remarks: ______

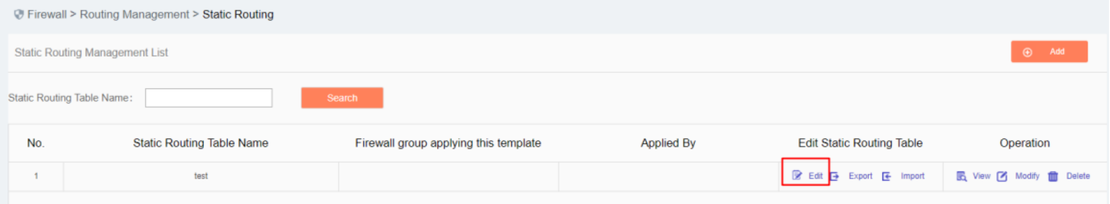
Fig.3-55 Add the Static Route

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



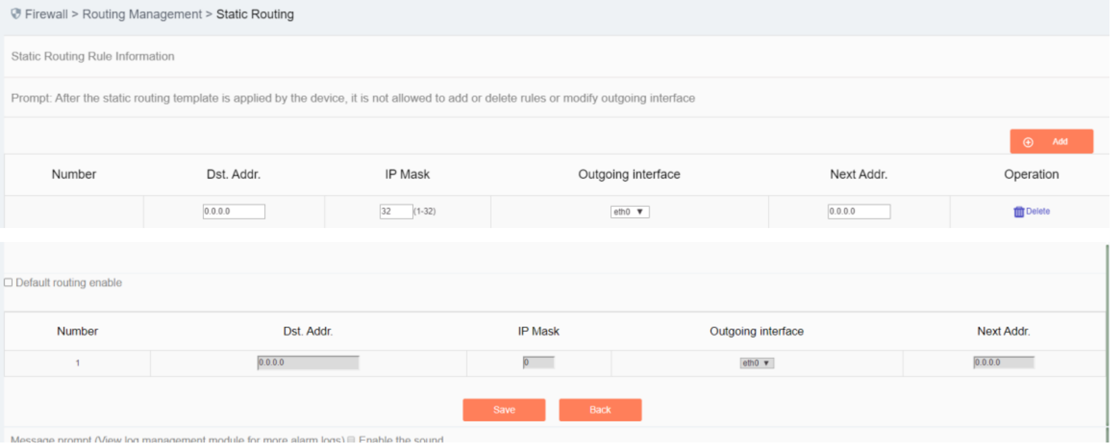
Firewall > Routing Management > Static Routing

Static Routing Management List

Static Routing Table Name: ______

No.	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation
1	test			Edit Export Import	View Modify Delete

Fig.3-56 Edit a Static Route Table Template



Firewall > Routing Management > Static Routing

Static Routing Rule Information

Prompt: After the static routing template is applied by the device, it is not allowed to add or delete rules or modify outgoing interface

Number	Dst. Addr.	IP Mask	Outgoing interface	Next Addr.	Operation
	0.0.0.0	32 (1-32)	eth0 ▼	0.0.0.0	Delete

□ Default routing enable

Number	Dst. Addr.	IP Mask	Outgoing interface	Next Addr.
1	0.0.0.0	0	eth0 ▼	0.0.0.0

Message prompt (View log management module for more alarm logs) □ Enable the sound

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

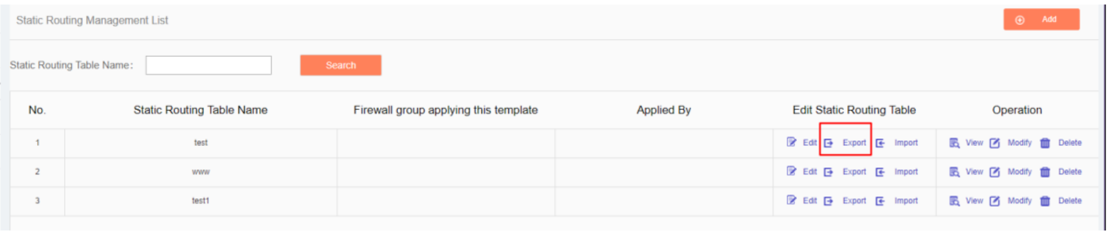
Outgoing interface	Outgoing interface content	
Next Addr.	Legitimate IP address	
Operation	Add	Add the static route rule information
	Default routing enable	Allow to edit default route enable
	Save	Save the static route rule information
	Back	Go back to the static route template list page without saving 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.

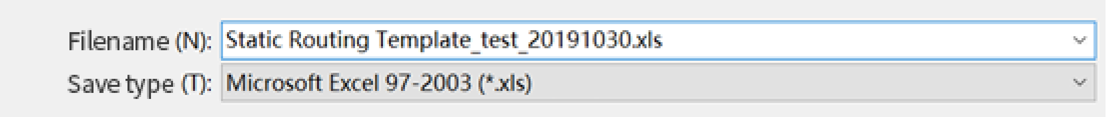


Static Routing Management List

Static Routing Table Name:

No.	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation
1	test			Edit Export Import	View Modify Delete
2	www			Edit Export Import	View Modify Delete
3	test1			Edit Export Import	View Modify Delete

Fig.3-181 Export Static Route Table Template



Filename (N): Static Routing Template_test_20191030.xls

Save type (T): Microsoft Excel 97-2003 (*.xls)

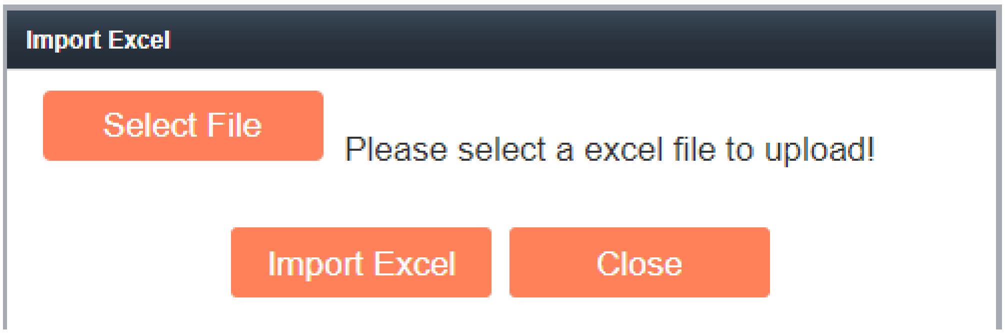
Fig.3-58 Excel Generated by Static Route Table

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.

- Click [Select File] to select an edited Excel template
- Click <Import Excel> to execute the import operation
- Click <Close> to abandon the import operation, close the [Excel import] page.

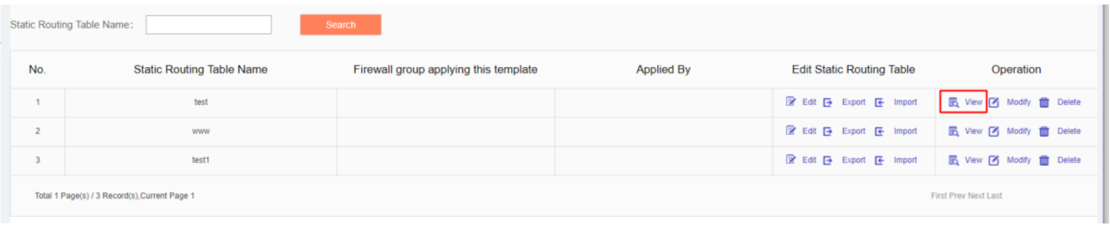


Please select a excel file to upload!

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

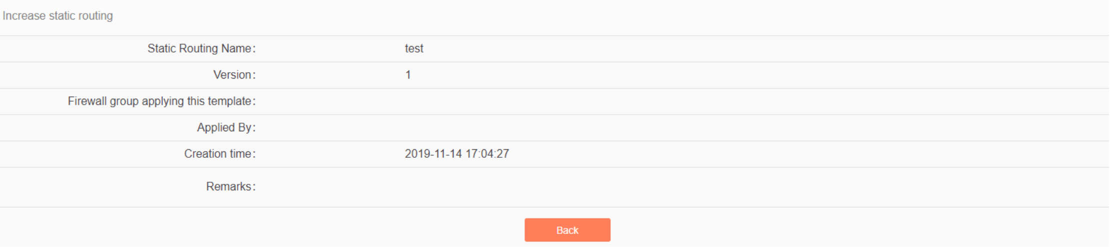


Static Routing Table Name:

No.	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation
1	test			Edit Export Import	View Modify Delete
2	www			Edit Export Import	View Modify Delete
3	test1			Edit Export Import	View Modify Delete

Total 1 Page(s) / 3 Record(s),Current Page 1

Fig.3-60 View the Static Route Table



Increase static routing

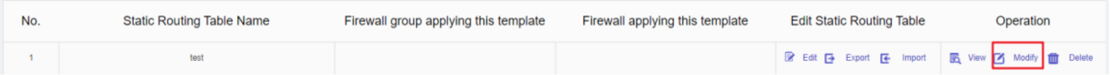
Static Routing Name:	test
Version:	1
Firewall group applying this template:	
Applied By:	
Creation time:	2019-11-14 17:04:27
Remarks:	

Fig.3-61 Static Route Information

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

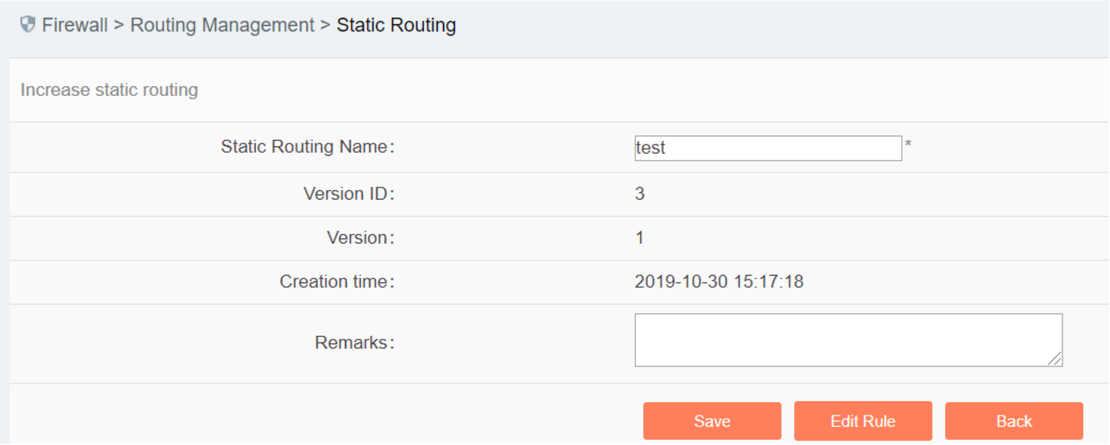
3.5.2.8. Modify a static route management list

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



No.	Static Routing Table Name	Firewall group applying this template	Firewall applying this template	Edit Static Routing Table	Operation
1	test			Edit Export Import	View Modify Delete

Fig.3-62 Modify the Static Route Table



Firewall > Routing Management > Static Routing

Increase static routing

Static Routing Name:	test *
Version ID:	3
Version:	1
Creation time:	2019-10-30 15:17:18
Remarks:	

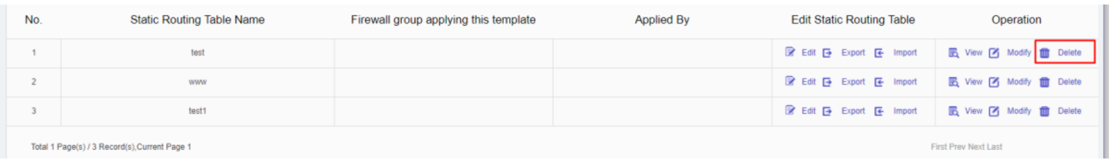
Fig.3-63 Static Route Information

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

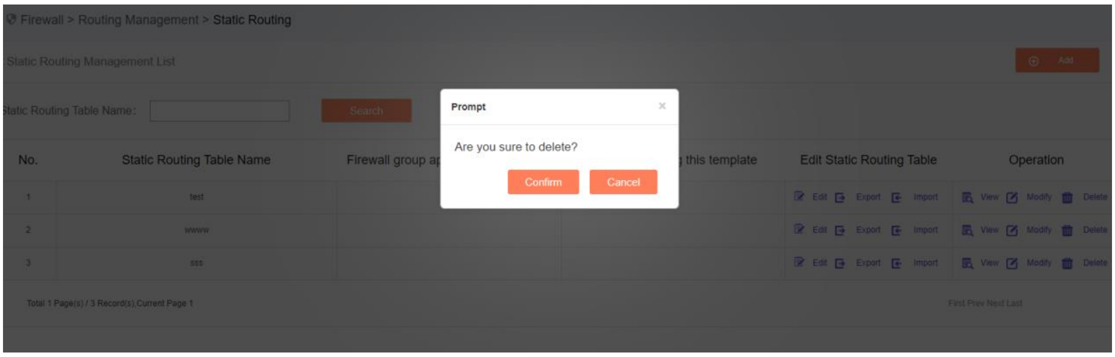
In the [Static Route Management List] display list page, click [Delete] to delete the static route template, as shown in the figure



No.	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation
1	test			Edit Export Import	View Modify Delete
2	www			Edit Export Import	View Modify Delete
3	test1			Edit Export Import	View Modify Delete

Total 1 Page(s) / 3 Record(s),Current Page 1

Fig.3-64 Static Route Table Template



Firewall > Routing Management > Static Routing

Static Routing Management List

Static Routing Table Name:

Prompt

Are you sure to delete?

No.	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation
1	test			Edit Export Import	View Modify Delete
2	wwww			Edit Export Import	View Modify Delete
3	sss			Edit Export Import	View Modify Delete

Total 1 Page(s) / 3 Record(s),Current Page 1

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):

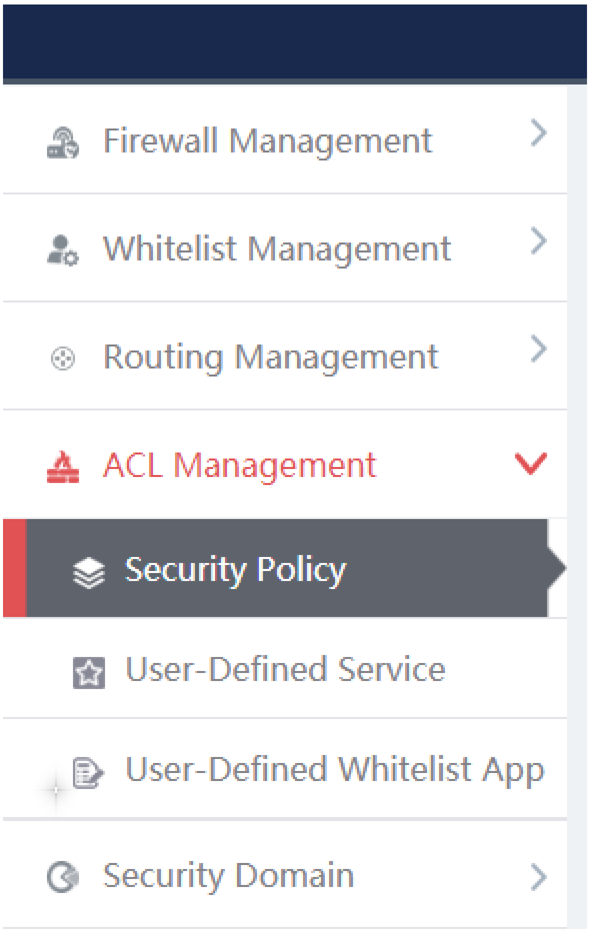
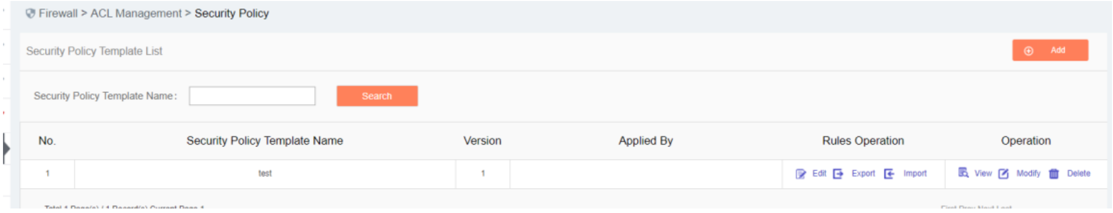


Fig.3-66 Selecting Security Policy Management



Firewall > ACL Management > Security Policy

Security Policy Template List

Security Policy Template Name:

No.	Security Policy Template Name	Version	Applied By	Rules Operation	Operation
1	test	1		Edit Export Import	View Modify Delete

Fig.3-67 Security Policy Management

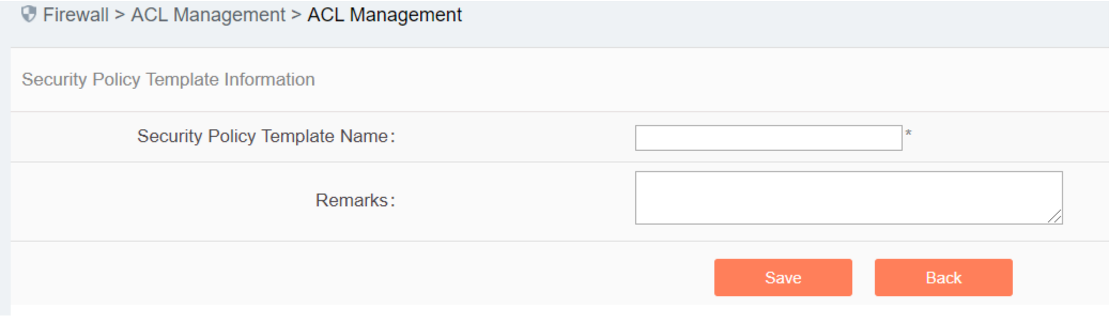
View the information on all security policy templates in the system, with the meanings given below:

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):



Firewall > ACL Management > ACL Management

Security Policy Template Information

Security Policy Template Name: *

Remarks:

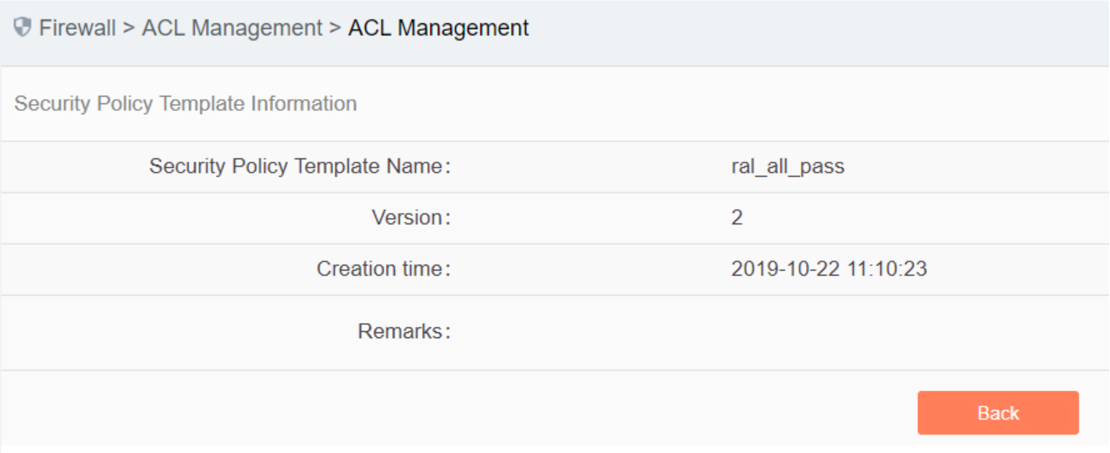
Fig.3-68 Security Policy Template Add Page

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):



Firewall > ACL Management > ACL Management

Security Policy Template Information

Security Policy Template Name: ral_all_pass

Version: 2

Creation time: 2019-10-22 11:10:23

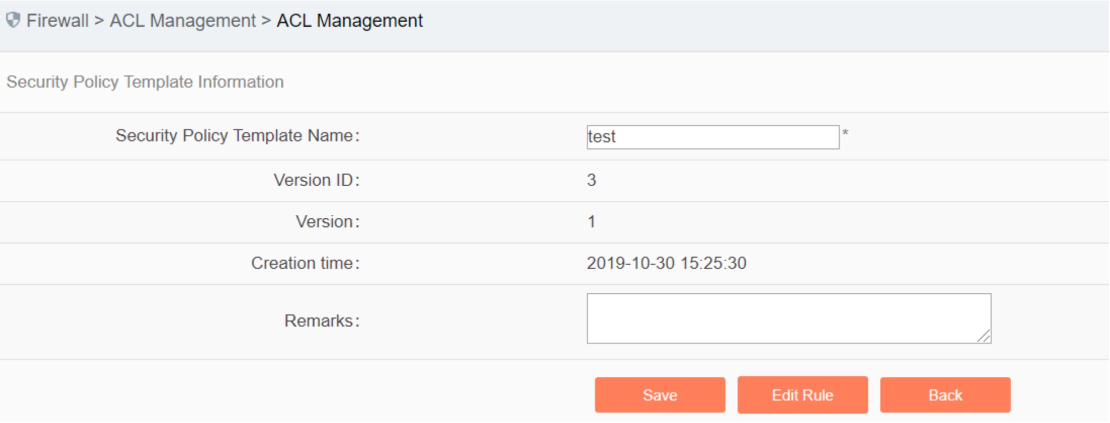
Remarks:

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):



Firewall > ACL Management > ACL Management

Security Policy Template Information

Security Policy Template Name: test *

Version ID: 3

Version: 1

Creation time: 2019-10-30 15:25:30

Remarks:

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

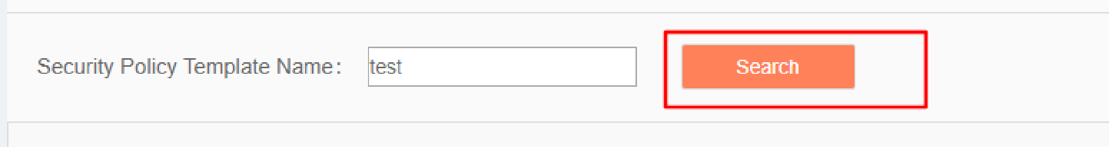
3.6.3.3. Delete a security policy template

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):



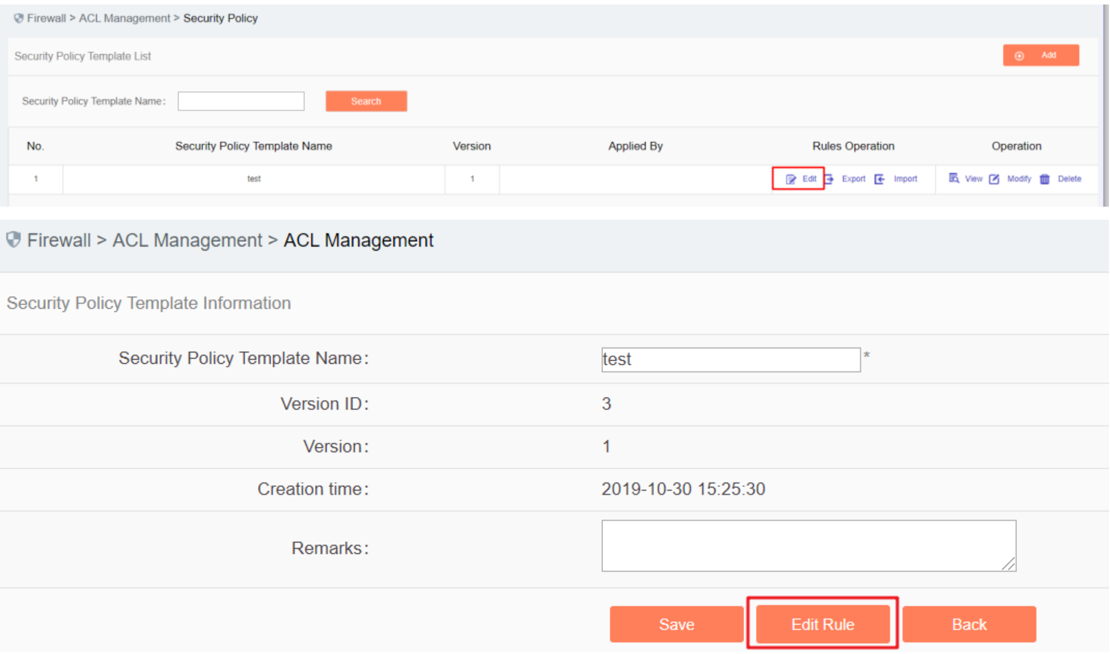
Security Policy Template Name: test

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):



Firewall > ACL Management > Security Policy

Security Policy Template List

Security Policy Template Name:

No.	Security Policy Template Name	Version	Applied By	Rules Operation	Operation
1	test	1		Edit Export Import	View Modify Delete

Firewall > ACL Management > ACL Management

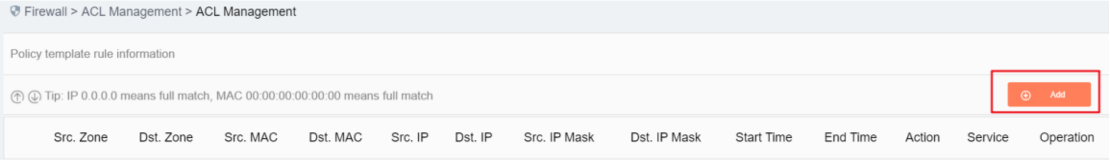
Security Policy Template Information

Security Policy Template Name:	test *
Version ID:	3
Version:	1
Creation time:	2019-10-30 15:25:30
Remarks:	

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):



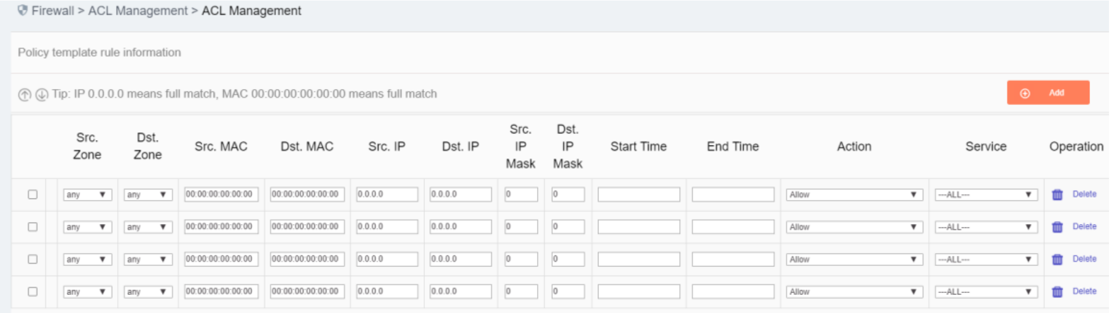
Firewall > ACL Management > ACL Management

Policy template rule information

Tip: IP 0.0.0.0 means full match, MAC 00:00:00:00:00:00 means full match

Src. Zone	Dst. Zone	Src. MAC	Dst. MAC	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Start Time	End Time	Action	Service	Operation

Fig.3-73 Security Policy Rule Add Buttons



Firewall > ACL Management > ACL Management

Policy template rule information

Tip: IP 0.0.0.0 means full match, MAC 00:00:00:00:00:00 means full match

	Src. Zone	Dst. Zone	Src. MAC	Dst. MAC	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Start Time	End Time	Action	Service	Operation
□	any	any	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow	---ALL---	Delete
□	any	any	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow	---ALL---	Delete
□	any	any	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow	---ALL---	Delete
□	any	any	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow	---ALL---	Delete

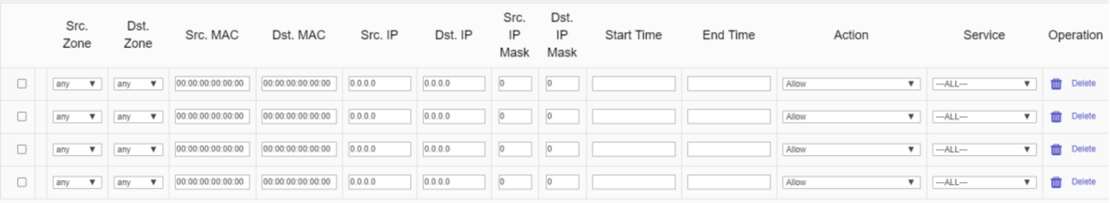
Fig.3-74 New Security Policy Rules

Tab.21 Instruction to Security Policy Rule Fields

<table>
<tr><th>Column Names</th><th colspan="2">Instructions</th></tr>
<tr><td>Src. Zone</td><td colspan="2">The security area initiating a data request, with "any" indicating full match</td></tr>
<tr><td>Dst. Zone</td><td colspan="2">The destination security area for the data request, with "any" indicating full match</td></tr>
<tr><td>Src. MAC</td><td colspan="2">The MAC address initiating a data request, in format of "00:00:00:00:00:00"</td></tr>
<tr><td>Dst. MAC</td><td colspan="2">The destination MAC address requesting the data, in the format of "00:00:00:00:00:00"</td></tr>
<tr><td>Src. IP</td><td colspan="2">The IP address initiating a data request, in dotted decimal format</td></tr>
<tr><td>Dst. IP</td><td colspan="2">The destination IP address requesting data, in dotted decimal format</td></tr>
<tr><td>Src. IP mask</td><td colspan="2">The mask of the source IP, with the value taken usually from 0 to 32</td></tr>
<tr><td>Dst. IP mask</td><td colspan="2">The mask of the destination IP, with the value taken usually from 0 to 32</td></tr>
<tr><td>Start Time</td><td colspan="2">The starting point-in-time at which the rule takes effect</td></tr>
<tr><td>End Time</td><td colspan="2">The last point-in-time at which the rules are no longer valid</td></tr>
<tr><td>Action</td><td colspan="2">When the rule is hit, the firewall processes the packet, passes, blocks, or passes and logs it</td></tr>
<tr><td>Service</td><td colspan="2">The service types supported by the rule</td></tr>
<tr><td rowspan="2">Operation</td><td>Save</td><td>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</td></tr>
<tr><td>Back</td><td>Ignore all modifications and go back to the security policy management template information list display page</td></tr>
</table>

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):



	Src. Zone	Dst. Zone	Src. MAC	Dst. MAC	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Start Time	End Time	Action	Service	Operation
□	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	🗑 Delete
□	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	🗑 Delete
□	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	🗑 Delete
□	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	🗑 Delete

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

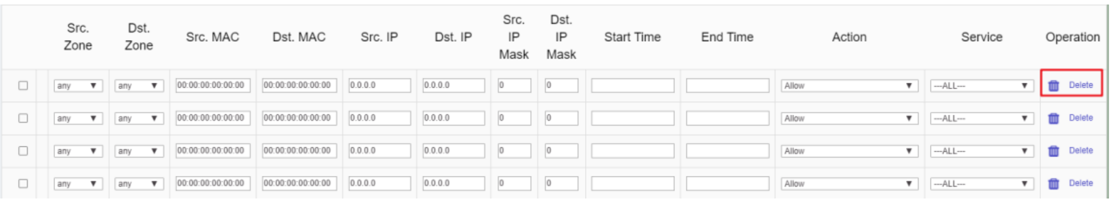
If the template is new, the rule item is blank when viewed, and the rules can be viewed after completing the corresponding add operation as per the following section. Click <Back> and go back to the [Security Policy Management] template list display page.

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, a 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):



	Src. Zone	Dst. Zone	Src. MAC	Dst. MAC	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Start Time	End Time	Action	Service	Operation
☐	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	Delete
☐	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	Delete
☐	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	Delete
☐	any ▼	any ▼	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow ▼	---ALL--- ▼	Delete

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 firewall 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.

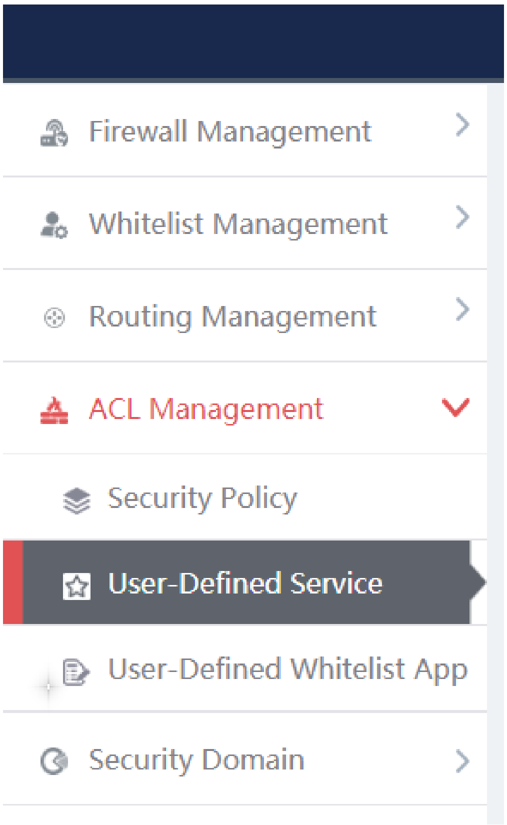
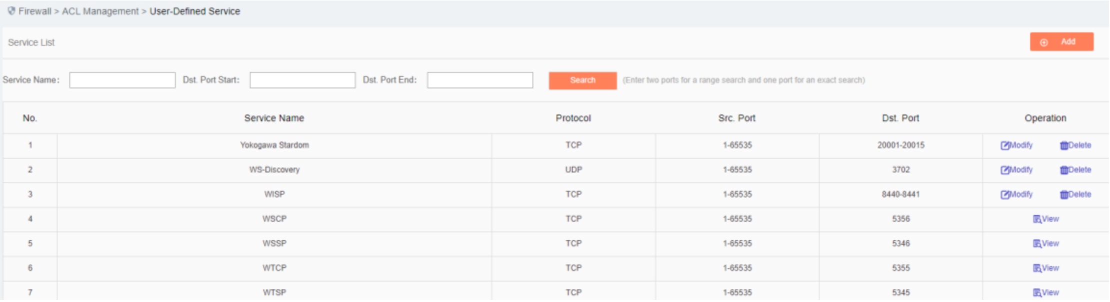


Fig.3-77 Selecting a custom service

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):



Firewall > ACL Management > User-Defined Service

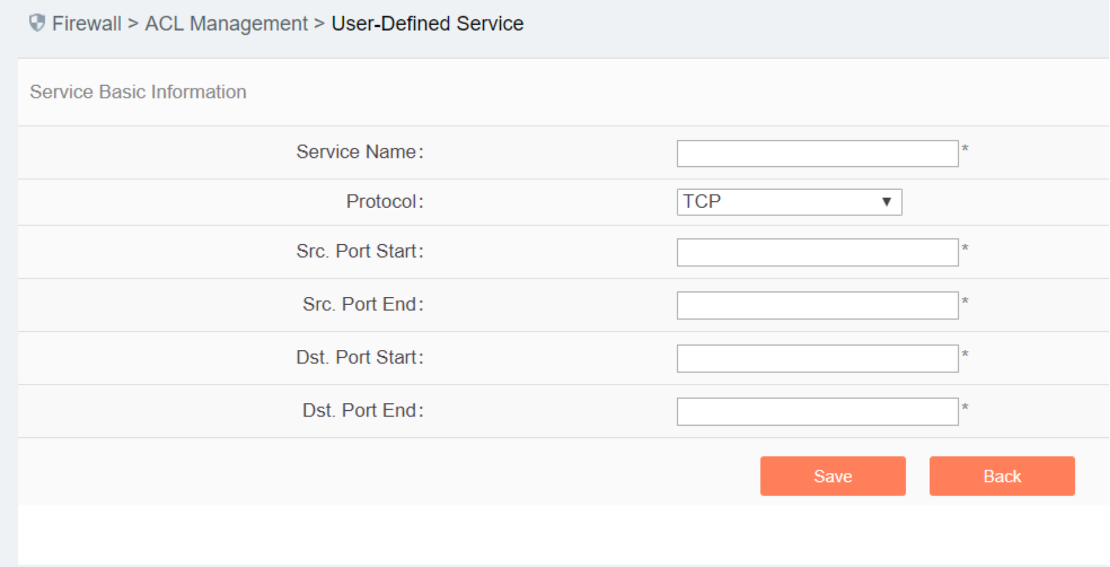
Service List

Service Name: Dst. Port Start: Dst. Port End:

(Enter two ports for a range search and one port for an exact search)

No.	Service Name	Protocol	Src. Port	Dst. Port	Operation
1	Yokogawa Stardom	TCP	1-65535	20001-20015	Modify Delete
2	WS-Discovery	UDP	1-65535	3702	Modify Delete
3	WISP	TCP	1-65535	8440-8441	Modify Delete
4	WSCP	TCP	1-65535	5356	View
5	WSSP	TCP	1-65535	5346	View
6	WTCP	TCP	1-65535	5355	View
7	WTSP	TCP	1-65535	5345	View

Fig.3-78 Custom Service Add Button



Firewall > ACL Management > User-Defined Service

Service Basic Information

Service Name:	*
Protocol:	TCP ▼
Src. Port Start:	*
Src. Port End:	*
Dst. Port Start:	*
Dst. Port End:	*

Fig.3-79 Custom Service Add Page

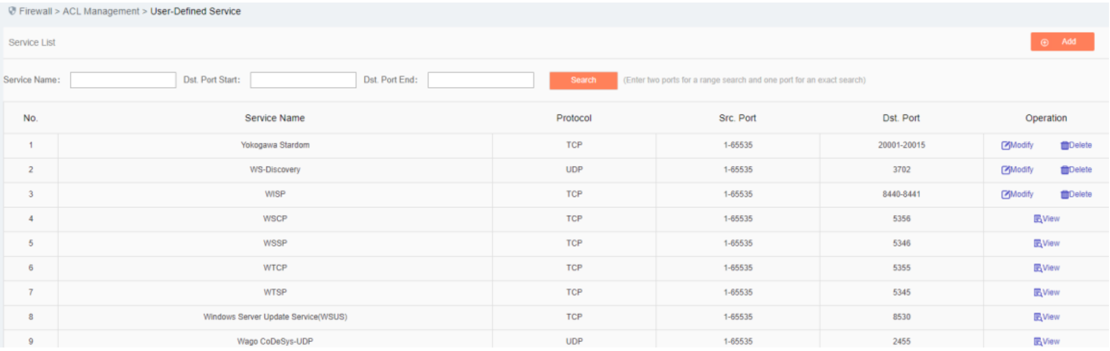
Tab.22 Instruction to custom service Add Fields

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):



Firewall > ACL Management > User-Defined Service

Service List

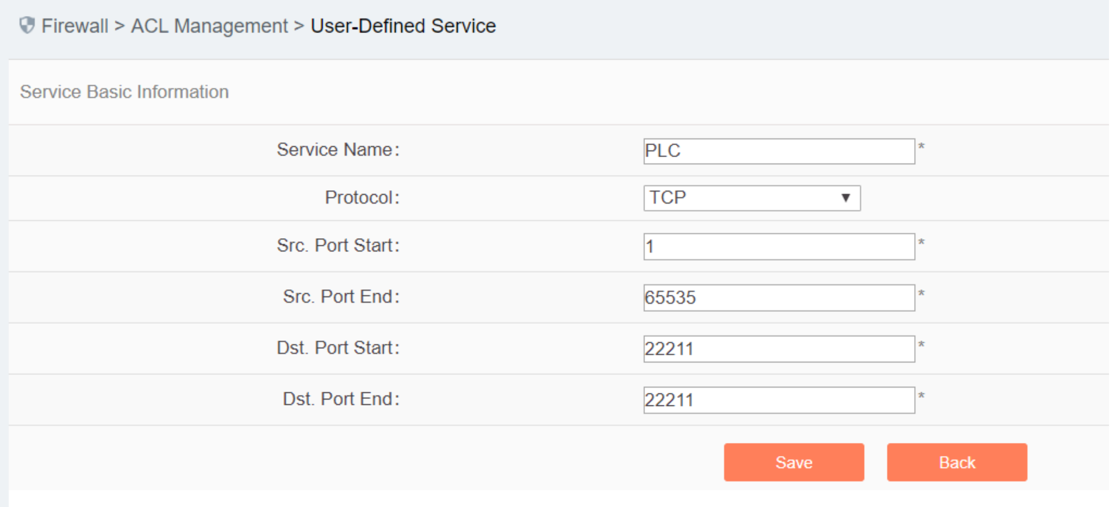
Add
Service Name:
Dst. Port Start:
Dst. Port End:
Search
(Enter two ports for a range search and one port for an exact search)

No.	Service Name	Protocol	Src. Port	Dst. Port	Operation
1	Yokogawa Stardom	TCP	1-65535	20001-20015	Modify Delete
2	WS-Discovery	UDP	1-65535	3702	Modify Delete
3	WISP	TCP	1-65535	8440-8441	Modify Delete
4	WSCP	TCP	1-65535	5356	View
5	WSSP	TCP	1-65535	5346	View
6	WTCP	TCP	1-65535	5355	View
7	WTSP	TCP	1-65535	5345	View
8	Windows Server Update Service(WSUS)	TCP	1-65535	8530	View
9	Wago CoDeSys-UDP	UDP	1-65535	2455	View

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):



Firewall > ACL Management > User-Defined Service

Service Basic Information

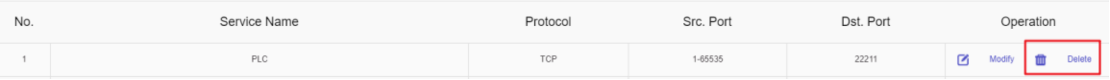
Service Name:	PLC *
Protocol:	TCP ▼
Src. Port Start:	1 *
Src. Port End:	65535 *
Dst. Port Start:	22211 *
Dst. Port End:	22211 *

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):



No.	Service Name	Protocol	Src. Port	Dst. Port	Operation
1	PLC	TCP	1-65535	22211	Modify Delete

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):

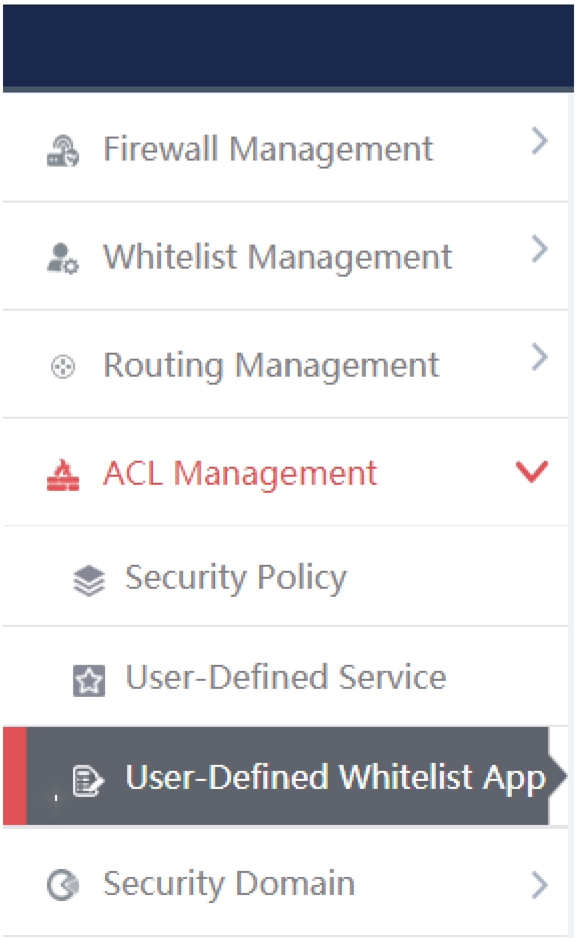
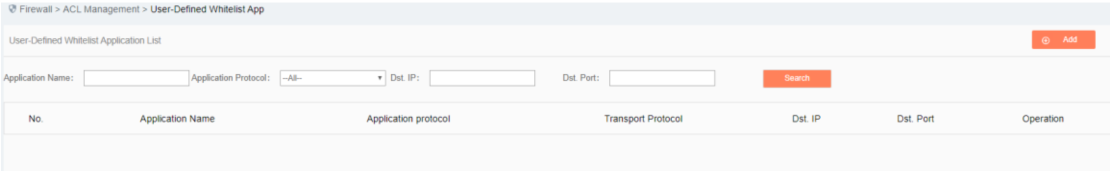


Fig.3-83 Selecting a User-Defined Whitelist Application



Firewall > ACL Management > User-Defined Whitelist App

User-Defined Whitelist Application List

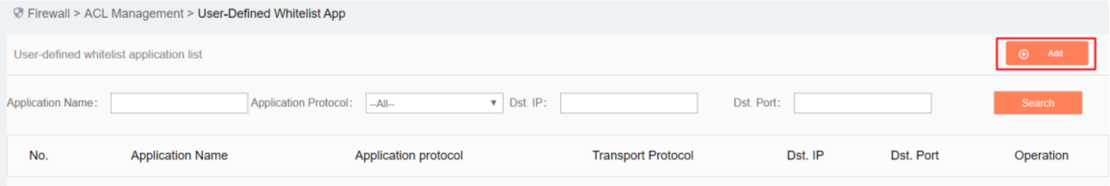
Application Name: Application Protocol: --All-- Dst. IP: Dst. Port:

No.	Application Name	Application protocol	Transport Protocol	Dst. IP	Dst. Port	Operation

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):



Firewall > ACL Management > User-Defined Whitelist App

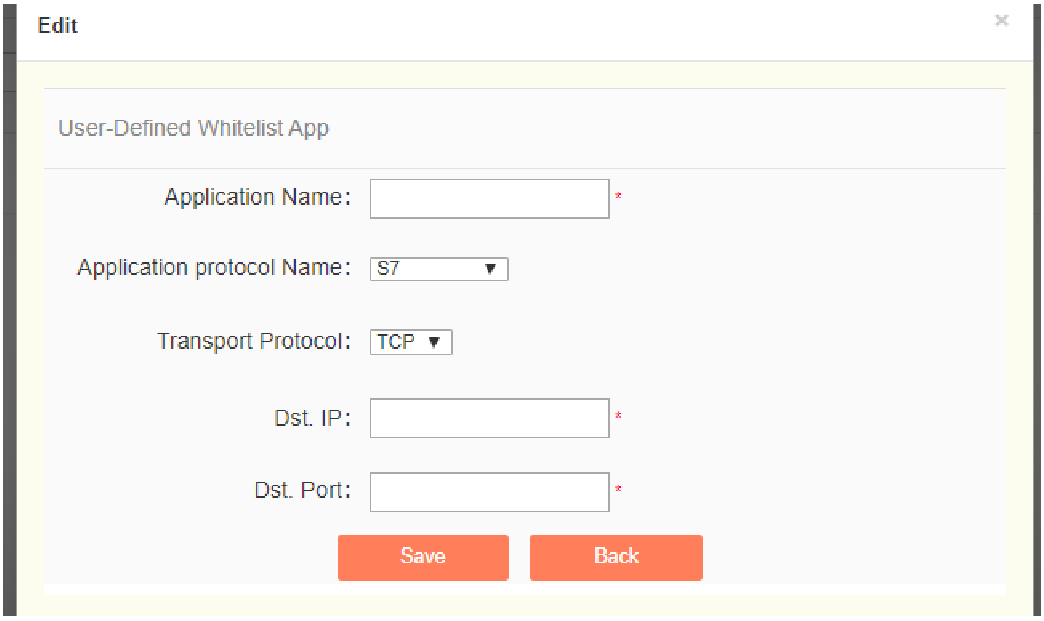
User-defined whitelist application list

Add

Application Name: Application Protocol: --All-- Dst. IP: Dst. Port: Search

No.	Application Name	Application protocol	Transport Protocol	Dst. IP	Dst. Port	Operation

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



Edit

User-Defined Whitelist App

Application Name: *

Application protocol Name: S7

Transport Protocol: TCP

Dst. IP: *

Dst. Port: *

Save Back

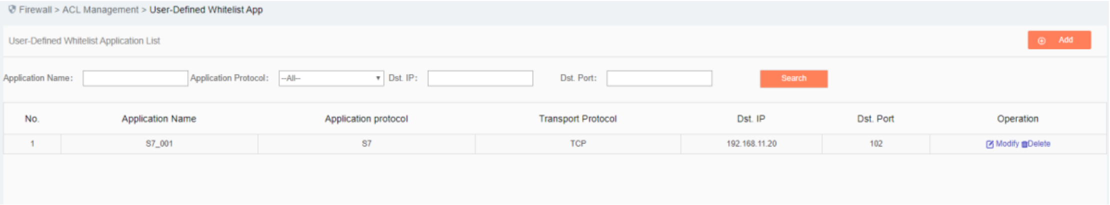
Fig.3-86 User-Defined Whitelist Application Add Page

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):


Firewall > ACL Management > User-Defined Whitelist App

User-Defined Whitelist Application List

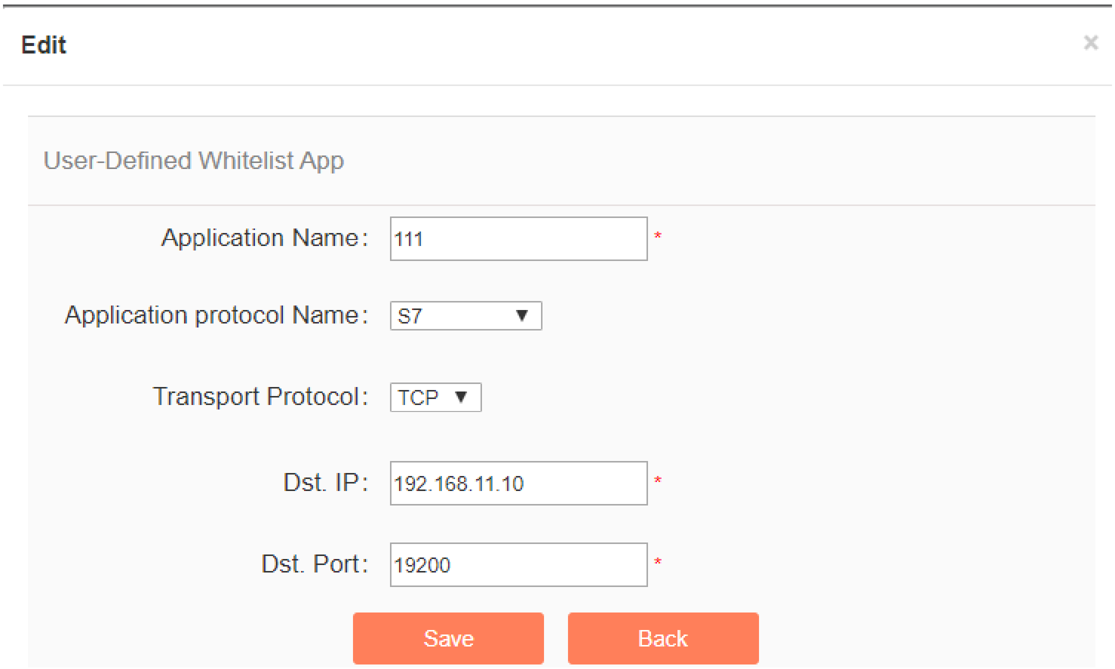
Application Name: Application Protocol: --All-- Dst. IP: Dst. Port:

No.	Application Name	Application protocol	Transport Protocol	Dst. IP	Dst. Port	Operation
1	S7_001	S7	TCP	192.168.11.20	102	Modify Delete

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):


Edit

User-Defined Whitelist App

Application Name: 111 *

Application protocol Name: S7

Transport Protocol: TCP

Dst. IP: 192.168.11.10 *

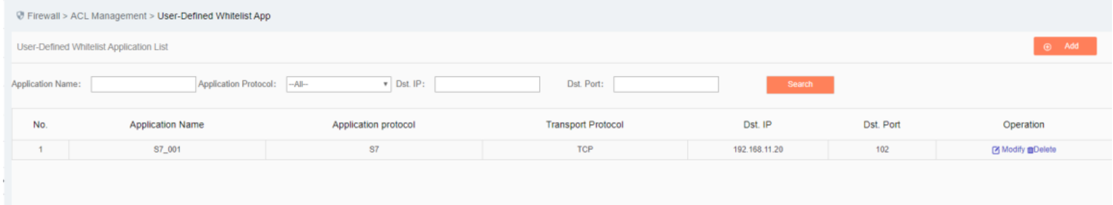
Dst. Port: 19200 *

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):


Firewall > ACL Management > User-Defined Whitelist App

User-Defined Whitelist Application List

Application Name: Application Protocol: --All-- Dst. IP: Dst. Port:

No.	Application Name	Application protocol	Transport Protocol	Dst. IP	Dst. Port	Operation
1	S7_001	S7	TCP	192.168.11.20	102	Modify Delete

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 firewall 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):

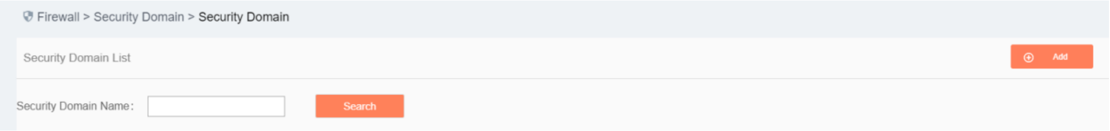


Fig.3-90 Security Domain Add Button

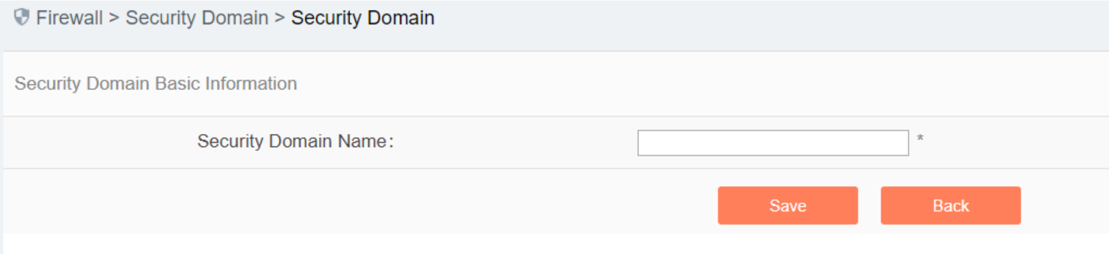

Firewall > Security Domain > Security Domain
Security Domain Basic Information
Security Domain Name:
*
Save
Back

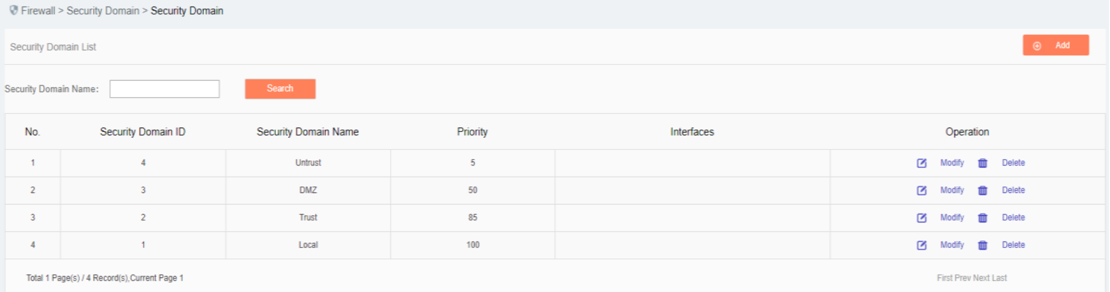
Fig.3-91 Security Domain Add Page

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):



Firewall > Security Domain > Security Domain

Security Domain List

Security Domain Name:

No.	Security Domain ID	Security Domain Name	Priority	Interfaces	Operation
1	4	Untrust	5		Modify Delete
2	3	DMZ	50		Modify Delete
3	2	Trust	85		Modify Delete
4	1	Local	100		Modify Delete

Total 1 Page(s) / 4 Record(s),Current Page 1

Fig.3-92 Security Domain Management Page

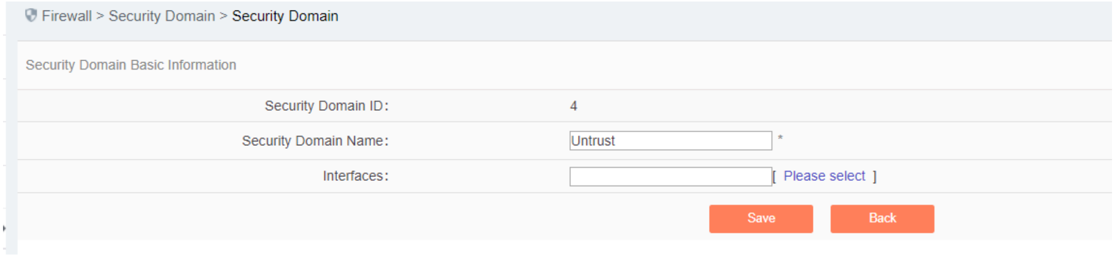
There are two basic Security Domain types, that is, Security Domains built in by the system, and Security Domains created by a user himself. The former only allows to modify the priority, including these two properties of firewalls; the latter can modify all other properties except ID. View all the Security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



Firewall > Security Domain > Security Domain

Security Domain Basic Information

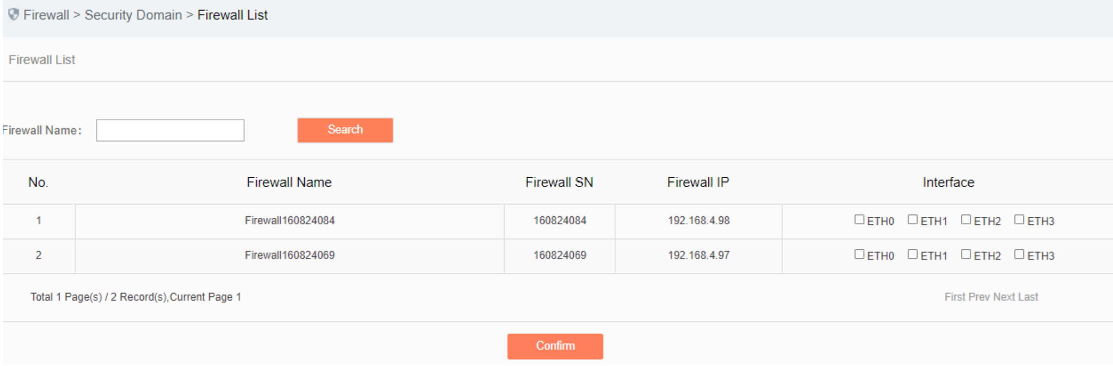
Security Domain ID: 4

Security Domain Name: Untrust *

Interfaces: [Please select]

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):



Firewall > Security Domain > Firewall List

Firewall List

Firewall Name:

No.	Firewall Name	Firewall SN	Firewall IP	Interface
1	Firewall160824084	160824084	192.168.4.98	□ETH0 □ETH1 □ETH2 □ETH3
2	Firewall160824069	160824069	192.168.4.97	□ETH0 □ETH1 □ETH2 □ETH3

Total 1 Page(s) / 2 Record(s),Current Page 1

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.

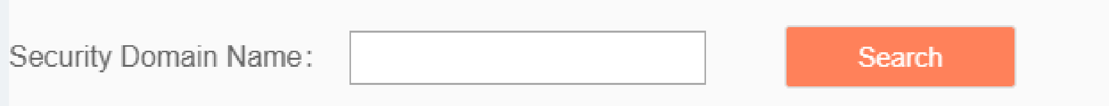
3.7.5. Delete a Security Domain

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):



Security Domain Name:

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):

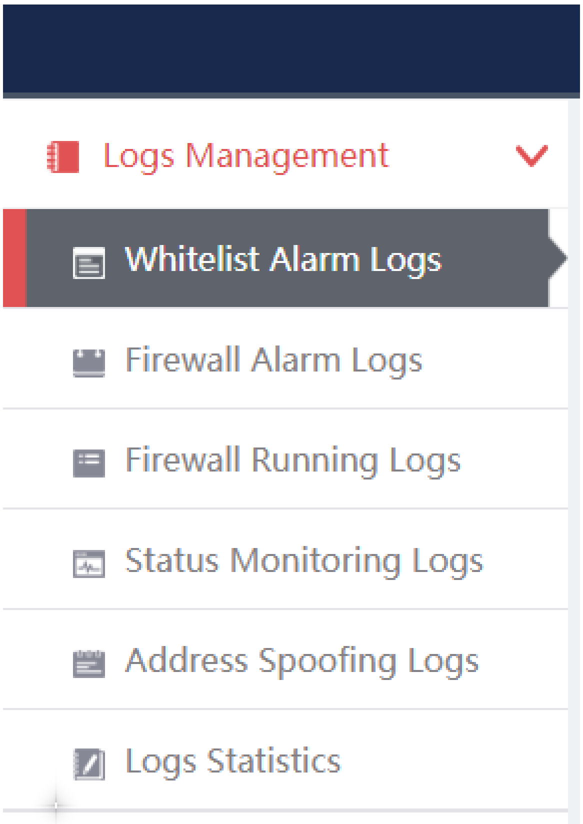
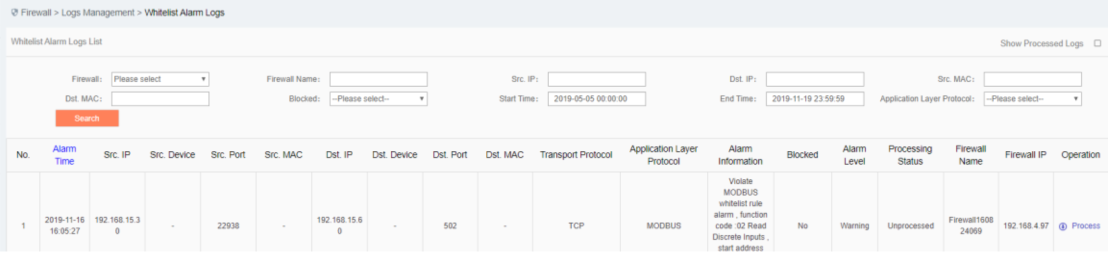


Fig.3-96 Whitelist Alarm Log Menu



Firewall > Logs Management > Whitelist Alarm Logs

Whitelist Alarm Logs List

Show Processed Logs □

Firewall: Please select ▾ Firewall Name: Src. IP: Dst. IP: Src. MAC:

Dst. MAC: Blocked: --Please select-- ▾ Start Time: 2019-05-05 00:00:00 End Time: 2019-11-19 23:59:59 Application Layer Protocol: --Please select-- ▾

Search

No.	Alarm Time	Src. IP	Src. Device	Src. Port	Src. MAC	Dst. IP	Dst. Device	Dst. Port	Dst. MAC	Transport Protocol	Application Layer Protocol	Alarm Information	Blocked	Alarm Level	Processing Status	Firewall Name	Firewall IP	Operation
1	2019-11-16 16:05:27	192.168.15.30	-	22938	-	192.168.15.60	-	502	-	TCP	MODBUS	Violate MODBUS whitelist rule alarm , function code :02 Read Discrete Inputs , start address	No	Warning	Unprocessed	Firewall160824069	192.168.4.97	Process

Fig.3-97 Whitelist Alarm Log List Page

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

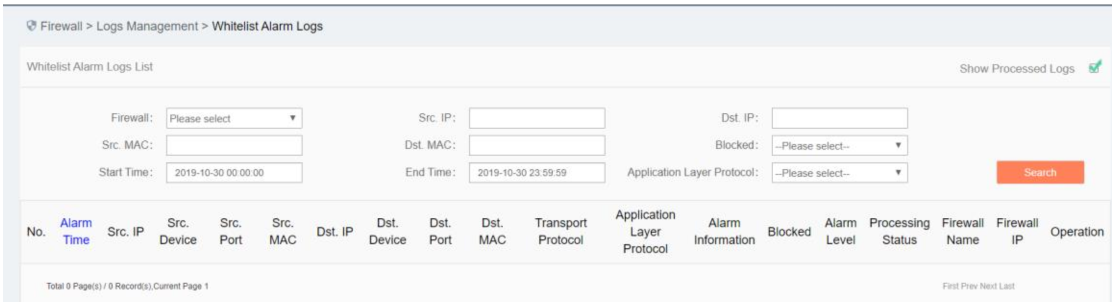
Tab.26 Instruction to Whitelist Alarm Log Display

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):



Firewall > Logs Management > Whitelist Alarm Logs

Whitelist Alarm Logs List

Show Processed Logs ☑

Firewall: Please select

Src. IP:

Dst. IP:

Src. MAC:

Dst. MAC:

Blocked: --Please select--

Start Time: 2019-10-30 00:00:00

End Time: 2019-10-30 23:59:59

Application Layer Protocol: --Please select--

Search

No.	Alarm Time	Src. IP	Src. Device	Src. Port	Src. MAC	Dst. IP	Dst. Device	Dst. Port	Dst. MAC	Transport Protocol	Application Layer Protocol	Alarm Information	Blocked	Alarm Level	Processing Status	Firewall Name	Firewall IP	Operation

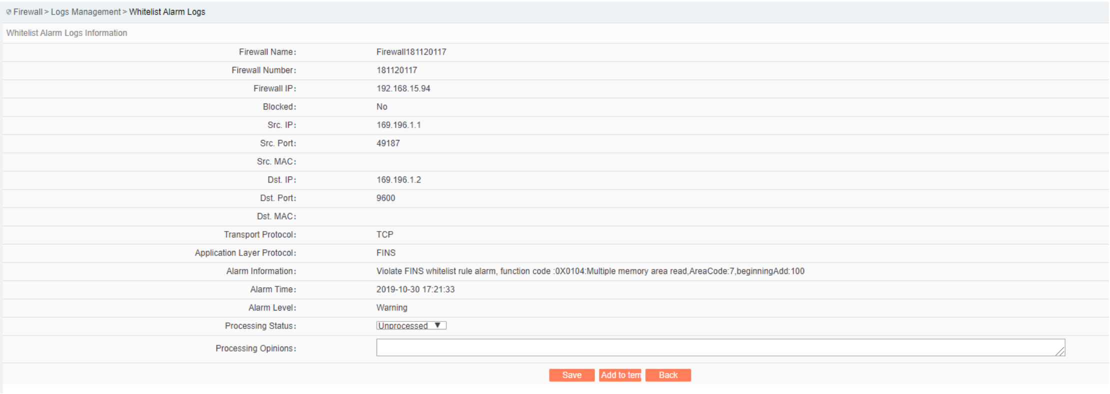
Total 0 Page(s) / 0 Record(s),Current Page 1

First Prev Next Last

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):


Firewall > Logs Management > Whitelist Alarm Logs

Whitelist Alarm Logs Information

Firewall Name:	Firewall181120117
Firewall Number:	181120117
Firewall IP:	192.168.15.94
Blocked:	No
Src. IP:	169.196.1.1
Src. Port:	49187
Src. MAC:	
Dst. IP:	169.196.1.2
Dst. Port:	9600
Dst. MAC:	
Transport Protocol:	TCP
Application Layer Protocol:	FINS
Alarm Information:	Violate FINS whitelist rule alarm, function code :0X0104:Multiple memory area read,AreaCode:7,beginningAdd:100
Alarm Time:	2019-10-30 17:21:33
Alarm Level:	Warning
Processing Status:	Unprocessed ▼
Processing Opinions:	

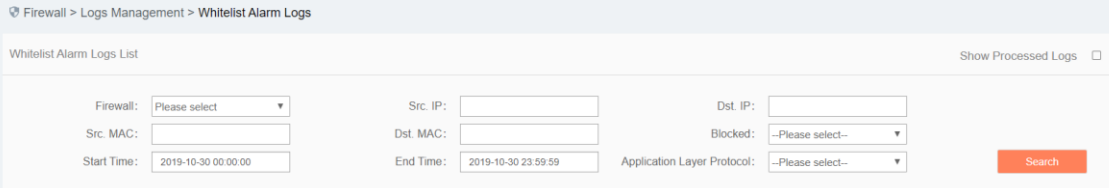
Fig.3-99 Whitelist Alarm Processing Page

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):


Firewall > Logs Management > Whitelist Alarm Logs

Whitelist Alarm Logs List

Show Processed Logs □

Firewall:	Please select ▼	Src. IP:		Dst. IP:	
Src. MAC:		Dst. MAC:		Blocked:	--Please select-- ▼
Start Time:	2019-10-30 00:00:00	End Time:	2019-10-30 23:59:59	Application Layer Protocol:	--Please select-- ▼

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, if 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):

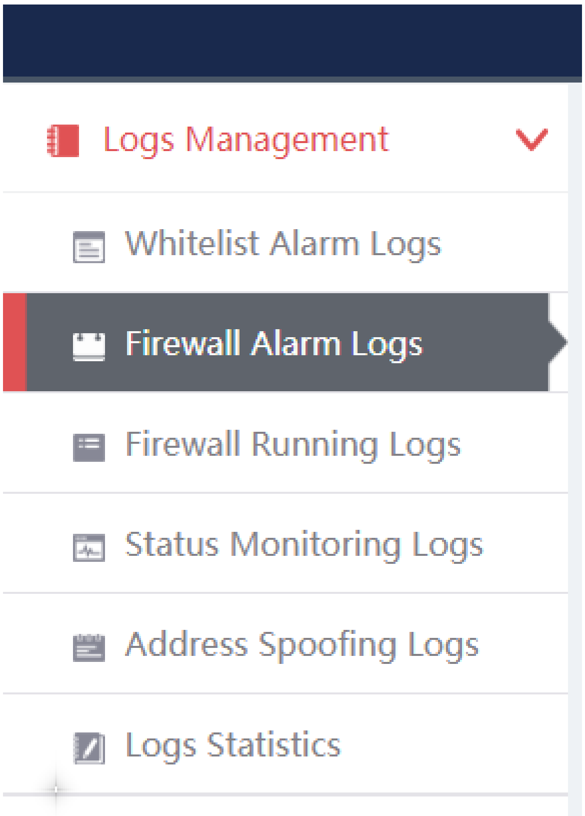
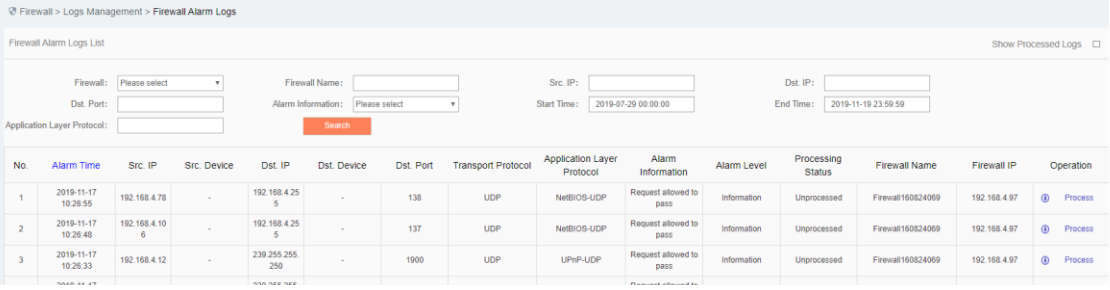


Fig.3-101 Firewall Alarm Log Menu


Firewall > Logs Management > Firewall Alarm Logs

Firewall Alarm Logs List

Show Processed Logs □

Firewall: Please select ▾
Firewall Name:
Src. IP:
Dst. IP:
Dst. Port:
Alarm Information: Please select ▾
Start Time: 2019-07-29 00:00:00
End Time: 2019-11-19 23:59:59
Application Layer Protocol:

Search

No.	Alarm Time	Src. IP	Src. Device	Dst. IP	Dst. Device	Dst. Port	Transport Protocol	Application Layer Protocol	Alarm Information	Alarm Level	Processing Status	Firewall Name	Firewall IP	Operation
1	2019-11-17 10:26:55	192.168.4.78	-	192.168.4.255	-	138	UDP	NetBIOS-UDP	Request allowed to pass	Information	Unprocessed	Firewall160824069	192.168.4.97	Process
2	2019-11-17 10:26:48	192.168.4.106	-	192.168.4.255	-	137	UDP	NetBIOS-UDP	Request allowed to pass	Information	Unprocessed	Firewall160824069	192.168.4.97	Process
3	2019-11-17 10:26:33	192.168.4.12	-	239.255.255.250	-	1900	UDP	UPnP-UDP	Request allowed to pass	Information	Unprocessed	Firewall160824069	192.168.4.97	Process

Fig.3-102 Firewall Alarm Log List Page

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

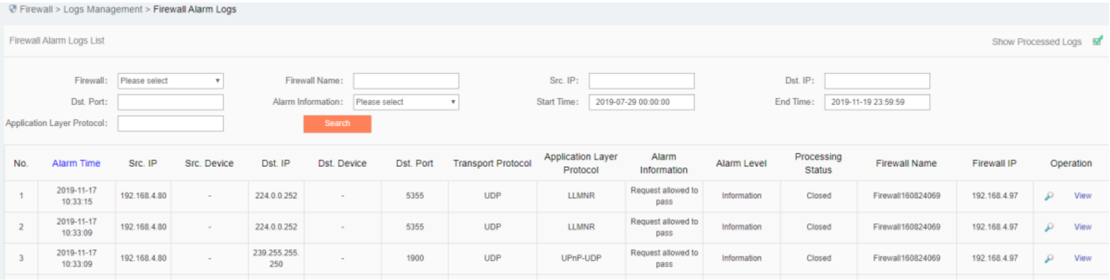
Tab.27 Instruction to Firewall Alarm Log Display

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):



Firewall > Logs Management > Firewall Alarm Logs

Firewall Alarm Logs List

Show Processed Logs ☑

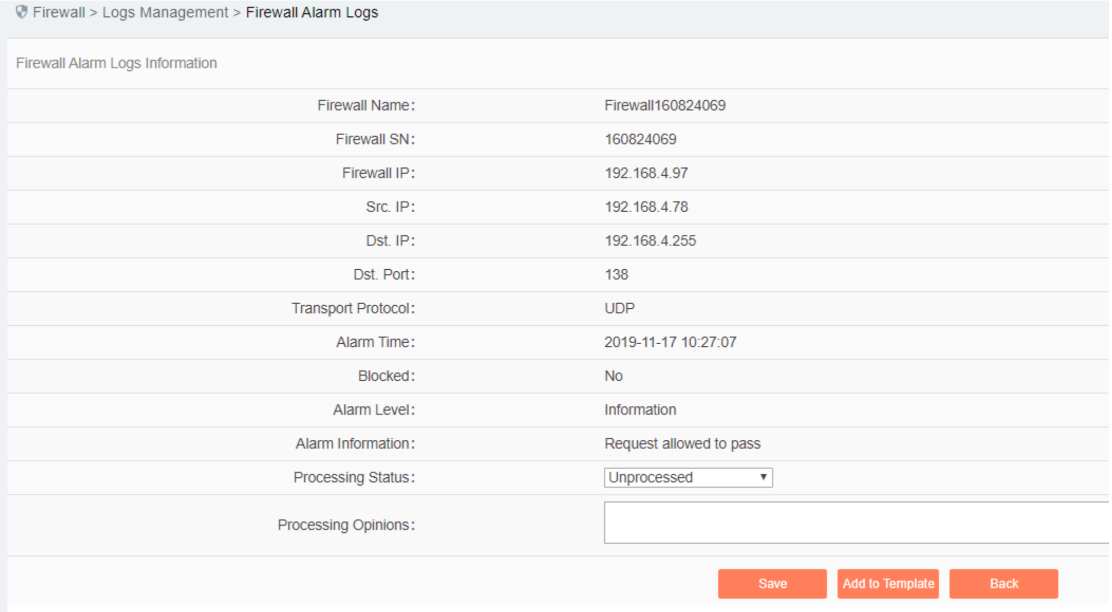
Firewall: Please select
Firewall Name:
Src. IP:
Dst. IP:
Dst. Port:
Alarm Information: Please select
Start Time: 2019-07-29 00:00:00
End Time: 2019-11-19 23:59:59
Application Layer Protocol:

No.	Alarm Time	Src. IP	Src. Device	Dst. IP	Dst. Device	Dst. Port	Transport Protocol	Application Layer Protocol	Alarm Information	Alarm Level	Processing Status	Firewall Name	Firewall IP	Operation
1	2019-11-17 10:33:15	192.168.4.80	-	224.0.0.252	-	5355	UDP	LLMNR	Request allowed to pass	Information	Closed	Firewall160824069	192.168.4.97	View
2	2019-11-17 10:33:09	192.168.4.80	-	224.0.0.252	-	5355	UDP	LLMNR	Request allowed to pass	Information	Closed	Firewall160824069	192.168.4.97	View
3	2019-11-17 10:33:09	192.168.4.80	-	239.255.255.250	-	1900	UDP	UPnP-UDP	Request allowed to pass	Information	Closed	Firewall160824069	192.168.4.97	View

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):



Firewall > Logs Management > Firewall Alarm Logs

Firewall Alarm Logs Information

Firewall Name:	Firewall160824069
Firewall SN:	160824069
Firewall IP:	192.168.4.97
Src. IP:	192.168.4.78
Dst. IP:	192.168.4.255
Dst. Port:	138
Transport Protocol:	UDP
Alarm Time:	2019-11-17 10:27:07
Blocked:	No
Alarm Level:	Information
Alarm Information:	Request allowed to pass
Processing Status:	Unprocessed ▾
Processing Opinions:	

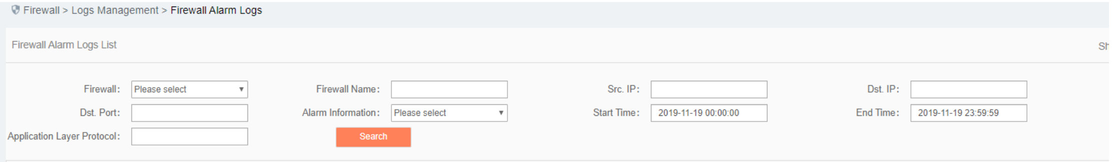
Fig.3-104 Firewall Alarm Processing Page

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):



Firewall > Logs Management > Firewall Alarm Logs

Firewall Alarm Logs List

Firewall:	Please select ▾	Firewall Name:		Src. IP:		Dst. IP:	
Dst. Port:		Alarm Information:	Please select ▾	Start Time:	2019-11-19 00:00:00	End Time:	2019-11-19 23:59:59
Application Layer Protocol:							

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):

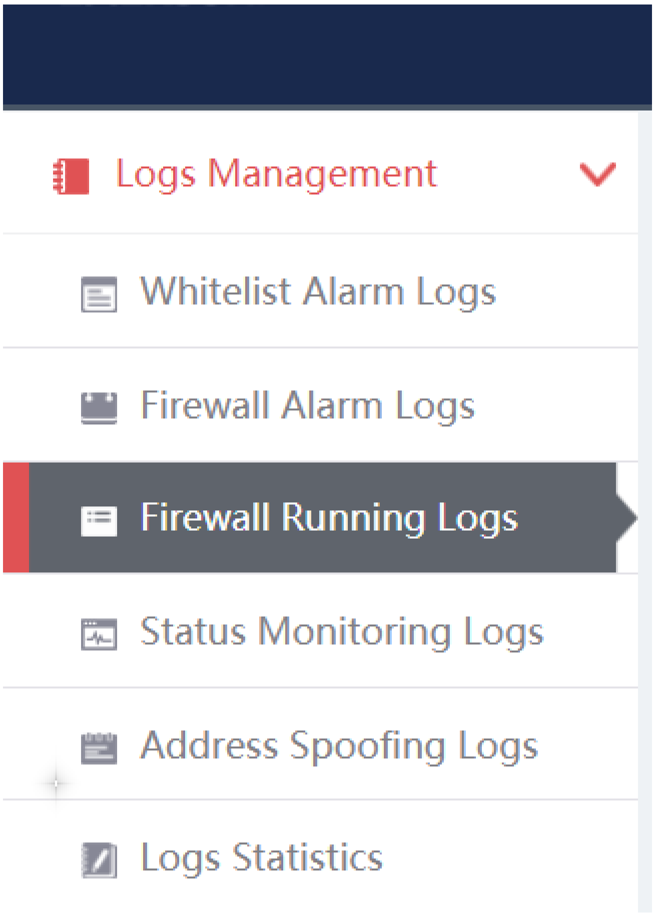
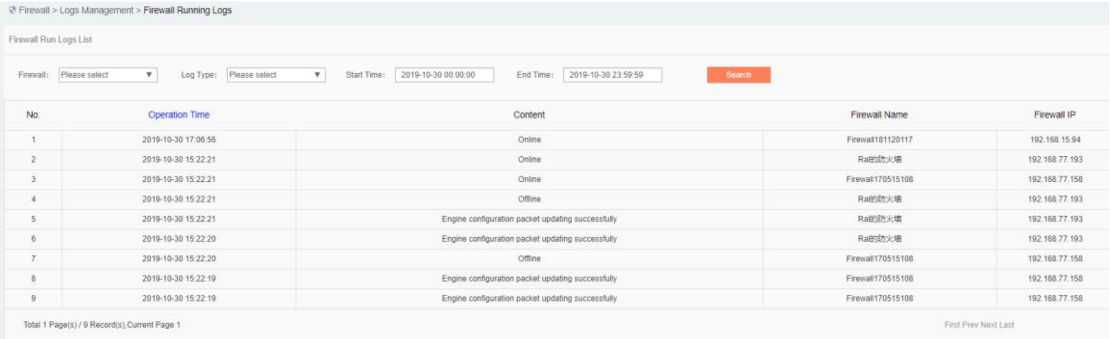


Fig.3-106 Firewall Run Log Menu



Firewall > Logs Management > Firewall Running Logs

Firewall Run Logs List

Firewall: Please select ▼ Log Type: Please select ▼ Start Time: 2019-10-30 00:00:00 End Time: 2019-10-30 23:59:59 Search

No.	Operation Time	Content	Firewall Name	Firewall IP
1	2019-10-30 17:06:56	Online	Firewall181120117	192.168.15.94
2	2019-10-30 15:22:21	Online	Rai的防火墙	192.168.77.193
3	2019-10-30 15:22:21	Online	Firewall170515108	192.168.77.158
4	2019-10-30 15:22:21	Offline	Rai的防火墙	192.168.77.193
5	2019-10-30 15:22:21	Engine configuration packet updating successfully	Rai的防火墙	192.168.77.193
6	2019-10-30 15:22:20	Engine configuration packet updating successfully	Rai的防火墙	192.168.77.193
7	2019-10-30 15:22:20	Offline	Firewall170515108	192.168.77.158
8	2019-10-30 15:22:19	Engine configuration packet updating successfully	Firewall170515108	192.168.77.158
9	2019-10-30 15:22:19	Engine configuration packet updating successfully	Firewall170515108	192.168.77.158

Total 1 Page(s) / 9 Record(s),Current Page 1

First Prev Next Last

Fig.3-107 Firewall Run Log List Page

View the information on all industrial firewall 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):

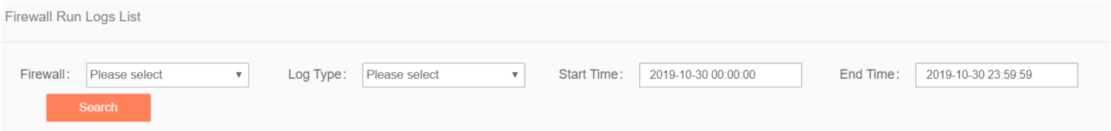


Fig.3-108 Retrieving a Firewall Run Log

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):

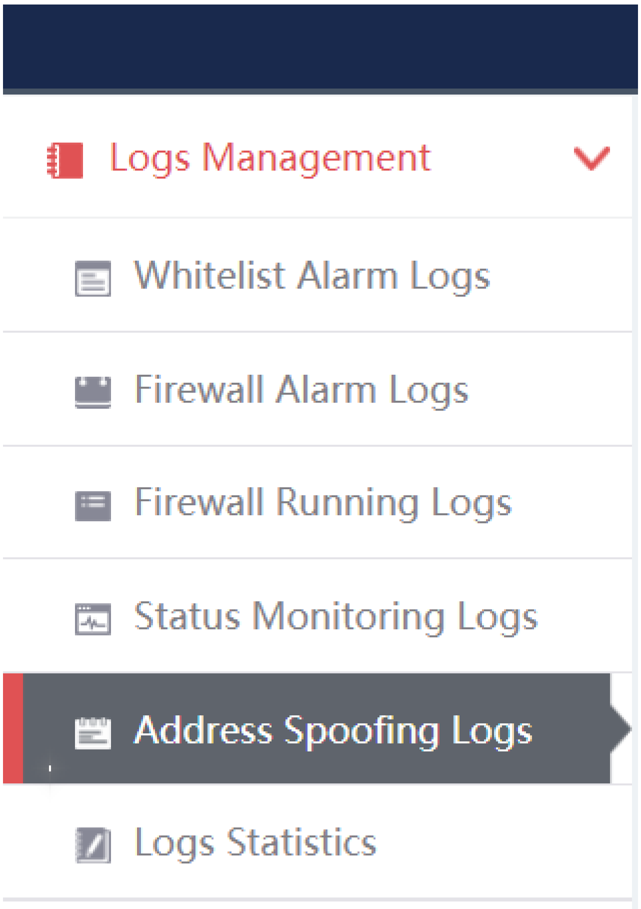
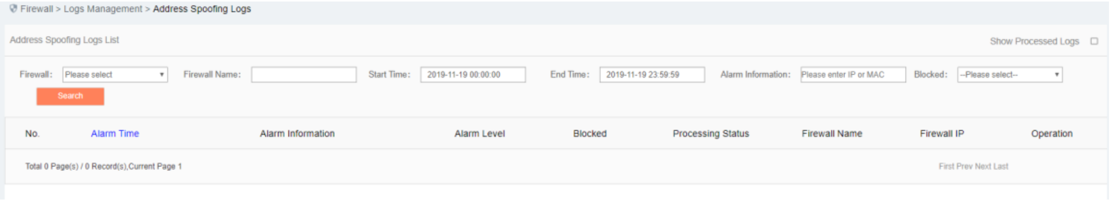


Fig.3-109 Whitelist Alarm Log Menu



Firewall > Logs Management > Address Spoofing Logs

Address Spoofing Logs List

Show Processed Logs □

Firewall: Please select ▾ Firewall Name: Start Time: 2019-11-19 00:00:00 End Time: 2019-11-19 23:59:59 Alarm Information: Please enter IP or MAC Blocked: --Please select-- ▾

Search

No.	Alarm Time	Alarm Information	Alarm Level	Blocked	Processing Status	Firewall Name	Firewall IP	Operation

Total 0 Page(s) / 0 Record(s),Current Page 1

First Prev Next Last

Fig.3-110 Address Spoofing Log List Page

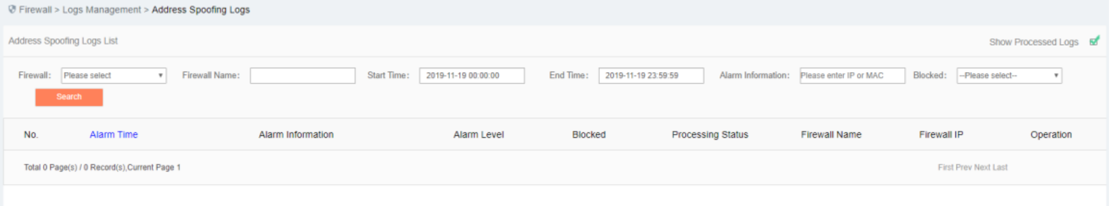
View the information on all address spoofing log s, with the meanings given below:

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):



Firewall > Logs Management > Address Spoofing Logs

Address Spoofing Logs List

Show Processed Logs ☑

Firewall: Please select ▾ Firewall Name: Start Time: 2019-11-19 00:00:00 End Time: 2019-11-19 23:59:59 Alarm Information: Please enter IP or MAC Blocked: --Please select-- ▾

Search

No.	Alarm Time	Alarm Information	Alarm Level	Blocked	Processing Status	Firewall Name	Firewall IP	Operation

Total 0 Page(s) / 0 Record(s),Current Page 1

First Prev Next Last

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 log

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):

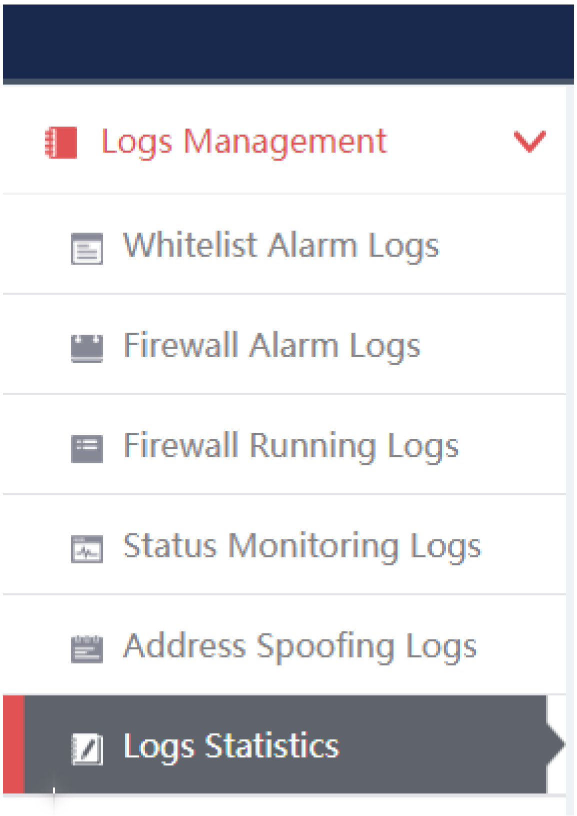
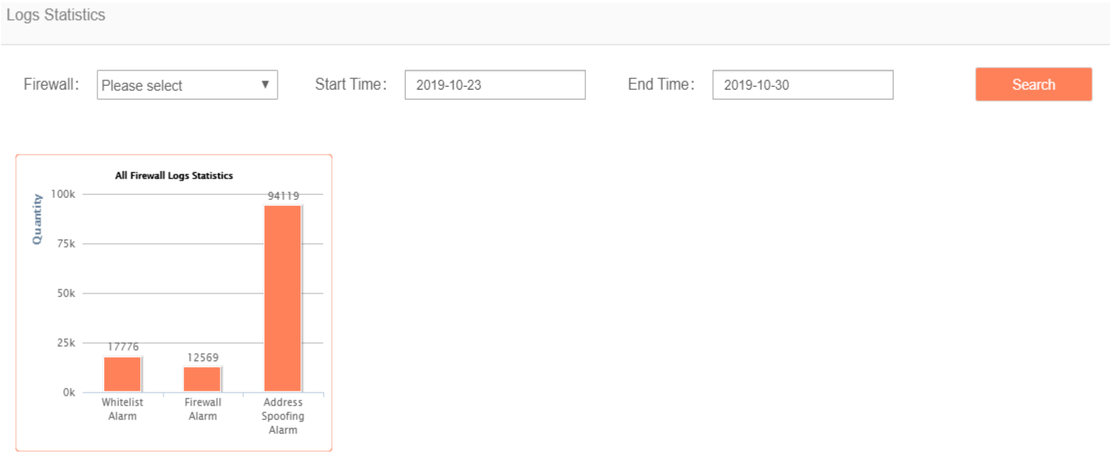


Fig.3-112 Log Statistics Menu



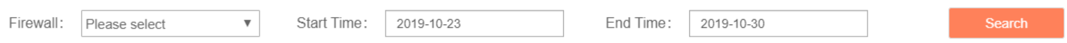
Logs Statistics

Firewall: Please select ▼ Start Time: 2019-10-23 End Time: 2019-10-30 Search

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):



Firewall: Please select ▼ Start Time: 2019-10-23 End Time: 2019-10-30 Search

Fig.3-114 Retrieving Log Statistical Data

4. System Configuration

4.1. System Overview

After successfully logging in the firewall 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):

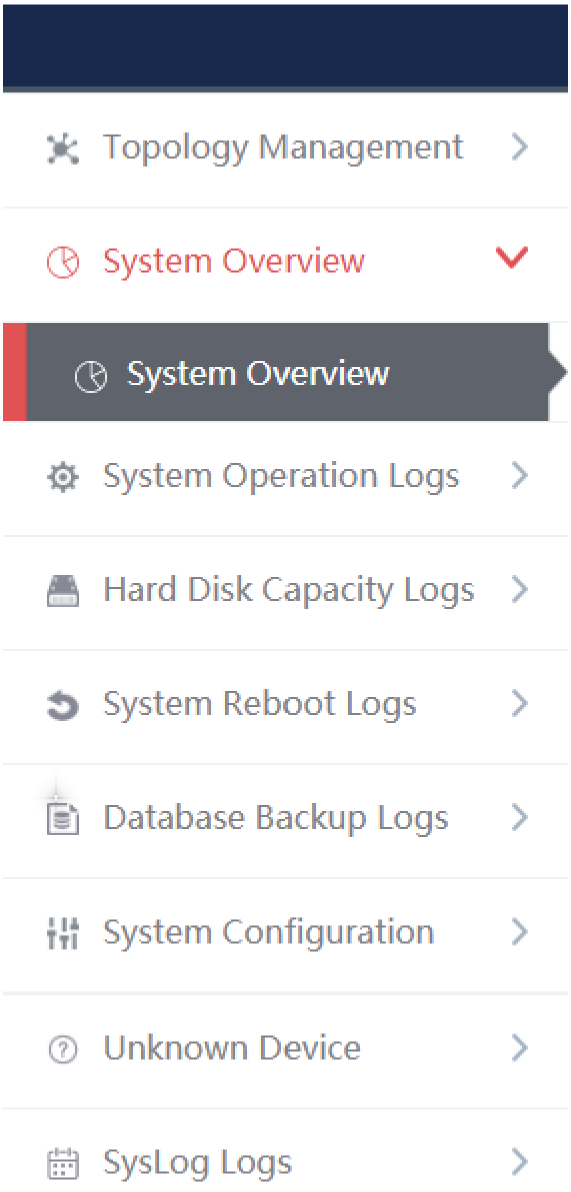


Fig.6-1 System Overview Menu Bar

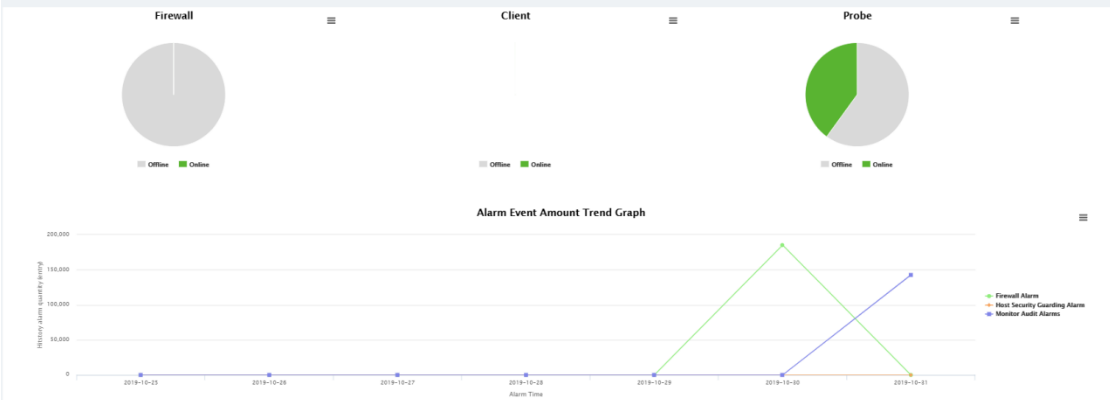


Fig.6-2 System Overview Page

4.1.1. System Overview Display

System overview can view the online status of industrial firewall (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.

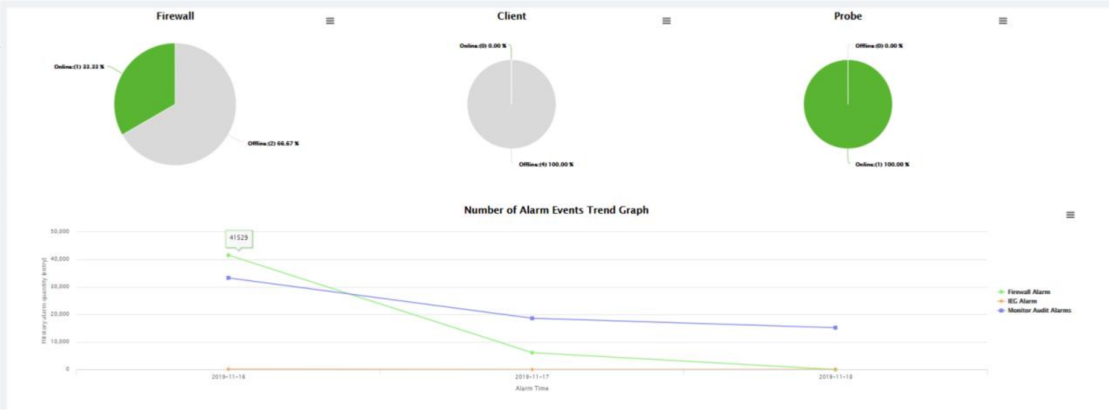


Fig.6-3 Online Status of Device

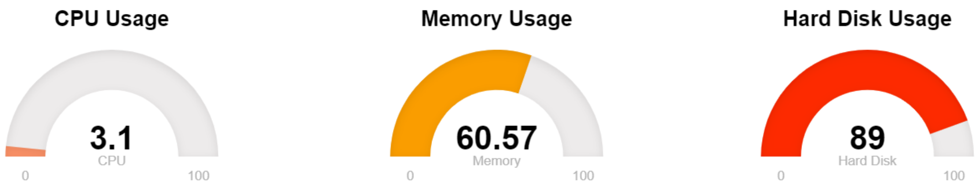
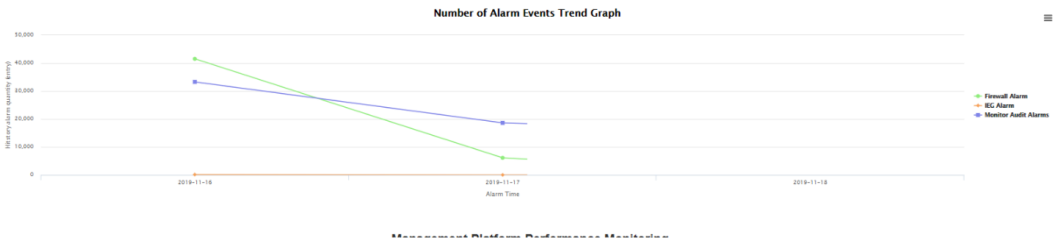


Fig.6-4 Firewall Platform Performance Monitoring



2

Fig.6-5 Alarm Trend

4.2. System Operation Log

After successfully logging in the firewall 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):

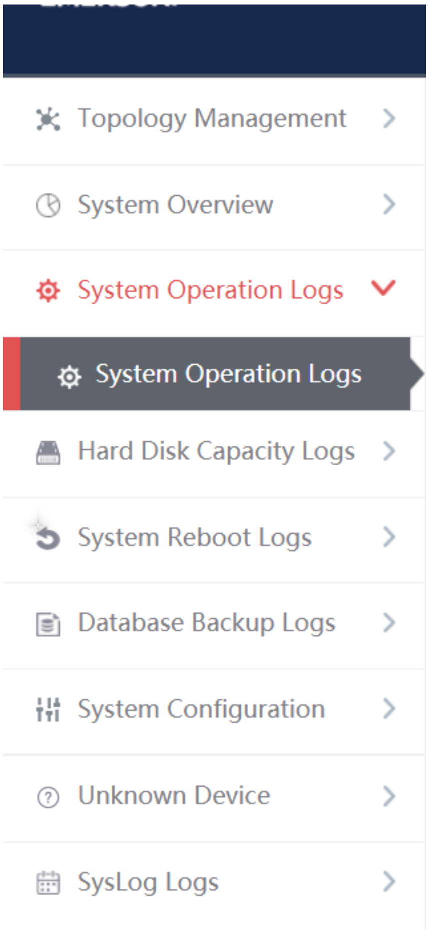
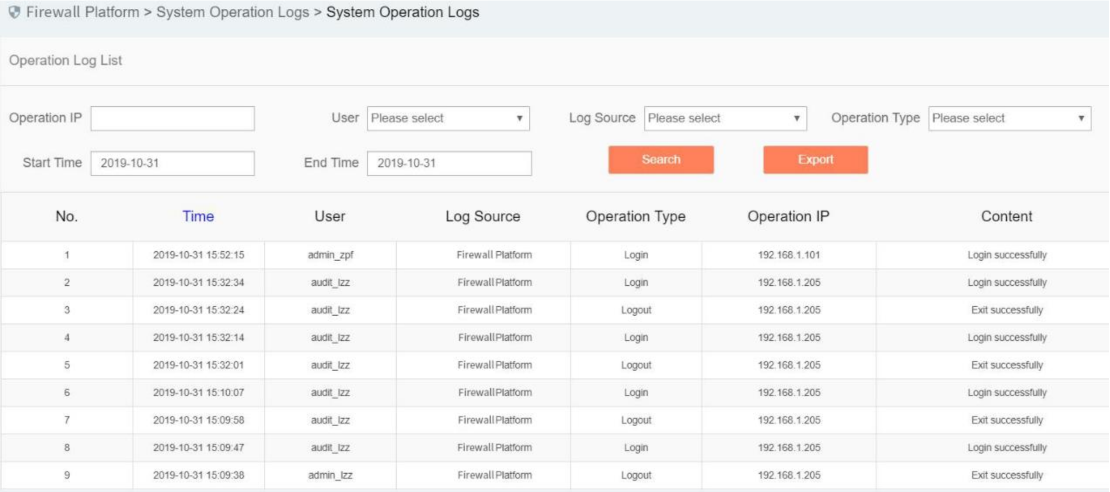


Fig.6-6 System Operation Log Menu Bar



Firewall Platform > System Operation Logs > System Operation Logs

Operation Log List

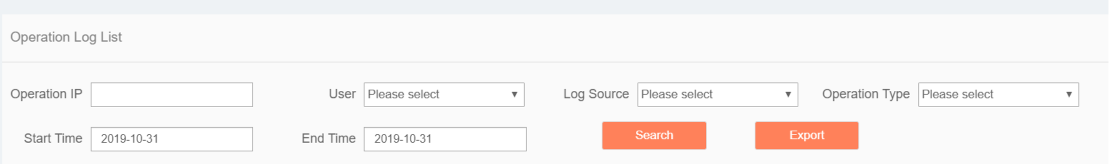
Operation IP
User Please select
Log Source Please select
Operation Type Please select
Start Time 2019-10-31
End Time 2019-10-31

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

Fig.6-7 System Operation Log Page

4.2.1. Retrieve a Log

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



Operation Log List

Operation IP

User Please select

Log Source Please select

Operation Type Please select

Start Time 2019-10-31

End Time 2019-10-31

Fig.6-8 Query Conditions

4.3. Hard Disk Utilization Logs

After successfully logging in the firewall 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):

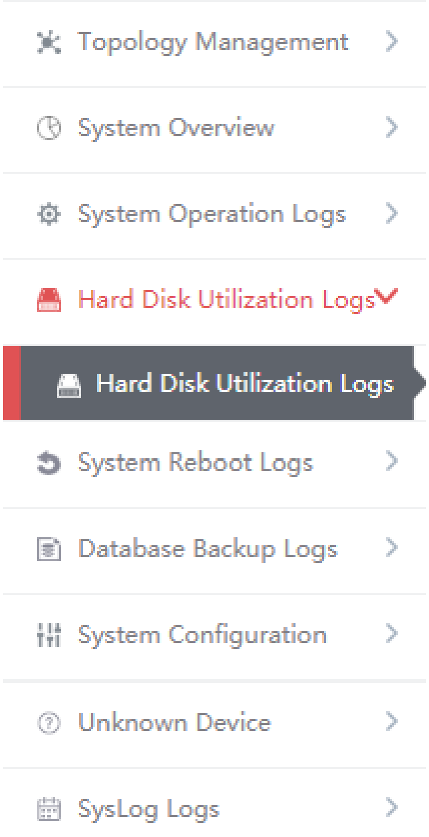
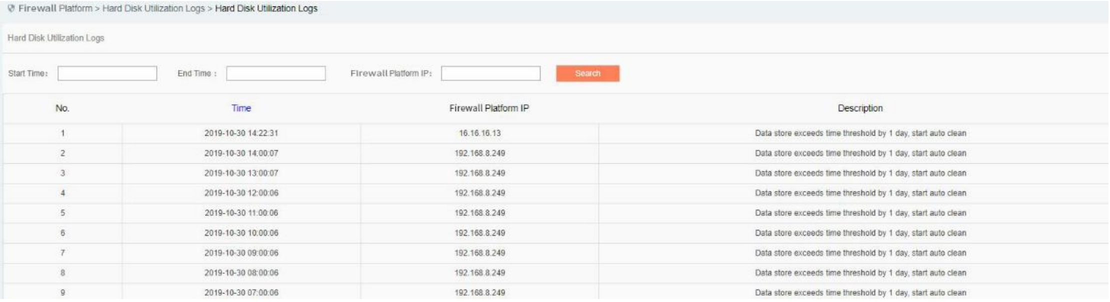


Fig.6-9 Hard Disk Utilization Logs Menu Bar



Firewall Platform > Hard Disk Utilization Logs > Hard Disk Utilization Logs

Hard Disk Utilization Logs

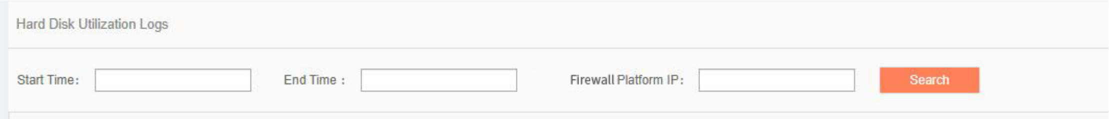
Start Time: End Time : Firewall Platform IP: Search

No.	Time	Firewall Platform IP	Description
1	2019-10-30 14:22:31	16.16.16.13	Data store exceeds time threshold by 1 day, start auto clean
2	2019-10-30 14:00:07	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean
3	2019-10-30 13:00:07	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean
4	2019-10-30 12:00:06	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean
5	2019-10-30 11:00:06	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean
6	2019-10-30 10:00:06	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean
7	2019-10-30 09:00:06	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean
8	2019-10-30 08:00:06	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean
9	2019-10-30 07:00:06	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean

Fig.6-10 Hard Disk Utilization Logs Page

4.3.1. Retrieve a Log

In the [Hard Disk Utilization Logs] list page, retrieve a log according to the conditions. (as shown in Fig.6-11):



Hard Disk Utilization Logs

Start Time: End Time : Firewall Platform IP: Search

Fig.6-11 Retrieve Conditions

4.4. System Restart Log

After successfully logging in the firewall 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):

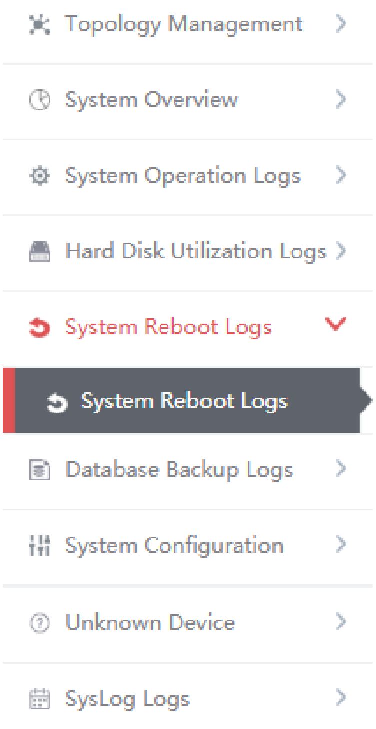
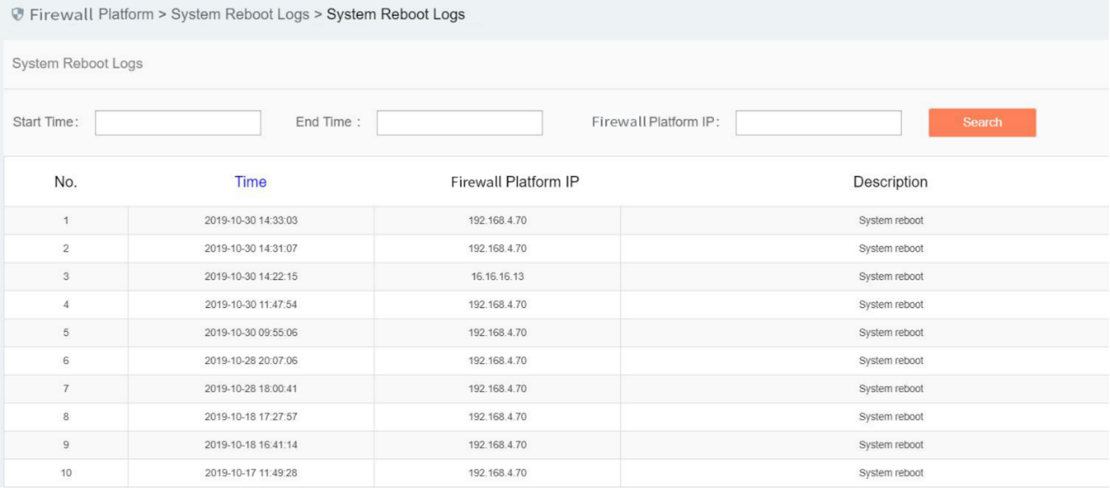


Fig.6-12 System Restart Log Menu Bar



Firewall Platform > System Reboot Logs > System Reboot Logs

System Reboot Logs

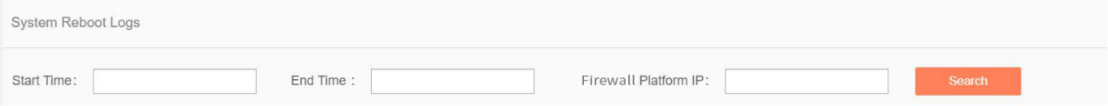
Start Time: ______ End Time : ______ Firewall Platform IP: ______ Search

No.	Time	Firewall Platform IP	Description
1	2019-10-30 14:33:03	192.168.4.70	System reboot
2	2019-10-30 14:31:07	192.168.4.70	System reboot
3	2019-10-30 14:22:15	16.16.16.13	System reboot
4	2019-10-30 11:47:54	192.168.4.70	System reboot
5	2019-10-30 09:55:06	192.168.4.70	System reboot
6	2019-10-28 20:07:06	192.168.4.70	System reboot
7	2019-10-28 18:00:41	192.168.4.70	System reboot
8	2019-10-18 17:27:57	192.168.4.70	System reboot
9	2019-10-18 16:41:14	192.168.4.70	System reboot
10	2019-10-17 11:49:28	192.168.4.70	System reboot

Fig.6-13 System Restart Log Page

4.4.1. 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):



System Reboot Logs

Start Time: ______ End Time : ______ Firewall Platform IP: ______ Search

Fig.6-14 Retrieve Conditions

4.5. Database Backup Log

After successfully logging in the firewall 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):

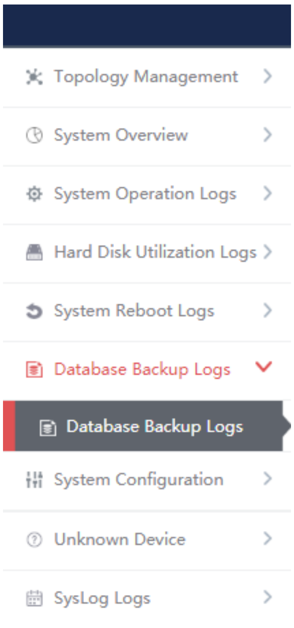
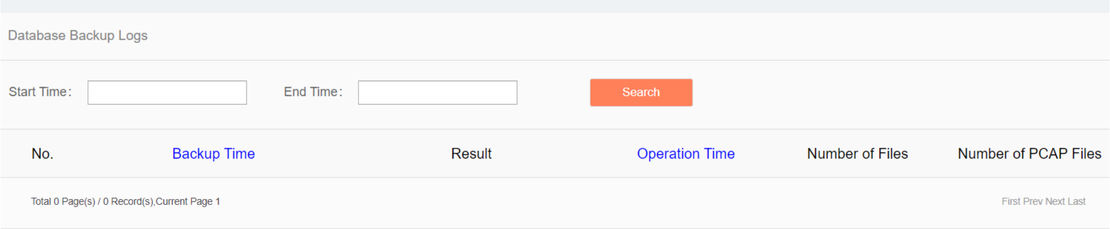


Fig.6-15 Database Backup Log Menu Bar



Database Backup Logs

Start Time: End Time: Search

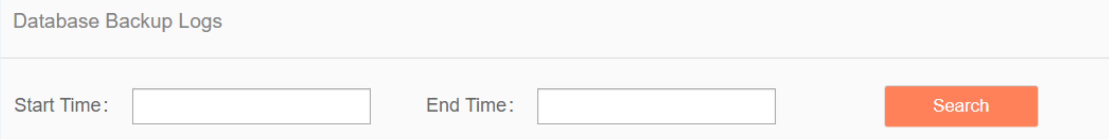
No.	Backup Time	Result	Operation Time	Number of Files	Number of PCAP Files

Total 0 Page(s) / 0 Record(s),Current Page 1

Fig.6-16 Database Backup Log Page

4.5.1. Retrieve a Log

In the [Database Backup Logs] list page, retrieve the log according to the conditions. (as shown in Fig.6-17):



Database Backup Logs

Start Time: End Time: Search

Fig.6-17 Retrieve Conditions

4.6. System Configuration

4.6.1. Password Management

Log in as the configuration administrator, find [System Configuration/Password Management] in the left navigation bar (as shown in Fig.6-18):

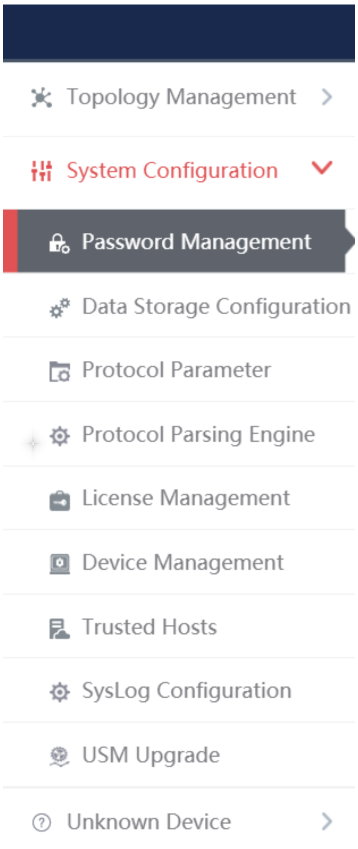


Fig.6-18 Password Management Menu Bar

Log in as auditor, find [System Configuration/Password Management] in the left navigation bar (as shown in Fig.6-19):

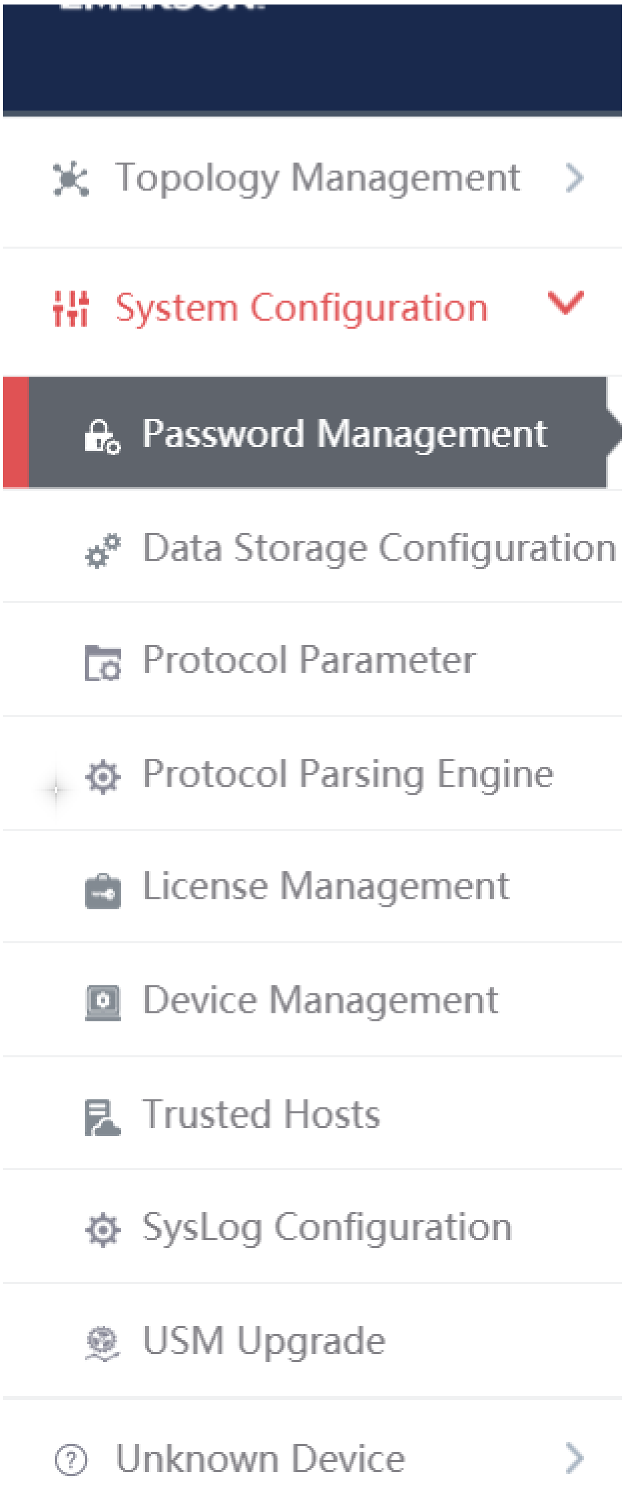


Fig.6-19 Password Management Menu Bar

Log in as the system operator, find [System Configuration/Password Management] in the left navigation bar (as shown in Fig.6-20):

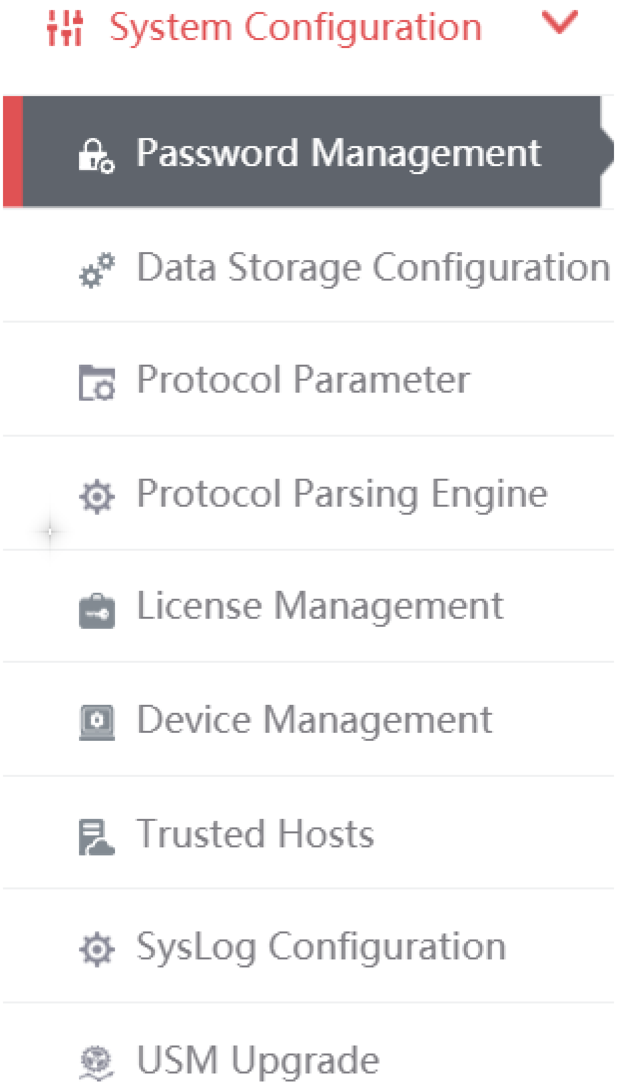
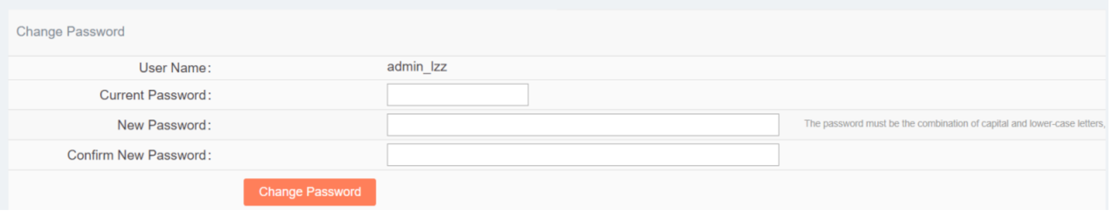


Fig.6-20 Password Management Menu Bar

Click Menu to see the password management page on the right (as shown in Fig.6-22):



Change Password

User Name: admin_lzz

Current Password:

New Password: The password must be the combination of capital and lower-case letters,

Confirm New Password:

Fig.6-22 Password Management Page

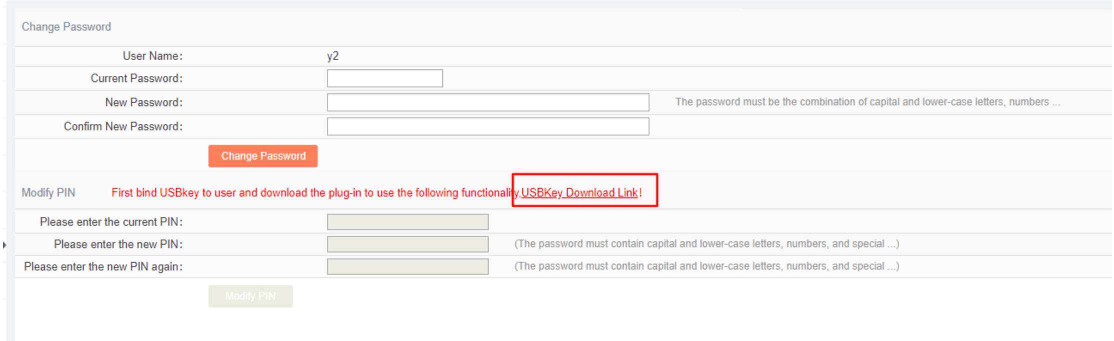
4.6.1.1. Reset a password

Reset the password for the user having currently logged in, fill in the password and click <Save>.

4.6.1.2. 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:



Change Password

User Name: y2

Current Password:

New Password: The password must be the combination of capital and lower-case letters, numbers ...

Confirm New Password:

Change Password

Modify PIN First bind USBkey to user and download the plug-in to use the following functionality.USBKey Download Link!

Please enter the current PIN:

Please enter the new PIN: (The password must contain capital and lower-case letters, numbers, and special ...)

Please enter the new PIN again: (The password must contain capital and lower-case letters, numbers, and special ...)

Modify PIN

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.

4.6.2. User Management

The firewall 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.

4.6.2.1. 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):

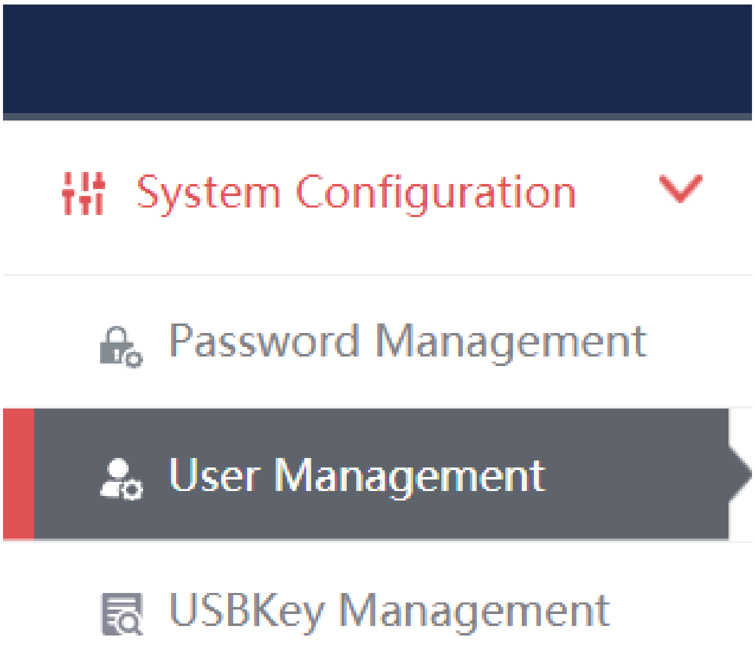
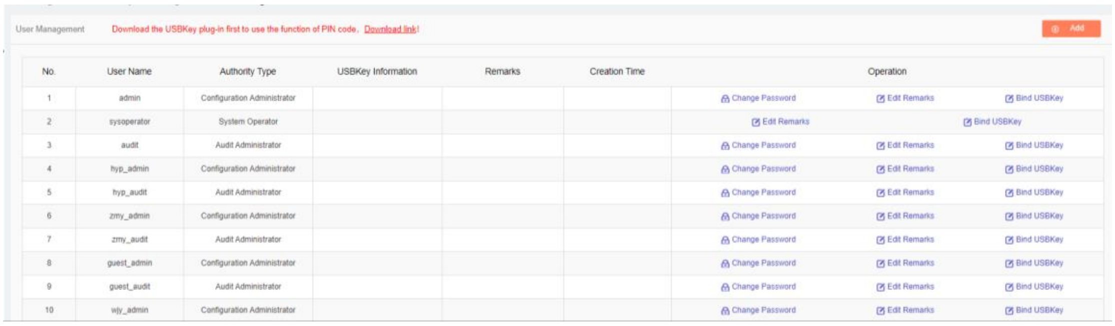


Fig.6-24 User administration menu



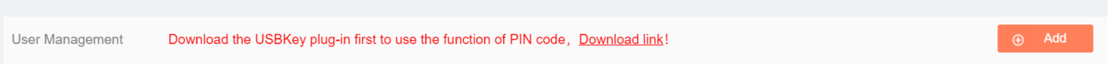
User Management Download the USBKey plug-in first to use the function of PIN code, Download link! Add

No.	User Name	Authority Type	USBKey Information	Remarks	Creation Time	Operation
1	admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
2	sysoperator	System Operator				Edit Remarks Bind USBKey
3	audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
4	hyp_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
5	hyp_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
6	zmy_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
7	zmy_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
8	guest_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
9	guest_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
10	wjy_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey

Fig.6-25 User managed list page

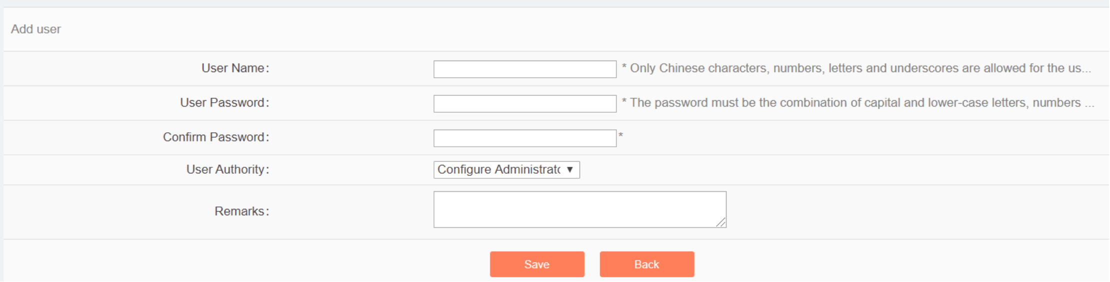
4.6.2.2. Add user

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):



User Management Download the USBKey plug-in first to use the function of PIN code, Download link! Add

Fig.6-26 User Add Button



Add user

User Name:		* Only Chinese characters, numbers, letters and underscores are allowed for the us...
User Password:		* The password must be the combination of capital and lower-case letters, numbers ...
Confirm Password:		*
User Authority:	Configure Administrat(▾	
Remarks:		

Save Back

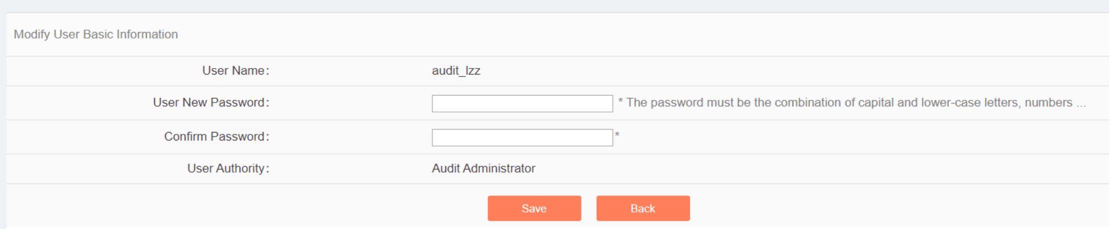
Fig.6-27 User Add Page

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

4.6.2.3. 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):



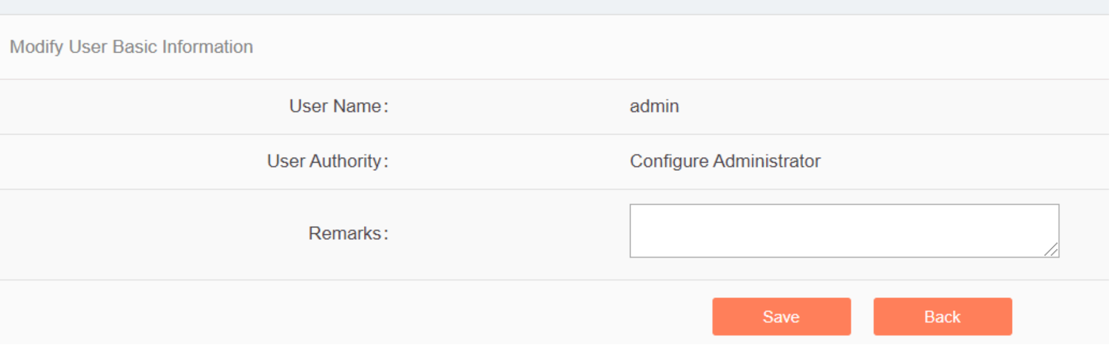
Modify User Basic Information

User Name:	audit_lzz
User New Password:	* The password must be the combination of capital and lower-case letters, numbers ...
Confirm Password:	*
User Authority:	Audit Administrator

Fig.6-28 Modify a Password Page

4.6.2.4. 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):



Modify User Basic Information

User Name:	admin
User Authority:	Configure Administrator
Remarks:	

Fig.6-29 Modify a Remark Page

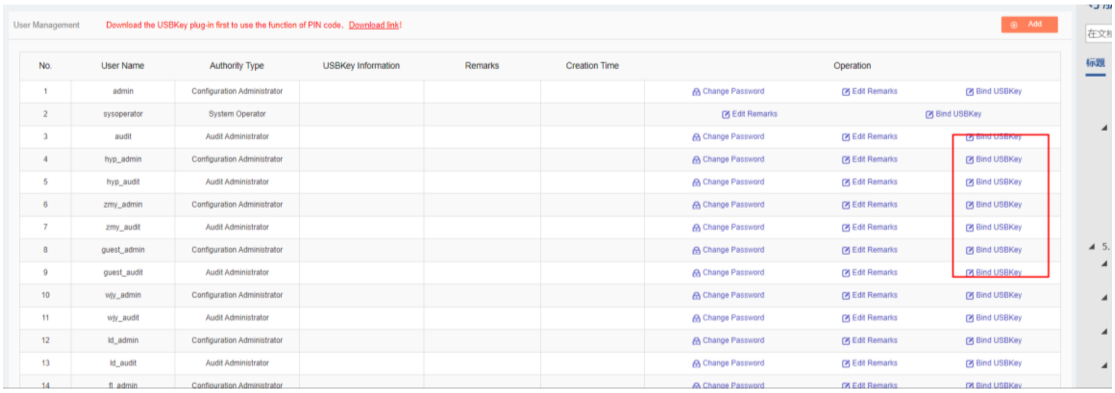
4.6.2.5. Delete a user

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.

4.6.2.6. 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):

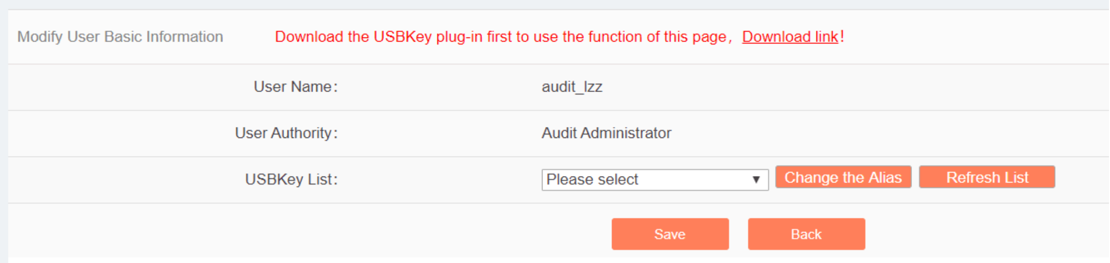


User Management

Download the USBKey plug-in first to use the function of PIN code. Download link!

No.	User Name	Authority Type	USBKey Information	Remarks	Creation Time	Operation
1	admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
2	sysoperator	System Operator				Edit Remarks Bind USBKey
3	audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
4	hyp_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
5	hyp_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
6	zmy_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
7	zmy_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
8	guest_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
9	guest_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
10	wjy_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
11	wjy_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
12	ld_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey
13	ld_audit	Audit Administrator				Change Password Edit Remarks Bind USBKey
14	fl_admin	Configuration Administrator				Change Password Edit Remarks Bind USBKey

Fig.6-30 Bind a USBKey Button


Modify User Basic Information Download the USBKey plug-in first to use the function of this page，Download link!

User Name: audit_lzz

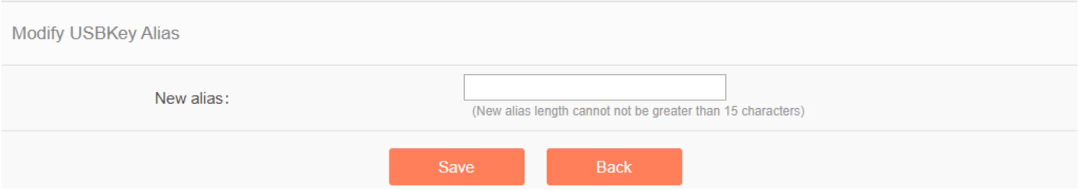
User Authority: Audit Administrator

USBKey List: Please select

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):


Modify USBKey Alias

New alias:

(New alias length cannot not be greater than 15 characters)

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.

4.6.2.7. 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):

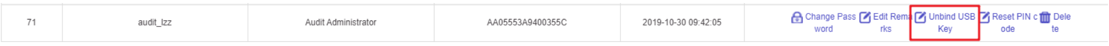
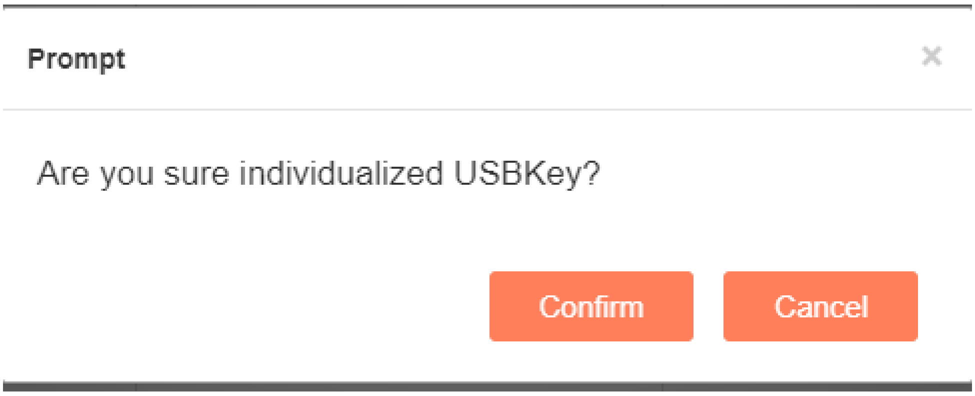

71	audit_lzz	Audit Administrator	AA05553A9400355C	2019-10-30 09:42:05	Change Password Edit Remarks Unbind USBKey Reset PIN code Delete

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):


Prompt

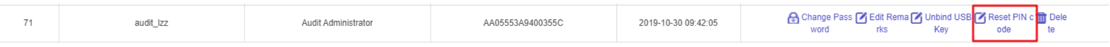
Are you sure individualized USBKey?

Fig.6-34 Unbind a USBKey Confirm Page

4.6.2.8. 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.

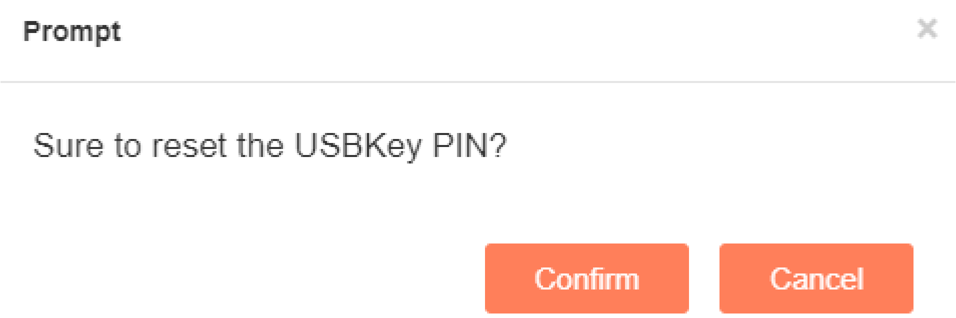
Log in as the system operator, click <Reset a PIN Code> under the user operation list with the PIN code to be unbound under [User Management] (as shown in Fig.6-35):



71	audit_lzz	Audit Administrator	AA05553A9400355C	2019-10-30 09:42:05	Change Password Edit Remarks Unbind USB Key Reset PIN code Delete

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.



Prompt

Sure to reset the USBKey PIN?

Fig.6-36 Unbind a USBKey Confirm Page

4.6.3. USBKey Management

The operation page is used to change an alias and reset a PIN code for USBKeys. To use the functions, download and properly 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):

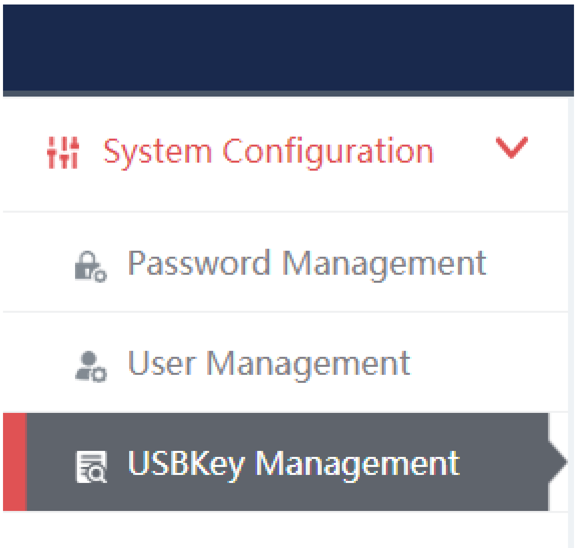
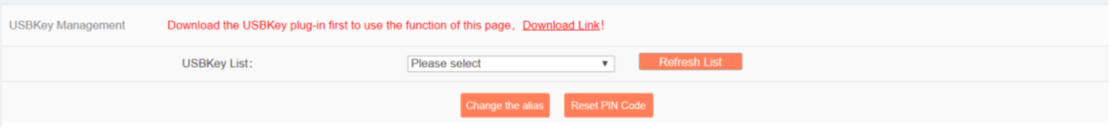


Fig.6-37 Usbkey Management Navigation



USBKey Management

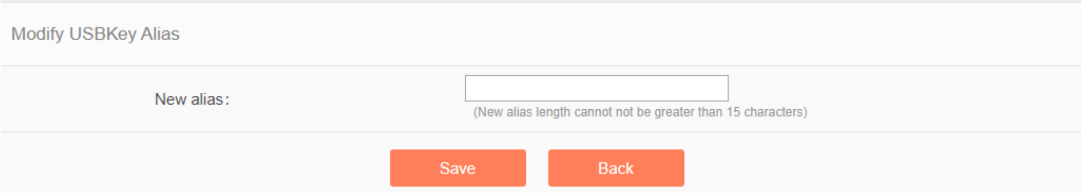
Download the USBKey plug-in first to use the function of this page, Download Link!

USBKey List: Please select

Fig.6-38 USBKey Management Page

4.6.3.1. 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):



Modify USBKey Alias

New alias:

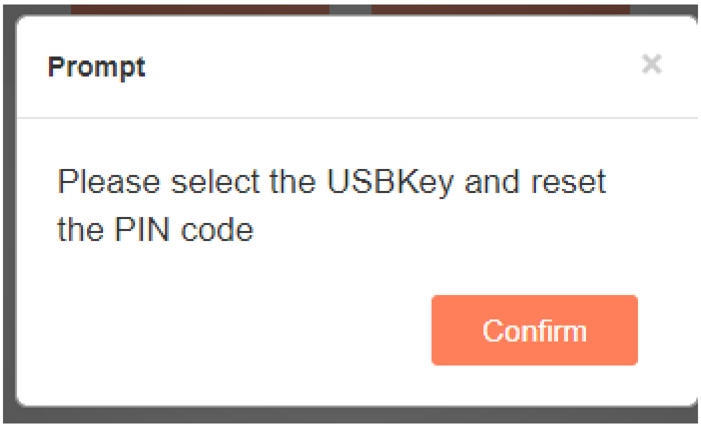
(New alias length cannot not be greater than 15 characters)

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.

4.6.3.2. 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):



Prompt

Please select the USBKey and reset the PIN code

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.

4.6.4. Database Storage Cycle Configuration

It is used to configure the firewall 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):

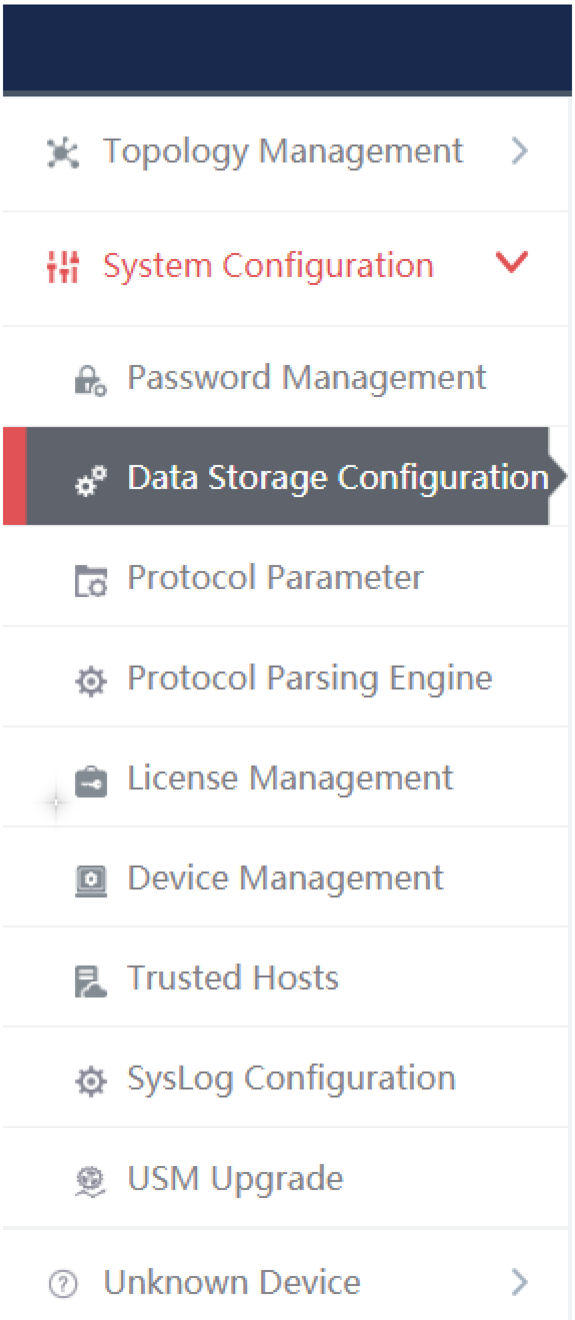
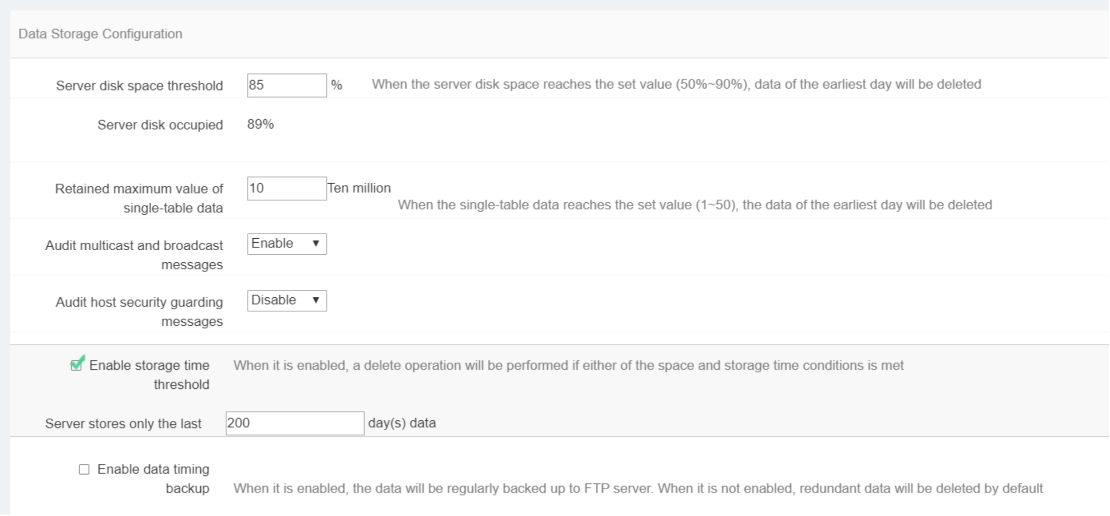


Fig.6-41 Database Storage Cycle Configuration



Data Storage Configuration

Server disk space threshold 85 % When the server disk space reaches the set value (50%~90%), data of the earliest day will be deleted

Server disk occupied 89%

Retained maximum value of single-table data 10 Ten million When the single-table data reaches the set value (1~50), the data of the earliest day will be deleted

Audit multicast and broadcast messages Enable ▼

Audit host security guarding messages Disable ▼

☑ Enable storage time threshold When it is enabled, a delete operation will be performed if either of the space and storage time conditions is met

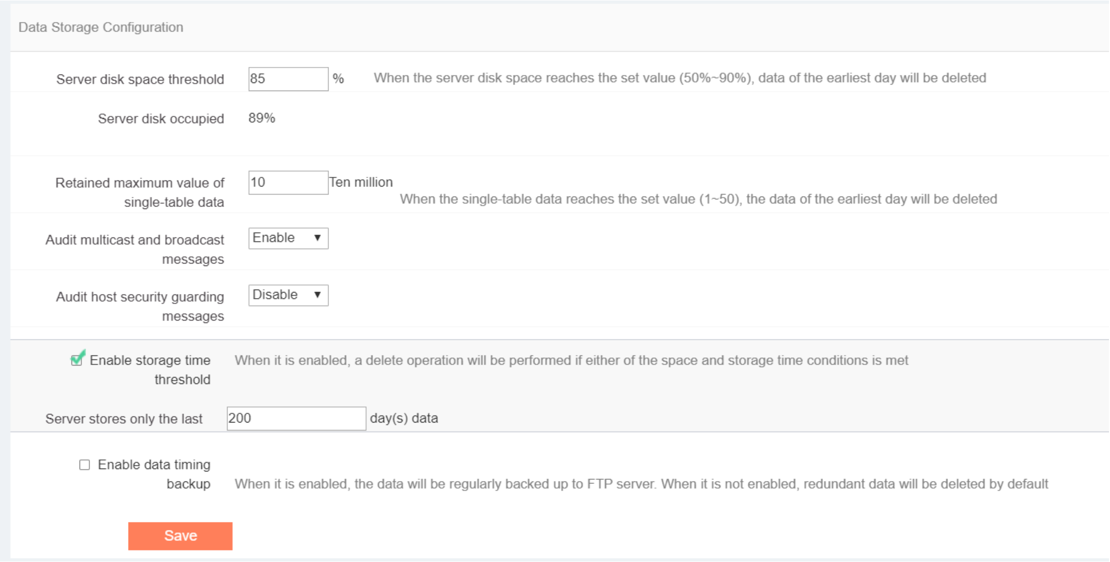
Server stores only the last 200 day(s) data

□ Enable data timing backup When it is enabled, the data will be regularly backed up to FTP server. When it is not enabled, redundant data will be deleted by default

Fig.6-42 Database Storage Cycle Configuration Page

4.6.4.1. 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):



Data Storage Configuration

Server disk space threshold 85 % When the server disk space reaches the set value (50%~90%), data of the earliest day will be deleted

Server disk occupied 89%

Retained maximum value of single-table data 10 Ten million When the single-table data reaches the set value (1~50), the data of the earliest day will be deleted

Audit multicast and broadcast messages Enable ▼

Audit host security guarding messages Disable ▼

☑ Enable storage time threshold When it is enabled, a delete operation will be performed if either of the space and storage time conditions is met

Server stores only the last 200 day(s) data

□ Enable data timing backup When it is enabled, the data will be regularly backed up to FTP server. When it is not enabled, redundant data will be deleted by default

Fig.6-43 save the configuration

4.6.5. Protocol Parameter Configuration

4.6.5.1. 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.

4.6.5.2. 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):

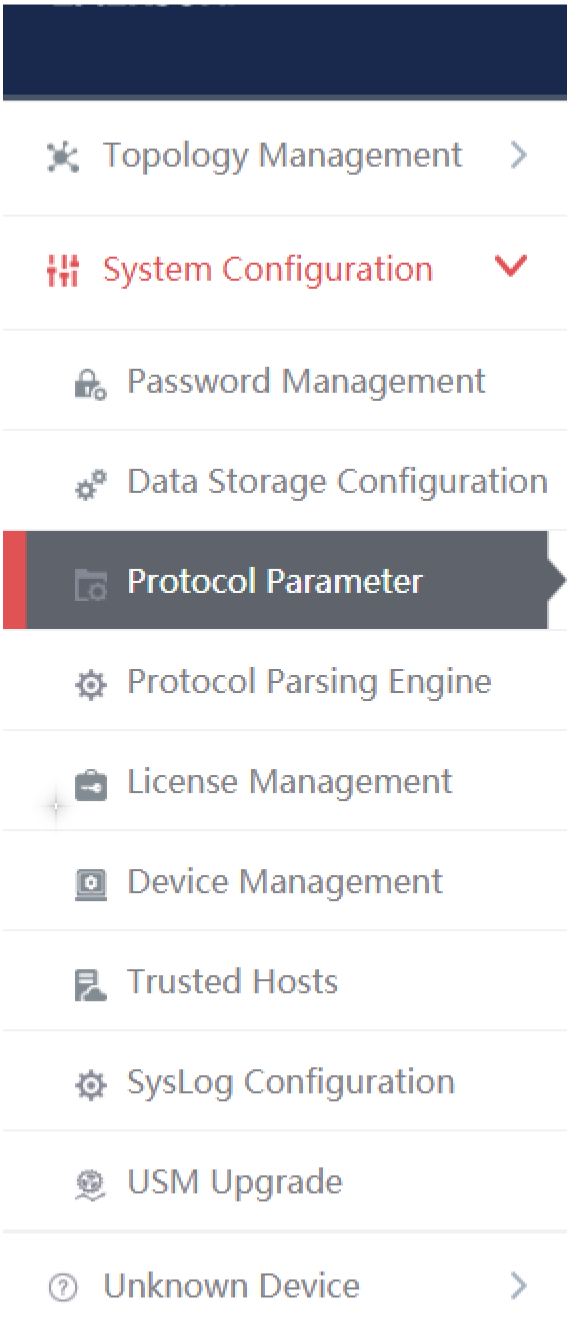
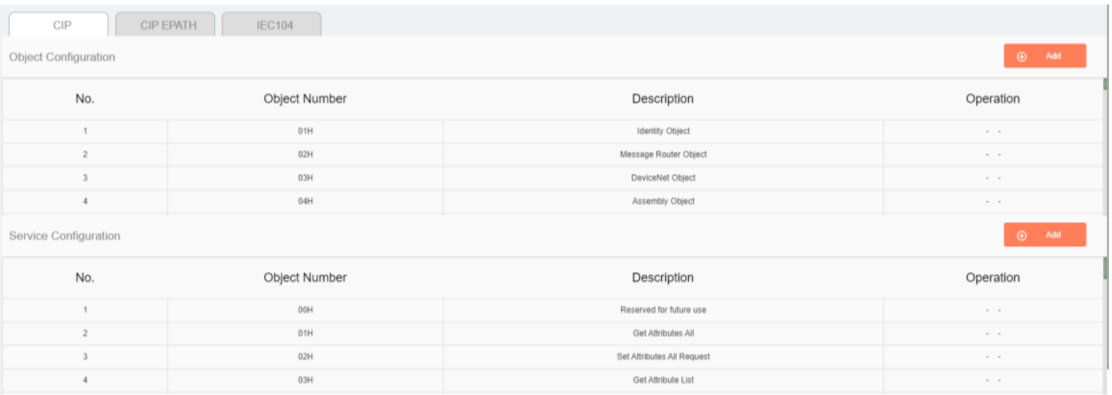


Fig.6-44 Selecting Protocol Parameter Configuration



Object Configuration

No.	Object Number	Description	Operation
1	01H	Identity Object	- -
2	02H	Message Router Object	- -
3	03H	DeviceNet Object	- -
4	04H	Assembly Object	- -

Service Configuration

No.	Object Number	Description	Operation
1	00H	Reserved for future use	- -
2	01H	Get Attributes All	- -
3	02H	Set Attributes All Request	- -
4	03H	Get Attribute List	- -

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

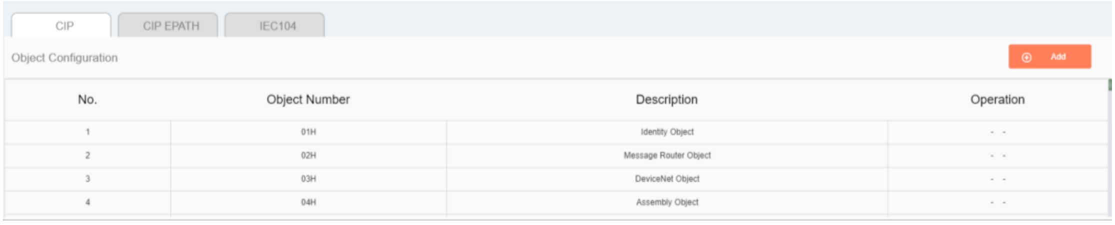
Column Names	**Instructions**	
Service no.	The standard services provided under the CIP Protocol and custom services in the industrial field are displayed in hexadecimal values	
Description	Specific meaning of service	
Operation	Modify	Modify the descriptive information on user-defined CIP service, unable 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

<table>
<tr><th>Column Names</th><th colspan="2">Instructions</th></tr>
<tr><td>CMD</td><td colspan="2">The CMD number in a PCCC message embedded in the CIP protocol, displayed in hexadecimal values</td></tr>
<tr><td>FNC</td><td colspan="2">The FNC number in a PCCC message embedded in the CIP protocol, displayed in hexadecimal values</td></tr>
<tr><td>Description</td><td colspan="2">The method description uniquely determined by the CMD and FNC combination in PCCC</td></tr>
<tr><td rowspan="2">Operation</td><td>Modify</td><td>Redefine the method uniquely determined by the CMD and FNC combination, unable to modify the standard method defined by PCCC</td></tr>
<tr><td>Delete</td><td>Delete the user-defined method uniquely determined by the CMD and FNC combination, unable to delete the standard method defined by PCCC</td></tr>
</table>

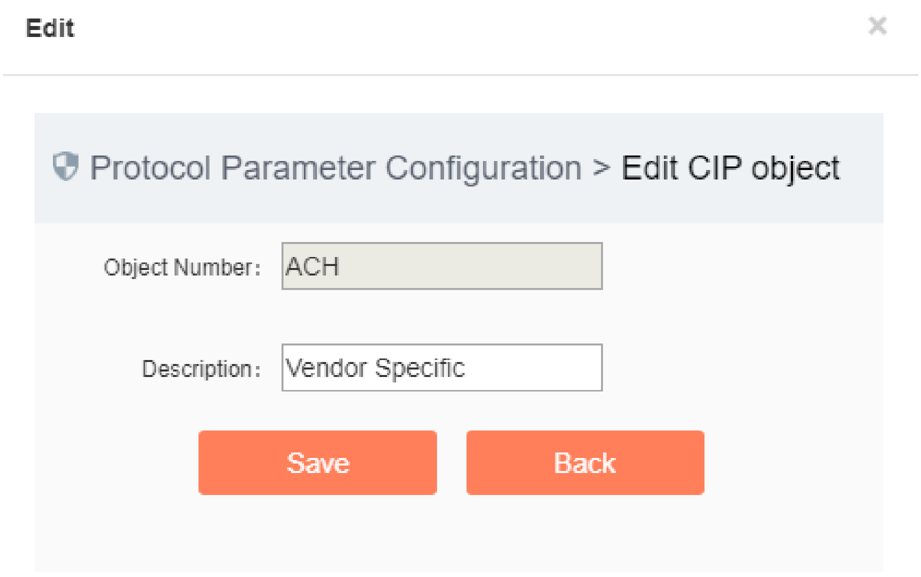
4.6.5.3. CIP configuration addition

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):



No.	Object Number	Description	Operation
1	01H	Identity Object	- -
2	02H	Message Router Object	- -
3	03H	DeviceNet Object	- -
4	04H	Assembly Object	- -

Fig.6-46 CIP Protocol Object Configuration Addition Button



Object Number: ACH

Description: Vendor Specific

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.

4.6.5.4. CIP Configuration modification

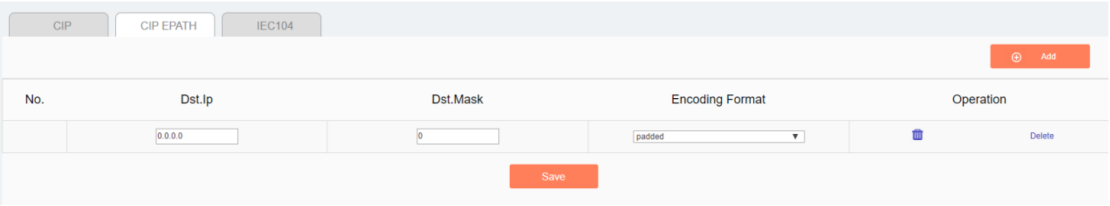
Please refer to the modification instructions under 6.6.5.2 Protocol Parameter Configuration Operation Column.

4.6.5.5. CIP Configuration deletion

Please refer to the modification instructions under 6.6.5.2 Protocol Parameter Configuration Operation Column.

4.6.5.6. 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.

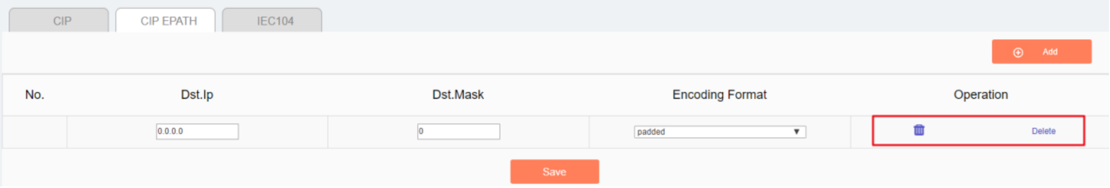


No.	Dst.Ip	Dst.Mask	Encoding Format	Operation
	0.0.0.0	0	padded	Delete

Fig.6-48 CIP EPATH Configuration Page

4.6.5.7. CIP EPATH Configuration deletion

Click <Delete> to delete a rule (Fig.6-49).

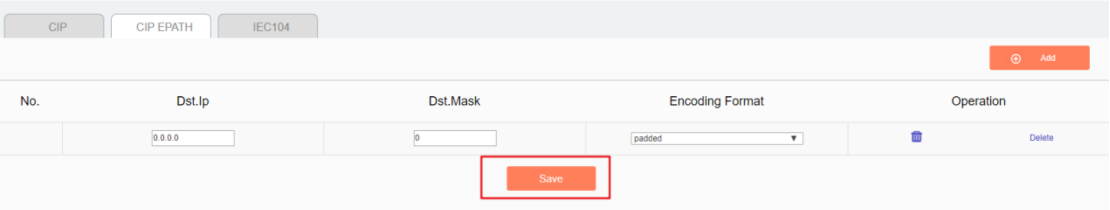


No.	Dst.Ip	Dst.Mask	Encoding Format	Operation
	0.0.0.0	0	padded	Delete

Fig.6-49 CIP EPATH Deletion Operation

4.6.5.8. CIP EPATH Configuration saving

Click <Save> to save all rules and distribute them to the device (as shown in Fig.6-50):

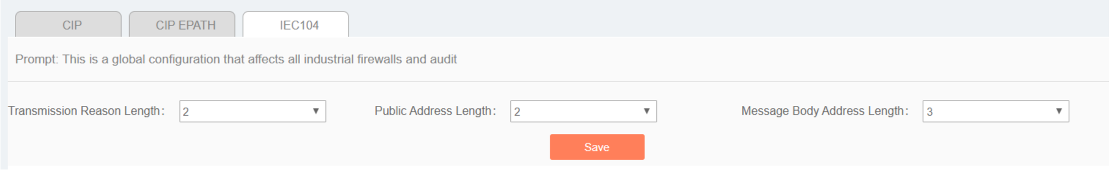


No.	Dst.Ip	Dst.Mask	Encoding Format	Operation
	0.0.0.0	0	padded	Delete

Fig.6-50 CIP EPATH Saving operation

4.6.5.9. IEC104 Configuration

Click the tab and skip to the IEC104 configuration page (Fig.6-51):



Prompt: This is a global configuration that affects all industrial firewalls and audit

Transmission Reason Length: 2

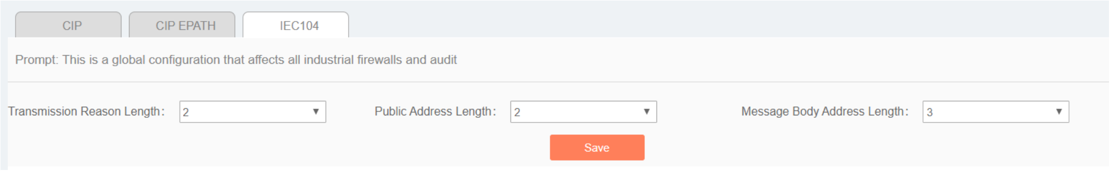
Public Address Length: 2

Message Body Address Length: 3

Fig.6-51 IEC104 Configuration Page

4.6.5.10. IEC104 Configuration saving

Click <Save> to save and distribute the page configuration (as shown in Fig.6-52):



Prompt: This is a global configuration that affects all industrial firewalls and audit

Transmission Reason Length: 2

Public Address Length: 2

Message Body Address Length: 3

Fig.6-52 IEC104 Saving

4.6.6. 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):

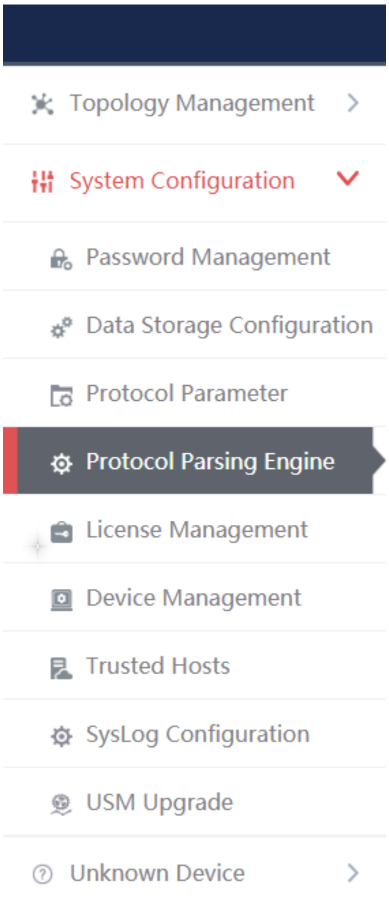
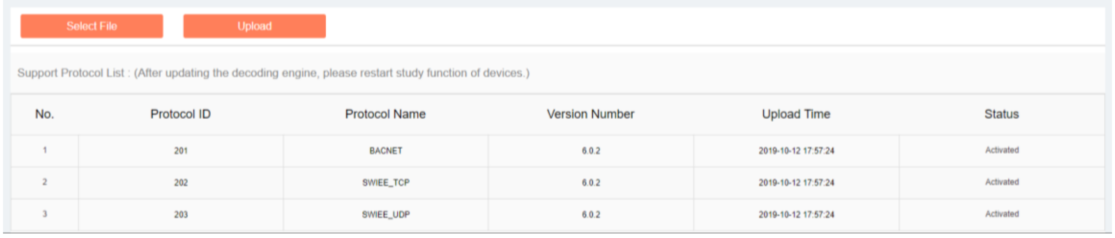


Fig.6-53 Decoding Engine Configuration Menu



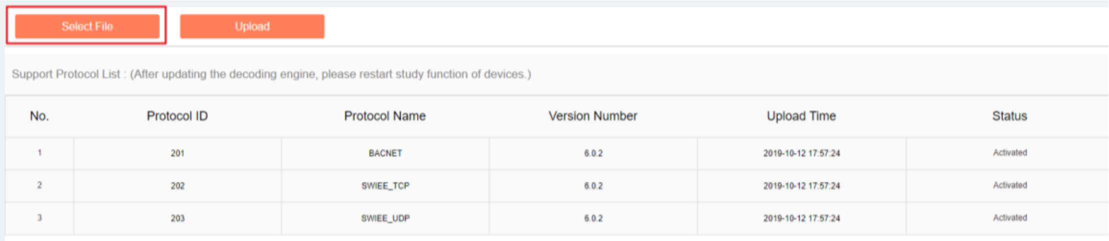
Support Protocol List : (After updating the decoding engine, please restart study function of devices.)

No.	Protocol ID	Protocol Name	Version Number	Upload Time	Status
1	201	BACNET	6.0.2	2019-10-12 17:57:24	Activated
2	202	SWIEE_TCP	6.0.2	2019-10-12 17:57:24	Activated
3	203	SWIEE_UDP	6.0.2	2019-10-12 17:57:24	Activated

Fig.6-54 Decoding Engine Configuration Page

4.6.6.1. 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):



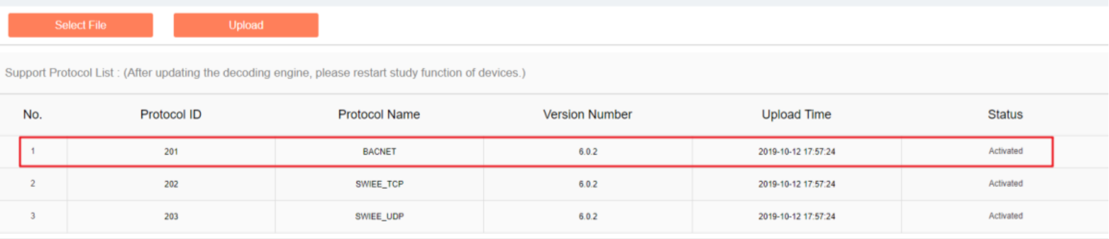
Support Protocol List : (After updating the decoding engine, please restart study function of devices.)

No.	Protocol ID	Protocol Name	Version Number	Upload Time	Status
1	201	BACNET	6.0.2	2019-10-12 17:57:24	Activated
2	202	SWIEE_TCP	6.0.2	2019-10-12 17:57:24	Activated
3	203	SWIEE_UDP	6.0.2	2019-10-12 17:57:24	Activated

Fig.6-55 Protocol Decoding Engine Upload Configuration File

4.6.6.2. Protocol parsing information display

After successful resolving, the firewall 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.



Support Protocol List : (After updating the decoding engine, please restart study function of devices.)

No.	Protocol ID	Protocol Name	Version Number	Upload Time	Status
1	201	BACNET	6.0.2	2019-10-12 17:57:24	Activated
2	202	SWIEE_TCP	6.0.2	2019-10-12 17:57:24	Activated
3	203	SWIEE_UDP	6.0.2	2019-10-12 17:57:24	Activated

Fig.6-56 Protocol Resolving Information Display

4.6.7. Authorization Management

To authorize functions such as [Industrial Firewall], 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):

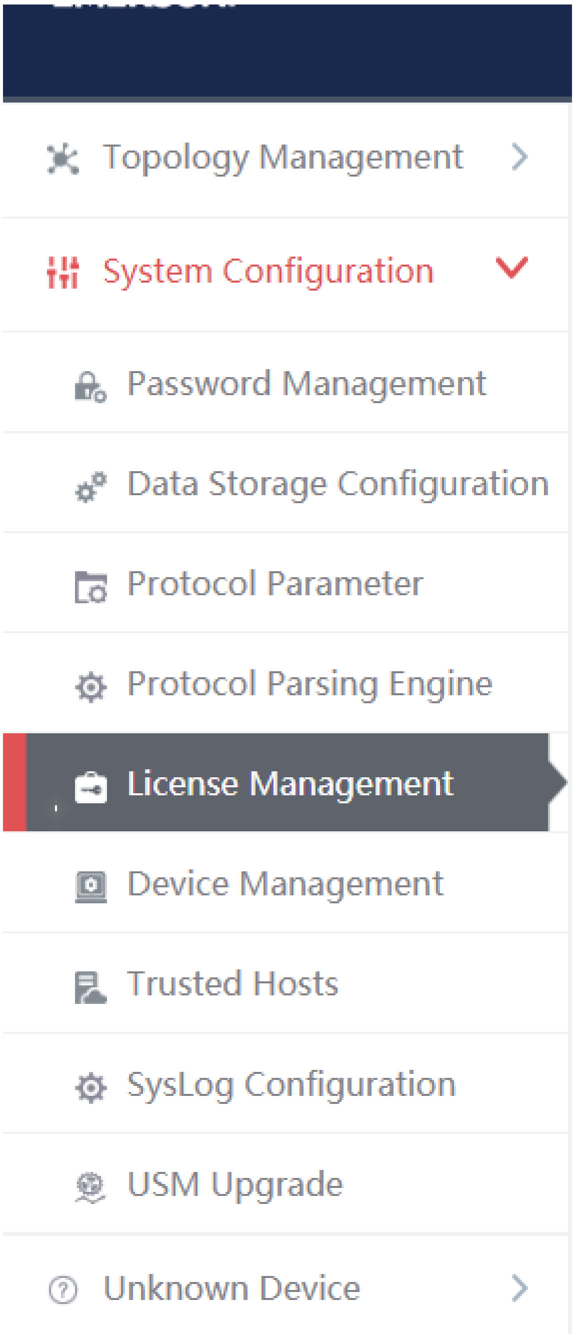
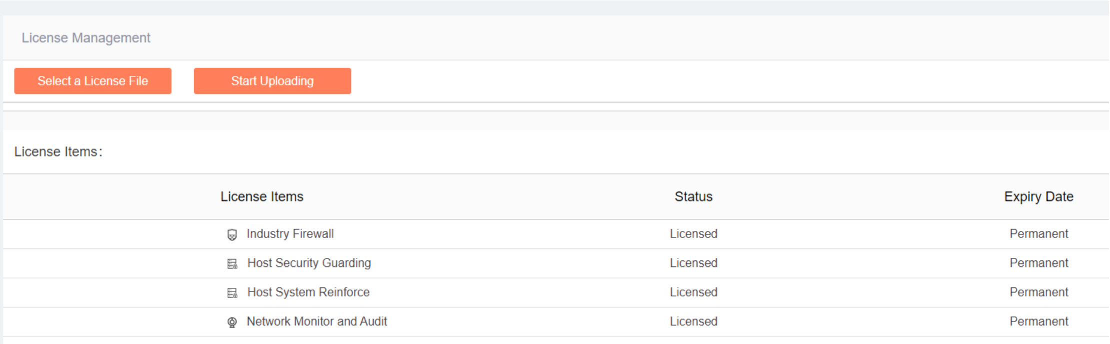


Fig.6-57 Authorization Management Menu Bar



License Items:

License Items	Status	Expiry Date
Industry Firewall	Licensed	Permanent
Host Security Guarding	Licensed	Permanent
Host System Reinforce	Licensed	Permanent
Network Monitor and Audit	Licensed	Permanent

Fig.6-58 Authorization Management Page

4.6.7.1. Start upload

Click <Please Select an Authorization File>, select the authorization file, click <Start Uploading> and execute the authorization.

4.6.8. Device Management

Device management is one of the important functions of the firewall 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):

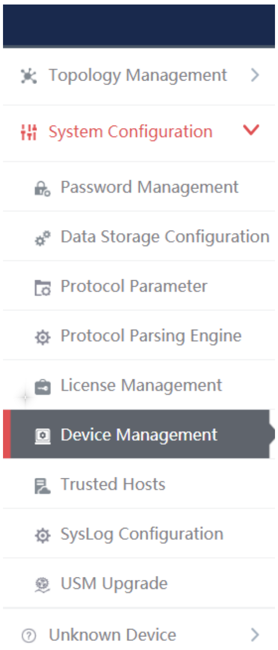
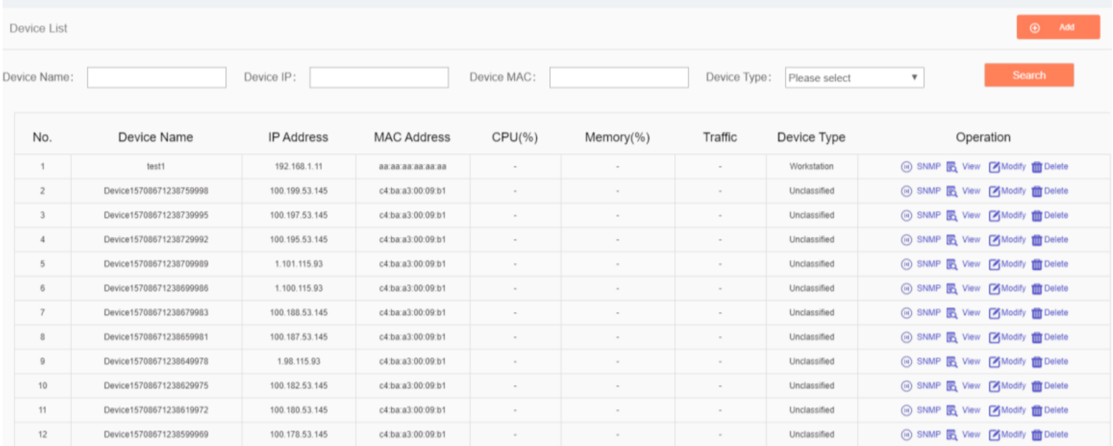


Fig.6-59 Device Management Menu



No.	Device Name	IP Address	MAC Address	CPU(%)	Memory(%)	Traffic	Device Type	Operation
1	test1	192.168.1.11	aa:aa:aa:aa:aa:aa	-	-	-	Workstation	SNMP View Modify Delete
2	Device15708671238759998	100.199.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
3	Device15708671238739995	100.197.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
4	Device15708671238729992	100.195.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
5	Device15708671238709989	1.101.115.93	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
6	Device15708671238699986	1.100.115.93	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
7	Device15708671238679983	100.188.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
8	Device15708671238659981	100.187.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
9	Device15708671238649978	1.98.115.93	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
10	Device15708671238629975	100.182.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
11	Device15708671238619972	100.180.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete
12	Device15708671238599969	100.178.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	SNMP View Modify Delete

Fig.6-60 Device Management Page

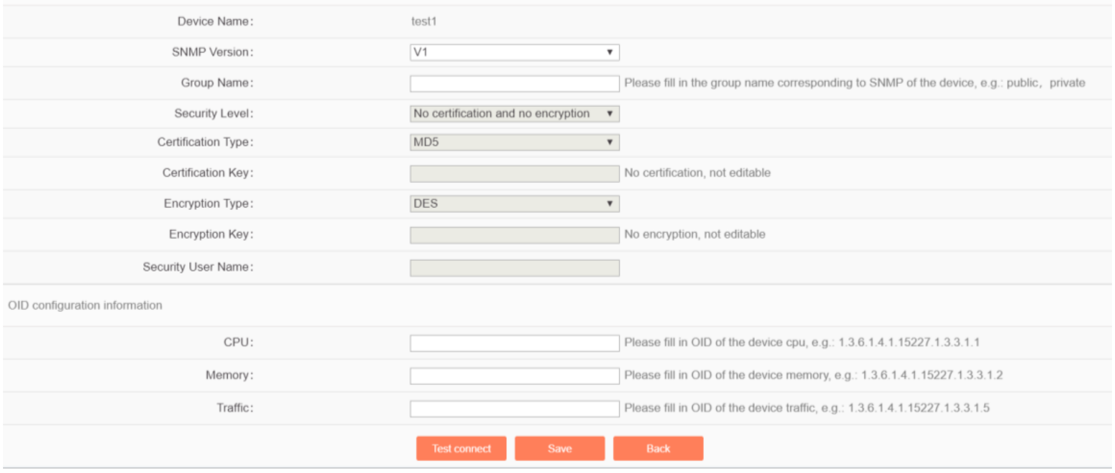
View all the device information in the system here, with the following meanings given:

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

4.6.8.1. 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):



Device Name:	test1	
SNMP Version:	V1	
Group Name:		Please fill in the group name corresponding to SNMP of the device, e.g.: public, private
Security Level:	No certification and no encryption	
Certification Type:	MD5	
Certification Key:		No certification, not editable
Encryption Type:	DES	
Encryption Key:		No encryption, not editable
Security User Name:		

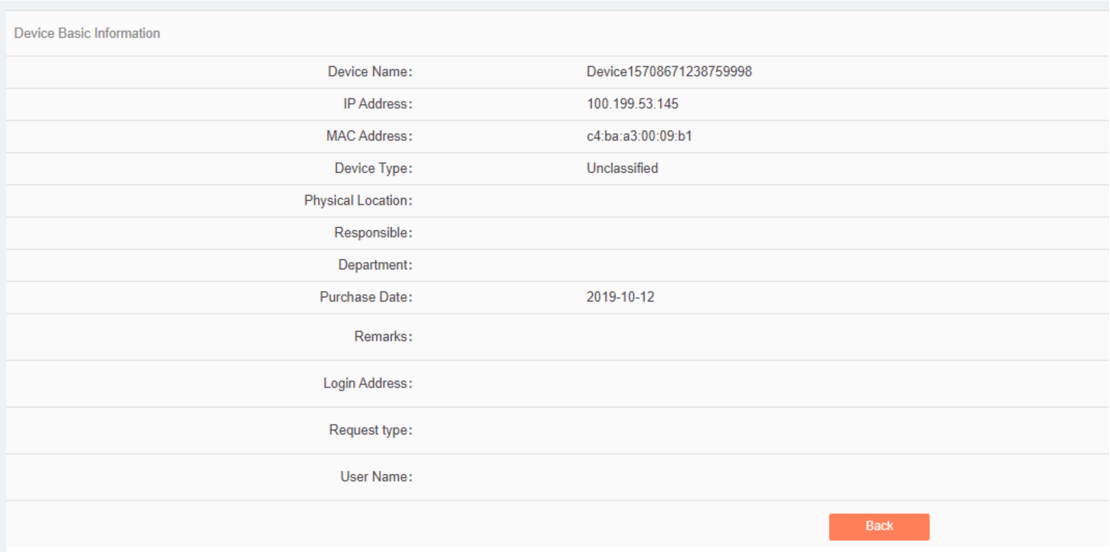
OID configuration information

CPU:		Please fill in OID of the device cpu, e.g.: 1.3.6.1.4.1.15227.1.3.3.1.1
Memory:		Please fill in OID of the device memory, e.g.: 1.3.6.1.4.1.15227.1.3.3.1.2
Traffic:		Please fill in OID of the device traffic, e.g.: 1.3.6.1.4.1.15227.1.3.3.1.5

Fig.6-61 SNMP Configuration

4.6.8.2. 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):



Device Basic Information

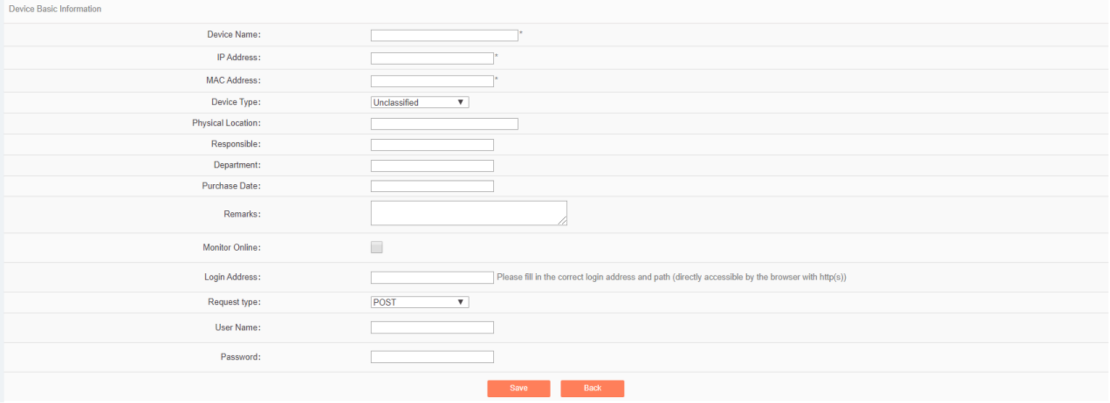
Device Name:	Device15708671238759998
IP Address:	100.199.53.145
MAC Address:	c4:ba:a3:00:09:b1
Device Type:	Unclassified
Physical Location:	
Responsible:	
Department:	
Purchase Date:	2019-10-12
Remarks:	
Login Address:	
Request type:	
User Name:	

Fig.6-62 Device Information View Page

Click <Back> and go back to the [Device Management] page.

4.6.8.3. 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):



Device Basic Information

Device Name:	*
IP Address:	*
MAC Address:	*
Device Type:	Unclassified ▼
Physical Location:	
Responsible:	
Department:	
Purchase Date:	
Remarks:	
Monitor Online:	□
Login Address:	Please fill in the correct login address and path (directly accessible by the browser with http(s))
Request type:	POST ▼
User Name:	
Password:	

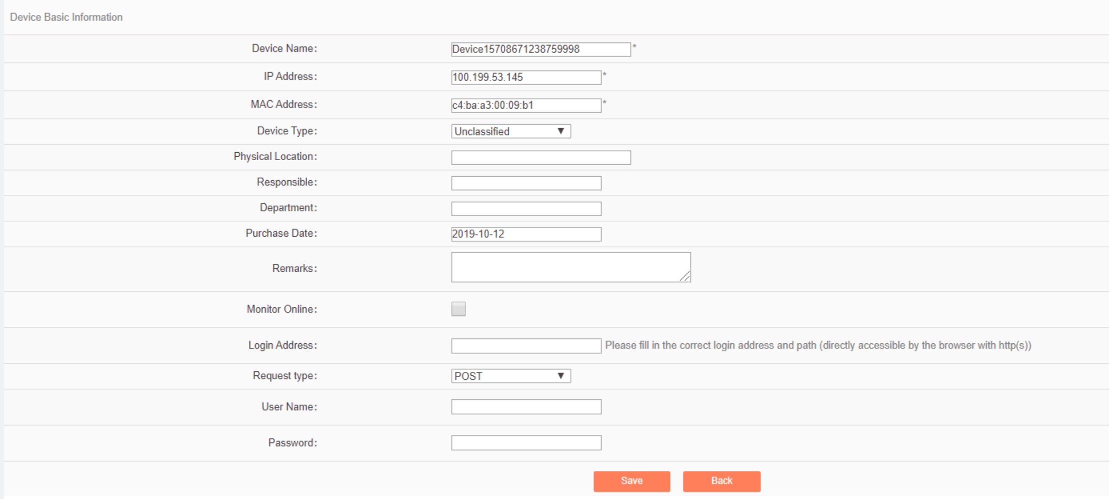
Fig.6-63 Device Add Page

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

4.6.8.4. 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):



Device Basic Information

Device Name:	Device15708671238759998 *
IP Address:	100.199.53.145 *
MAC Address:	c4:ba:a3:00:09:b1 *
Device Type:	Unclassified ▼
Physical Location:	
Responsible:	
Department:	
Purchase Date:	2019-10-12
Remarks:	
Monitor Online:	□
Login Address:	Please fill in the correct login address and path (directly accessible by the browser with http(s))
Request type:	POST ▼
User Name:	
Password:	

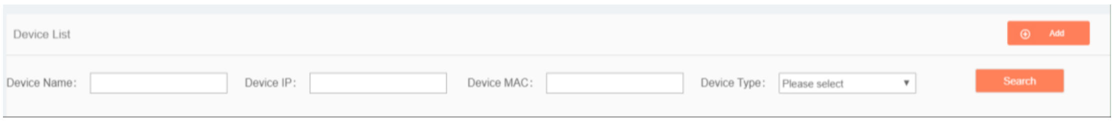
Fig.6-64 Device Basic Information Modification Page

4.6.8.5. Delete a device

Click <Delete> under the [Device Management] device list operation column, delete devices that are no longer in use.

4.6.8.6. Retrieve a device

In the [Device Management] device display list page, retrieve a device according to the conditions. (as shown in Fig.6-65):



Device List

Device Name:		Device IP:		Device MAC:		Device Type:	Please select ▼

Fig.6-65 Retrieve a Device

4.6.9. Trusted Host

The host accessing to the firewall platform is limited. In the initial case, any machine can access to the firewall platform only if it can be connected to the firewall platform server. Once a trusted host is configured, only machines that are added to the trusted host can access the firewall platform. The host where the firewall platform server is located can access to the firewall platform in any case.

4.6.9.1. 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):

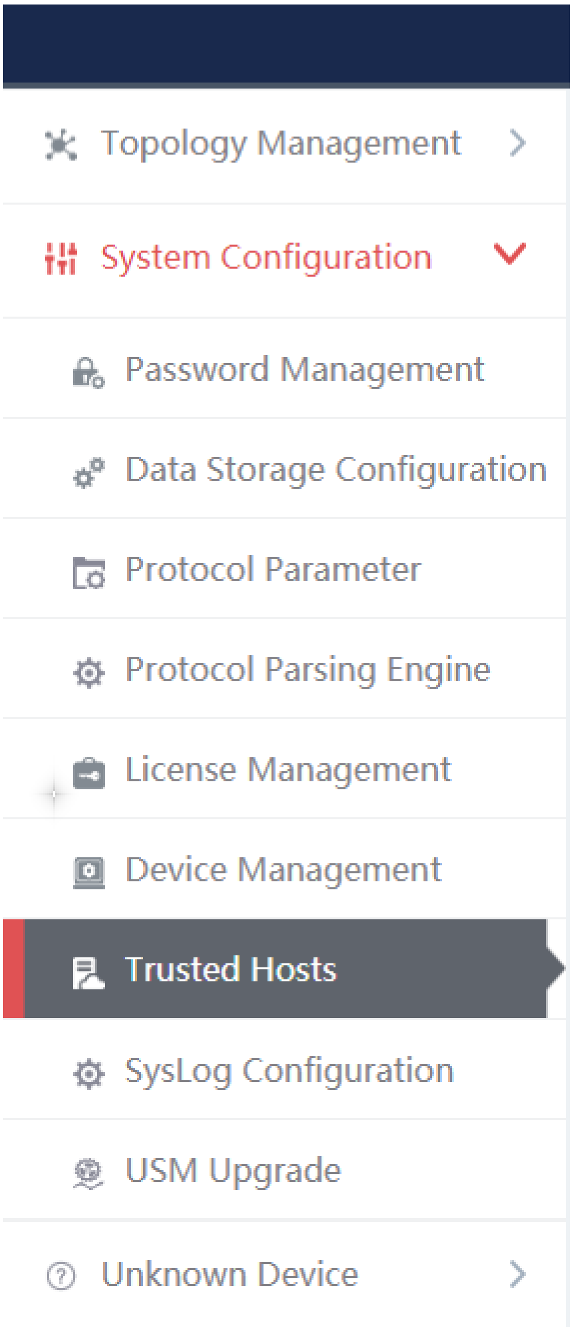
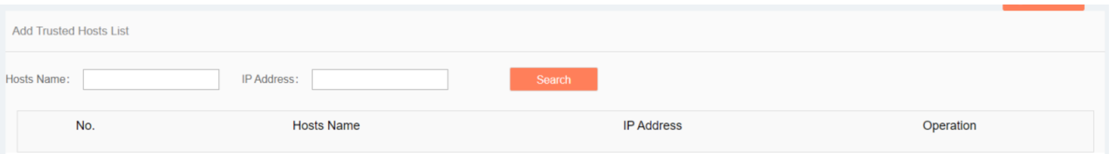


Fig.6-66 Trusted Host Menu



Add Trusted Hosts List

Hosts Name: IP Address: Search

No.	Hosts Name	IP Address	Operation

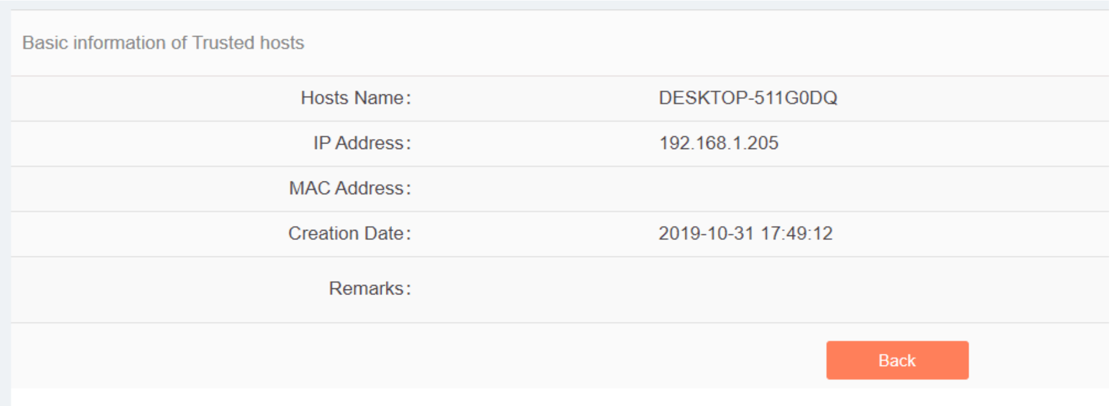
Fig.6-67 Trusted Host List Page

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):



Basic information of Trusted hosts

Hosts Name: DESKTOP-511G0DQ

IP Address: 192.168.1.205

MAC Address:

Creation Date: 2019-10-31 17:49:12

Remarks:

Fig.6-68 Trusted Host Information View Page

Click <Back> and go back to the [Trusted Host] page.

4.6.9.2. 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):

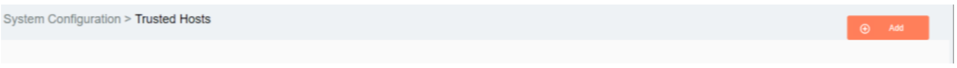
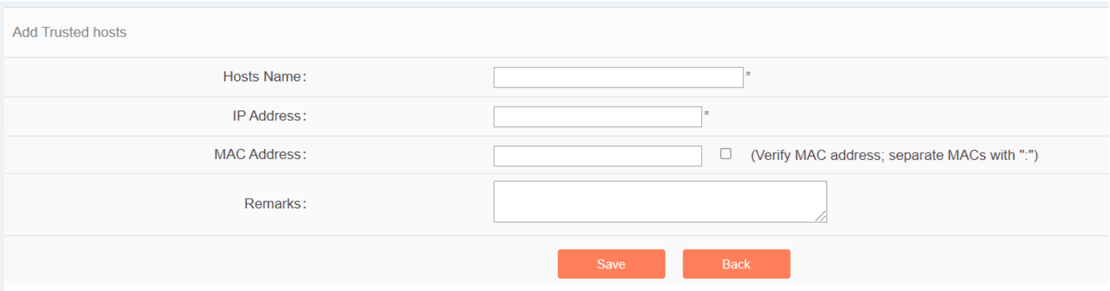


Fig.6-69 Trusted Host Add Button



Add Trusted hosts

Hosts Name: *

IP Address: *

MAC Address: □ (Verify MAC address; separate MACs with ":")

Remarks:

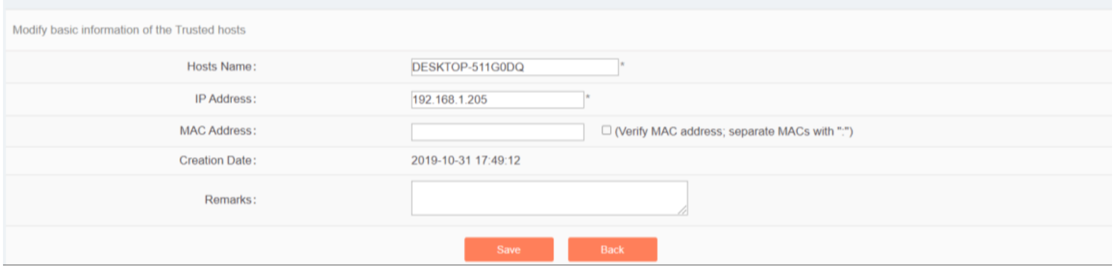
Fig.6-70 Trusted Host Add Page

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

4.6.9.3. 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):



Modify basic information of the Trusted hosts

Hosts Name: DESKTOP-511G0DQ *

IP Address: 192.168.1.205 *

MAC Address: □ (Verify MAC address; separate MACs with ":")

Creation Date: 2019-10-31 17:49:12

Remarks:

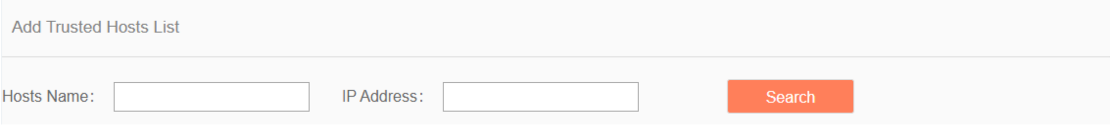
Fig.6-71 Trusted Host Basic Information Modification Page

4.6.9.4. 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.

4.6.9.5. 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):



Add Trusted Hosts List

Hosts Name:

IP Address:

Fig.6-72 Retrieving a Trusted Host

4.6.10. SysLog Configuration

4.6.10.1. 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.

4.6.10.2. 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):

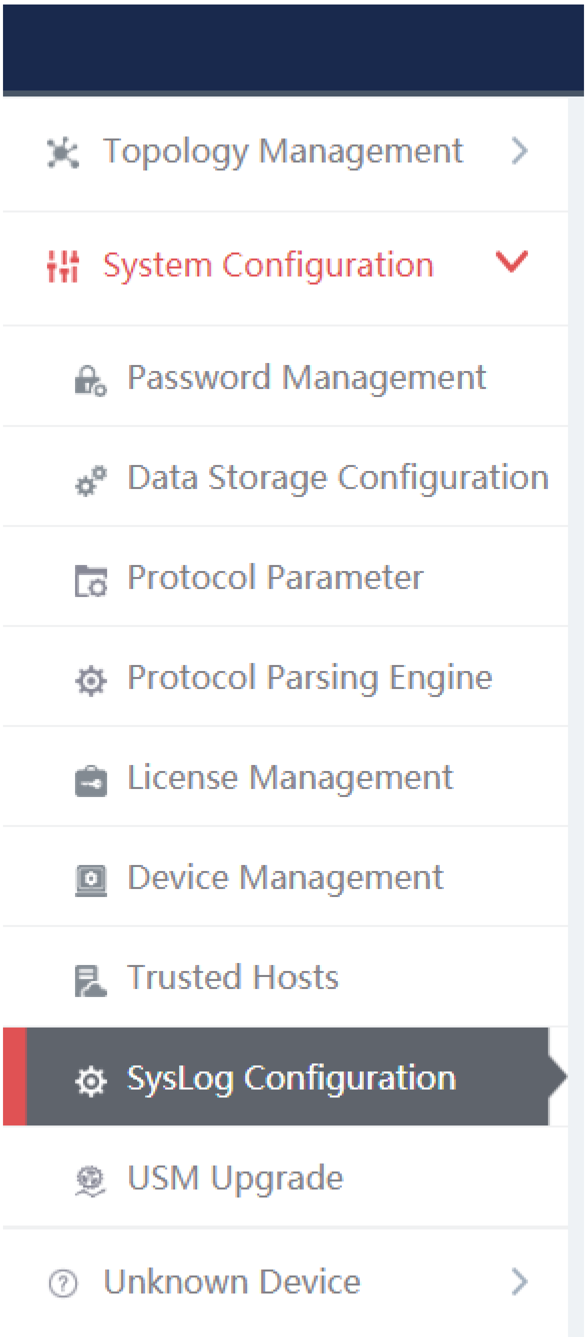
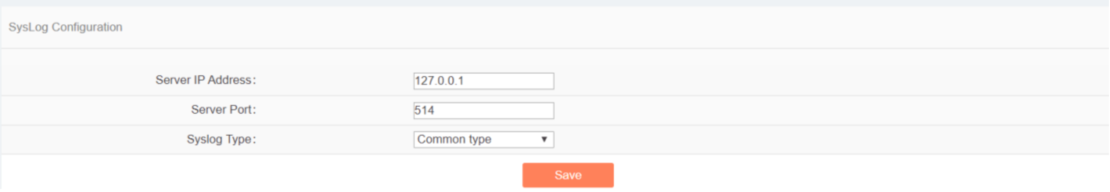


Fig.6-73 Menu



SysLog Configuration

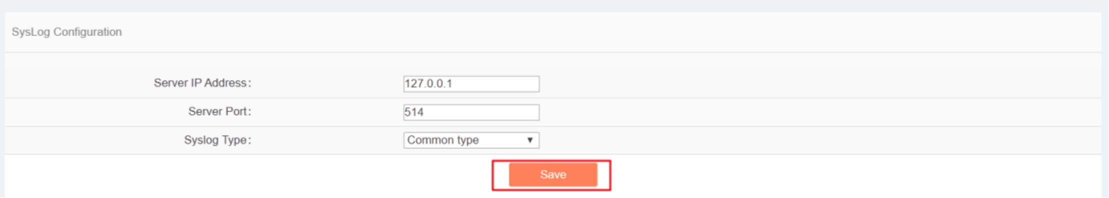
Server IP Address: 127.0.0.1

Server Port: 514

Syslog Type: Common type ▾

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):



SysLog Configuration

Server IP Address: 127.0.0.1

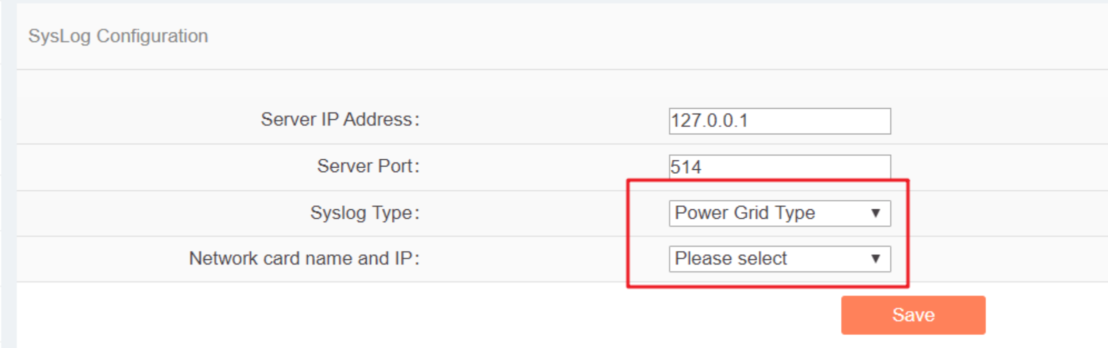
Server Port: 514

Syslog Type: Common type

Fig.6-75 Saving the sysLog Configuration

4.6.10.3. 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):



SysLog Configuration

Server IP Address: 127.0.0.1

Server Port: 514

Syslog Type: Power Grid Type

Network card name and IP: Please select

Fig.6-76 Grid Type

4.6.11. Firewall Platform Upgrade

The firewall platform upgrades to a new version of firewall platform functions, skip to the upgrade server for upgrade operation.

4.6.11.1. Firewall platform upgrade

Log in as the configuration administrator, click [System Configuration/Firewall Platform Configuration] (as shown in Fig.6-77), enter the firewall platform upgrade page. (as shown in Fig.6-78):

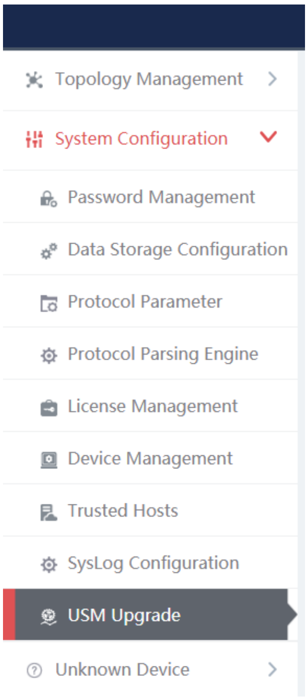


Fig.6-77 Firewall Platform Upgrade Menu Bar

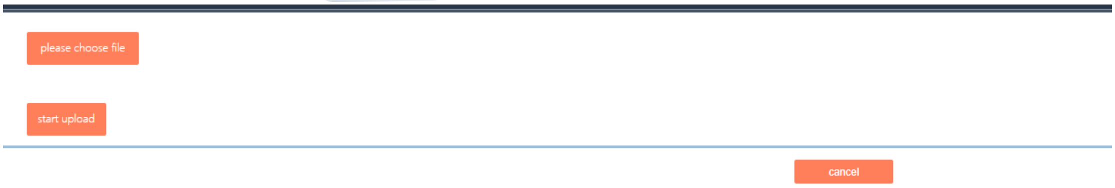


Fig.6-88 Firewall Platform Upgrade Page

4.6.11.2. Start upgrade

After selecting the upgrade file, click <Start Upload>, check the progress of the progress bar. After successful upgrade, access to the firewall platform. (as shown in Fig.6-89):

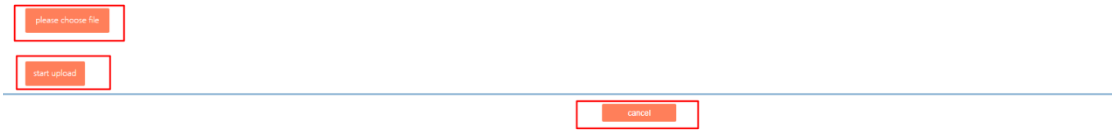


Fig.6-89 Start Upgrade

4.7. Topology Management

4.7.1. 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 firewall 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.

4.7.2. Topology

The firewall 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):

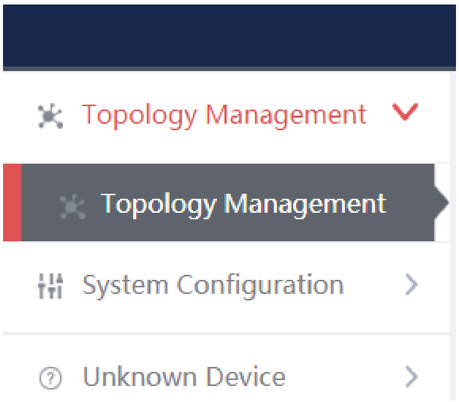


Fig.6-90 Device Management Menu

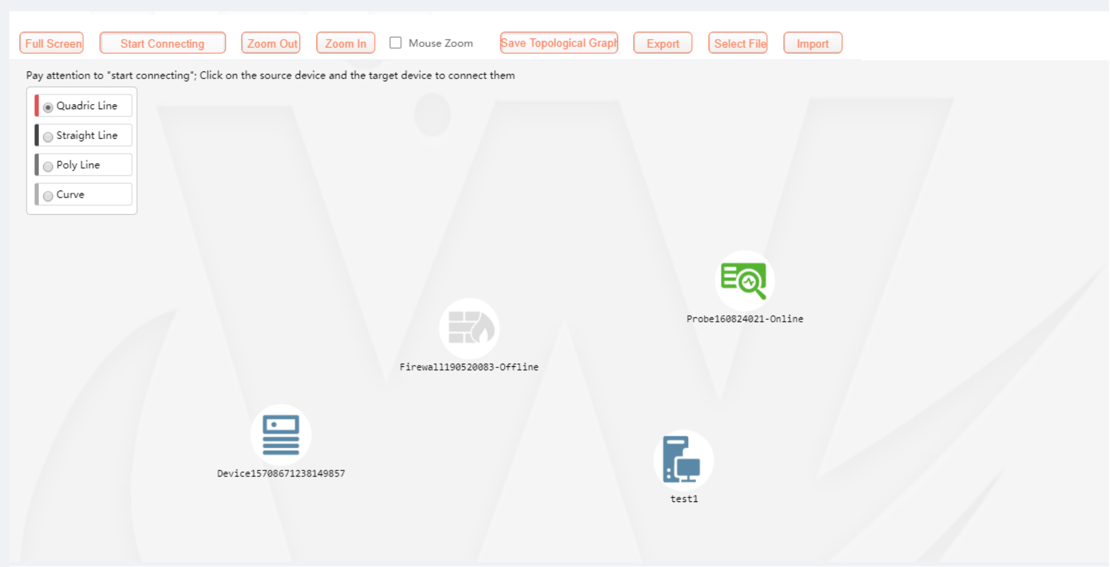


Fig.6-91 Device Management Page

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):

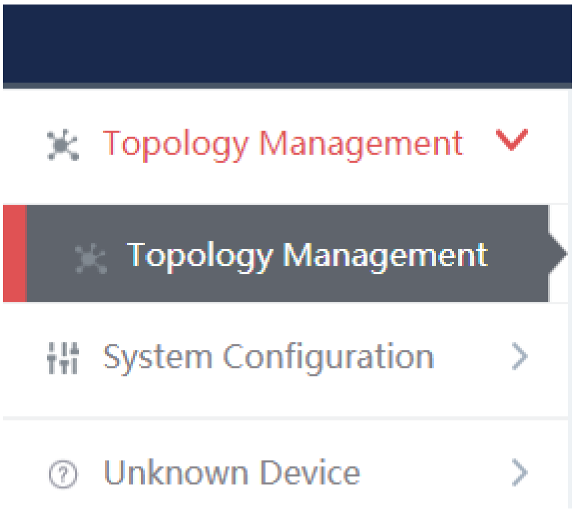


Fig.6-92 Device Management Menu

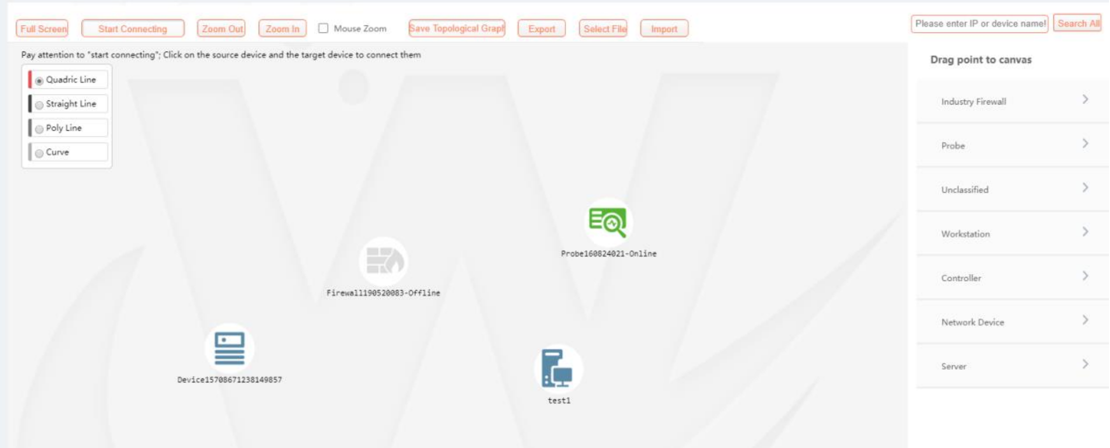


Fig.6-93 Device Management Page

4.7.2.1. Composition of network topology

The network topology of the firewall platform is mainly composed of devices and lines, with the devices including the following:

- Industrial firewall
- Probe
- Workstation
- Controller
- Network device
- Server
- Unclassified

(as shown in Fig.6-94):

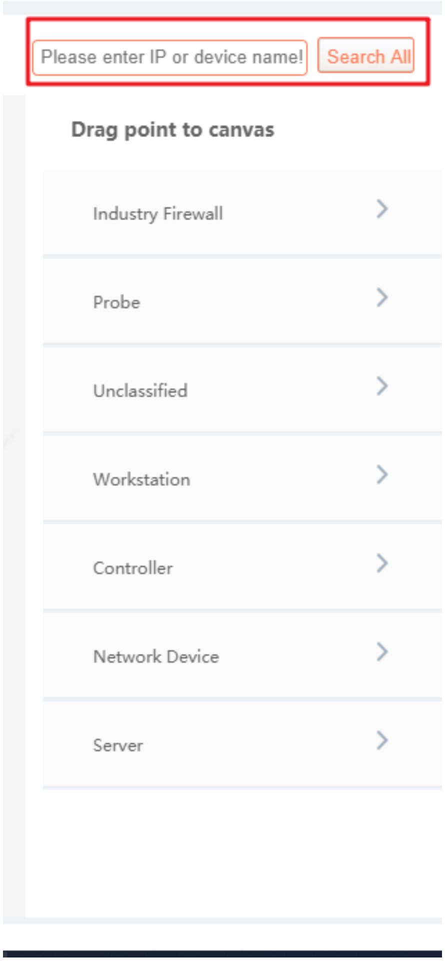
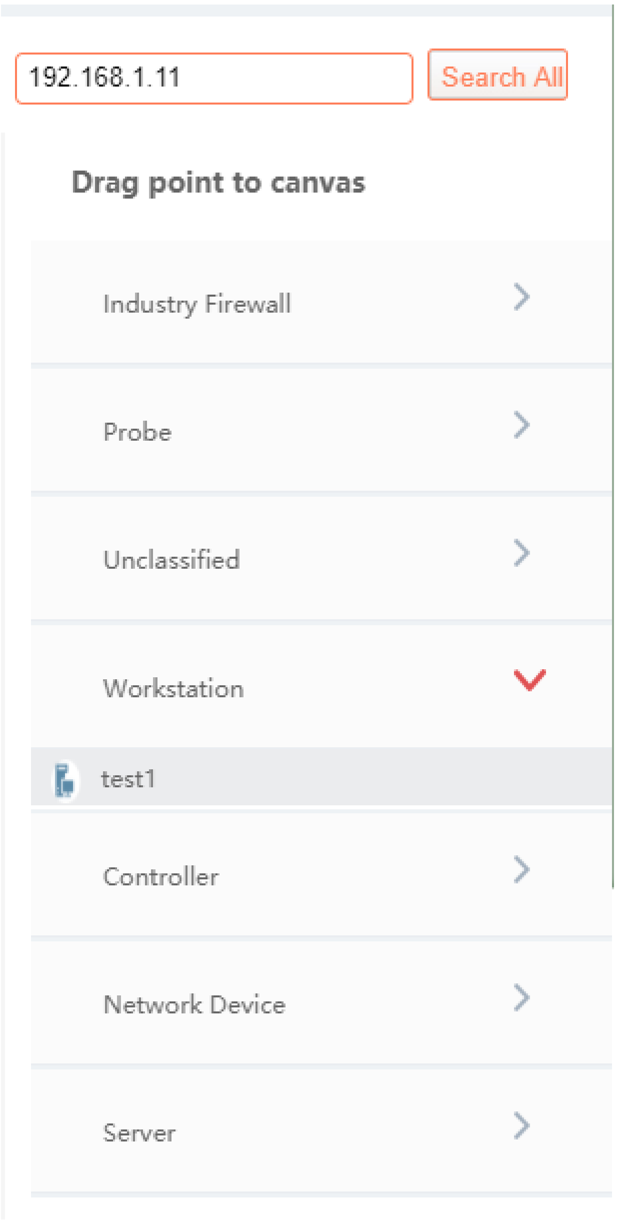


Fig.6-94 Topology Device List

4.7.2.2. 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):



192.168.1.11

Fig.6-95 Query Results

4.7.2.3. Edit a network topology

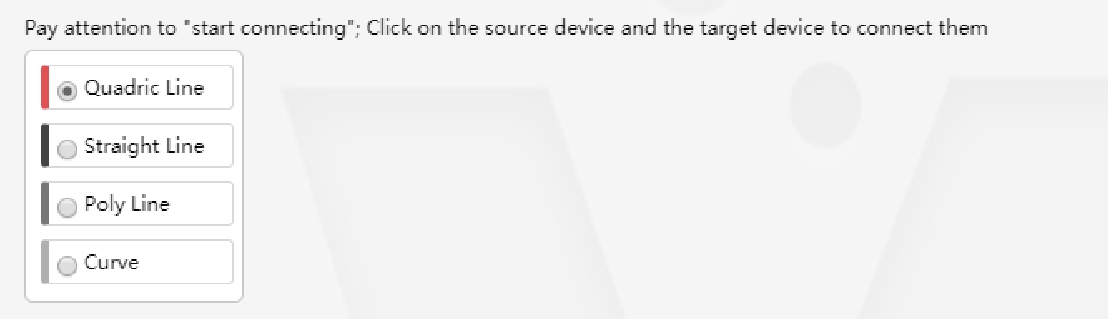
It is very convenient to edit the topology.

- **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:



Pay attention to "start connecting"; Click on the source device and the target device to connect them

● Quadric Line
○ Straight Line
○ Poly Line
○ Curve

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.

4.7.2.4. 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.

4.8. Unknown Device Detection

4.8.1. 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):

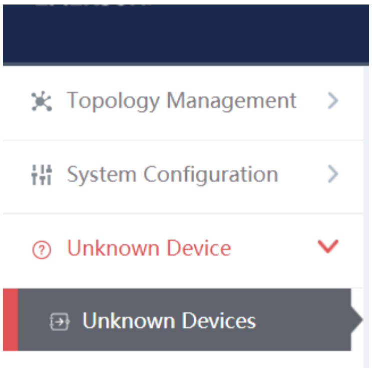
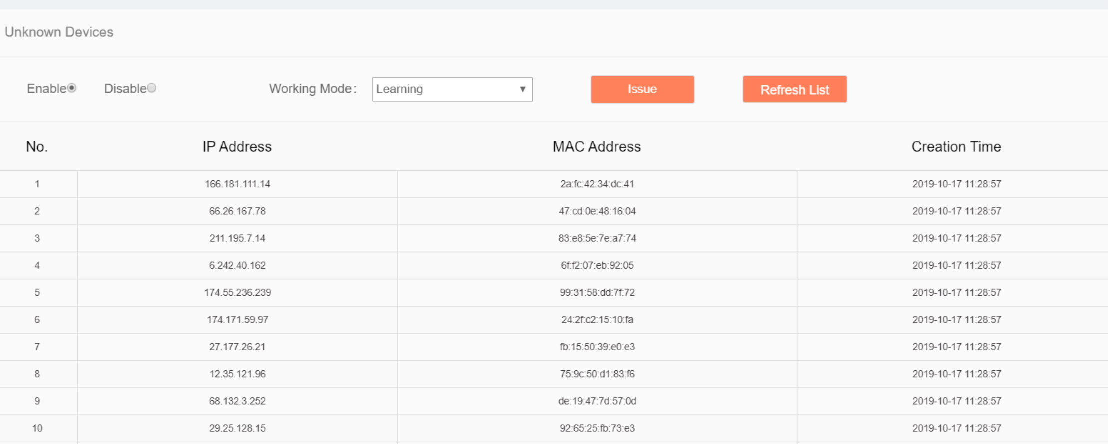


Fig.6-96 Unknown Device Detection Configuration Menu Bar


Unknown Devices

Enable◉ Disable○ Working Mode: Learning ▾

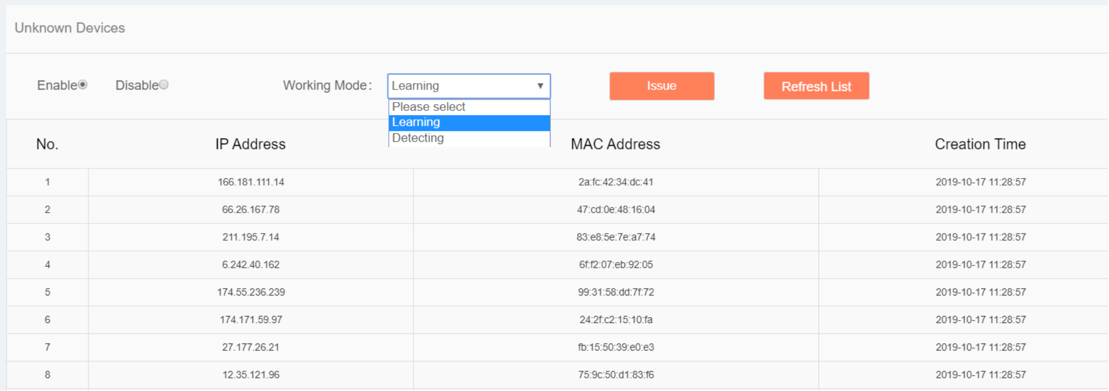
No.	IP Address	MAC Address	Creation Time
1	166.181.111.14	2a:fc:42:34:dc:41	2019-10-17 11:28:57
2	66.26.167.78	47:cd:0e:48:16:04	2019-10-17 11:28:57
3	211.195.7.14	83:e8:5e:7e:a7:74	2019-10-17 11:28:57
4	6.242.40.162	6f:f2:07:eb:92:05	2019-10-17 11:28:57
5	174.55.236.239	99:31:58:dd:7f:72	2019-10-17 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

4.8.1.1. 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):

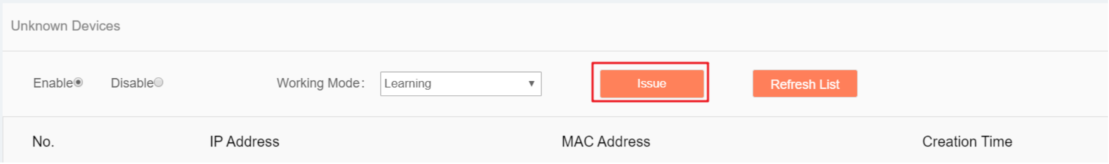

Unknown Devices

Enable◉ Disable○ Working Mode: Learning ▾

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

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):

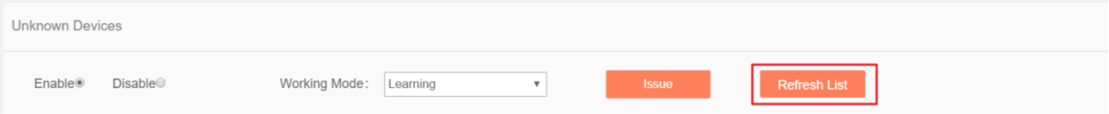

Unknown Devices

Enable◉ Disable○ Working Mode: Learning ▾

Fig.6-99 Detecting

Rule Edit

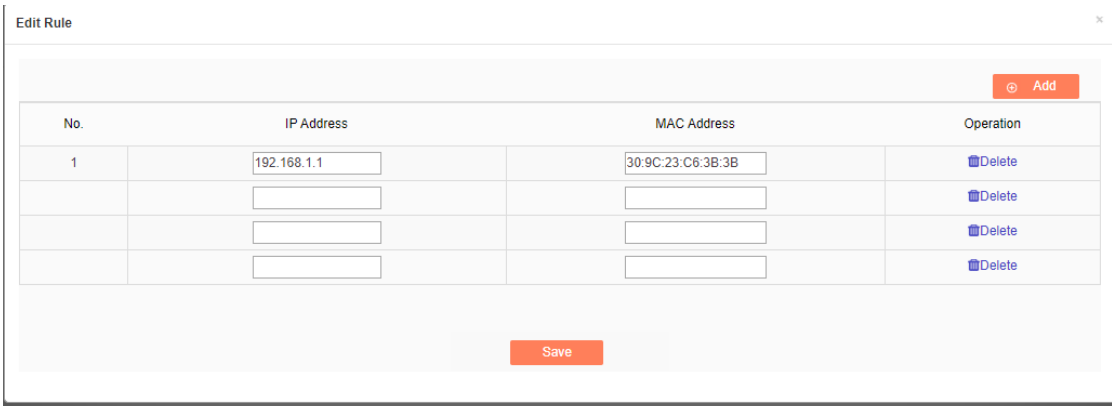
Click <Edit a Rule> and skip to the rule edit page. (as shown in Fig.6-100):


Unknown Devices

Enable◉ Disable○ Working Mode: Learning ▾

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):



Edit Rule ×

⊕ Add

No.	IP Address	MAC Address	Operation
1	192.168.1.1	30:9C:23:C6:3B:3B	Delete
			Delete
			Delete
			Delete

Save

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):

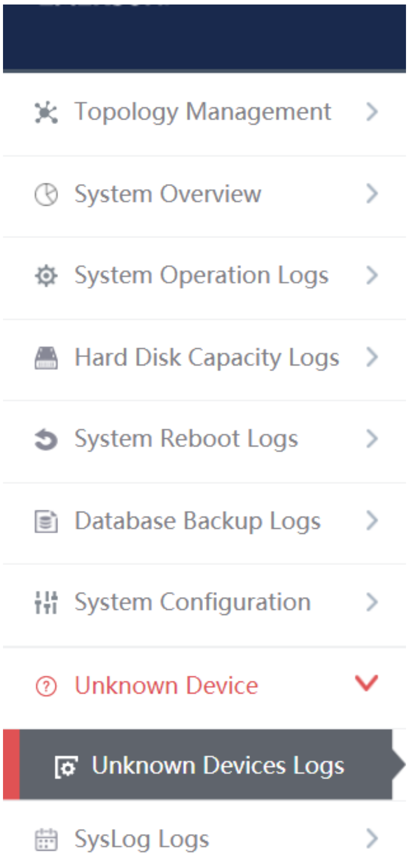
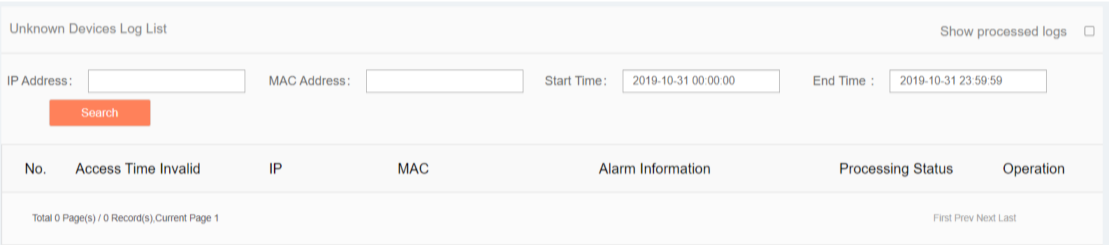


Fig.6-102 Unknown Device Detection Log Menu Bar



Unknown Devices Log List

Show processed logs □

IP Address: MAC Address: Start Time: 2019-10-31 00:00:00 End Time : 2019-10-31 23:59:59

Search

No.	Access Time Invalid	IP	MAC	Alarm Information	Processing Status	Operation

Total 0 Page(s) / 0 Record(s),Current Page 1

First Prev Next Last

Fig.6-103 Unknown Device Detection Log Page

Log list

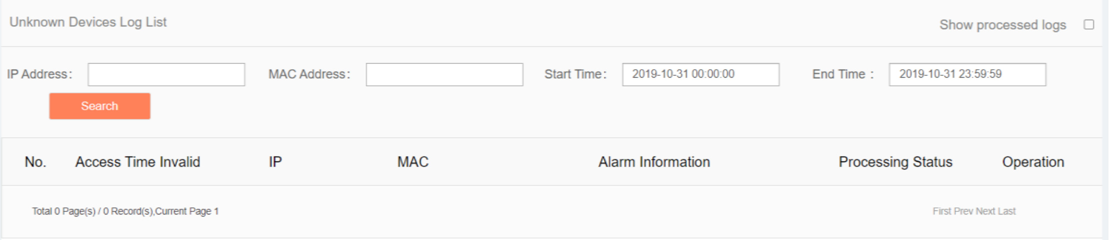
View all the log information on unknown device detection alarms here, with the meaning given below:

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):



Unknown Devices Log List

Show processed logs □

IP Address: MAC Address: Start Time: 2019-10-31 00:00:00 End Time : 2019-10-31 23:59:59

Search

No.	Access Time Invalid	IP	MAC	Alarm Information	Processing Status	Operation

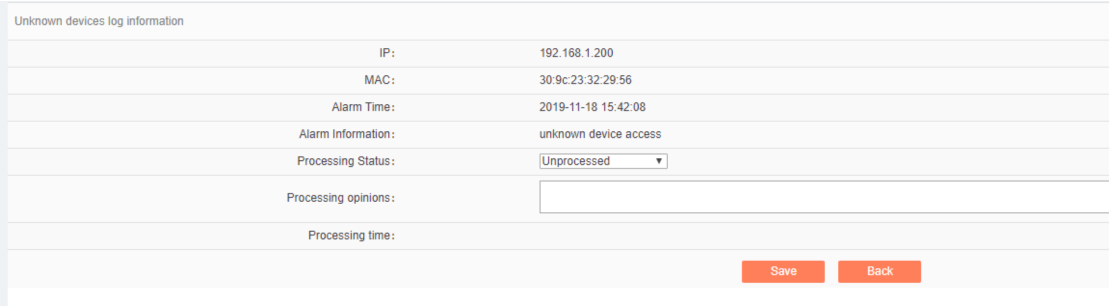
Total 0 Page(s) / 0 Record(s),Current Page 1

First Prev Next Last

Fig.6-104 Show Processed Unknown Device Detection Log List Page

4.8.1.2. 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:



Unknown devices log information

IP: 192.168.1.200

MAC: 30:9c:23:32:29:56

Alarm Time: 2019-11-18 15:42:08

Alarm Information: unknown device access

Processing Status: Unprocessed ▾

Processing opinions:

Processing time:

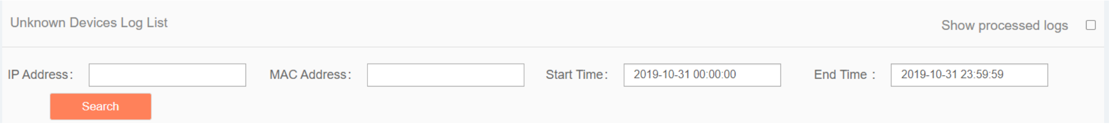
Save Back

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.

4.8.1.3. Retrieve a log

On the [Unknown Device Detection Logs] list page, retrieve an alarm based on the conditions. (as shown in Fig.6-106):



Unknown Devices Log List

Show processed logs □

IP Address: [ ] MAC Address: [ ] Start Time: 2019-10-31 00:00:00 End Time : 2019-10-31 23:59:59

Fig.6-106 Retrieving an Unknown Device Detection Log

4.9. 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):

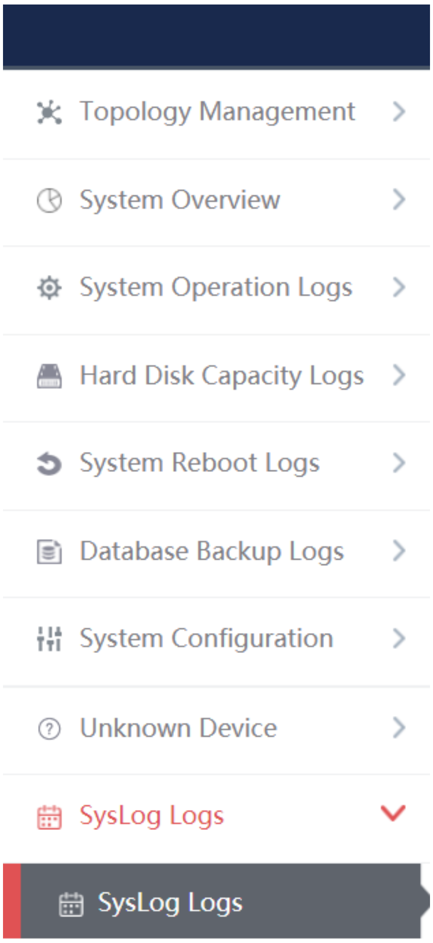
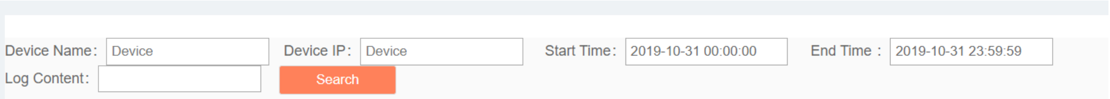


Fig.6-107 syslog Log Menu



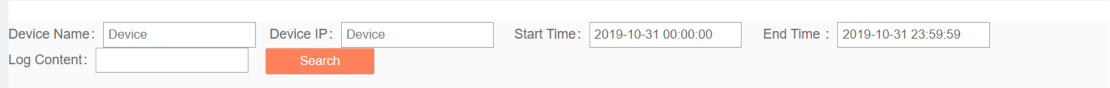
Device Name: Device Device IP: Device Start Time: 2019-10-31 00:00:00 End Time : 2019-10-31 23:59:59

Log Content: [ ]

Fig.6-108 syslog Log

4.9.1. Retrieve a Log

In the [SysLog Logs] list page, retrieve the log according to the conditions. (as shown in Fig.6-109):



Device Name: Device

Device IP: Device

Start Time: 2019-10-31 00:00:00

End Time : 2019-10-31 23:59:59

Log Content:

Fig.6-110 Log Query