

AVCOMM EdgeCommander User Manual



AVCOMM Technologies Inc.

EdgeCommander

User Manual

Copyright Notice

© AVCOMM. All rights reserved.

About This Manual

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



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

Disclaimer

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

Avcomm Online Technical Services

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



Contents

1.	Ov	erview of Unified Security Management	1
	1.1.	Unified Security Management Networking Diagram	1
	1.2.	Product Description	1
	1.3.	Operating Steps	2
	1.4.	About the Manual	4
	1.5.	How to Use the Manual	4
	1.6.	Provisions of Graphical Interface Format	4
2.	Lo	g in the Unified Security Management Platform	
	<u>.</u> 2.1.	Start the Unified Security Management Platform	
2	2.2. 2.2.	Log in the Management Platform	
	2.2.		
2	2.3.	View the Management Platform Version	7
2	2.4.	Exit the Management Platform	3
3.	Ind	ustrial Firewall	8
3	3.1.	Introduction to Products	B
	3.1.	1. Product Overview	8
	3.1.	2. Appearance and Description	9
	3.1.3	3. Instruction to Indicator Lights	9
	3.1.4	4. Technical Specifications	0
3	3.2.	Startup and Login1	3
	3.2.	1. Startup of Industrial Firewall 1	3
	3.2.2	2. CLI Application	4
3	3.3.	Firewall Management1	5
	3.3.	1. Introduction to Functions	5
	3.3.	2. Firewall Management	6
	3.3.	3. Authorization Management	3
	3.3.4	4. Firewall Upgrade	6
	3.3.	5. IP/MAC Address Binding	6
	3.3.	6. Group Management	9
	3.3.	7. Firewall Syslog Configuration	5
3	3.4.	Whitelist Management	6
	3.4.	1. Introduction to Functions	6
	3.4.2	2. Template Management	6
	3.4.	3. Whitelist Template Rule Management 4	1

INDUSTRIAL 3.5. 3.5.1. 3.5.2. 3.6. 3.6.1. 3.6.2. 3.6.3. 3.6.4. 3.6.5. 3.6.6. 3.7. 3.7.1. 3.7.2. 3.7.3. 3.7.4. 3.7.5. 3.7.6. 3.8. 3.8.1. 3.8.2. 3.8.3. Firewall Alarm Logs......72 Firewall Run Log75 3.8.4. 3.8.5. Address Spoofing Logs......77 3.8.6. 3.8.7. 4. Industrial Endpoint Guard(IEG)......81 4.1. 4.2. System Permissions81 4.3. 4.4. 4.4.1. 4.4.2. 4.5. 4.5.1. 4.5.2. 4.5.3. 4.5.4. 4.5.5. 4.6. 4.6.1. 4.6.2. AVCOMM Technologies Inc.

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



4.6.3.	System Integrity Check	
4.6.4.	Whitelist Management	
4.6.5.	Program Control	
4.6.6.	Alarm Processing	
4.6.7.	Process Audit	
4.7. Se	ecurity Baseline	90
4.7.1.	Safety Baseline Template	
4.7.2.	Security Baseline Configuration	
4.8. De	evice Management	96
4.8.1.	Windows Device Management	
4.8.2.	Linux Device Management	
4.8.3.	Registered USB Management	
4.9. Ac	cess Control	97
4.9.1.	Registry Protection Template	
4.9.2.	File Protection Template	
4.9.3.	File Protection Exception Template	
4.9.4.	Registry Protection Policy	
4.9.5.	File Protection Policy	
4.10. [·]	Two-factor Authentication	
4.10.1.	User Template	
4.10.2.	Authentication Policy	101
4.10.3.	Domain User Binding Information	103
4.11.	Basic Configuration	
4.11.1.	Basic Configuration	
4.11.2.	Operating System Log Audit	104
4.11.3.	Authorization Management	104
4.11.4.	Upload a Non-Whitelist File	105
4.11.5.	Installation Package Management	106
5. Monito	ring Audit	
5.1 Int	troduction to Products	
5.1.1	Product Overview	
5.1.2	Appearance and Description	
5.1.3.	Indicator Light Description	
5.1.4.	Technical Specifications	109
5.2. St	artup and Login	119
5.2.1.	Startup of Intelligent Monitoring Terminal	119
5.2.2.	Use of CLI	120
5.3. Int	telligent Monitoring Terminal Management	
5.3.1.	Introduction to Functions	



5	.4. 1	Policy Management	131
	5.4.1	Industrial Protocol Whitelist Template	132
	5.4.2	Protocol Detection Exception Template	142
	5.4.3	Critical Event Template	151
	5.4.4	User-Defined Rules	160
	5.4.5	Network Session Audit Template	162
	5.4.6	No Traffic Detection Template	170
5	.5. I	_og Management	177
	5.5.1	Introduction to Functions	177
	5.5.2	Industrial Protocol Whitelist Alarm	177
	5.5.3	Industrial Protocol Detection Alarm	181
	5.5.4	No Traffic Alarm	185
	5.5.5	Critical Event Alarm	187
	5.5.6	User-Defined Alarm	191
	5.5.7	Industrial Protocol Audit Log	194
	5.5.8	Network Session Audit Log	196
	5.5.9	Intelligent Monitoring Terminal Run Log	198
	5.5.1). Abnormal Traffic Log	200
5	.6. 3	System Configuration	
	5.6.1	Alarm Level Settings	202
	5.6.2	Instruction to Alarm Levels	203
5	.7. 1	Network Connection	
5	. 7. 1 5.7.1		
5		Introduction to Functions	204
5	5.7.1	Introduction to Functions Network Connection Baseline Configuration	204 204
5	5.7.1. 5.7.2	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration	
-	5.7.1. 5.7.2. 5.7.3. 5.7.4.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration	
-	5.7.1. 5.7.2. 5.7.3. 5.7.4.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram	
-	5.7.1 5.7.2 5.7.3 5.7.4	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram Abnormal Traffic Introduction to Functions	
-	5.7.1. 5.7.2. 5.7.3. 5.7.4. .8. 5.8.1.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram Abnormal Traffic Introduction to Functions Baseline Configuration	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram Abnormal Traffic Introduction to Functions Baseline Configuration	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram Abnormal Traffic Introduction to Functions Baseline Configuration Abnormal Traffic Monitoring Statistical Analysis	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.1. 5.8.2. 5.8.3. .9.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram Abnormal Traffic Introduction to Functions Baseline Configuration Abnormal Traffic Monitoring Statistical Analysis Historical Statistics of Network Traffic Messages	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3. 5.8.3. 5.9.1.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram Abnormal Traffic Introduction to Functions Baseline Configuration Abnormal Traffic Monitoring Statistical Analysis Historical Statistics of Network Traffic Messages Network Real-Time Traffic	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3. 5.8.3. 5.9.1. 5.9.2.	Introduction to Functions Network Connection Baseline Configuration Network Traffic Baseline Configuration Network Connection Diagram Abnormal Traffic Introduction to Functions Baseline Configuration Abnormal Traffic Monitoring	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3. 5.8.3. 5.9.1. 5.9.2. 5.9.3.	Introduction to Functions	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3. 5.9.1. 5.9.2. 5.9.3. 5.9.4.	Introduction to Functions	
5	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3. 5.9.1. 5.9.2. 5.9.3. 5.9.4. 5.9.5. 5.9.6.	Introduction to Functions	
5 5 6.	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3. 5.9.1. 5.9.2. 5.9.3. 5.9.4. 5.9.5. 5.9.6. Sys i	Introduction to Functions	
5 5 6.	5.7.1. 5.7.2. 5.7.3. 5.7.4. 5.8.1. 5.8.2. 5.8.3. 5.9.1. 5.9.2. 5.9.3. 5.9.4. 5.9.5. 5.9.6. Sys i	Introduction to Functions	

	— INDUSTRIALIT—	
6.2.1.	Retrieve a Log	231
6.3. Hai	rd Disk Utilization Logs	
6.3.1.	Retrieve a Log	
6.4. Svs	stem Restart Log	233
6.4.1.	Retrieve a Log	
6.5. Dat 6.5.1.	tabase Backup Log Retrieve a Log	
•	stem Configuration	
6.6.1.	Password Management	236
6.6.2.	User Management	238
6.6.3.	USBKey Management	243
6.6.4.	Database Storage Cycle Configuration	245
6.6.5.	Protocol Parameter Configuration	
6.6.6.	Decoding Engine Configuration	252
6.6.7.	Authorization Management	253
6.6.8.	Device Management	255
6.6.9.	Trusted Host	259
6.6.10.	SysLog Configuration	263
6.6.11.	Management Platform Upgrade	264
6.7. Top	pology Management	
6.7.1.	Introduction to Functions	
6.7.2.	Topology	266
6.8. Un	known Device Detection	
6.8.1.	Unknown Device Detection Configuration	271
6.9. Sys	sLog Log	
6.9.1.	Retrieve a Log	277



1. Overview of Unified Security Management

1.1. Unified Security Management Networking Diagram



1.2. Product Description

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

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

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

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

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

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

1.3. Operating Steps

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





1.4. About the Manual

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

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

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

1.5. How to Use the Manual

The Manual mainly give a detailed description of industrial firewalls, host reinforcement, monitoring & audit, and system configuration as much as possible.

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

1.6. Provisions of Graphical Interface Format

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



2. Log in the Unified Security Management Platform

2.1. Start the Unified Security Management Platform

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

After the startup of the management platform, the Google Chrome can be enabled on a host that is available to the management platform online (the Google Chrome is recommended), enter https://192.168.8.88440/ or a website similar to the following:

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

http://192.168.8.8:8080 (old version)

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

Description:			
If the browser reports an error as she	own in the following figure, simply click "	Advanced " below th	e browser
	<u>192.168.4.204 (unsafe)</u>		
page, then select "	".		
	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\KeyExchangeA lgorithms\Diffie-Hellman] Right-click and select New, then select DWDRD (32-bit), change the name to ClientMinKeyBitLength and modify the data to 00000200.





2.2. Log in the Management Platform

2.2.1.Normal Login

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



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

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

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

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

2.2.2.Two-Factor Authentication Login

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

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

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

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

2.3. View the Management Platform Version

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



			粒、
& Probe Management →	In Probe > Probe Management > Probe Management		导
■ Policy Management >			Ret 把
Network Connection	Probe : Online Status: Please select Probe SN: Probe IP:		65-R
Abnormal Traffic >	No Probe Probe IP	Work Mode Online Status Operation	
System Configuration >	Table (Fright) / O Recently, Carriert Page 1		
	Product Name: Avcomm M		
	Product Version:V100R00SC01B610		
	Product Type PWCS-C-SIEM		
			1

Fig.2-3 Version Information on Management Platform

2.4. Exit the Management Platform

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



Fig.2-4 management platform exit.

3. Industrial Firewall

3.1. Introduction to Products

3.1.1.**Product Overview**

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



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

3.1.2. Appearance and Description



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

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

⁽⁶⁾ Service network port, 10/100/1000BASE-T adaptive Ethernet port; there are two pairs, with those connected closely as a pair. Any one of the two pairs can be used as the entrance and the other as the exit. Do not cross the two pairs.

3.1.3.Instruction to Indicator Lights

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



Fig.3-2 Indicator Lights

Tab 1 Instruct	tion to Indicate	or Lights of Indu	strial Firewall
Inc. I monue	non to marcate	JI LIGHUS OI IIIQU	Sului i newuli

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



		NO in green	The power supply is normal, the host is
			powered on normally
Running indicator		NC	The device is not powered on or breaks
light	RUN		down
		Flashing in	The device works regularly
		green	
		Flashing in red	The device fails or undergoes a network
			attack.
Bypass indicator	BP	NC	The BPYASS function is not started
light		NO	The BYPASS function is enabled
Ethernet port	MGMT	NC	The corresponding interface is in an
indicator light	ETH1/ETH2/ET		unconnected state
	H3/ETH4	Color of	The green color indicates that the current
		indicator lights	operation is based on a gigabit rate.
			The orange color indicates that the current
			operation is based on a megabit rate
		The indicator	The interface has been established
		light is	
		normally on	
		The indicator	The interface is sending and receiving data
		light flashes	

3.1.4. Technical Specifications

Tab.2 Technical Specification for Industrial Firewalls

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



Intelligent learning	Help to generate rules by intelligent protocol detection				
	Help to generate rules by intelligent protocol detection				
rules					
Rule test mode	Provide test modes to verify the correctness of security rules and business applicability				
Three-level	The administrator permis	sions are separately divide	d for the approval		
permission	administrator, the configuration administrator and auditor				
management					
Local cache of logs	The security logs can be sent to the log server or to a local cache				
IP/MAC address	Support manually or learning to establish the IP, MAC binding relationship,				
binding	avoiding address spoofing				
User-defined	Identify the industrial control protocol according to the customer's actual				
whitelist application	business on site, so as to facilitate the preparation free of misinformation				
Unknown device detection	Quickly discover illegally connected devices				
Session	Inquiry ongoing sessions in real time and individually set the session aging				
management	time				
Performance characte	ristics				
Number of data	More than 100,000 points				
collection points					
Packet delay	Less than 100µs based on	the full configuration poli	icy		
Concurrent	300000	300000	300000		
connections	300000	300000	300000		
	Unlimited				
User limit	Auto bypass when in case of a power failure or system exception				
User limit Bypass function	Auto bypass when in case	e of a power failure or syst	em exception		



r		- INDUSTRIALT	
Processor	Dedicated multi-core	Dedicated multi-core	Dedicated multi-core
	network processor	network processor	network processor
Memory	DDR3 1G	DDR3 1G	DDR3 2G
Log storage	4G	4G	4G
Business port	Business port 6 gigabit combo port		16 gigabit ports +6 gigabit combo ports +2 gigabit SFP+ ports
Bypass	3 RJ45 interface	6 RJ45 interface	11 RJ45 interface
Management port	1 port 10/100/1000 Mbps adaptive	1 port 10/100/1000 Mbps adaptive	1 port 10/100/1000 Mbps adaptive
Serial interface	RJ45 debugging port	RJ45 debugging port	
USB interface	1 port, USB 2.0	1 port, USB 2.0	1 port, USB 2.0
Dimensions/power sup	oply/operating environme	ent	
Working environment	Temperature: -40 ~ 75°C Humidity: 5%-95%, no condensation	Temperature: -10 ~ 60°C Humidity: 5%-95%, no condensation	Temperature: -10 ~ 60°C Humidity: 5%-95%, no condensation
Storage85°CenvironmentHumidity: 5%-95%, no condensation		Temperature: -40 ~ 85°C Humidity: 5%-95%, no condensation	Temperature: -40 ~ 85°C Humidity: 20%-80%, no condensation
MTBF	MTBF 250,000 hours 250,000 hours		250,000 hours
Power supply	Power supply 9-36VDC, Redundant power supply		100-240V AC, Redund ant power supply
Peak power consumption 14.5W,		Typical power consumption 26W, Max 46W	Typical power consumption 29W, Max 50W



Dimensions	00 150 105	4.40*400*44	4.40*400*44	
(WxDxH) mm	89x150x135mm	440*400*44mm	440*400*44mm	
Installation mathed	35mm standard DIN	Standard 19" rack	Standard 19" rack mou	
Installation method	rail clamping	mounting	nting	
Protection grade	Protection grade IP40		IP40	
Authentication CE, CB		CE, CB	CE, CB	

3.2. Startup and Login

3.2.1.Startup of Industrial Firewall

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



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

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

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

AVCOMM Technologies Inc.



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

3.2.2.CLI Application

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

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

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



Fig.3-4 CLI Interface

Introduction to Common Commands:

3.2.2.1.**Help**

CLI>help

Display the help information.

3.2.2.2. System statistics related.

CLI>show pkt stat

View message statistics at all levels.

CLI>show mgmtip

View the IP address information on the management port.

CLI>show fpa

View the FPA information, mainly on various memory statistics.

CLI>show mem pool

View the mem pool information.



3.2.2.3. Enter the system configuration view.

CLI> config

Enter the system configuration view for the following configuration.

3.2.2.4. Change the IP address of the management port.

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

CLI#set mgmtip <ip> [netmask]

Change the IP address of the device management port.

For example: change the IP address of the management port of Industrial Firewall A to 192.168.8.6. The full

command of the mask 255.255.255.0 is as follows:

CLI# set mgmtip 192.168.8.6 255.255.255.0

3.2.2.5. Set the address of the management platform.

CLI>show serverip

Check the IP address of the unified security management platform as configured in the industrial firewall CLI#set serverip <IPV4ADDR: serverip>

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

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

CLI>config

Set the industrial firewall gateway command,

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

3.3. Firewall Management

3.3.1.Introduction to Functions

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

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



configuration, it shall be removed from its own group.

3.3.2. Firewall Management

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

Ģ		Ğ	۵.	admin Welcome 🞝 About 🗗 Exit
		Fig.	3-5 Industrial Firewall in Upper Menu	Bar
			Firewall Management	>
			Whitelist Management	>
	(٩	Routing Management	>
		<u>À</u>	ACL Management	>
	(3	Security Domain	>

Fig.3-6 Firewall Management in Navigation Bar



>		Firewall Name:		Fire	wall IP:		Onlin	ne status: Pleas	e select	• Wor	k Mode Please	select	Ŧ	Search	
>	No.	Firewall Name	Device	e 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	Firewall1608240 69		Memory Usage	160824069	192.168.4.97	Offline	Alert Mode	555	2	99	2	Disabled	2019-11-13 20:0 0:06	View Modify Delete Upgrav Factory Reset Backup Policy
	Tota	al 1 Page(s) / 1 Reco	rd(s),Current Page 1											First Prev Next L	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 management platform (that is,
	online) or not connected (that is, offline)
Work Mode	Under which operation mode the current industrial firewall is in, the new industrial
	firewall is defaulted to "initial state".
Whitelist	The template name of the whitelist rules that are applied to the industrial firewall, if
Template Name	blank, it means that currently the industrial firewall has no whitelist rules set yet
Whitelist	The template version of the whitelist rules that are applied to the industrial firewall,
Template	the version and the template ID uniquely determine a set of whitelist rules, each edit
Version	whitelist and save, with the version number automatically +1 after each time the
	whitelist is edited and saved.
ACL Template	The template name of the ACL rules that are applied to the industrial firewall, if blank,
Name	it means that currently the industrial firewall has no ACL rules set yet

AVCOMM Technologies Inc.



Г

ACL Template						
Version	The template ve	ersion 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 edite	ed and saved.				
Time	The last time the industrial firewall goes online					
Online						
	View	View more detailed information on industrial firewalls, view the				
	K View	authorized function of each industrial firewall under the sub-page				
	Modify	Modify and set the information, operation mode, whitelist template				
	Modify	and security policy rules, etc. of industrial firewall				
Operation	Delete	Delete the offline industrial firewall, unable to delete the online				
	💼 Delete	industrial firewall. After deleting the industrial firewall, click				
		"Display Deleted Ones" to view and restore the information				
	Upgrade	Upgrade the software running on the industrial firewall online. Only				
	(T) Upgrade	when the industrial firewall is online can this operation be conducted,				
		refer to Section 3.3.4 Firewall Upgrade				
	Restore the	One-key reset the factory settings of fire walls devices				
	factory					
	settings.					
	Factory Reset					
	Back up all	Copy all policies being applied on the source device to one or more				
	policy	other online and non-learning devices for distribution				
	applications					
	Backup Po					



3.3.2.1. Information view

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

Firewall > Firewall Management > View	
Firewall Basic Information	
Firewall Name:	Firewall160824069 Kiew 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	💽 ОЕТНО 💽 ОЕТН1 💟 ОЕТН2 💽 ОЕТН3
Message Out	

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):



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
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	et individual whitelist for the firewall!)
Whitelist Template:	whitelist_390
Firewall security Policy Template	
Security Policy Template Name:	ACL-LHB V
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	
d Enable	Edit IP-MAC configuration
Session Aging Time Setting	
TCP Aging Time	1 Minute(s)
UDP Aging Time	1 Minute(s)
Firewall Syslogs Setting	
Server IP Addr.:	
Server Port:	
Device Grab Configuration	
Message In	ЕТНО С ЕТН1 С ЕТН2 С ЕТН3
Message Out	💽 🛛 ЕТНО 💽 🗆 ЕТН1 💽 🗆 ЕТН2 💽 🗆 ЕТН3

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

AVCOMM Technologies Inc.

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

	- INDUSTRIAL IT-
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	The security policy template currently used for the industrial firewall,
Name	optional
IP/MAC Addr. Binding	Configure IP/MAC address binding rules
Session Aging Time	Set the session aging time for TCP and UDP connections.
Setting	Check grab network port, support to capture the message of any one or more
Device Grab	ports including eht0, eth1, eth2, eth3, eth4, and eth5. It is possible to specify
Configuration	to capture the incoming, outgoing or two-way message of each port. The



	manageme	management platform stores the captured messages according to the				
	device ports, and can to query and download the messages.					
	Message query and Download can view all messages captured network port					
	capture pac	capture packet to capture all messages by network port grab package, which				
	can be dow	can be downloaded				
	And down	And download.				
	Save All modification information will be saved to the database an					
	taken into effect and returned to the industrial firewal					
Operation		information list display page.				
	Back Ignore all modifications and go back to the industrial fire					
	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
	Firewall1608240 69	CPU Usage Memory Usage	160824069	192.168.4.97	Online	Initial State					Disabled	2019-11-21 14:2 7:14	 View Modify Delete Factory Reset Backup Policy
Total	Total 1 Page(s) /1 Records).Current Page 1 First Prev. Not. Last						ext Last						

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 dele	ted 🗆
Firewall Name:	Firewall IP:	Online status: Please select	• Wo	ork Mode Please select	Y	Search



3.3.3.Authorization Management

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



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

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

• Manually activate it through the unified security management platform

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

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

3.3.3.1. Check authorization.

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

Firewall > Firewall Management > View				
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
	Download File Renew Authorization	
	Back	

Fig.3-14 Authorization Details View Page

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

Download File

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

Renew Authorization

Update the authorization information on the current industrial firewall.

Back

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

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

3.3.3.2. Update the firewall authorization information.

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



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

Please select...

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

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

Back

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



3.3.4. Firewall Upgrade

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

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

Firewall Upgrade				
Select File	Please select a file	e to upgrade		
	Start Upgrade	Close		

Fig.3-16 Industrial Firewall Upgrade File Selection

➢ Select File

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

Start Upgrade

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

Close

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

3.3.5.IP/MAC Address Binding

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



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				
	Edit IP-MAC cor	figuration		
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):





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 Recor	d(s),Current Page 1 First P	rev 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 P	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):

ning Data		
Learning Data Tip:	Entries added through learning data are	e automatically saved to the rule list!
IP Addr.:	MAC Addr.:	Search Add the selected
Vo.	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


	Firewal	Firewall > Firewall Management > Group Management									
	Group List									Add	
•		Group Name:		Searc	h						
	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 F	Page(s) / 1 Record(s),Current P	lage 1							First Prev Next Last	

Fig.3-23 Group List Display Page

View the information on all industrial firewall groups in the system here, with the meaning as follows: Tab.5 Instruction to Group Management List Display

Column Names	Instructions			
Group Name	an industrial firewall group name that is easy to remember, for example			
	"6#DCS Industrial Firewall Group"			
Work Mode	The operati	ion mode which currently all industrial firewalls under the group		
	are in, whic	ch means being in the initial status if without any additions		
Whitelist Template	The name	of the whitelist rule template applied to all industrial firewalls		
Name	under the g	group; If blank, it means that no whitelist rule is currently set in		
	the group			
Whitelist Template	The version	n of the whitelist rule template applied to all industrial firewalls		
Version	under the group.			
ACL Template	The name of the ACL template applied to all industrial firewalls under the			
Name	group; If blank, it means that no whitelist rule is currently set in the group.			
ACL Template	The version of the ACL template applied to all industrial firewalls under the			
Version	group.			
IP/MAC Status	The state of IP/MAC Binding Status, Enable means on, Disbale means off			
Firewalls	Industrial firewalls contained in the group			
	View	View more detailed information on the group		
	Modify	Modify and set group information, operation modes, whitelist		
Onemation	templates, firewall rules, industrial firewalls contained and so			
Operation		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):

@ Firewall > Group List	Firewall Management > C	Group Management							⊕ Add
c	iroup Name:		Search						
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 Pa	ge(s) / 1 Record(s),Current Pag	je 1							First Prev Next Last

Fig.3-24 Firewall Group Add Buttons

Group Basic Information	
Firewall Group Name:	*
Remarks:	
	Save Back

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 I	nformation							
	Work Mode:		In	itial State				
Deploy Mode	e Information							
	Deploy Mode:		Т	ansparent Mode				
Applied Whit	elist Template Setting	9						
	Whitelist Template	Name:						
Firewalls								
No.	Firewall Name	Firewall SN	Firewall IP	Online status	Work Mode	Whitelist Template Name	Whitelist Template Version	Time Online



Firewall static routing configuration	
Functional state: disabled	
Firewall Interface Configuration:	
Static Routing Table Name :	
Firewall Syslogs Setting	
Functional state: disabled	
Server IP Addr.:	
Server Port:	
	Back

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):

Firewall :	> Firewall Management > 0	Group Management							
Group List									⊙ Add
	Group Name:		Search						
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		E, View 🛛 Modify 🛢 Delete
Total 1 Pa	age(s) / 1 Record(s),Current Pa	ge 1							First Prev Next Last
				Fig.3-2	7 Modify	Button			
Fire	wall > Firewall Ma	inagement > Grou	up Management						
Group I	Basic Information								
		Firewall Group	Name:		test	×			
		Re	marks:						
Firewal	lls								
		Firew	all List:		[Please select the	e firewall]			
Work N	Node Information								
		Work	Mode:		Initial State		•		
Deploy	ment mode info	rmation (* It can	only select trans	sparent mode if	this group has n	o firewall.)			
		D	eploy Mode:		Trans	sparent Mode	*		
Applie	Applied Whitelist Template Setting								
7 uppilo	a mitolist fomp								
		White	elist Template		S7 s	ub-protocol read	I-only whitelist t∈ ▼	·	
Firewa	Firewall security Policy Template								
	Sec	curity Policy Tem	plate Name:		Pleas	se select	*		



Firewall static route configuration (* configure only in routing mode)				
Firewall Interface Configuration:	Routing Physical Interface			
Static Routing Table Name:	Please select V			
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:				
	Save Back			

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=""></select>
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

AVCOMM°
— INDUSTRIALIT —

	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 nan	user to name the whitelist template generated by learning			
	7. If the op	eration mode of the group is changed, the operation modes of all			
	industrial firewalls under the group will be changed				
Whitelist Template	It means th	he 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	It means the security policy template name used by the group. Changes will				
Name	affect all industrial firewalls under the group				
IP/MAC Addr. Binding	Enable and edit IP/MAC address binding				
Session Aging Time	Set the sess	sion aging time for TCP and UDP connections			
Setting					
	Save	Save all modification information to the database and make it			
		come into effect, and go back to the [Group Information Display			
Operation	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									
rewall Name:	Firewall	IP:	Online st	atus: Please select	• Work Mode:	Please select	Whitelist Template	Name: Please select	▼ Search
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	Firewall 160824069	160824069	192.168.4.97	Online	Initial State			2019-11-14 11:56:36	a
Tital 1 Page(s) / 2 Record(s), Current Plage 1 First Prev Next Last									
Confirm									





Select the required industrial firewall in the opened page, click "Select" in the last row of "Operations"; deselect " $\sqrt{}$ " 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):

Firewall :	Frevail > Frevail Management > Group Management								
Group List	@ Add								
	Group Name: Search								
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 4 De	Tabel & Bassado / & Bassadio Accessed Bassa &						First Draw March Last		

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):

Firewall > Firewall Management > Group Management									
Group List									
Group Name: Search									
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		民 View 🗹 Modify 💼 Delete



3.3.7. Firewall Syslog Configuration

3.3.7.1. Configuration process

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

Tab.8 Instruction to Firewall	Syslog	Configuration
-------------------------------	--------	---------------

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



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

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

See	the	diagram	below:
Sec	une	ulagram	0010 %

Firewall Syslogs Setting	
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 different in view of technical concepts and product realization.

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

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

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

3.4.2. Template Management

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



Fig.3-33 Select Whitelist Template Management

Firewa	II > Whitelist Management > Template Managemen	t					
Template	Management List) Add
Whitelist Ter	mplate Name:	Search					
No.	Whitelist Template Name	Version	Firewall group applying this template	Applied By	Edit Whitelist	Ope	ration
1	admin_123456	1			🕼 Edit 🗗 Export 💽 Import	🖪 View 🗹 N	odify 🎁 Dele
2	S7 sub-protocol full match whitelist template	1			Export	E,	View
3	S7 sub-protocol read-only whitelist template	1			Export	B ,	View
4	FINS read-only whitelist template	1			Export	B ,	View
5	FINS full match whitelist template	1			Export	B ,	View
6	Profinet IO read-only whitelist template	1			Export	E,	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	A whitelist template name that is easy to remember, for example "Whitelist				
Name	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	All firewall groups that are using this whitelist template				
this template					
Applied By	All independent industrial firewalls that are using the whitelist template				



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

Pirewall > White	elist Management > Template Management					
Template Managem	nent List					Add
Whitelist Template Na	me: Search					
No.	Whitelist Template Name	Version	Firewall group applying this temptate	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	🕼 Edt 🗗 Export 🕞 Import	🛐 View 🕑 Modify 💼 Delete
4	S7 sub-protocol full match whitelist template	1			B Expor	B), View
5	S7 sub-protocol read-only whitelist template	310			B Expor	E, View

Fig.3-35 Whitelist Template Add Button

\Im Firewall > Whitelist Management > Template Management	
Add whitelist template	
Whitelist Template Name:	•
Remarks:	
	Save Back

Fig.3-36 Whitelist Template Add Page

Tab.10 Instruction to Whitelist Template Add Information

Column Nan	nes	Instructions
Whitelist	Template	Define a meaningful whitelist template name that is easy to understand and
Name		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:	
	Back

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):

emplate	Management List						Add
itelist Te	mplate Name:		Search				
No.	Whitelist Template Name	Version	Firewall group applying this template	Firewall applying this template	Edit Whitelist	Ope	ration
1	admin_rxd20191022112946	1			😰 Edit 📑 Export 💽 Import	🖪 View 🗹 🛚	lodify
2	S7 sub-protocol full match white list template	1			Export	E.	View
3	S7 sub-protocol read-only white list template	1			Export	E.	View
4	FINS read-only white list template	1			Export	B ,	View
	FINS full match white list template				Export	6	View



Firewall > Whitelist Management > Template Management	
Whitelist Template Information	
Whitelist Template Name:	admin_rxd20191022112946 *
Version:	1
Creation time :	2019-10-22 11:29:50
Remarks:	
	Save Edit Whitelist Back

Fig.3-39 Whitelist Template Modification Page

Tab. 11 Instruction to Whitelist Template Modification Information

	Column Names	Instructions
--	--------------	--------------



Whitelist Template	Define a meaningful whitelist template name that is easy to understand and					
Name	remember	emember				
Remarks	Optional, addi	ptional, additional explanatory information				
	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				
Operation Edit		Click and go to the Whitelist Edit page for each specific				
	Whitelist	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	民 View 🗹 Modify 前 Delete
Export	K 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):



Firewa	all > Whitelist Management > Template Management						
Template	Management List						Add
Whitelist Te	mplate Name:	Search					
No.	Whitelist Template Name	Version	Firewall group applying this template	Applied By	Edit Whitelist	Ope	ration
1	admin_123456	1			🕼 Edit 🗗 Export 💽 Import	🖪 View 🗹 N	lodify 💼 Delete
2	S7 sub-protocol full match whitelist template	1			Export	B .	View
3	S7 sub-protocol read-only whitelist template	1			Export	B .	View
4	FINS read-only whitelist template	1			Export	B .	View
5	FINS full match whitelist template	1			Export	B .	View
6	Profinet IO read-only whitelist template	1			Export	B .	View
7	Profinet IO full match whitelist template	1			Export	5	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 in the near future.

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

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

Edit Whitelist	Operation
📝 Edit 💽 Export 💽 Import	民 View 🗹 Modify 前 Delete
Export	K View
T' 2 42 T	

Fig.3-42 Edit Button

	-INDUSTRIAL IT-
Firewall > Whitelist Management > Template Management	
Whitelist Template Information	
Whitelist Template Name:	admin_rxd20191022112946 *
Version:	1
Creation time:	2019-10-22 11:29:50
Remarks:	
	Save Edit Whitelist Back

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):

OPC	S7	MODBUS	CIP	MMS	IEC104 DNP3	PROFINET	FINS Mnet Sysn	net
ACS625_ENGINEE	R MACS625_MN	NET MACS625_S	NET					
otocol Wildcard Parame	ter 🚭 Syntax Check							
ompt: IP is "0.0.0.0" me	ans configure all 🕋 🕁)						⊕ Add
No.	Src. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Transport Protocol	Interface	Operation	Delete
nge Control 💮 🕁								⊕ Add
No. Tag I	lame S	rc. 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	0.0" means configure all	(\mathbb{D})						⊕ Add
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

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	A method under a specific interface as defined in the OPC protocol
Name)	specification, taken from the drop-down box.

Tab.12 Instruction to OPC Whitelist Item Field

		- INDUSTRIALIT-
	Save	Save all modification information to the database and make
		it come into effect, and go back to the Whitelist Template
Operation		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):

	Ø	Firewall	>	Whitelist	Managem	nent >	Template	Management	
--	---	----------	---	-----------	---------	--------	----------	------------	--

	OPC		S7		MODBUS		CIP			MMS	IEC104	DNP3	PRC	FINET	INS		
Protoco	ol Wildca	rd Parameter	Syntax Che	ck													
Prompt	: IP is "0	.0.0.0" means co	nfigure all 🕥	(\downarrow)												Ad	d
	No.	Src	. IP	D	st. IP	Src. I	P Mask		Dst	IP Mask	Transport Protocol	Interface		Operati	on	D	elete
		0.0.0		0.0.0.0		0			0		TCP	IOPCAsynclO3	Ŧ	ReadMaxAge	Ŧ		Delete
		0.0.0.0		0.0.0.0		0			0		TCP	IOPCAsynclO3	Ŧ	ReadMaxAge	¥		Delete
		0.0.0		0.0.0.0		0			0		TCP	IOPCAsynclO3	Ŧ	ReadMaxAge	Ŧ		Delete
Range (Control (€ Ad	d
	No.	Tag Name	Src.	IP	Dst. IP		Src. IP Mask	Dst. IP N	lask	Interface	Operation	Item ID	Data Typ	pe Min. Value	Max. Value		Delete
			0.0.0.0		0.0.0.0		0	0		IOPCAsyncIO3 V	WriteVQ1 ¥		Boolean	×			Delet
			0.0.0.0		0.0.0.0		0	0		IOPCAsynclO3 V	WriteVQ1 ¥		Boolean	¥			Delet e

Fig.3-46 OPC Whitelist Information View Page

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

3.4.3.3. Modify an OPC whitelist item.

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

3.4.3.4. Modify an OPC range.

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

3.4.3.5. Delete an OPC whitelist item.

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



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

OP MACS625		S7 MACS625_M	MODBI	US S625_SNET	CIP	MMS	IEC10	I4 DI	NP3 PRC	DFINET	FINS	et Sysnet		
	– Icard Parameter													
rompt IP is "0.0.0" means configure all 💮 🕒									⊕ /	Ndd				
	lo.	Src. IP	Dst	IP	Src. IP Mask	Dst.	IP Mask	Transport Protocol	Interfac	ce .	Operatio	n		Delete
	0.0.0.0		0.0.0.0	0		0		TCP	IOPCAsynclO3	Ŧ	ReadMaxAge			Delete
	0.0.0.0		0.0.0.0	0		0		TCP	IOPCAsynclO3	٣	ReadMaxAge	٣	1	Delete
	0.0.0.0		0.0.0.0	0		0		TCP	IOPCAsynclO3	٣	ReadMaxAge			Delete
ange Contro No.	Tag Nam	e S	irc. IP	Dst. IP	Src. IP Mask	Dst. IP Mask	Interface	Operation	Item ID	Data Type	Min. Value	Max. Value	⊕ A	Delete
		0.0.0		0.0.0	0	0	IOPCAsynclO3	WriteVQ1 ¥		Boolean V				Delet e
		0.0.0.0		0.0.0	0	0	IOPCAsynclO3	WriteVQ1 ¥		Boolean V				Delet e
						_								

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:

```
    Firewall > Whitelist Management > Template Management
    OPC S7 MODBUS CIP MMS IEC104 DNP3 PROFINET FINS Mnet Sysnet
    MACS625_SNET MACS625_SNET
    Protect Wide Parameter Service Concerning to the service concerning t
```

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):

rte Order										
Modbus Int16 Endian	Modbus Int	32 Endian	Modb	us Float Endian			Modbu	is Double Endian		
FFH2 FFH1 V	FFH4 FFH3 FF	FH2 FFH1 V	FFH4 FF	FH3 FFH2 FFH1 V		FFH8 FFH7 FFH6 FFH5 FFH4 FFH3 FFH2 FFH1 V			Ŧ	
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	De

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.

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

Tab.13 Instruction to Modbus Click Field

AVCOMM Technologies Inc.



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):

Whitelist Template:	Modbus full match whi 🔻 *		
	Please select	*	
	admin_rxd20191022112946		
	S7 sub-protocol full match white list template		
irewall security Policy Template	S7 sub-protocol read-only white list template		
	FINS read-only white list template		
Security Policy Template Name:	FINS full match white list template		
	PROFINET IO read-only white list template		
	PROFINET IO full match white list template		
Terrer II station and a second and (* second such a second s	PROFINET DCP read-only white list template		
irewall static route configuration (* configure only in routing mode)	PROFINET DCP full match white list template		
	DNP3 full match white list template		
Firewall Interface Configuration:	DNP3 read-only white list template		
r ite india interfaces configuration i	IEC104 full match white list template		
Otatia Dautian Table Nama	IEC104 read-only white list template		
Static Routing Table Name:	MMS full match white list template		
	MMS read-only white list template		
	CIP full match white list template		
/lessage prompt (View log management module for more alarm logs) 🗆 Enable			
	Modbus full match white list template		
Time Type Firewall IP Firewall Name	Ala Modbus read-only white list template	•	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.

Firewal	I > Whitelist Management > Template Management								
Template	Management List) Add		
Whitelst Templale Name: Branch									
No.	Whitelist Template Name	Version	Firewall group applying this template	Applied By	Edit Whitelist	Ope	ration		
1	120191116154958	1			🕼 Edit 🗗 Export 🛃 Import	民 View 🕑 Mi	odify 💼 Delete		
2	sysnet	3			🕅 Edit 🕒 Export 💽 Import	民 View 🕑 Mi	odify 💼 Delete		
3	WWW	4		Firewall160824069	I₽ Edit G Export G Import	🖪 View 🕑 Mi	odify 💼 Delete		
4	S7 sub-protocol full match whitelist template	1			E Expor	B,	View		
5	S7 sub-protocol read-only whitelist template	1			B t t	B,	View		
6	FINS read-only whitelist template	1			B t t	R,	View		
7	FINS full match whitelist template	1			⊕ Expor	R,	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 another network segment s (not the network segment where the interface is located). It is necessary to configure the interface IP and the static route table. The network segments where an interface is located can forward data mutually.

3.5.2.Static Route

3.5.2.1. Page navigation

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







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:	Search

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

Firewall > Routing Management > Static Routing		
Static Routing Management List		● Add
Static Routing Table Name: Search	•	
Fig.3-54 Ad	d the Static Route Management Template	
Firewall > Routing Management > Static Routing		
Increase static routing		
Static Routing Name:	*	
Remarks:		
	Save Back	

Fig.3-55 Add the Static Route

Tab.14 Instruction to Adding a Static Route Template

Column Names	Instructio	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 re	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

				8	
Firewall > Ro	uting Management > Static Routing				
Static Routing Ma	anagement List				● Add
Static Routing Table	e Name:	Search			
No.	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation
1	test			📝 Edit 🔁 Export 💽 Import	民 View 🗹 Modify 🎁 Delete

Fig.3-56 Edit a Static Route Table Template

nomali - reducing Maria	gement > Static Routing					
tic Routing Rule Informati	ion					
mpt: After the static routir	ng template is applied by the devi	ce, it is not allowed to add o	or delete rules or modify outgo	ing interface		
						⊕ Add
Number	Dst. Addr.	IP Mask	Outgoing	interface	Next Addr.	Operation
	0.0.0.0	32 (1-32)	eth0	¥	0.0.0.0	🛅 Delete
ault routing enable						
Number	Dst. Addr.		IP Mask	Outgoing inter	face	Next Addr.
	0.0.0.0	_	0	eth0 ¥		0.0.0.0

Fig.3-57 Static Route Rule Information

Tab.15 Instruction to Filling in Static Route Rule Items

Column Names	Instructions	Instructions		
Dst. Addr.	Legitimate IP addre	ess		
IP Mask	Numbers 1-32			
Outgoing interface	Outgoing interface	content		
Next Addr.	Legitimate IP addre	Legitimate IP address		
Operation	Add	Add the static route rule information		
	Default routing	Allow to edit default route enable		
	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.	egitimate IP address	
IP Mask	Numbers 1-32	
Outgoing interface	Outgoing interface content	

	AVCOMM
	— INDUSTRIALIT —
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	Static Routing Management List							
Static R	Set	arch						
No	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation			
1	test			🕼 Edit 🕞 Export 💽 Import	民 View 🗹 Modify 📋 Delete			
2	www			📝 Edit 🔁 Export 💽 Import	民 View 🗹 Modify 📋 Delete			
3	test1			📝 Edit 🔁 Export 💽 import	民 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)	$^{\vee}$

Fig.3-58 Excel Generated by Static Route Table

3.5.2.6. Import a static route management list.

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

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

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



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



atic Routing Tal	ble Name:	earch			
No.	Static Routing Table Name	Firewall group applying this template	Applied By	Edit Static Routing Table	Operation
1	test			📝 Edit 🗗 Export 💽 Import	民 View 🗹 Modify 🌐 Delet
2	www			📝 Edit 🔁 Export 💽 Import	民 View 🗹 Modify 🎁 Dele
3	test1			😰 Edit 🔁 Export 💽 Import	民 View 🗹 Modify 🃋 Dele
Total 1 Page(s	s) / 3 Record(s),Current Page 1				First Prev Next Last

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:	
	Back

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	民 View 🗹 Modify 🏛 Delete
		Fig.3-62 Mo	dify the Static Rou	te Table	
Firew	all > Routing Management >	Static Routing			
Increase	e static routing				
	Static Routing	Name:	test	*	
	Ver	sion ID:	3		
	,	Version:	1		
	Creati	on time:	2019-10-30 15:17	7:18	
	R	emarks:			//
			Save	Edit Rule	Back

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	

	— INDUSTRIALIT—
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	民 View 🗹 Modify 🎁 Delete
2	www			🗭 Edit 📑 Export 💽 Import	民 View 🗹 Modify 🎁 Delete
3	test1			🗭 Edit 📑 Export 💽 Import	民 View 🗹 Modify 🎁 Delete
Total 1 F	Page(s) / 3 Record(s).Current Page 1			F	irst Prev Next Last



Fig.3-64 Static Route Table Template

Fig.3-65 Confirmation Box

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

3.6. ACL Management

3.6.1.Introduction to Functions

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

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



3.6.2. Security Policy Template Management

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



Fig.3-66 Selecting Security Policy Management

	Firewall > ACL Manager	ment > Security Policy				
	Security Policy Template Lis	t				⊕ Add
	Security Policy Template Na	me: Search				
	No.	Security Policy Template Name	Version	Applied By	Rules Operation	Operation
- L	1	test	1		🕞 Edit 📑 Export 💽 Import	🛱 View 🗹 Modify 🌐 Delete
	Tatal 5 Dagata) (5 Dagardia) Cu	want Dana 4			,	Seal Draw March Land

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	A security	policy template name that is easy to remember, for example
Name	"6#DCS In	bound Security Policy Template"
Version	The versio	n of security policy template, the version and the template ID
	uniquely d	etermine a set of security policy rules. The version number will
	automatica	lly +1 after each time the security policy is edited and saved
Applied By	All indepe	endent industrial firewalls that are using this security policy
	template	
	Edit	Click to enter the specific security policy rule item edit page
Rules Operation	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
	View	View more detailed information on security policy templates
Onemation	Modify	Modify and set the information on security policy templates
Operation	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:	
	Save Back

Fig.3-68 Security Policy Template Add Page

Tab.19 Instruction to Security Policy Template Add Information

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

AVCOMM Technologies Inc.

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



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:	
	Back

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:	
	Save Edit Rule Back

Fig.3-70 Security Policy Template Modification Page

Tab.20 Instruction to Security Policy Template Modification Information

Column Names Instructions



Security Policy	Modify the name of t	he security policy template
Template Name		
Remarks	Optional, additional e	explanatory information
	Save	Save all modification information to the database and
		make it come into effect, and go back to the [Security
		Policy Management] page
Operation	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 Search
--

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):



Security Policy Template List					⊕ Add			
Security Policy Template Name:	Search							
No.	Security Policy Template Name	Version	Applied By	Rules Operation	Operation			
1	test	1		🕞 Edit 🗗 Export 💽 Import	民 View 🗹 Modify 💼 Delete			
Firewall > ACL M	lanagement > ACL Management							
Security Policy Temp	plate Information							
Secur	ity Policy Template Name:		test	*				
	Version ID:		3					
	Version:		1					
	Creation time:		2019-10-30 15:25:3	30				
	Remarks:							
			Save	Edit Rule	Back			

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	e information										_	
⑦ ④ Tip: IP 0.0.0	0 means full match	n, MAC 00:00:00	:00:00:00 means	s full match								● Add
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

💎 Fire	ewall >	ACL	Manage	ment > ACL M	anagement									
Policy	templa	te rule	e informa	tion										
1	Tip: IP	0.0.0.	0 means	full match, MA	C 00:00:00:00:00) means full ma	itch						⊙	Add
	Sr Zo		Dst. Zone	Src. MA	C Dst. MAC	Src. IP	Dst. IP	Src. IP Mask	Dst IP Mas	Start Time	End Time	Action	Service	Operation
	any	٣	any	v 00:00:00:00:0	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow	ALL ¥	Delete
	any	¥	any	Ø0:00:00:00:00	00:00:00:00:00:00	0.0.0	0.0.0.0	0	0			Allow	ALL ¥	Delete
	any	۳	any	r 00:00:00:00.0	00.00.00.00.00.00	0.0.0	0.0.0.0	0	0			Allow	ALL ¥	Delete
	any	Ŧ	any	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

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

AVCOMM Technologies Inc.



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

3.6.4.2. View a security policy rule item.

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

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 V	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 V	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	0.0.0.0	0	0			Allow		Delete
any 🔻	any V	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, an execution action and service of a specific security policy rule, click <Save> after the modification.

3.6.4.4. Delete a security policy rule.

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

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 V	any V	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 V	any V	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 V	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 management platform, users can also define their own services provided by other servers in the network.

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





Fig.3-77 Selecting a custom service.

3.6.5.1. Add a User-Defined service.

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

Firewall:	@ Firewall > ACL Management > User-Defined Service								
Service List					⊕ Add				
Service Name	: Dst. Port Start: Dst. Port End:	Search (Enter tw	o ports for a range search and one port for an e	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	RView				
5	WSSP	TCP	1-65535	5346	民View				
6	WTCP	TCP	1-65535	5355	民View				
7	WTSP	TCP	1-65535	5345	E 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:	*
	Save Back



Column Names	Instruction	15				
Service Name	The custom	application name that cannot conflict with an existing one				
Protocol	Drop dowr	n to select the transport layer protocol on which the service				
	depends	depends				
Src. Port Start	The source	The source start port used by the service, from 1 to 65535, enter 1 if not				
	available	available				
Src. Port End	The Source	The Source end port used by the service, from 1 to 65535, enter 65535 if not				
	available	available				
Dst. Port Start	The destina	tion start port used by the service, from 1 to 65535				
Dst. Port End	The destina	tion end port used by the service, from 1 to 65535, same to that				
	of the desti	nation start port if there is only one port				
	Save	Save all modification information to the database and make				
		it come into effect, and go back to the custom service list				
Operation		display page				
	Back Ignore all modifications and go back to the custon					
		list display page				

Tab.22 Instruction to custom service Add Fields



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):

Pirewall >	@ Firewall > ACL Management > User-Defined Service								
Service List					⊕ Add				
Service Name:	Service Name: Dst. Port Start: Dst. Port End: (Enter two ports for a range search and one port for an ewad search)								
No.	Service Name	Protocol	Src. Port	Dst. Port	Operation				
1	Yokogawa Stardom	TCP	1-65535	20001-20015	Modify Del	ete			
2	WS-Discovery	UDP	1-65535	3702	Modify Del	ete			
3	WISP	TCP	1-65535	8440-8441	Modify Del	ete			
4	WSCP	TCP	1-65535	5356	E View				
5	WSSP	TCP	1-65535	5346	Kiew				
6	WTCP	TCP	1-65535	5355	E View				
7	WTSP	TCP	1-65535	5345	E View				
8	Windows Server Update Service(WSUS)	TCP	1-65535	8530	Kliew				
9	Wago CoDeSys-UDP	UDP	1-65535	2455	Kview				

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 *
	Save Back

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 💼 Davies								
Fig.3-82 Custom service Delete Button								

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



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):





Firewall > ACL Man	@ 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.3-84 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 white	list 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

E	dit	1	×
	User-Defined Whitelist App		
	Application Name:	*	
	Application protocol Name:	S7 •	
	Transport Protocol:	TCP V	
	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	Drop down to select the industrial protocol with the application layer to be customized					
Name						
Transport Protocol	Drop down to	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					
	Save	Save all modification information to the database and make it come into				
Onemation		effect, and go back to the custom whitelist application list display page				
Operation	Back	Back Ignore all modifications and go back to the custom whitelist application				
		list display page				

AVCOMM Technologies Inc.

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



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):

Pirewall >	@ Firewall > ACL Management > User-Defined Whitelist App								
User-Defined	User-Defined Whitelist Application List								
Application Nam	Application Name: Application Protocol: -A8- Dat. IP: Dat. Port: Search								
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 V		
Transport Protocol:	TCP V		
Dst. IP:	192.168.11.10	*	
Dst. Port:	19200	*	
	Save	Back	

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):
Pirewall > AC	CL Management > User-Defined Whitelist Ap	p				
User-Defined W	Initelist Application List					Add
Application Name:	Application Protoc	ol: _All Dst. IP:	Dst. Port:	Search		
No.	Application Name	Application protocol	Transport Protocol	Dst. IP	Dst. Port	Operation
1	S7_001	87	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 management platform adopts interface division to realize Security Domain management.

3.7.2.Add a Security Domain

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

Pirewall > Security Domain > Security Domain	
Security Domain List	● Add
Security Domain Name: Search	

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						
curity Domaii	n List				li Add	
Security Domain Name: Search						
No.	Security Domain ID	Security Domain Name	Priority	Interfaces	Operation	
1	4	Untrust	5		Modify 💼 Delete	
2	3	DMZ	50		🔀 Modify 💼 Delete	
2 3	3	DMZ Trust	50 85		 Modify <a>Delete Modify <a>Delete 	

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 assign						
	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 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.

	Pirewall > Security Domain > Security Domain						
	Security Domain Basic Information						
	Security Domain ID:	4					
	Security Domain Name:	Untrust *					
	Interfaces:	[Please select]					
•		Save Back					

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):

P Firewall > Security Domain > Firewall List					
Firewall List					
Firewall Name: Search					
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 Pag	ie(s) / 2 Record(s),Current Page 1			First Prev Next Last	

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 Na	ime:		Search	

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.

Dote:

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

@ Fire	@ Firewail> Logs Management > Whitelist Alarm Logs																	
Whiteli	st Alarm Logs	List															Show Process	ied Logs 🛛
	Fireu Dst. M Sea	AC:	elect	T	Firewall Nan Block		elect *		Src. II Start Tim		20	Dst. IP:	2019-11-19 23:5	9.59	5 Application Layer	Protocol: -F	flease select	¥
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	192.168.15.3 0		22938		192.168.15.6 0		502		TCP	MODBUS	Violate MODBUS whitelist rule alarm, function code:02 Read Discrete Inputs, start address	No	Warning	Unprocessed	Firewall1608 24069	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

AVCOMM Technologies Inc.

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



Dst. IP	The destination	The destination IP address requesting data, in dotted decimal format					
Dst. device	Displays "-" v	Displays "-" when there is no device name, otherwise displays the name of the					
	destination dev	destination device					
Dst. Port	The port used l	The port used by the target machine of the request					
Transport Protocol	The protocol ty	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 rele	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 alarm	s 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):

0	arm Src. IP	Src.	Src. Port	Src. MAC	Dst. IP	Dst. Device	Dst. Port	Dst. MAC	Transport	Application Layer	Alarm	Blocked	Alarm Level	Processing Status	Firewall Name	Firewall	Operatio
	Start Time	: 2019-1	0-30 00:00:	00		Er	nd Time:	2019-10-3	10 23 59 59	Application	Layer Protocol:	Please	select	٣		Sear	ich
	Src. MAC					Ds	st. MAC:				Blocked:	Please	select	٣			
	Firewall	: Please	select	٣			Src. IP:				Dst. IP:						
rinonarr	Alarm Logs Lis														Show	Processed	Logs

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 V
Processing Opinions:	
	Save Add to term Back

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

Fig.3-100 Retrieving a Whitelist Alarm Log

3.8.3.Firewall Alarm Logs

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

3.8.3.1. Log list

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





Fig.3-101 Firewall Alarm Log Menu

Firev	vall > Logs Mana	gement > Firew	all Alarm Logs											
Firewall	Alarm Logs List												Show Pro	cessed Logs 🗆
Applicatio	Flewall: Please select Flewall Name: Src. IP: Dot. IP: Dat. Port: Aams Information: Please select Start Time: 2019-07-29 00:00:00 End Time: 2019-11-19 23:59:59													
NO.	Alarm Time	Src. IP	Src. Device	Dst. IP	Dst. Device	Dst. Port	Transport Protocol	Application Layer Protocol	Alarm	Alarm Level	Processing Status	Firewall Name	Firewall IP	Operation
1	2019-11-17 10:26:55	192.168.4.78	-	192.168.4.25 5	-	138	UDP	NetBIOS-UDP	Request allowed to pass	Information	Unprocessed	Firewall160824069	192.168.4.97	Process
2	2019-11-17 10:26:48	192.168.4.10 6		192.168.4.25 5		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
	2010 11 17			220.255.255					Desugat allowed to					

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

AVCOMM Technologies Inc.

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



Dst. port	The port used	by the target machine of the request				
Transport Protocol	The protocol ty	ype of transport layer used by the message				
Application Layer	Specific application types					
Protocol						
Alarm Information	Information on	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	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):

Firev	₫ Firevall > Logs Management > Firevall Alarm Logs														
Firewall	irevall Alarm Logs List Show Processed Logs 🧃														
Applicatio	Fixewall: Piezes select Fixewall Name: Src. IP: Dot. IP: Dit. Port: Aam Information: Piezes select Start Time: 2019-07-29 00 00.00 End Time: 2019-11-19 23 59:59 opplication Layer Protocol: Search Search Search Search 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	Oper	ration
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	P	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	P	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	۶	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):



	— INDUSTRIALII —
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:	
	Save Add to Template Back

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 Alarm Logs Li	ist							St
Firew. Dst. Po	all: Please s	select	Firewall Name : Alarm Information :		Src. IP: Start Time :	Dst. IP: End Time:	2019-11-19 23:59:59	
Application Layer Protoc	:ol:		Search	n				

Fig.3-105 Retrieving a Firewall Alarm Log

3.8.4. Firewall Run Log

III > Loos Management > Firewall Alarm Loos

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

rewall Ru	i 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	Fire
1	2019-10-30 17:06:56	Online	Firev
2	2019-10-30 15:22:21	Online	R
3	2019-10-30 15:22:21	Online	Firev
4	2019-10-30 15:22:21	Offine	R
5	2019-10-30 15:22:21	Engine configuration packet updating successfully	R
6	2019-10-30 15:22:20	Engine configuration packet updating successfully	R
7	2019-10-30 15:22:20	Offine	Firew
8	2019-10-30 15:22:19	Engine configuration packet updating successfully	Firew
9	2019-10-30 15:22:19	Engine configuration packet updating successfully	Firev

Fig.3-107 Firewall Run Log List Page

View the information on all industrial firewalls run logs, with the meanings given below: Tab.28 Instruction to Firewall Run Log Display

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



Operating Time

Log generation time

3.8.4.2. Retrieve a log.

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

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							

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 > L	Logs Management > Address Spoof	ing Logs						
Address Spool	ofing Logs List						Show	Processed Logs
	Please select Firewall I search	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	¥
No.	Alarm Time	Alarm Information	Alarm Level	Blocked	Processing Status	Firewall Name	Firewall IP	Operation
Total 0 Page	e(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 alar	ms 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):

Address Spoofing Logs Lds Freewall Names: Start Times: 2019-11-19 02 00:00 End Times: 2019-11-19 22 39:59 Alarm Information: Please enter IP or MAC: Blocked: -Please select	Firewall > Logs Management > Address	s Spoofing Logs						
Bearch No. Alarm Information Alarm Level Blocked Processing Status Firewall Name Firewall IP Operation	Address Spoofing Logs List						Show P	rocessed Logs 🖬
		Firewall Name: Start Tim	b: 2019-11-19 00:00:00	End Time: 2019-11-19 23:59:5	9 Alarm Information:	Please enter IP or MAC	Blocked:Please select	Ÿ
Total 0 Page(s) / 0 Record(s),Current Page 1 First Prev Next Last	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 logo.

Refer to other log processing methods.

3.8.7.Log Statistics

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

3.8.7.1. Display

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





Fig.3-112 Log Statistics Menu

Firewall:	Please sel	ect		Start Time:	2019-10-23	End Time:	2019-10-30	Search
1.0.01	All Firewall	Logs Statistics						
100k - 75k -			94119					
0 75k -			_					
50k —								
251								
25K -	17776	12569						
0k –								
0k —	Whitelist Alarm	Firewall Alarm	Address Spoofing					



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 V	Start Time:	2019-10-23	End Time:	2019-10-30	Search	
		Fig.3	-114 Retrieving	Log Statistic	cal Data		
			AVCOMM Tech				_
333	West Loop North	, Suite 460	Houston, TX 770	24, USA ir	nfo@avcomm.us	www.avcomm.us	



4. Industrial Endpoint Guard (IEG)

4.1. Introduction to Products

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

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

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

4.2. System Permissions

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

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

4.3. Real-time Alarm

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

@ IEG > Real-	-time Alarm > Real-time Alar	m						
TOP10 program	n alarm on the day		TOP10 program alarm client on the day		Alarm Quantity Trend	Program Device	Number of Alarms on the day	(
125			2k -		1,500	1202	Туре	Times
100 95	92 92 92 92 1	92 92 91 91 91	1251 1k		1.000	211	Program Device	1282
75				9			Client Overview	
50			04	. March	500	195	Deployment	9
25			ACTION AND A DESCRIPTION OF A DESCRIPTIO	and a	0 11-12 11-13 11-14 11-15	11-16 11-17 11-18	Online Online Rate	3
Latest alarm, up	p to 25 records displayed						Prog	ram Alarm Device Alarm
No.	Time	Client Name	Client IP	System User	Program Path	Log Type	Resul	t
1	2019-11-18 10:19:55	CHENNIAN-WIN7	192.168.3.51	SYSTEM	c:program files (x86)\ieglworkstationdefender\w/chostreinfor cement.dll	Non-whitelist Program Alarm	Non-control mode execution: pas- iled	sed, whitelist verification: fa
2	2019-11-18 10:19:54	CHENNIAN-WIN7	192.168.3.51	SYSTEM	c:\program files (x86)lieg\workstationdefender\wlcdata.dll	Non-whitelist Program Alarm	Non-control mode execution: pas: iled	sed, whitelist verification: fa
3	2019-11-18 10:19:54	CHENNIAN-WIN7	192 168 3 51	SYSTEM	c torooram files /x861lied/workstationdefender/w/cudisk dll	Non-whitelist Program Alarm	Non-control mode execution: pas:	sed, whitelist verification: fa

Fig.4-1 Real-time Alarm Page

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



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

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

4.4. Log Management

4.4.1.Log Classification

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

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

AVCOMM Technologies Inc.



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

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

Real-time Alarm >	Ø IEG > L	.og Management > Program	Alarm									
Log Management		Log Type:	All			Client Name:			Cli	ent IP:		
Program Alarm Device Alarm		Query Period:	1day 🔻			Start Time :			End	Time :		
A Firewall Log		Include Path:				Se	arch Export					
应 OS Log	No.	Time	Client Name	Client IP	System User	Program Path	Parent Process	Company Name	Product Name	Version	Log Type	Result
🖩 Run Log						c lusers administrator appdat allocalikings off wps office 1	c:\users\administrator\appdata\loca	Zhuhai Kinosoft Office			Non-whitelist Program	Non-control mode execution:
📕 Linux Login an	1	2019-11-18 10:26:56	CHENNIAN-WIN7	192.168.3.51	Administrator	0.1.0.5559\wtoolex\updatese If.exe	likingsoft/wps office\10.1.0.5559\off ice6\wps.exe	Software Co.,Ltd	WPS Office	10,1,0,5559	Alarm	passed, whitelist verification: failed
Access Control Alarm						c/users/administrator/appdat	c:\users\administrator\appdata\loca					Non-control mode execution:
Unauthorized Externa	2	2019-11-18 10:26:55	CHENNIAN-WIN7	192.168.3.51	Administrator	allocalikingsoftwps office/1 0.1.0.5559/office6/auth.dll	Rkingsoft/wps office/10.1.0.5559/wt oolex/wpsnotify.exe	Zhuhai Kingsoft Office Software Co.,Ltd	WPS Office	10,1,0,5559	Non-whitelist Program Alarm	passed, whitelist verification: failed
	3	2019-11-18 10:26:55	CHENNIAN-WIN7	192.168.3.51	Administrator	c:\usersladministrator\appdat allocallkingsoftwps office\1 0.1.0.5559\wtoolex\wpsnotif y.exe	c:\users\administrator\appdata\loca likingsoft\wps office\10.1.0.5559\off ice6\wps.exe	Zhuhai Kingsoft Office Software Co.,Ltd	WPS Office	10,1,0,5559	Non-whitelist Program Alarm	Non-control mode execution: passed, whitelist verification: failed



IEG > Log Management > Device	Alarm					
lient Name: Search Export	Client IP:	Туре :	Search •	Query Period: 1day	Start Time :	End Time :
No.	Time	Client Name	Client IP	System User	Туре	Content
Total 0 Page(s)/ 0 Record(s) Current F	Page 1 Page(s)					First Prev Next Last Goto

Fig.4-3 Device Alarm

Ø IEG > Log Management	> Firewall Log							
Client Name: Search Export	Clie	int IP:	Type: Sear	ch v	Query Period: 1day	• Start Time :		End Time :
No.	Time	Client Name	Client IP	Туре			Content	
Total 0 Page(s)/ 0 Record(s)	Current Page 1 Page(s)							First Prev Next Last Goto GO

Fig.4-4 Firewall Alarm Log

IEG > Log Mana	agement > OS Log							
Log Source				Log Type:	Please select *		Event Level:	Please select *
Event ID :				Client Name:			Client IP:	
Start Time	: 2019-11-1	8		End Time :	2019-11-18		Search Export	
No.	Time	Туре	Source	Event Level	Event ID	Client Name	Client IP	Description
Total 0 Page(s) / 0	0 Record(s),Current Page	Page(s)						First Prev Next Last

Fig.4-5 Operating System Log

IEG > Log Mana	gement > Run Log				
Client Name:	Client IP: Log Type: F	Vease select Start Time : 2019-11-18	End Time : 2019-11-18 Search Export		
No.	Time	Client Name	Client IP	Log Type	Content
1	2019-11-18 10:27:53	yicexp-9fa8f6b9	192.168.3.215	Online	Online
2	2019-11-18 10:13:33	yicexp-9fa8f6b9	192.168.3.215	Offline	Offline
3	2019-11-18 10:05:22	yicexp-9fa8f6b9	192.168.3.215	Online	Online

Fig.4-6 Run Log



Fig.4-7 Access Control Alarm

Client Name: Client IP: Login IP: Login User: Login Times: 1447 Start Time : End Time : Exact Exact Client IP OS Login IP User Name Teminal Login Times: 1447 Start Time : End Time : Start Time : <td< th=""><th>IEG > Log Management > Linux Log</th><th>gin and Logout Logs</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></td<>	IEG > Log Management > Linux Log	gin and Logout Logs							
		Client IP:		Login IP:	Log on User:	Log	pin Times: 1day • Start Time :	End Time :	
Total Draget(s)/ D Record(s) Current Page 1 Paget(s)	Client Name	Client IP	OS	Login IP	User Name	Terminal	Login Times *	Logout Time	Status
	Total 0 Page(s)/ 0 Record(s) Current	Page 1 Page(s)							First Prev Next Last

Fig.4-8 Linux Login and Logout Log

4.4.2.Log Query and Export

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

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

4.5. IEG Management

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

4.5.1.Client Monitoring

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

Client Group	Whole Network	 Client Name: 			Client IP:			Online Status:	Please selec	t •	OS:	Please select	•	Self-protection:	Please select •
larm Prompt	Please select	Program Co	ntrol: Please	e select	Common USI	B: Please sel	ed 🔹	Safe USB:	Please select	*	Two-factor:	Please select	*	Search	
No.	Client Name	Computer Name	Client IP	Online Status	os	CPU Usage	Memory Usage	Self-protection	Alarm Prompt	Program Contro	USB En	ible Common USB	Safe USB	Two-factor	Operation
1	yicexp-9fa8f6b9	yicexp-9fa8f6b9	192.168.3.215	Online	Windows XP	4%	23%	Disable	Enable	Close		Read&Write	Read&Write	Enable	More View Boot System Loading File Set the Alias Refre

Fig.4-9 Client Monitoring



4.5.2. Group Management

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

₩Whole Network	Add a group Mo	lify Delete			
	Name:		Director:	Telephone:	
	Description:				A

Fig.4-10 Group Management

4.5.3.Client Group

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

♥ IEG > IEG Management > Client Group					
Whole Network Whole Network	Add a Client	Aass Delete			
	0	No.	Client Name	Client IP	Operation
		1	Admin-PC2	192.168.3.216	mDeleto
	0	2	WIN-7-YICE	192.168.3.38	ff Delete
		3	CHENNIAN-WIN7	192.168.3.51	1 Delete
		4	ES130	192.168.3.21	m Delete
		5	WIN7-32-xwk	192.168.3.32	mDelete



4.5.4. Client Uninstallation

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

♥ IEG > IEG Management >	Client Uninstall				
Client Group: Whole Netwo	rk • Client Name:	Client IP:	Search		
No.	Client Name	Client IP	OS	Online Status	Operation
1	yicexp-9fa8t6b9	192.168.3.215	Windows XP	Online	Uninstall Force to uninstall
2	WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Offline	Uninstall Force to uninstall

Fig.4-12 Client uninstallation



4.5.5.Client Upgrading

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

0	IEG > IEG Management > (client Upgrade					
	OS Type : Linux •	Upgrade Packet: Please	selec ¥ Issue				
	Client Group: Whole Netwo	ork • OS Type: Linux	Online Status: All Client Name	e: Client IP:	Search		
1		No.	Client Name	Client IP	OS	Online Status	Version

Fig.4-13 Client upgrading

4.6. Program Whitelist

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

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

4.6.1.Scan Exception Template

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

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

♥ IEG > Program V	Whitelist > Scan Exception Template			
Add	Te	mplate Name:	Search	
No.	Template Name	OS Type	Description	Operation
Total 0 Page(s)/ 0	Record(s) Current Page 1 Page(s)			First Prev Next Last Goto 🥅 GO

Fig.4-14 Scan Exception Template

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

	- INDUSTRIAL IT-	
Program Whitelist > Scan Exception	un Template	
de	windowstam??): windowstawstam??) cannot be set as soan avcantion nath	
	windowslaystem32; c'windowslayswow64; c'winntsystem32; cannot be set as scan exception path Exception Path Not Scanned	Operation
frectory c. c.\windows c.\winnti, c		
frectory c. c.\windows c.\winnti, c		Operation

Fig.4-15 Template Configuration Interface

4.6.2. Process Audit Template

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

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

IEG > Program	Whitelist > Process Audit Template			
Add	Temp	Nate Name:	OS Type : Please select *	Search
No.	Template Name	OS Type	Description	Operation
Total 0 Page(s)/	0 Record(s) Current Page 1 Page(s)			First Prev Next Last Goto

Fig.4-16 Process Audit Template

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

♥ IEG > Program Whitelist > Pro	ess Audit Template	
Note: The process can only configu	e the file path; the configuration folder path or directory will not take effect!	⊙ Add
No.	Process	0
	FILESS	Operation
	Frocess Reference Romat: c:VILClient.exe	Delet e



4.6.3.System Integrity Check

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

IEG > Program Whitelist	t > System Integrity Check					
System integrity check (requ	ires reboot system to take effec	t): Enable *	Issue			
Client Group: Whole Netw	OS Type: Please	selec Online Status: All Client Nar	Client IP:	Search		î
	No.	Client Name	Client IP	OS	Online Status	System Integrity Check
	1	yicexp-9fa8f6b9	192.168.3.215	Windows XP	Online	Disable
	2	WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Offline	Disable

Fig.4-18 System Integrity Check Interface

4.6.4. Whitelist Management

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



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

	yicexp-9fa8f6b9	
No.	Path	
1	C:\Windows\System32\format.com	
2	C:\Windows\System32\wbem\WMIC.exe	

Fig.4-19 No Scan Path Interface

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

IEG Management >	♥ IEG > Pro	EG > Program Whitelist > Whitelist Management								
🄹 Program Whitelist 💦 🗸 🗸										
Scan Exception Template	Client Gro	Client Group: Whale Network Client Name: Client IP: Search								
Process Audit Template	Voces Audit Template Please select scan exception template + Scan A Stop At									
System Integrity Check	-									
😰 Whitelist Management		Client Name	Client IP	OS	Online Status	Scanning Mode	Update Time *	Whitelist Quantity	Operation	
相 Program Control		yicexp-9fa8f6b9	192.168.3.215	Windows XP	Online	update completed	2019-11-18 10:55:58	7606	Whitelist Scan Exception	

Fig.4-20 Whitelist Management Interface

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

/iew W	/hitelis1			
₿ IE	G > W	hitelist Management > Whitelist		
	Delete	Export Back		File Name Search put hashcode
	No.	File		Hash Value
	1	C:\DOCUMENTS AND SETTINGS\ALL USERS\APPLI \MICROSOFT\OFFICE\UICAPTIONS\1033\ENVELOP		FE7EF5C5370C12A7E9186812BF02EE22 DCC877BF
	2	C:\DOCUMENTS AND SETTINGS\ALL USERS\APPLI \MICROSOFT\OFFICE\UICAPTIONS\1033\GRINTL32	005C949699DC382EA030670257E169111 9E528F1	
	3	C:\DOCUMENTS AND SETTINGS\ALL USERS\APPLI MICROSOFT\OFFICE\UICAPTIONS\1033\GRINTL32		1F86B16311A7507368E854E599E83BF5C 7812A0F

Fig.4-21 Viewing the Whitelist Interface

4.6.5.Program Control

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

∂ IEG > Progr	am Whitelist >	Program Control				MM al it —	C.	
ogram Control:	Please selec	tesue						
Client Group:	Whole Netwo	Nonine Status: All	Client Name: Cl	ent IP:	Search			
	No.	Client Name	Client IP	os	Online Status	Scanning Mode	Whitelist Quantity	Program Control
	1	yicexp-9fa8f5b9	192.168.3.215	Windows XP	Online	update completed	7606	Close
0	2	WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Offine	Initialize		Close

Fig.4-22 Program Control Interface

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

4.6.6.Alarm Processing

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

	Whether	Client Name: Query Period: Iday • to Add to the Whitelist: No •		Clie Start	nt IP:		Include Path: End Time : Search Add to Whitelist Export
0	No.	Client Name	Client IP	Alarm Time	Program Path	Number of Alarms	Whether to Add to the Whitelist
0	1	CHENNIAN-WIN7	192.168.3.51	2019-11-18 10:26:56	c.lusersladministrator/appdata/local/kingsoft/wps office \10.1.0.5559/wtoolex/updateseft.exe	10	No
0	2	CHENNIAN-WIN7	192.168.3.51	2019-11-18 10:26:55	c:/users/administrator/appdata/local/kingsoft/wps office \10.1.0.5559/wtoolex/wpsnotify.exe	17	No
0	3	CHENNIAN-WIN7	192.168.3.51	2019-11-18 10:26:55	c:\users\administratoriappdata\local\kingsoft\wps office \10.1.0.5559\office6\auth.dll	21	No
3	4	CHENNIAN-WIN7	192.168.3.51	2019-11-18 10:26:55	c:lusers\administrator\appdata\local\kingsoft\wps office \10.1.0.5559\wtoolex\wpsupdate.exe	13	No
0	5	CHENNIAN-WIN7	192.168.3.51	2019-11-18 10:26:53	c:lusersladministrator/appdatallocalikingsoffiwps office \10.1.0.5559ioffice8igfiplugins\imageformats\qqif4.dll	1	No

Fig.4-23 Alarm Processing Interface

4.6.7. Process Audit

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

V IEG > Prog	@ IEG > Program Whitelist > Process Audit									
OS Type : Windows • Process Audit Switch : Disable • Process Audit Template : Please selec • towe										
Chert Group: Whole Networks OS Type: Please selec * Online Status: All * Client Name: Client IP: Status										
	No.	Client Name	Client IP	OS	Online Status	Program Control	Process Audit			
	1	yicexp-9fa8f6b9	192.168.3.215	Windows XP	Online	Disable	Disable			
	2	WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Offine	Disable	Disable			

Fig.4-24 Process Audit Interface

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



ocess Audit P	Policy Information	
	Client Name: shilili-rhel6.6-64	Client IP: 192.168.4.201
No.		Configuration Item
1	/process_audit/1.sh	
2	/process_audit/10.sh	
3	/process_audil/11.sh	
4	/process_audit/12.sh	
5	/process_audit/13.sh	
6	/process_audit/14.sh	
7	/process_audit/15.sh	
8	/process_audit/16.sh	
9	/process_audit/17.sh	
10	/process_audit/18.sh	
11	/process_audit/19.sh	
12	/process_audit/2.sh	
13	/process_audit/20.sh	
14	/process_audit/21.sh	
15	/process_audit/22.sh	
16	/process_audit/23.sh	
17	/process_audit/24.sh	
46	/process_audit/50.sh	
47	/process_audit/51.sh	
48	/process_audit/52.sh	
49	/process_audit/53.sh	
50	/process_audil/54.sh	
51	/process_audit/55.sh	
52	/process_audit/56.sh	
53	/process_audil/57.sh	
54	/process_audit/58.sh	
55	/process_audit/59.sh	
56	/process_audit/6.sh	
57	/process_audit/60.sh	
58	/process_audit/61.sh	
59	/process_audit/62.sh	
60	/process_audit/63.sh	
61	/process_audit/64.sh	
62	/process_audit/7.sh	
	/process_audit/8.sh	
63		

Fig.4-25 Process Audit Interface

4.7. Security Baseline

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

4.7.1.Safety Baseline Template

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



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

🖲 IEG >	IEG > Security Baseline > Security Baseline Template								
	Add	Template Name:	OS Type : Please select •	Search					
No.	Template Name	OS Type	Description	Operation					
1	close	Windows	close	🔀 Basic 💊 Rule 💁 Copy as 📋 Delete					
2	search	Windows		🐻 Basic 👒 Rule 🗳 Copy as 🏢 Delete					
3	expert configuration	Linux	System high reinforcement configuration, which is the default configuration of the system and cannot be modified	To View Basic Rule 🔹 View Configuration 🗳 Copy as					
4	important configuration	Linux	System moderately reinforcement configuration, which is the default configuration of the system and cannot be modified	$\fbox{\sc c}$ View Basic Rule $\sc c \sc \s$					
5	smart configuration	Linux	System common reinforcement configuration, which is the default configuration of the system and cannot be modified	🔽 View Basic Rule 🗳 View Configuration 🗳 Copy as					
6	expert configuration	Windows	System high reinforcement configuration, which is the default configuration of the system and cannot be modified	🔽 View Basic Rule 🛛 🖕 View Configuration 🖓 Copy as					

Fig.4-28 Security Baseline Default Template Interface

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

ule			
Select	No.	Baseline Name	Parameter Value
4	1	Open Auditing the Success or Failure of System Event	
4	2	Open Auditing the Success or Failure of [System] Logon Events	
ø	3	Open Auditing the Success or Failure of Object Access	
0	4	Open Auditing the Failure of Privilege Use	
a,	5	Open Auditing the Non-auditing of Process Tracking	
Ø	6	Open Auditing the Success or Failure of Policy Changing	
9	7	Open Auditing the Success or Failure of Account Management	
4	8	Open Auditing the Failure of Directory Service Access	
a	9	Open Auditing the Success or Failure of Account Logon Events	
0	10	Password must meet complexity requirement	
	11	Minimum number of characters for the password length	8
9	12	Enforce Password History	3
a a	13	Maximum number of days for the password	90
	14	Disable Guest Account	
4	15	Account Lockout Threshold Invalid Logon Attempts	1
7	16	Account Lockout Duration Minutes	15
- 	10	Reset Account Lockout Counter minutes	15
- 			15
- 	18	Clear virtual memory pagefile at shutdown	
- 	19	Don't display last signed-in at logon	
- 	20	Don't require Ctrl+Alt+Del at logon	
v 7	21	Do not allow anonymous enumeration of SAM accounts	
•	22	Do not allow anonymous enumeration of SAM accounts and shares	
v	23	Disable AutoPlay	
v	24	Disable Share by default	
v	25	The maximum system log capacity (MB), which will cover logs older than 30 days	100
v	26	The maximum size of the security log (MB), which will cover logs older than 30 days	100
v	27	The maximum size of the application log (MB), which will cover logs older than 30 days	100
v	28	Session maximum idle time (minutes) at which time the session will be suspended	15
a	29	Disable floppy disk replication and access to all drives and folders	
a	30	Forbid Recovery Console Autologon	
a	31	Forbid system shutdown before loaon	
a	32	Past logons saved in buffer	3
a	33	Disallow saving credentials or .netpassports for cyber identification	
\$	34	Forbid sending remote assistance invitation from local computer	
a	35	Close recovery and auto-restart	
v	36	Forbid Autologon at startup	
a	37	Forbid users changing IP	
V	38	Forbid users changing computer name (requires restarting system application)	
a	39	Enable User Account Control Setting (UAC requires restarting system application)	
a	40	Change remote desktop default service port	13389
\$	41	OS basic components enable DEP (requires restarting system application)	
7	42	OS and all processes enable DEP (requires restarting system application)	

Fig.4-29 Windows Expert Template Page

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



Security Baseline : Rule	roncy rempiate						
Select	No.		Baseline Name	Param	neter Valu		
7	1	Set the limit min	utes for the account login timeout (restart for linx 42)		15		
a	2	Minimum numb	er of characters for the password length		8		
a	3	The new passw	ord is at least 3 characters different from the old password				
a	4	The new passw	ord must contain at least 1 capital letter				
đ	5	The new passw	ord must contain at least 1 lowercase letter				
7	6	The new passw	ord must contain at least 1 numeric				
7	7	The new passw	ord must contain at least 1 special character				
4	8	pwdfailntimes			3		
ø	9	Maximum numb	er of days for the password		90		
4	10	The minimum p	assword usage period is 0 days				
9	11	/etc/passwd/ 1	le permissions 644				
4	12	/etc/shadow/	ile permissions 640				
a	13	UMASK Default	s to 022				
đ	14	Enable the limit	number of reserved history commands		200		
9	15	The system mu	st enable the audit service				
a		16	The system must create a log file				
a	17		Ensure that system log files can only be appended				
a	18		Ensure that the contents of the polled history log file cannot be modified				
a	19		The system must enable the audit service				
a		20	The system must create an audit log file				
a		21	Backup Firewall Policy				
a		22	BASH shell-breaking vulnerability detection				
a		23	OpenSSL Heart Bleeding Vulnerability Detection				
*		24	System firewall on state detection				
\$		25	Only the UID of the ROOT account is 0				
a		26	Detect default accounts that are not needed in the system				
a		27	Rename the ROOT Account Name				
V		28	Disable ROOT account remote login				
		29	Non-owner file is forbidden in the system command directory				
	30		The 777-permission file is forbidden in the system command directory				
a		31	Ordinary users can switch to ROOT account	Dask			
v	32	FTP service shutdow	m status detection				
4	55 Double i fit dionyn		rous login				
v							
a	35	The system support	the RDP protocol.				
V	36	Disable TELNET ren	note management mode				
V	37	Use encrypted remo	te management mode				
V	38	Web service shutdo	vn status detection				
v	39	Mail service shutdow	/n status detection				
a	40	Syncookie Function	On-state Detection				

Fig.4-30 Linux Expert Template Page

Template Copy (Fig. 4-31):

.

42 43



×
*
Windows
Not exceeding 256 characters
Back

Fig.4-31 Template Copy Interface

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

Host Security Guarding > Security	y Baseline	> Policy Template	
test: Rule			
	11	Minimum number of characters for the password length	8 Range (2-14)
a t	12	Mandatory number of history passwords	3 Range (2-24)
a t	13	Maximum number of days for the password	90 Range (2-999)
a t	14	Disable Guest Account	
a t	15	Invalid login times for the account locks the threshold	3 Range (2-999)
a t	16	Minutes for the account locked	15 Range (2-999)
a t	17	Reset account lock counter how many minutes later	15 Range (2-999)
a	18	Clear virtual memory page file when shutting down	
a t	19	Do not display the last user name when log in	
	20	No need to press Ctrl+Alt+Del when log in	
a t	21	Do not allow anonymous enumeration of SAM accounts	
a t	22	Do not allow anonymous enumeration of SAM accounts and shares	
	23	Close Auto-play	
	24	Close Default Sharing	

Fig.4-32 Copied Template Rule Edit Interface

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



SSH Remote Login Configuration X										
Note: The starting time starts at 0 seconds and the ending time ends at 59 seconds.										
StartIP	EndIP	StartTime	StopTime	User	Operation					
			Save							

Fig.4-33 Editing SSH Remote Logon Rules

4.7.2. Security Baseline Configuration

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

♥ EG > Security Baseline > Security Baseline Configuration								
OS Type : Windows	OS Type : Windows • Security Baseline Template : Plasse selec • Itoue							
Client Group: Whole Net	Client Oroup: Mhole Network- OS Type : Please selec * Online Status: All * Client Name: Client IP: Sourch							
•	No.	Client Name	Client IP	OS	Online Status	Baseline Level	Detail	
0	1	redhat7.4-hch	192.168.3.154	Linux	Online	Expert Level	View Strategy	
	2	WIN-IP2601UDS48	192.168.3.16	Windows 7	Online	Not Configured	View Strategy	
	3	yicexp-9fa8f6b9	192.168.3.215	Windows XP	Offline	Expert Level	View Strategy	
	4	WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Offline	Not Configured	View Strategy	

Fig.4-34 Policy Configuration Interface

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

@ IEG > Security Baseline > Detail				
Security Baseline Configuration Information	n			
Client Name	: yicexp-9fa8f6b9	Client IP: 192.168.3.215	Policy Configuration Time: 2019-11-18 11:42:47	
No.	Baseline Name		Status	
1	Open Auditing the Success or Failure of System Event		Matched	
2	Open Auditing the Success or Failure of [System] Logon Events		Matched	
3	Open Auditing the Success or Failure of Object Access		Matched	
4	Open Auditing the Failure of Privilege Use		Matched	
5	Open Auditing the Non-auditing of Process Tracking		Matched	
6	Open Auditing the Success or Failure of Policy Changing		Matched	
7	Open Auditing the Success or Failure of Account Management		Matched	
8	Open Auditing the Failure of Directory Service Access		Matched	
9	Open Auditing the Success or Failure of Account Logon Events		Matched	
10	Password must meet complexity requirement		Matched	
11	Minimum password length is 8 characters		Matched	
12	Enforce Password History 3		Matched	
13	Maximum Password Age: 90 days		Matched	
14	Disable Guest Account		Matched	
15	Account Lockout Threshold 3 Invalid Logon Attempts		Matched	
16	Account Lockout Duration 15 Minutes		Matched	

Fig.4-35 Windows Client Configuration View

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



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

Fig.4-36 Old Windows Client Configuration View

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

rihy Roseline Configuration Inform	nation	
rity Baseline Configuration Inform Client	Name: redhat7.4-hch Client IP: 192.168.3.154	Policy Configuration Time: 2019-11-18 11:56:39
No.	Baseline Name	Status
1	Set account login timeout limit to 15 minutes	Matched
2	Password length is at least 8 characters	Matched
3	The new password is at least 3 characters different from the old password	Matched
	The new password is at least 3 characters dimensit from the old password The new password must contain at least 1 capital letter	Matched
4		
5	The new password must contain at least 1 lowercase letter	Matched
6	The new password must contain at least 1 numeric	Matched
7	The new password must contain at least 1 special character	Matched
8	Password login failed 3 times will lock the account 5 minutes	Matched
9	The maximum password period is 90 days	Matched
10	The minimum password usage period is 0 days	Matched
11	/etc/passwd/ file permissions 644	Matched
12	/etc/shadow/ file permissions 640	Matched
13	UMASK Defaults to 022	Matched
14	Enable history command retention limit to 4	Matched
15	The system must enable the audit service	Matched
16	The system must create a log file	Matched
17	Ensure that system log files can only be appended	Matched
18	Ensure that the contents of the polled history log file cannot be modified	Matched
19	The system must enable the audit service	Matched
20	The system must create an audit log file	Matched
21	Backup Firewall Policy	Matched
22	BASH shell-breaking vulnerability detection	Manual Configuration is Recommended
23	OpenSSL Heart Bleeding Vulnerability Detection	Matched
24	System firewall on state detection	Matched
25	Only the UID of the ROOT account is 0	Matched
26	Detect default accounts that are not needed in the system	Manual Configuration is Recommended
27	Rename the ROOT Account Name	Manual Configuration is Recommended
28	Disable ROOT account remote login	Manual Configuration is Recommended
29	Non-owner file is forbidden in the system command directory	Matched
30	The 777-permission file is forbidden in the system command directory	Matched
31	Ordinary users can switch to ROOT account	Matched
32	FTP service shutdown status detection	Matched
33	Disable FTP anonymous login	Manual Configuration is Recommended
34	The root directory free space cannot be less than 10%	Matched
35	The system supports the RDP protocol.	Manual Configuration is Recommended
36	Disable TELNET remote management mode	Matched
37	Use encrypted remote management mode	Matched
38	Web service shutdown status detection	Matched
39	Mail service shutdown status detection	Matched
40	Syncookie Function On-state Detection	Matched
41	OS DEP startup status detection (requires restart)	Matched
42	Prohibit giving permission to change host IP address	Matched
43	Forbid non root users changing computer name	Matched
44	Only SSH is allowed when users log in remotely	Matched
44	The password must not contain the account name.	Matched
40		
40		
46	Restrict SSH remote login for a specified IP address range host Limit the maximum number of SSH connections and alert when the number of connections exceeds 500	Manual Configuration is Recommended Matched

AVCOMM Technologies Inc. 333 West Loop North, Suite 460 Houston, TX 77024, USA | info@avcomm.us | www.avcomm.us 95



4.8. Device Management

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

4.8.1. Windows Device Management

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

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

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

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

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

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

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

IEG > Device Manager	ment > Windows Device								
Common USB: Please sele	Safe USB: Please	selec V CD-ROM: Please s	Wireless Netwo	ork Card: Please selec *		Iss	ue		
Client Group: Whole N	etwork Online Status:	II Y Client Name:	Client I	P:	Search				
•	No.	Client Name	Client IP	OS	Online Status	Common USB	Safe USB	CD-ROM	Wireless Network Card
	1	yicexp-9fa8f6b9	192.168.3.215	Windows XP	Online	Read&Write	Read&Write	Enable	Enable
	2	WIN-RPOAL6VAKH6	192 168 3 65	Windows 7	Offline	Read&Write	Read&Write	Enable	Enable

Fig.4-38 Peripheral Control Interface

4.8.2. Linux Device Management

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

IEG > Device Man	₹ IEG > Device Management > Linux Device						
USB Switch Control :	Enable • Iss	ue -					
Client Group: Whole	Client Group: Whole Network • Client Name: Client IP: Online Status: All • USB Enable: Please select • Status						
	No.	Client Name	Client IP	Online Status	USB Enable		
	1	redhat7.4-hch	192.168.3.154	Online	Disable		

Fig.4-39 Linux Device Management



4.8.3.Registered USB Management

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

IEG > Device Ma	anagement > Register USB								
Register Control:	Register Read&Write Control: Read	Write & Execute							
	le Network Client Name: Introl: Please select USB ID: USB	Client IP:			Online Status: All	▼ USB Enable: P	Nease select 🔹 Register	r Status: Please select 🔹	Insert Status: Please select
	USB Identification Code	Client Name	Client IP	OS	Online Status	USB Enable	Register Status	Insert Status	Read&Write Control
Total 0 Page(s)/ 0	0 Record(s) Current Page 1 Page(s)								First Prev Next Last

Fig.4-40 Registered USB Management

4.9. Access Control

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

Note: Linux does not support the registry protection template.

4.9.1. Registry Protection Template

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

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

Ac	5d	Template Name :	Search	
No.	Template Name	OS Type	Description	Operation
1	asdsa	Windows		17 Basic Skule Delete DExport E-Import
Total 1 Page	s(s)/ 1 Record(s) Current Page 1 Page(s)			First Prev Next Last Goto 🔤 GO

Fig.4-41 Registry Template Configuration Interface

ns under HKEY_USERS and H	KEY_CURRENT_USER are not supported		6
No.	Registry	Data Type	Operation
	It cannot be empty, reference format: HKEY_LOCAL_MACHINE\WARE\DESCRIPTION\System	(item •	Delete
	It cannot be empty, reference format: HKEY_LOCAL_MACHINEWARDWARE\DESCRIPTION/System	item •	Delete
	It cannot be empty, reference format: HKEY_LOCAL_MACHINEWARDWARE\DESCRIPTION\System	litern 🔻	Delete

Fig.4-42 Registry Rule Configuration Interface

4.9.2. File Protection Template

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



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

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

🖲 IEG > A	IEG > Access Control > File Protection Template						
	Add	Template Name:	OS Type : Please select •	Search			
No.	Template Name	OS Type	Description	Operation			
1	sfa	Linux		🕼 Basic 💁 Rule 💼 Delete 📑 Export 💽 Import			
2	fd	Windows		🕼 Basic 🗳 Rule 💼 Delete 📑 Export 💽 Import			
Total 1 Page(s) 2 Record(s) Current Page 1 Page(s)							

Fig.4-43 File Protection Template Configuration Interface

tion File Operation
۵۸ ن
€ AM
0 AM
© A41
€ A4
© ^at
© va
File Operation
Delete
File

Fig.4-44 File Protection Rule Configuration Interface

4.9.3.File Protection Exception Template

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

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

Ad	d	Template Name:	Search	
NO.	Template Name	OS Type	Description	Operation
1	sad	Windows		🛱 Basic 🔍 Rule 🛢 Delete 🖪 Export 🗈 Import
Total 1 Page	(s)/ 1 Record(s) Current Page 1 Page(s)			First Prev Next Last Goto GO

Fig.4-45 File Protection Exception Template Configuration Interface

	IEG > Access Control > File Protection Exception Template Rule				
Prompt: Ca	Prompt: Can configure file or directory, the directory has to be ended with "".				
Ma	On a financial sector and the film				
No.	Configuration File	Operation			
IND.	Configuration File	Operation Delete			





4.9.4. Registry Protection Policy

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

IEG > Access Control > Registry Protection Policy							
OS Type: [Windows • Alarm Mode: [Intercept And Alarm •] Registry Protection Template: [Please select •]							
Client Group: Whole Netv	Client Group: Whole Network OS Type: Windows V Online Status: All V Client Name: Client IP: Search						
	No.	Client Name	Client IP	OS	Online Status	Alarm Mode	Registry Protection
	1	WIN-IP2601UDS48	192.168.3.16	Windows 7	Online	Close	View Strategy
	2	yicexp-9fa8f6b9	192.168.3.215	Windows XP	Online	Close	View Strategy
	3	WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Offline	Close	View Strategy

Fig.4-56 Registry Protection Policy Interface

4.9.5.File Protection Policy

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

VIEG PAU	n EC > ACCESS CONTROL > PRE Protection Poincy							
OS Type : [Windows • Alarm Mode: [Intercept An: • File Protection Template: [Peace selec •] File Protection Exception Template: [Peace selec •] Incom								
Client Grou	Client Group: Whole Network OS Type : [Please selec * Online Status: All * Client Name: Client IP:]							
	No.	Client Name	Client IP	OS	Online Status	Alarm Mode	File Protection	File Protection Exception
	1	redhat7.4-hch	192.168.3.154	Linux	Online	Intercept And Alarm	View Strategy	
	2	WIN-IP2601UDS48	192.168.3.16	Windows 7	Online	Close	View Strategy	View Strategy
0	2	WIN-IP2601UDS48 yicexp-9fa8f6b9	192.168.3.16	Windows 7 Windows XP	Online	Close	View Strategy View Strategy	View Strategy View Strategy

Fig.4-57 File Protection Policy Interface

4.10. Two-factor Authentication

4.10.1. User Template

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

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



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

Add Template		×
Template Name:	*	
OS Type:	Windows •	
Description:	Not exceeding 256 characters	
Save	Back	

Fig.4-69 User Template Add Interface

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

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

IEG > Two-factor Authentication > User Template					
Ad	id .	Template Name :	OS Type : Please select •	Search	
No.	Template Name	OS Type	Description	Operation	
1	yuanhi	Windows		🕫 Basic 💁 Rule 🛢 Delete	
2	yice	Windows		🕫 Basic 🔍 Rule 🛢 Delete	
Total 1 Page(s) / 2 Record(s) Current Page 1 Page(s) First Prev Nett Last Gelo G0					

Fig.4-70 User Template List Interface

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



IEG > Two-factor Authentication > Local User

Add User	To use Ukey password mode, download the USBKey plug-in first, <u>Download Link</u> !		
	OS Type:	Windows	
	User Name:	* Only Chinese characters, numbers, letters and underscores are allowed and the to	
	User Group:	Please select	
	Password:	*Password length range is [8,32]	
	Confirm Password:	*	
	Authentication Mode:	Common Password Mode	
	Description:		
		Save Back	

Fig.4-71 Add User Interface Normal Password

IEG > Two-factor Authentication > Local User				
User To use Ukey password mode, download the USBKey plug-in first, <u>Download Link</u> !				
OS Type:	Windows			
User Name:	* Only Chinese characters, numbers, letters and underscores are allowed and the to			
User Group:	Please select Custom User Group			
Password:	*Password length range is [8,32]			
Confirm Password:	т			
Authentication Mode :	Ukey Password Mode			
USBKey List:	Please select Change the Allas Refresh List			
Description:				
	Save Back			

Fig.4-72 Add User Interface Normal USBKey Password

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

IEG > Two-factor Authentication > User Template > Re	ule	
Modify Password		
User Name:	asdsa	
Current Password:		
New Password:		Password length range is [8,32]
Confirm New Password :]
		Save Back

Fig.4-73 Modify Password Interface

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

♥ IEG > Two-factor Authentication > User Template > Rule				
User Binding USBKey Download the USBKey plug-in first to use the function of this page. Download Link				
	User Name:	asdsa		
	USBKey List:	46755A523B022A60-sssssss Change Alias Refresh List		
		Save Back		

Fig.4-74 User Binding USBKey Interface

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

4.10.2. Authentication Policy

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


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

Ø IEG > I	Wo-factor #	Authentication > Authentica	tion Policy									
	Two-fac	OS : Windows			OS Passwor	Local User: Enab		Forbid	User Template: P OS Security Mode: D		Issue	
wo-factor /	OS: Please select • Client Orop: Whole Network • Client Neme: Client IP: Online Status: Ad • Demain Name: • ctdr Authentication: * Please select • Sharoh Search											
	NO.	Client Name	Client IP	OS	Online Status	Domain Name	Whether to Bind UKey	Two-factor Authentication	OS Password Authentication	Forbid OS Security Mode	Local User	Operation
	1	Admin-PC2	192.168.3.216	Windows Vista	Offline	-	No	Disabled	Disabled	Disabled	Enable	User Managemen
	2	CHENNIAN-WIN7	192.168.3.51	Windows 7	Online	test.com	No	Disabled	Disabled	Disabled	Enable	User Managemen
	3	ES130	192.168.3.21	Windows 2000	Offline		No	Disabled	Disabled	Disabled	Enable	User Managemer
	4	redhat7.4-hch	192.168.3.154	Linux	Online		No	Disabled	Enable	Disabled	Enable	User Managemer

Fig.4-75 Authentication Policy Interface

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

lient Name	: CHENNIAN-WIN7		Client IP: 192.168.3.51	User name:	Search			
No.	User name	User Group	Create Type	Enable Status	Authentication Mode	USBKey Name	Hard Ware Serial Number	Operation
1	Administrator	Administrators	Create Locally	Enable	Password Authentication			USBKeyBind
2	fani	Administrators, Users	Create Locally	Enable	Password Authentication			USBKeyBind
3	Guest	Guests	Create Locally	Enable	Password Authentication			USBKeyBind
4	test	Users	Create Locally	Enable	Password Authentication			USBKeyBind
5	user	Users	Create Locally	Enable	Password Authentication			USBKeyBind
6	yhl	Administrators	Crate on Management Platfo rm	Enable	Password Authentication			USBKeyBind
7	yuanhi	Users	Create Locally	Enable	Password Authentication			USBKeyBind
8	yutong	Users	Create Locally	Enable	Password Authentication			USBKeyBind

Fig.4-76

User Management Interface

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

🥲 IEG >	S > Two-factor Authentication > Authentication Policy > User Management								
C Nar	Client In- Indhat7.4-hoh Client IP: 192.188.3.154 OS: Linux User name: Standa								
No.	User Name	User Group	Enable Status	Authentication Mode	USBKey Name	Hard Ware Serial Number	Operation		
1	root	root	Enable	Password Authentication	-		Bind USBKey Reset Password Modify Group Delete		
2	redhat	redhat	Enable	Password Authentication	-		Bind USBKey Reset Password Modify Group Delete		
					Bac	k			



4.10.3. **Domain User Binding Information**

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

𝔅 IEG > Two-factor Auth	IEG > Two-factor Authentication > Domain User Binding							
Download the USB	Download the USBKay plug-in first to use the function of this page. Download Link							
Add	Hard War	e Serial Number:		Domain Name: Please select *		Search		
No.	Domain Name	Domain User Name	USBKey Name	Hard Ware Serial Number	Binding Time	Operation		
Total 0 Page(s)/ 0 Reco	Total 0 Page(s)/ 0 Record(s) Current Page 1 Page(s)							

Fig.4-78 Domain User Binding List Interface

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

Add Domain User Binding							
USBKey List:	Please select Refresh List						
Domain Name:	*						
Domain User Nam e:	*						
	Save Back						

Fig.4-79 Domain User Binding Interface

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

4.11. Basic Configuration

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

4.11.1. Basic Configuration

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



protection and alarm prompt.

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

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

Note: the Linux client is incapable of alarm prompt.

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

VILO > Dasic									
OS Type:	OS Type: Windows • Self-protection: Please selec • Alarm Prompt: Please selec • Issue								
Client Group	Client Group: Whole Network OS Type: Please selec * Online Status: All * Client Name: Client IP: Statch								
	N0.	Client Name	Client IP	OS	Online Status	Self-protection	Alarm Prompt		
	1	redhat7.4-hch	192.168.3.154	Linux	Online	Enable			
	2	WIN-IP2601UDS48	192.168.3.16	Windows 7	Online	Disable	Enable		
	3	yicexp-9fa8f6b9	192.168.3.215	Windows XP	Online	Disable	Enable		
	4	WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Online	Enable	Enable		

Fig.4-86 Basic Configuration Interface

4.11.2. **Operating System Log Audit**

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

🛛 IEG > Basir	G > Basic Configuration > OS Log Audit								
OS Log A	OS Log Audit : Enable • Audit Cycle: 1 • day(s) Insue								
OS Type	OS Type: Please selec * Clent Group: Mhole Network Online Status: All * Clent Name: Clent IP: Search								
	No.	Client Name	Client IP	OS	Online Status	Upload System Log	Audit Cycle		
	1	redhat7.4-hch	192.168.3.154	Linux	Online	Disable			
	2	WIN-IP26O1UDS48	192.168.3.16	Windows 7	Online	Enable	1		
	3	yicexp-9fa8f6b9	192.168.3.215	Windows XP	Online	Disable			
		WIN-RPOAL6VAKH6	192.168.3.65	Windows 7	Online	Disable			

Fig.4-87 Operating System Log Audit Interface

4.11.3. Authorization Management

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



IEG > Basic Configuration > License Management

Please Select a License File Start Upload	
Authorization Expiration Date :	2020/12/31
Number of total authorized points :	444
Number of Remaining License Points :	441
	Program Whitelist
	Access Control

Authorization Function List :

Access Control
Security Baseline
Two-factor Authentication
Unauthorized External Connection
Device Management



-> · 🛧 🏪	> This PC	> Local Disk (C:)	~	Ö Se	arch Local Disk (C:)	
)rganize 🔻 🛛 Ne	w folder					
 Quick access Desktop Downloads Documents Pictures This PC OneDrive This PC Network 	* [lame PerfLogs Program Files Program Files (x86) Users Windows 20180801114148-9001-00f10030-0999.lcs	Date modified 7/16/2016 7:47 PM 8/21/2019 11:43 AM 10/28/2019 11:39 8/21/2019 11:42 AM 10/28/2019 12:22 8/1/2018 11:41 AM	Type File folde File folde File folde File folde File folde LCS File	2r 2r 2r	1 KB
	File <u>n</u> ame:	20180801114148-9001-00f10030-0999.lcs		~ A	ll Files <u>O</u> pen	Cancel

Fig.4-89 Selecting a License File

4.11.4. Upload a Non-Whitelist File

When this function is enabled, if the registered IEG client system has executed the executable program in the non-whitelist, and the executable program is less than 5M, the executable program will be uploaded to the unified safety management platform for future audit. Functional interface (see Fig.4-90):

AVCOMM Technologies Inc. 333 West Loop North, Suite 460 Houston, TX 77024, USA | info@avcomm.us | www.avcomm.us 105

		- INDUSTRIALIT-
IEG > System Settings > Upload Non-white List File		
Upload Non-white List File:	Disable	Y
		Save

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

Installation Package Management 4.11.5.

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

IEG > Basic Configurati	G > Basic Configuration > Installation Package										
Add	Add Tip: The size of uploading package must be less than 200M. The number of uploading packages must not exceed 10.										
N0.	Name	MD5	File Size (unit: MB)	Upload Time	Operation						
1	engine_ipdlError.pkg	55bf92365a6fc5da51ec79d9a85bbced	0.00	2019-11-18 14:44:52	78 Download 🗯 Delete						
Total 1 Page(s) 1 Record(s) Current Page 1 Page(s)											

Fig.4-91 Installation Package Management Interface

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

A	dd Installation Package		×
	File Upload:	Select File	
	File Name:	The file name is automatically created after the file is uploaded	
	File Size:	The file size is automatically created after the file is uploaded	
		Save Back	

Fig.4-92 Add Installation Package Page

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

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

Add Tip: The size of uploading package must be less than 200M. The number of uploading packages must not exceed 10.									
No. Name MD5 File Size (unit: MB) Upload Time Opera									
	engine_ipdlError.pkg	55bf92365a6fc5da51ec79d9a85bbced	0.00	2019-11-18 14:44:52	Download Delete				

Fig.4-93 Installation Package Operation Button



5. Monitoring Audit

5.1 Introduction to Products

5.1.1 Product Overview

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

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

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

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



5.1.2 Appearance and Description



Fig.5-1 Appearance of Intelligent Monitoring Terminal

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

5.1.3.Indicator Light Description

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



Fig.5-2 Indicator Light

Tab.30 Instruction to Intelligent Monitoring Terminal

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



Dur light		NC	The desire is not assured as as buschedown
Run light		NC	The device is not powered on or breaks down
	RUN	Flashing in	The device works regularly
		green	
		Flashing in	The device fails or undergoes a network
		red	attack.
Bypass indicator	BP	NC	The bypass function is not enabled
light		NO	The bypass function is enabled
Ethernet electrical	MGMT	NC	The corresponding interface is in an
interface indicator	ETH1/ETH2/E		unconnected status
light	TH3/ETH4	Color of	The green color indicates that the current
		indicator	operation is based on a gigabit rate.
		lights	The orange color indicates that it is currently
			operating at 100 megabits
		The indicator	The interface has been established
		light is	
		normally on	
		The indicator	The interface is sending and receiving data
		light flashes	

5.1.4. Technical Specifications

Tab.31 Technical Specifications for Intelligent Monitoring Terminals

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

AVCOMM Technologies Inc.

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



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

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



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



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



		load change and other key		For S7 protocol: 26
		events.		request downloads, 27
		events.		start download, 28
				complete downloads,
				29 request upload, 30
				start upload, 31
				complete uploads,
				40CPU start, 41CPU
				stop
			This rule supports up	1,000 entries
			to	1,000 entries
			For one month,	1 111 / 1
			support up to	1 million entries
		Network connection real-	Provide a connection	
		time view, real-time	with the	
		graphical display of all	configuration	Support
			interface well-	
		the monitoring range, and	configured.	
		abnormal network	Exception	
		connections highlighted in	connections need to	
		red.	be stored in the	Store historical
			database and used in	connection data for up
		view, graphical display of	the history view from	-
		all network connections	being established to	
			ended	
		for a certain time period,	Connection details	
		·	include time (start,	
Network	Network	connections highlighted in	end), source MAC,	
connection	connection	red.	source IP address,	
statistics	view	Double-click an IP to	source port,	
		display details of each	destination MAC,	There is no upper limit
		connection connected to	destination IP	for the number of
		such an IP.	address, destination	entries displayed in real
		Support filtering based on		time
		source and destination IP	number of messages	
		addresses, only displaying	(upstream,	
		connection views related to	downstream), number	
		a certain IP address.	of bytes (upstream,	
			downstream)	
		source and destination ports,		
		only displaying connection		
		views related to a certain	display: number of	Support
		port.	nodes connected by	
		port.	each IP node; number	

AVCOMM°
— INDUSTRIAL IT —

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

		which can skip to detailed messages.	Message number TOP N can be set	N range: 1-50
		The hosts and network devices sorted according to the number of outflow, inflow and total messages	The type of message statistics is available for drop-down options	Drop-down options include all, send and receive
		are shown in a bar chart,	Port statistics TOP N can be set	N range: 1-50
		which can skip to detailed messages. The hosts and network devices sorted by outflow, inflow and total connection	The type of port statistics is available for drop-down options	Drop-down options include all, source port and destination port
		ports within a certain time range are shown in a bar chart, which can skip to detailed messages. The hosts and network devices sorted by	All statistics can be configured with a time range	Support
Operation mode support	The system can work in multiple modes	Learning mode: the system collects learning data in this mode to assist in generating whitelist rules. In this mode, there is no alarm for the whitelist, with other alarms normally generated Operation mode: for messages violating the whitelist rules and the protocols, give an alarm for messages of user-defined rules, no traffic rules and key events, which can be viewed in the management center	Effective time for switching the mode	<38
Deployment mode support	The terminal device can be	According to the actual network requirements, the	Bypass deployment	Support



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



1		TREES	TRIALIT —	1
			User-defined rules	Support
			Network session audit template management	Support
			Alarms supported	Industrial protocol whitelist alarm Industrial protocol
			include	alarm
		make statistics and		No traffic alarm
Alert stat		summarize all alarm		User-defined alarm
		information in the system	Graphical display	Support, including histograms, pie charts and trend charts
			Statistical result export	Support PNG, JPG, SVG and PDF format export
			A special tool authorizes the specified device	Support
Authoriz: control		The intelligent monitoring terminal is authorized to play the role in monitoring and audit	prompted when	Support
			It is in the yellow background color when the authorization is less than 1 month, and in the red background color in case of expired authorization	Support
	1	The status information or	Information refresh time	<58
	Terminal device status view	the device can be viewed in real time in the management		CPU usage
			nt Statuses that can be viewed include	Memory usage
				Hard disk usage



		RIALIT —	•
		Automatic upgrade of the management platform	Not support
		Manual upgrade of the management platform	Support
Upgrade management	All components within the system can be upgraded	Automatic upgrade of the intelligent monitoring terminal	Not support
	seamlessly	Manual local upgrade of the intelligent monitoring terminal	Support
		The management platform upgrades the intelligent monitoring terminal	Support
Remote management	Able to configure and manage policies in the system remotely	Manage the system based on the Web method	Support
		Need to authenticate the user's ID	Support
		User separation of powers	Support, including the system operator, the configuration administrator, auditor
Permission authentication	ID authentication	Password strength	Length 8-16, a combination of upper and lower case letters, numbers, special characters (#@! ~%^&*)
	Trusted host	IP authentication	Support
		MAC authentication	Support, optional
All alarms and	Log storage mode	Database	Support, MySQL
log data Storage generated by	Log storage cycle	Support up to	3 months
management the system wil be saved to the	A 1.1. (A dedicated tool is available for query	Support
server for		Process alarm incidents	Support



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

5.2. Startup and Login

5.2.1.Startup of Intelligent Monitoring Terminal

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





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

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

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

5.2.2.Use of CLI

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

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

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

cavium-linux login: winicssec Password: Entering character mode Escape character is '^]'. === WELCOME TO WNT CLI === CLI>

Fig.5-4 Command Line Interface - Common View



5.2.2.1.**Help**

CLI>help

Display help information.

5.2.2.2. System statistics related.

CLI>show pkt stat

View message statistics at all levels.

CLI>show fpa

View the FPA information, mainly on various memory statistics.

CLI>show mem pool

View the mem pool memory information.

CLI>config

Enter the system view.

5.2.2.3. Service-related

CLI# show log level Level: TRACE (5) View the log level. CLI# show log plane View the enabling of a module log CLI# set log level <level> Set the log level. CLI# set log plane <module id> [dp|mp|ap|cl]

Set/disable a module log.

5.2.2.4. Set the IP address of the management platform.

CLI>show serverip

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

CLI#set serverip 192.168.8.8

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

Set the industrial firewall gateway command,

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



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

CLI#set sma deploy mode access.

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

CLI#set sma deploy mode port-mirror.

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

CLI# set sma deploy mode mirror-forward.

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

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

CLI#set mgmtip 192.168.8.6

Change the IP address of the intelligent monitoring terminal.

5.3. Intelligent Monitoring Terminal Management

5.3.1.Introduction to Functions

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

5.3.2.Intelligent Monitoring Terminal Management

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





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

Probe > P	Probe Management > Pro	be Management					
Probe list						Show Dele	ted Probe
Probe:		Online Status: Please select	Probe SN:		Probe IP:		Search
No.	Probe	Device Status	Probe SN	Probe IP	Working Status	Online Status	Operation
1	Probe160824004	CPU Utsage Memory Usage Hard Disk Utage 18.63 0 25.43 0 37.37 00	160824004	192 168 77 157	Initial State	Online	Modify Delete Delete Delete Factory Reset Backup Policy

Fig.5-6 Intelligent Monitoring Terminal Management Page

View the current running status of the intelligent monitoring terminal, with the following meanings: Tab.32 Instruction to Intelligent Monitoring Terminal Management List Display

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



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



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

5.3.2.1. Information view

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

Probe	ProbeManagement > Modify	
Probe Ba	asic Information	
	Probe:	Probe160824004 *
	Probe SN:	160824004
	Probe IP:	192.168.77.157
	Software Version:	V200R005C01B122
	Online Status:	Online
	Time online:	2019-10-28 17:29:17
	Industrial Protocol Detection	
	Protocol Detection Exception Template:	Please select
	Protocol Detection Exception Template Version:	
	No-Traffic Detection	
	No-Traffic Detection Template:	Please select
	No-Traffic Detection Template Version:	
	Critical Event Detection	
	Critical Event Template:	Please select ▼
	Critical Event Detection Template Version:	
	Network Session Audit	
	Network Session Audit Template:	Please select ▼
	Network Session Audit Template Version:	



		1110	0 0 1 1	1 / 1 1 1				
Session Aging Time Setting								
	TCP Aging Time	3	Minute(s)					
	UDP Aging Time	3	Minute(s)					
Deployment Mode								
	Deployment Mode:	Bypass	¥					
ICS Protocol Logs								
	ICS Protocol Logs:	Record	V					
Save Alarm Message (*Prompt: Saving alarm messages w	ill consume more storage spacel)							
User-Defined Alarm Protocol	Alarm 🗆 Retain All Messages							
Device Grab Configuration								
	Message In				□ ETH0 💽 □ ETH1 💽	🗆 ETH2 💽	C ETH3	
	Message Out				□ ETH0	🗆 ETH2 💽	C ETH3	
		Message Search And Downloa	Save	Back	Search Session Table			

Fig.5-7 Intelligent Monitoring Terminal Information View Page

This page contains more details about the selected device.

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

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

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

Tab.33 Instruction to Intelligent Monitoring Terminal Details

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



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



5.3.2.2. Delete an intelligent monitoring terminal.

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

No.	Probe	Device Status	Probe SN	Probe IP	Working Status	Online Status	Operation
1	Probe150824004		160824004	192.168.77.157	Initial State	Online	E Model Delete ⊕ Upgra ⊘ Authori de ze ⊕ Factory Reset ₪ Backup Polic y

Fig.5-8 Deleting the Intelligent Monitoring Terminal

5.3.2.3. Intelligent monitoring terminal upgrade

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

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



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

Please select an upgrade file

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

➢ Start upload.

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

➢ Close

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

5.3.2.4. Authorization management

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



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

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

Manually activated through the management platform

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

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

5.3.2.4.1. Check authorization.

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

Ø Probe > Probe Management > Leense Management					
Detailed license information					
Device IP:		160824004			
Customer		Null			
Authorize	:	Unauthorized			
License Detail:	License Detail:				
OP	C Protocol Monitoring Module			Authorized	2021-08-26 19:30:28
Modbus TCP Protocol Monitoring Module			Authorized	2021-08-26 19:30:28	
S7 Protocol Monitoring Module		Authorized	2021-08-26 19:30:28		
Anomaly Traffic Monitoring Module			Authorized	2021-08-26 19:30:28	
Critical Event Monitoring Module			Authorized	2021-08-26 19:30:28	
IEC104 Protocol Monitoring Module			Authorized	2021-08-26 19:30:28	
DNP3 Protocol Monitoring Module			Authorized	2021-08-26 19:30:28	
MMS Protocol Monitoring Module				Authorized	2021-08-26 19:30:28
CIP Protocol Monitoring Module				Authorized	2021-08-26 19:30:28
Profinet Protocol Monitoring Module			Authorized	2021-08-26 19:30:28	
FIN	NS Protocol Monitoring Module	5		Authorized	2021-08-26 19:30:28
		•	Download Renew License Back		

Fig.5-10 Authorization Details View Page

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

 \triangleright Renew License

Update the authorization information on the current intelligent monitoring terminal

Download

Download the authorization file for the current intelligent monitoring terminal.

 \triangleright Back

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



5.3.2.4.2. Update the intelligent monitoring terminal authorization information.

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

V Probe > Probe Management > License Management	
Get the latest ficense file	
Salved Please select a loanse file Upleast Back	

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

➢ Select a file.

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

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

Back

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

5.3.2.5. Retrieve an intelligent monitoring terminal.

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

Probe >	Probe Management > Probe	Management					
Probe list						Show Delet	ed Probe
Probe:		Online Status: Please select	obe SN:		Probe IP:		Search
No.	Probe	Device Status	Probe SN	Probe IP	Working Status	Online Status	Operation
1	Probe160824004	CPU Usage Henry Usage Her Dub Usage	160824004	192.168.77.157	Initial State	Offline	Modify Delete Upgrade Authorize Factory Reset Reckup Policy
Total 1 Pa	Total 1 Page(s) / 1 Record(s),Current Page 1 First Prev Hord Last						

Fig.5-12 Retrieving an Intelligent Monitoring Terminal

5.4. Policy Management

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



5.4.1.Industrial Protocol Whitelist Template

5.4.1.1. Introduction to functions

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

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

5.4.1.2. Template management

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



Fig.5-13 Selecting an Industrial Protocol Whitelist Template



Probe > Policy Manager	ment > Whitelist Template				
Template Management List					⊛ Add
Template Name:	Search				
No.	Template Name	Version	Applied By	Edit	Operation
1	S7 sub-protocol full match whitelist template	1		E+Export	Ca Basic
2	S7 sub-protocol read-only whitelist template	1		EFExport .	ta Basic
3	FINS read-only whitelist template	1		EFExport .	ta Basic
4	FINS full match whitelist template	1		E}Export	ta Basic
5	Profinet IO RT read-only whitelist template	1		EFExport .	ta Basic
6	Profinet IO RT full match whitelist template	1		E+Export	ta Basic

Fig.5-14 Whitelist Template Management

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

Tab.34 instruction to Whitelist Template List Display	Tab.34	instruction	to Whitelist	Template Lis	st Display
---	--------	-------------	--------------	--------------	------------

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

5.4.1.3. Add a whitelist template.

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



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

Probe > Policy Mana	igement > Whitelist Template				
Template Management I	ist				⊙ Add
emplate Name :	Searc	h			
No.	Template Name	Version	Applied By	Edit	Operation
1	asdsa	1		Export E Import	to Basic 💁 Rule 💼 e
2	888	6	Probe160824084	Export E Import	🔀 Basic 🛛 💁 Rule
3	S7 sub-protocol full match whitelist templat e	1		■Export	Ta Basic
4	S7 sub-protocol read-only whitelist templat e	1		⊡ Export	🐻 Basic
5	FINS read-only whitelist template	1		Export	Ta Basic
6	FINS full match whitelist template	1		DExport	ta Basic

Fig.5-15 Whitelist Template Add Button

Add Template		×
Template Name:	*	
Remarks:		
Save	Back	

Fig.5-16 Whitelist Template Add Page

Tab.35 Instruction to Whitelist Template Add Information

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

5.4.1.4. Export a whitelist template.

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



Fig.5-17 Industrial Protocol Whitelist Template Export Button

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



Fig.5-18 Example of Exported an Excel File

5.4.1.5. Import a whitelist template.

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



E	dit	Operation
Export	⊡ Import	🐻 Basic 🗳 Rule 🍈 Delete
Export	E Import	🐻 Basic 🔹 Rule 🍈 Delete
Export	E Import	🐻 Basic 🗳 Rule 🍈 Delete
Export	🗲 Import	🐻 Basic 🗳 Rule 🍈 Delete
■Export	E Import	🐻 Basic 🗳 Rule 🍈 Delete

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

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

Import Excel			
Select file	Please select a file to import		
	Import Excel	Close	

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

5.4.1.6. Basic industrial protocol whitelist template configuration

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



E	dit	Operation
Export	⊡ Import	🐻 Basic 🗳 Rule 🏾 🍿 Delete
Export	E Import	🐻 Basic 🗳 Rule 🏢 Delete
Export	E Import	🐻 Basic 🐴 Rule 🍈 Delete
Export	E Import	🐻 Basic 🐴 Rule 🍈 Delete
Export	E Import	🐻 Basic 🐴 Rule 🏢 Delete

Fig.5-21 Whitelist Template Basic Configuration

Ø Probe > Policy Management > Whitelist Template				
Template Information				
Template Name :	asdsa			
Version:	1			
Applied By:				
Creation Time:	2019-11-16 18:37:59			
Remarks:				
	Save Back			

Fig.5-22 Whitelist Template Basic Configuration View Page

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

Tab.36 Instruction to Whitelist Template Basic Configuration Information

5.4.1.7. Industrial protocol whitelist template rule configuration

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

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


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

5.4.1.7.1. View an OPC whitelist item.

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

OP	C S7	MODBL	IS [DNP3	IEC104	CIP	MMS	PROFINET	FINS BA	CNETProtocol
SWIEE_T	CPProtocol SWIEE_U	DPProtocol								
Prompt: IP 0.	0.0.0 means configuring all									⊕ Add
No.	Src. IP		Dst. IP	Src. N	lask	Dst. Mask	Transport Protocol	Interface	Operation	Delete
Range Contro	bl									⊕ Add
	Name Src. IP	Dst. IP		Dst. Mask	Interface	Operation	Item ID D	ata Type Min. Value	Max. Value	Dele

Fig.5 -23 OPC Whitelist Item Information View Page

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

5.4.1.7.2. Add an OPC whitelist item.

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

Probe > Policy Ma	inagement > Whitel	ist Template							
OPC	S7	MODBUS	DNP3	IEC104	CIP	MMS	PROFINET	FINS	BACNETProtocol
SWIEE_TCPProtocol	SWIEE_UDPProto	col							

Prompt	IP 0.0.0.0 mear	ns configuring all										(ا	Add
No.	5	Src. IP	Dst. IP	Src	Mask	Dst. Mask	Transport Pro	tocol	Interface		Operation	[Delete
	0.0.0.0	0.0	.0.0	0		0	TCP		IOPCAsynclO3	ReadMaxAge	٣	D	Delete
	0.0.0.0	0.0	.0.0	0		0	TCP		IOPCAsynclO3	ReadMaxAge	٣	Û	Delete
	0.0.0.0	0.0	1.0.0	0		0	TCP		IOPCAsyncIO3	ReadMaxAge	٣	Û	Delete
ange C	control											€	Add
lo.	Tag Name	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Interface	Operation	Item ID	Data Type	Min. Value	Max. Value		Delete
		0.0.0	0.0.0	0	0	IOPCAsynciO3 V	WriteVQ1 V		Boolean V				Delete
		0.0.0.0	0.0.0.0	0	0	IOPCAsynciO3 V	WriteVQ1 V		Boolean V				Delete
		0.0.0.0	0.0.0.0	0	0	IOPCAsynciO3 V	WriteVQ1 V		Boolean 🔻				Delete

Fig.5-25 Industrial Protocol Whitelist Template Add Page

Tab.37 Instruction to OPC Whitelist Item Fields

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



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

Tab.38 Instruction to OPC Range Whitelist Item Fields

5.4.1.7.3. Modify an OPC whitelist item.

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

5.4.1.7.4. Delete an OPC whitelist item.

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

Prompt: IF	0.0.0.0 means configuring all								⊕ A	Add
No.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Transport Protocol	Interface	Operation		C	Delete
	0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsynclO3	ReadMaxAge	۳	1	Delete
	0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsynci03	ReadMaxAge	۳	Û	Delete
	0.0.0.0	0.0.0.0	0	0	TCP	IOPCAsynci03	ReadMaxAge	۳	1	Delete

Fig.5-26 Industrial Protocol Whitelist Template Delete Button

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

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



5.4.1.7.5. Modbus protocol whitelist configuration

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

5.4.1.7.6. Basic Modbus whitelist items

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

5.4.1.7.7. Modbus range control

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

Probe >	Policy Management	> Whitelist	Template							
OPC	C S7		MODBUS	DNP3	IEC104	CIP	MMS	PROFINET	FINS	BACNETProtocol
SWIEE_TO	CPProtocol SWIEE_	UDPProtocol								
rompt: IP 0.0	0.0.0 means configuring al	1								⊕ Add
No.	Src. IP	Dst. IP	Src.	Mask	Dst. Mask	Function	Start Addr.	End Addr.	Transport Protocol	Delete
Range Co Byte Order	ontrol Enable									
Mod	dbus Int16 Endian		Modbus Int32 End	dian	Modbus Flor	at Endian		Modbus	Double Endian	
	dbus Int16 Endian		Modbus Int32 End		Modbus Flor				Double Endian 15 FFH4 FFH3 FFH2 FFH1	¥
	FFH2 FFH1 ¥									▼ ⊙ Add

Fig.5-27 Modbus Protocol Range Enablement

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

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

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

Tab.39 Instruction to Modbus Click Fields



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

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

5.4.1.8. Delete a whitelist item.

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

1	asfa	1		Export E Import	🐻 Basic 🐴 Rule 🔟 Delete				
No.	Whitelist Template Name	Version	Applied By	Edit	Operation				
Whitelist Temp	late Name :	Search							
Template Ma	Template Management List								
Probe > I	Probe > Policy Management > Whitelist Template								

Fig.5-28 Industrial Protocol Whitelist Template Delete Button

5.4.1.9. Retrieve a whitelist template.

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

Template Management List	
Template Name:	Search

Fig.5-29 Retrieving a Whitelist Template



5.4.2.Protocol Detection Exception Template

5.4.2.1. Introduction to functions

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

5.4.2.2. Template management

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



Fig.5-30 Selecting a Protocol Detection Exception Template

				-INDUSTRIAL IT			
Template I	Template Management List						
Template Na	ime:		Search				
No.	Template Name	Version		Applied By		Edit	Operation
1	dfsa	1			🕒 Exp	oort 💽 Import	🔀 Basic 🐴 Rule 🍵 Delete
2	liupeng	4		Probe 160824084	🕒 Exp	oort 💽 Import	🔀 Basic 😋 Rule
Total 1 F	Total 1 Page(s) / 2 Records), Current Page 1 Prov Next Last						

Fig.5-31 Protocol Detection Exception Template Management

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

Tab.40 Instruction to Protocol Detection	on Excention Template List Display
1ab.+0 mstruction to 1 lotocol Detection	on Exception remplate List Display

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

5.4.2.3. Add a protocol detection exception template.

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

Fig.5-32 Protocol Detection Exception Template Add Button



Add Template	×
Template Name:	*
Remarks:	
Save	Back

Fig.5-33 Protocol Detection Exception Template Add Page

Tab.41 Instruction to Protocol Detection Exception Template Add Information

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

5.4.2.4. Export a protocol detection exception template.

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

- INDUSTRIALIT-			
E	dit	Operation	
Export	E Import	🐻 Basic 🐴 Rule 🍈 Delete	
Export	F Import	🐻 Basic 🐴 Rule 🏢 Delete	
Export	E Import	🐻 Basic 🐴 Rule 🍈 Delete	

Fig.5-34 Protocol Detection Exception Template Export Button

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

A	В	С	D	E	F	G
Template ID	Version	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol
IP exception t		otion template 🕘 🕀			: •	

A	В	С	D	E	F	G
Femplate ID	Version	Src. MAC	Dst. MAC	Src. MAC Mask	Dst. MAC Mask	Protocol
IP exception te		ption template 🛛 🕀			: •	

Fig.5-35 Example of an Exported Excel File



5.4.2.5. Import a protocol detection exception template.

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

Edi	it	Opera	tion
Export	E Import	🐻 Basic 🐴 Rule	🔟 Delete
Export	E Import	🐻 Basic 🐴 Rule	前 Delete
Export	E Import	🐻 Basic 🐴 Rule	Delete

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

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

Import Excel			
Select file	Select file Please select a file to import		
	Import Excel	Import Excel Close	
			*

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

5.4.2.6. Basic configuration of protocol detection exception template

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



Ed	lit	Operation
Export	F Import	🐻 Basic 🔹 Rule 🏢 Delete
Export	F Import	🐻 Basic 🐴 Rule 🏢 Delete
Export	K Import	🐻 Basic 🐴 Rule 🏢 Delete

Fig.5-38 Protocol Exception Detection Template Basic Configuration

Probe > Policy Management > Protocol Detection Exception Template				
Template Information				
Template Name:	dfsa			
Version:	1			
Applied By:				
Creation Time:	2019-11-16 18:41:17			
Remarks:				
	Save Back			
	Buck			

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

Tab.42 Instruction to Whitelist Template Basic Configuration Information

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

5.4.2.7. Protocol detection exception template rule configuration

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

5.4.2.7.1. View protocol detection exception rules.

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



rule configurations (Fig.5-40):

Probe :	Policy Management > Proto	col Detection Exception Temp	late									
IP Rule MAC Rule												
Prompt: IP 0.0.0.0 means configuring all												
No.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol	Operation						
	0.0.0.0	0.0.0.0	0	0	OPC Y	Delete						
Probe >	Policy Management > Proto	col Detection Exception Temp	late									
	IP Rule MAC	Rule										
Prompt: M	AC 00:00:00:00:00:00 means o	configuring all				⊕ Add						
No.	Src. MAC	Dst. MAC	Src. MAC Mask	Dst. MAC Mask	Protocol	Operation						
	00:00:00:00:00:00	00:00:00:00:00:00	0	0	Please select	Delete						

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

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

5.4.2.7.2. Add a protocol detection exception rule.

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

IP Rule MAC Rule Prompt: IP 0.0 0.0 means configuring all 0 A No. Src. IP Dst. IP Src. Mask Protocol Operation		Probe > Policy Management > Protocol Detection Exception Template									
	IP Rule MAC Rule										
No. Src. IP Dst. IP Src. Mask Dst. Mask Protocol Operation	Prompt: IP 0	0.0.0.0 means configuring all					⊛	Add			
	No.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol	Operati	ion			
0.0.0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0											

Fig.5-41 Protocol Detection Exception Template Add Button

Probe > Policy Management > Protocol Detection Exception Template									
IP Rule MAC Rule									
Prompt:	IP 0.0.0.0 means configuring a	all				e	D Add		
No.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol	Ope	ration		
	0.0.0	0.0.0.0	0	0	OPC T		Delete		
	0.0.0.0	0.0.0.0	0	0	OPC		Delete		

Fig.5-42 Protocol Detection Exception Template Add Page

Tab 43	Instruction	to Protoc	ol Detection	Exception	IP Rule Fields
140.45	monuction	10 1 10100		LACOPTION	II Itule I leius

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

AVCOMM Technologies Inc.

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



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

Tab.44 Instruction to Protocol Detection Exception MAC Rule Fields

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

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

5.4.2.7.3. Modify a protocol detection exception rule.

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

5.4.2.7.4. Delete a protocol to detect exception rule.

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

1	P Rule M/	AC Rule					
rompt: IP	0.0.0.0 means configuring	all					€ Add
0.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol	Ope	eration
	0.0.0.0	0.0.0	0	0	OPC	•	Dele
	0.0.0.0	0.0.0.0	0	0	OPC	- 💼	Dele
IP	Policy Management > Pro	tocol Detection Exception Ter	nplate				
IP	Policy Management > Pro	tocol Detection Exception Ter	nplate				€ Add

Fig.5-43 Protocol Detection Exception Rule Delete Button

5.4.2.8. Delete a protocol detection exception template.

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

Probe	Probe > Policy Management > Protocol Detection Exception Template							
Template	Template Management List							
Template	ə:		Search					
No.	Template	Version	Applied By	Ec	lit	Operation		
1	test	1		Export	E Import	🐻 Basic 😋 Rule 📋 Delete		
2	wwww	1		Export	Import	🐻 Basic 💁 Rule 📋 Delete		
3	ess	1		Export	Import	🐻 Basic 🔥 Rule 🍵 Delete		

Fig.5-44 Protocol Detection Exception Template Delete Button



5.4.2.9. Retrieve a protocol detection exception template.

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

Template Management List		
Template Name:	Search	

Fig.5-45 Retrieving a Protocol Detection Exception Template

5.4.3. Critical Event Template

5.4.3.1. Introduction to functions

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

5.4.3.2. Template management

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

😤 Probe Management >
■ Policy Management ∨
Whitelist Template
Exception Template
No-Traffic Template
S Critical Event Template
User-Defined Rule
Net Session Template
Network Connection >
▲ Abnormal Traffic >
System Configuration >

Fig.5-46 Selecting a Critical Event Detection Template

Probe	Policy Management >	Critical Event Templa	te						
Template	Management List								⊕ Add
Template N	ime:		Search						
No.	Template Name	Version		Applied By	E	dit		Operation	
1	99	4			Export	E Import	Co Basic	Q Rule	1 Delete
Total 1	Page(s) / 1 Record(s),Current Page	age 1						Fits	t Prev Next Last

Fig.5-47 Critical Event Detection Template Management

View information on all critical event detection templates in the system here, with the meanings given below: Tab.39 Instruction to Protocol Detection Exception Template List Display

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

5.4.3.3. Add a critical event detection template.

Template Management List

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

Fig.5-48 Protocol Detection Exception Template Add Button



Add Template	×
Template Name: *	
Remarks:	
Save Back	

Fig.5-49 Protocol Detection Exception Template Add Page

Tab.40 Instruction to Critical Event Detection Template Add Information

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

5.4.3.4. Export a critical event detection template.

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

E	dit		Operatior	ו
Export	E Import	🐻 Basic	🐴 Rule	m Delete
Export	E Import	🐻 Basic		🐴 Rule

Fig.5-50 Critical Event Detection Template Export Button

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



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

Template ID	Version	Src. IP	Dst. IP	Src. Mask	Dst. Mask
IP rule configu	ration MAC rule cor	nfiguration 🕀			•

~	5		J	<u> </u>	
Template ID	Version	Src. MAC	Dst. MAC	Src. MAC Mask	Dst. MAC Mask
IP rule configu	uration MAC rule co	nfiguration 🕀			1
		(†)			•

Fig.5-51 Example of an Exported Excel File

5.4.3.5. Import a critical event detection template.

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



Edit	Operation
Export Export	🐻 Basic 🐴 Rule 🍈 Delete
Export Import	🔁 Basic 🐴 Rule

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

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

Import Excel						
Select file	Please select a fil	Please select a file to import				
	Import Excel					

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

5.4.3.6. Critical event detection template basic configuration

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

Edit			Operation	1
Export	€ Import	🐻 Basic	🐴 Rule	🛅 Delete
Export	🗲 Import	to Bas	ic	🐴 Rule

Fig.5-54 Critical Event Detection Template Basic Configuration



Probe > Policy Management > Critical Event Template					
Template Information					
Template Name:	hh				
Version:	3				
Applied By:	Probe160824084				
Creation Time:	2019-11-16 14:19:31				
Remarks:					
	Save Back				

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

Tab.41 Instruction to Childal Event Detection Dasic Computation informati	on
Tab.41 Instruction to Critical Event Detection Basic Configuration Informati	011

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

5.4.3.7. Critical event detection template rule configuration

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

5.4.3.7.1. View the critical event detection rules.

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



Probe >	Policy Management > Critical Event Ter	mplate			
	P Rule MAC Rule				
Prompt: IP	0.0.0.0 means configuring all				● Add
No.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Operation
	0.0.0	0.0.0.0	0	0	Delete
		Sav	e Back		
Probe :	> Policy Management > Critical Event Te	mplate			
	IP Rule MAC Rule				
Prompt: M	IAC 00:00:00:00:00:00 means configuring a	all			
No.	Src. MAC	Dst. MAC	Src. MAC Mask	Dst. MAC Mask	Operation
	00:00:00:00:00:00	00:00:00:00:00:00	0	0	Delete
		Sav	ve Back		

Fig.5-56 Critical Event Detection Rules View Page

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

5.4.3.7.2. Add the critical event detection rules.

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

FIDDE POI	icy Management > Critical Event Te	emplate				
IP Ru	le MAC Rule					
rompt: IP 0.0.0	0.0 means configuring all				⊕ Ad	
	Fi	g.5-57 Critical Event	Detection Template A	dd Button		
Probe > Poli	cy Management > Critical Event Te	mplate				
IP Rul	e MAC Rule					
ompt: IP 0.0.0	0.0 means configuring all					
No. Src. IP		Dst. IP	Src. Mask	Dst. Mask	Operation	
	0.0.0.0	0.0.0	0	0	ti De	
		Sav	e Back			
Probe > Polic	cy Management > Critical Event Te	mplate				
Probe > Polic		mplate				
IP Rul					Add	
IP Rul	e MAC Rule		Src. MAC Mask	Dst. MAC Mask	Operatio	

Fig.5-58 Critical Event Detection Template Add Page

Tab.45 Instruction to Critical Event Detection IP Rule Fields

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



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

Tab.46 Instruction to Critical Event Detection MAC Rule Fields

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

5.4.3.7.3. Modify the critical event detection rules.

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

5.4.3.7.4. Delete the critical event detection rules.

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



Probe > Policy	y Management > Critical Event Tem	plate			
IP Rule	MAC Rule				
Prompt: IP 0.0.0.0	0 means configuring all				⊕ Add
No.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Operation
	0.0.0.0	0.0.0.0	0	0	Delete
		Save	Back		
Probe > Policy	Management > Critical Event Tem	plate			
IP Rule	MAC Rule				
Prompt: MAC 00:	00:00:00:00:00 means configuring all				● Add
No.	Src. MAC	Dst. MAC	Src. MAC Mask	Dst. MAC Mask	Operation
	00:00:00:00:00	00:00:00:00:00:00	0	0	Delete
		Save	Back		

Fig.5-59 Critical Event Detection Rules Delete Button

5.4.3.8. Delete the critical event detection template.

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

V Probe > Policy Management > Critical Event Template									
Template Management List									
Template: Search									
No.	Template	Version	Applied By	Ed	it				
1	test	1		Export	F Import	Co Basic	🐴 Rule	💼 Delete	
2	1	4	Probe160824002	Export	E Import	Co Basic		🐴 Rule	

Fig.5-60 Critical Event Detection Template Delete Button

5.4.3.9. Retrieve a critical event detection template.

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

Template Name:		Search	

Fig.5-61 Retrieve a Critical Event Detection Template



5.4.4.User-Defined Rules

5.4.4.1. Introduction to functions

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

5.4.4.2. Rule configuration

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

👗 Probe Management >
Policy Management V
Whitelist Template
Exception Template
No-Traffic Template
S Critical Event Template
, 🖪 User-Defined Rule
Net Session Template
⊕ Network Connection >
▲ Abnormal Traffic >
System Configuration >

Fig.5-62 Selecting User-defined Rules.

No.	Src. IP		Src. Mask	Dst. IP	Dst.	Mask		Transpo	ort Protocol	Interface	Opera	ation	Delete
Prompt: IP 0.	.0.0.0 means co	nfiguring all											● Add
SWIEE_UDI	Р												
OPC		S7	MODBUS	DNP3	IEC104		CIP		MMS	PROFINET	FINS	BACNET	SWIEE_TCP
Probe > F	olicy Managen	nent > User-I	Defined Rule										

Fig.5-63 User-defined Rules

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



5.4.4.3. **OPC User-Defined Rule Configuration**

5.4.4.3.1. View the OPC user-defined rules.

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

	PC S7	MODBUS	DNP3	IEC104	CIP	PROFINET	FINS BACNE	SWIEE_TCP
SWIEE_U Prompt: IP	2 0.0.0.0 means configuri	ng all					1	
No.	Src. IP	Src. Mask	Dst. IP	Dst. Mask	Transport Protocol	Interface	Operation	Delete
	0.0.0.0	0	0.0.0.0	0	TCP	IOPCAsynclO3	ReadMaxAge V	Delete

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

5.4.4.3.2. Add the OPC user-defined rules.

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

	0.0.0.0	0		0.0.0.0	0	TCP	IOPCAsyncIO3	▼ ReadMaxAge	▼ 💼 Delete
No.	Src. IP	Sr	c. Mask	Dst. IP	Dst. Mask	Transport Proto	col Interface	Operation	Delete
rompt: IP	0.0.0.0 means	configuring all							⊕ Add
SWIEE_U	-			0110		011			
	PC	S7	MODBUS	DNP3	IEC104	CIP	MMS PROFINET	FINS	BACNET SWIEE_TC
Probe :	> Policy Manage	ement > User-D		1 - 8.0 00	010 0001 0		i iuu Dunon		
				Fig. 5-65	OPC User-d	efined Rule	Add Button		
ompt: IP	0.0.0.0 means	configuring all							● Add
SWIEE_U	JDP								
OF	PC	S7	MODBUS	DNP3	IEC104	CIP	MMS PROFINE	FINS	BACNET SWIEE_

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

Tab.47 Instruction to OPC User-defined Rule Fields

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



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

5.4.4.3.3. Modify the OPC user-defined rules.

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

5.4.4.3.4. Delete the OPC user-defined rules.

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

No.	Src. IP	Src. Mask	Dst. IP	Dst. Mask	Transport Protocol	Interface	Operation	Delete
								0
ompt: I	P 0.0.0.0 means configuri	ing all						⊕ Add
SWIEE_	UDP							
C	OPC S7	MODBUS	DNP3	IEC104	CIP MMS	PROFINET	FINS BACNE	ET SWIEE_TO

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

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

5.4.5. Network Session Audit Template

5.4.5.1. Introduction to functions

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

5.4.5.2. Template management

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





Template Management List				⊕ Add
Template Name:	Search			
No. Template Name	Version	Applied By	Edit	Operation
Total 0 Page(s) / 0 Record(s),Current Page 1				First Prev Next Last

Fig.5-69 Network Session Audit Template Management

View information on all network session audit templates in the system here, with the meanings given below: Tab.48 Instruction to Network Session Audit Template List Display

Column Names	Instructions
--------------	--------------



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

5.4.5.3. Add a network session audit template.

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

Template Management List

Fig.5-70 Network Session Audit Template



Add Template

Template Name:	*
Remarks:	
Save	Back

Fig.5-71 Network Session Audit Template Add Page

Tab.49 Instruction to Network Session Audit Template Add Information

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

5.4.5.4. Export the network session audit template.

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



Fig.5-72 Network Session Audit Template Export Button

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



Template ID	Version	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol	Src. Port Start	S
42	2	0.0.0.0	0.0.0.0	0	0	6	0	65535
	ession Audit Template	• +			: 4			

Fig.5-73 Example of an Exported Excel File

5.4.5.5. Import a network session audit template.

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

Edi	it	Operation			
Export	🗲 Import	🐻 Basic 🐴 Rule 🍿 Del	ete		

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

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



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

5.4.5.6. Network session audit template basic configuration

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



Fig.5-76 Network Session Audit Template Basic Configuration

Probe > Policy Management > Network Session Audit Template	
Template Information	
Template :	11
Version:	2
Applied By:	
Creation Time :	2019-10-15 11:07:20
Remarks:	
	Save Back

Fig.5-77 Network Session Audit Template Basic Configuration View Page Tab.50 Instruction to Network Session Audit Template Basic Configuration Information

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

5.4.5.7. Network session audit template rule configuration

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

5.4.5.7.1. View the network session audit rules.

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

	Alle Prompt: IP 0.0.0.0 means configuring all No. Src. IP Dst. IP Src. Mask Dst. Mask Protocol Src. Port Start Src. Port End Dst. Port Start Dst. Port End Perform the Action Operation									
Image: Construction of the construction of	Prompt: IP 0.0.0.0 means configuring all Image: No. Src. IP Dst. IP Src. Mask Dst. Mask Protocol Src. Port Start Src. Port End Dst. Port Start Dst. Port End Perform the Action Operation	Probe >	Policy Manager	ment > Network	Session Audit Te	emplate				
No. Src. IP Dst. IP Src. Mask Dst. Mask Protocol Src. Port Start Src. Port End Dst. Port Start Dst. Port End Perform the Action Oper	No. Src. IP Dst. IP Src. Mask Dst. Mask Protocol Src. Port Start Src. Port End Dst. Port Start Dst. Port End Perform the Action Operation				- 11					444
	1 0.0.0 0 0 0 0 0 TCP V 0 85535 0 85535 Record V 0 D									

Fig.5-78 Network Session Audit Rule View Page

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

5.4.5.7.2. Add the network session audit rules.

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

Probe	> Po	licy M	lanag	emen	t > Ne	etwork	Ses	sion	Audit	Tem	plate	•																								
Rule																																				
(∱) (J) Pro	ompt:	IP 0.0	0.0.0 n	neans	confi	guring	all																											۲	Add	
]	Fig	.5	-79	9 N	Jei	tw	ork	5	Ses	sic	n 4	Aι	adit	t Rı	ıle	e A	dd	Bu	tto	n								
Rule																																				
🗇 🕘 Pro	ompt:	IP 0.0).0.0 n	ieans	confi	guring	all																											⊕	Add	
No.		Src.	IP		Dst.	P	s	Src. N	lask		Dst.	Mask	¢	Pro	otocol		Src.	Port	Start		Src.	Port E	nd		Dst. P	ort Sta	art	C	st. Po	rt End	Perfo	m the	e Actio	on (Oper	atic
□ 1	0.	0.0.0		0.0	.0.0		0	,			0]	TC	P V		0				655	535			0				65535		R	ecord	۳		۵	Dele
																	Save			С	Close															

Fig.5-80 Network Session Audit Rule Add Button

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

Tab.51 Instruction to Network Session Audit Rule Fields

AVCOMM Technologies Inc.



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

5.4.5.7.3. Modify the network session audit rules.

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

5.4.5.7.4. Delete the network session audit rules.

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

Probe	Policy Manage	ement > Network	Session Audit Te	emplate							
Rule											
🗇 🕁 Pr	ompt: IP 0.0.0.0 m	eans configuring a	ill.							€	Add
No.	Src. IP	Dst. IP	Src. Mask	Dst. Mask	Protocol	Src. Port Start	Src. Port End	Dst. Port Start	Dst. Port End	Perform the Action	Operation
□ <u>1</u>	0.0.0.0	0.0.0	0	0	TCP V	0	65535	0	65535	Record	🔟 Delete

Fig.5-81 Network Session Audit Rule Delete Button

5.4.5.8. Delete a network session audit delete button.

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

Probe > Policy M	anagement > Network	Session Audit Templ	ate						
Template Manageme	ent List						۲	Add	
Template Name:		Search							
No.	Template Name	Version	Applied By	Ed	it	C	Operatio	n	
1	sad	1		Export	⊡ Import	ta Basic 😋	& Rule	Delete]
Total 1 Page(s) / 1 Re	ecord(s),Current Page 1					F	First Prev I	Next Last	





5.4.5.9. Retrieve a network session audit template.

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

Template Name:	Search

Fig.5-83 Retrieving a Network Session Audit Template

5.4.6.No Traffic Detection Template

5.4.6.1. Introduction to functions

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

5.4.6.2. Template management

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

A Probe Management >
■ Policy Management ∨
Whitelist Template
Exception Template
Scritical Event Template
User-Defined Rule
Net Session Template
Network Connection >
▲ Abnormal Traffic >
System Configuration >

Fig.5-84 Selecting a No Traffic Detection Template



Fig.5-85 No Traffic Detection Template Management

View information on all no traffic detection templates in the system here, with the meanings given below: Tab.52 Instruction to Network Session Audit Template List Display

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

5.4.6.3. Add a no traffic detection template.

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

 Probe > Policy Management > No-Traffic Template

 Template Management List

 Add
 Add

Fig.5-86 No Traffic Detection Template Add Button



Ad	d Template		×
	Template Name:	*	
	Remarks:		
	Save	Back	

Fig.5-87 No Traffic Detection Template Add Page

Tab.53 Instruction to No Traffic Detection Template Add Information

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

5.4.6.4. Export a no traffic detection template.

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

Edit		Operation		
Export	E Import	to Basic	🐴 Rule	<u> </u> Delete
Export	F Import	to Basic	🐴 Rule	前 Delete

Fig.5-88 No Traffic Detection Template Export Button

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



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

м	U	U	U	L	1	9
Template ID	Version	Src. IP	Dst. IP	Dst. Port	Transport Protocol	No-Traffic Time
1	2	0.0.0.0	0.0.0.0	0	6	5
No-traffic	detection template	÷				



5.4.6.5. Import a no traffic detection template.

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



Fig.5-90 No Traffic Detection Template Import Rules

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






5.4.6.6. No traffic detection template basic configuration

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

Edit		Operation				
Export	E Import	🐻 Basic	🐴 Rule	🛅 Delete		
Export	E Import	🐻 Basic	🐴 Rule	🛅 Delete		

Fig.5-92 No Traffic Detection Template Basic Configuration

Probe > Policy Management > No-Traffic Template	
Template Information	
Template :	import222
Version:	2
Applied By:	
Creation Time :	2019-10-15 11:05:12
Remarks:	
	Save Back

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

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

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

5.4.6.7. No traffic detection template rule configuration

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



5.4.6.7.1. View the no traffic detection rules.

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

Probe > Policy Management > No-Traffic Template									
Rule	Rule								
Prompt: IP	0.0.0.0 means configuring all					⊕ Add			
No.	Src. IP	Dst. IP	Dst. Port	Transport Protocol	No-Traffic Interval (Second)	Operation			
1	0.0.0	0.0.0	0	TCP	5	Delete			

Fig.5-94 No Traffic Detection Rule View Page

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

5.4.6.7.2. Add the no traffic detection rules.

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

V Probe > Po	Probe > Policy Management > No-Traffic Template											
Rule												
Prompt: IP 0.0	0.0.0 means configuring all					⊕ Add						
		Fig.5-95	No Traffic Det	ection Rule Add But	ton							
Probe > Po	blicy Management > No-Tr	affic Template										
Rule												
Prompt: IP 0.0	0.0.0 means configuring all					⊕ Add						
No.	Src. IP	Dst. IP	Dst. Port	Transport Protocol	No-Traffic Interval (Second)	Operation						
1	0.0.0.0	0.0.0	0	TCP	5	Delete						
			Save	Close								

Fig.5-96 No Traffic Detection Rule Add Item

Tab.55 Instruction to No Traffic Detection Rule Fields

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

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

5.4.6.7.3. Modify no traffic detection rules.

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

5.4.6.7.4. Delete the no traffic detection rules.

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

Probe >	Probe > Policy Management > No-Traffic Template									
Rule	Rule									
Prompt: IP (0.0.0.0 means configuring all					⊕ Add				
No.	Src. IP	Dst. IP	Dst. Port	Transport Protocol	No-Traffic Interval (Second)	Operation				
No. 1	Src. IP	Dst. IP	Dst. Port	Transport Protocol	No-Traffic Interval (Second)	Operation Delete				

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

5.4.6.8. Delete a no traffic detection template.

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

Edit	Operation
Export 💽 Import	🔂 Basic 🛛 🐴 Rule 🗂 Delete
Export Market Import	🐻 Basic 🛛 🐴 Rule 🏾 🍈 Delete

Fig.5-98 No Traffic Detection Template Delete Button



5.4.6.9. Retrieve a no-traffic detection template

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

Search	ne:
--------	-----

Fig.5-99 Retrieving a No Traffic Detection Template

5.5. Log Management

5.5.1.Introduction to Functions

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

5.5.2. Industrial Protocol Whitelist Alarm

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

5.5.2.1. Log list

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





Fig.5-100 Industrial Protocol Whitelist Alarm Menu



19 Pr	obe > Log	s Manager	nent > Whitelist	Alarm													
White	list Alarm															Show Proces	ssed Logs C
		Probe:	Please select			Prot	ie:				Src. IP:			Dst	IP:		
		Src. MAC:				Dst. MA	c:				Start Time:	2019-11-18 00:00:00		End T	ime: 2019	-11-18 23:59:59	9
Арр	lication Lay	er Protocol:	Please select	ı ۱		Sea	rch										
No.	Alarm Time	Src. IP	Src. Device	Src. Port	Dst. IP	Dst. Device	Dst. Port	Transport Protocol	Application Layer Protocol	Src. MAC	Dst. MAC	Description	Alarm Level	Processing Status	Probe	Probe IP	Operation
1	2019-11-1 8 15:10:12	192.168.15.2 46	Device157406101 377445	1500	192.168.15.2 37		102	TCP	S7			Violate S7 whitelist rule alarm , start CPU	Emergen Cy	Unprocessed	Probe160824 084	192.168.4.98	Process
2	2019-11-1 8 15:10:12	192.168.15.2 46		1500	192.168.15.2 37		102	TCP	S7			Violate S7 whitelist rule alarm , download request	Emergen cy	Unprocessed	Probe160824 084	192.168.4.98	Process
2	2019-11-1	192.168.15.2	Device157406101	1500	192.168.15.2	Device157406101	102	TOP	97			Violate S7 whitelist rule alarm ,	Emergen	Upprocessed	Probe160824	102 109 4 00	@ Process

Fig.5-101 Industrial Protocol Alarm List Page

View all the log information on whitelist alarms here, with the meaning given below: Tab.56 Instruction to Whitelist Alarm Log Display

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

AVCOMM Technologies Inc.



Operation	Process	Further processing of alarm information

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

view the processed logs. (As shown in Fig.5-102):

	Probe:	Please select	Ŧ	Probe:				Sro	. IP:			Dst	IP:		
	Src. MAC:			Dst. MAC:				Start T		-18 00:00:00		End Ti		9-11-18 23:59:59	
Application Lay	ver Protocol:	Please select	٣	Search											
Alarm		Src. Device			Dst. Port	Transport	Application		Dst. MAC	Description	Alarm	Processing	Probe	Probe IP	Opera

Fig.5-102 Displaying Processed Whitelist Alarm List Page

5.5.2.2. Process a log.

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

Probe > Logs Management > Whitelist Alarm > Process	
Logs Information Processing	
Alarm Time	2019-10-31 13:55:52
Src. IP:	169.254.92.32
Src. Port:	49187
Dst. IP:	169.254.91.133
Dst. Port:	9600
Src. MAC:	
Dst. MAC:	·
Transport Protocol:	TCP
Application Layer Protocol:	FINS
Description:	Violate S7 whitelist rule alarm , start CPU
Alarm Level:	Emergency
Probe:	Probe160824084
Probe IP:	192.168.4.98
Processing Status:	Unproce: •
Processing Opinions:	
Processing Time:	
	Save Add to Baseline Back

Fig.5-103 Industrial Protocol Whitelist Alarm Processing Page

5.5.2.2.1. **Close the log.**

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

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



5.5.2.2.2. Add a baseline.

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

5.5.2.2.3. Export a message.

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

5.5.2.3. Retrieve a log.

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

Probe: Probe: Src. IP: Dst. IP: 0104.0410.000.00 014.0400.000.00 014.0400.000.00 014.0400.000.00	igs 🗆	Show Processed Lo					Alarm	3
		Dst. IP:		Src. IP:	Probe:	lect *	Probe: P	
SIC. MAC: Stall time: 2019-11-10 00 00 00 End time: 2019-11-10 00 00 00		End Time: 2019-11-18 23:59:59	2019-11-18 00:00:00	Start Time:	Dst. MAC:		Src. MAC:	
Application Layer Protocol:Piease select • Scarch					Search	elect •	tion Layer Protocol:	



5.5.3.Industrial Protocol Detection Alarm

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

5.5.3.1.Log list

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









Probe > Logs Managem	ent > ICS Protoco	I Alarm												
ICS Protocol Alarm													Show Proces	sed Alarms
Probe : Src. MAC : Application Layer Protocol :	Please selectPlease select	¥		Probe: Dst. MAC: Search				Src. IP: Start Time:	2019-11-18 00:00	1:00		Ost. IP:	019-11-18 23:59:5	9
No. Alarm Time Src. IP	Src. Device	Src. Port	Dst. IP	Dst. Device	Dst. Port	Src. MAC	Dst. MAC	Transport Protocol	Application Layer Protocol	Alarm Level	Processing Status	Probe	Probe IP	Operation
Total 0 Page(s) / 0 Record(s),C	urrent Page 1 Page(s)												First F	Prev Next Last

Fig.5-106 Industrial Protocol Detection Alarm List Page

View all the log information on industrial protocol alarms here, with the meaning given below:	
Tab.57 Instruction to Industrial Protocol Detection Alarm Display	

Column Names	Instructions							
Alarm Time	Time when a	an alarm occurs						
Src. IP	The IP addre	ess initiating a data request, in dotted decimal format						
Src. device	The system a	automatically generates a source device name according to the						
	source IP, su	pporting custom source device name						
Src. port	The port use	d by the machine initiating the data request						
Dst. IP	The destinati	on IP requesting data, in dotted decimal format						
Dst. Device	The system a	automatically generates a destination device name according to						
	destination I	P, supporting custom destination device name						
Dst. Port	The port use	The port used by the requested destination machine						
Src. MAC	The MAC address initiating a data request							
Dst. MAC	The destinati	on MAC address requesting the data						
Transport Protocol	The protocol	type of transport layer used by the message						
Application Layer	Specific appl	lication protocol types						
Protocol								
Alarm Level	Warning of p	possible damage levels						
Probe	An intelliger	nt monitoring terminal name that is generated by the system or						
	named by us	ers, which is easy to remember						
Probe IP	The IP addr	ess assigned by the intelligent monitoring terminal, in dotted						
	decimal form	nat						
Operation	Process	Further processing of alarm information						

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



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

Probe	> Logs	Manageme	ent > ICS Protoco	l Alarm												
CS Proto	ocol Alari	m													Show Process	sed Alarms
		Probe:	Please select	٣		Probe:				Src. IP:			D	st. IP:		
		Src. MAC:				Dst. MAC:				Start Time:	2019-11-18 00:00	:00	End	Time:	2019-11-18 23:59:59	•
Applicat	tion Laye	Protocol:	Please select	٣		Search										
	Alarm Time	Src. IP	Src. Device	Src. Port	Dst. IP	Dst. Device	Dst. Port	Src. MAC	Dst. MAC	Transport Protocol	Application Layer Protocol	Alarm Level	Processing Status	Probe	Probe IP	Operati
Total 0	Page(s) / (0 Record(s),Cu	rrent Page 1 Page(s)												First P	rev Next La

Fig.5-107 Displaying Processed Protocol Alarm List Page

5.5.3.2. Process a log.

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

Probe > Logs Management > Protocol Alarm Logs	
Logs Information Processing	
Alarm Time :	2019-10-31 14:16:48
Src. IP:	
Src. Port:	
Dst. IP:	
Dst. Port:	· · · · · · · · · · · · · · · · · · ·
Src. MAC:	00:03:1d:0c:70:cc
Dst. MAC:	00:1b:1b:ae:28:e3
Transport Protocol:	
Application Layer Protocol:	PROFINET DCP
Alarm Level:	Error
Probe:	Probe160824021
Probe IP:	192.168.15.194
Processing Status:	Unproci v
Processing Opinions:	
Processing Time:	
	Save Back

Fig.5-108 Industrial Protocol Alarm Processing Page

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

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

5.5.3.3. Retrieve a log.

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

			M [®]		
Probe > Logs Management > ICS Protocol Alarm					
ICS Protocol Alarm					Show Processed Alarms
Probe: Please select • Src. MAC: Application Layer Protocol:Please select •	Probe: Dst. MAC: Search	Src. IP: Start Time: 2	2019-11-18 00:00:00	Dst. IP:	2019-11-18 23 59 59

Fig.5-109 Retrieving an Industrial Protocol Detection Alarm

5.5.4.No Traffic Alarm

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

5.5.4.1. Log list

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



Fig.5-110 No Traffic Alarm Menu



Prob	e > Logs Mana	agement > No-	Traffic Alarm									
No-Traf	ffic Alarm										Show Proc	essed Alarms
F	Probe: Please	select	٠	Probe:		Dst. P	ort:	Alarm Status: All	۲	Search		
No.	Src. IP	Dst. IP	Dst. Port	Protocol	Alarm Level	Status	No-Traffic Start Time	No-Traffic End Time	Processing Status	Probe	Probe IP	Operation
1	192.168.1.13/3 2	192.168.4.78/3 2	32	UDP	Warning	Alarming	2019-11-18 11:49:18		Unprocessed	Probe160824084	192.168.4.98	Process
2	3.3.3/3/32	0.0.0/0	32	TCP	Warning	Alarming	2019-11-18 11:49:18		Unprocessed	Probe160824084	192.168.4.98	Process
3	192.168.4.44/3 2	0.0.0/0	32	TCP	Warning	Alarming	2019-11-18 11:49:18	-	Unprocessed	Probe160824084	192.168.4.98	Process
4	192.168.1.13/3 2	192.168.4.78/3 2	32	UDP	Warning	Alarming	2019-11-18 10:57:44		Unprocessed	Probe160824084	192.168.4.98	Process
5	3.3.3/32	0.0.0/0	32	TCP	Warning	Alarming	2019-11-18 10:57:44		Unprocessed	Probe160824084	192.168.4.98	Process

Fig.5-111 No Traffic Alarm List Page

View all the log information on no traffic alarms here, with the meaning given below: Tab.58 Instruction to No Traffic Alarm Log Display

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

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed. Check <Show Processed Logs> on the right side of the [No Traffic Alarm] Whitelist Alarm List tab. (as shown in Fig.5-112):

Prob	Probe > Logs Management > No-Traffic Alarm											
No-Traf	-Traffic Alarm Show Processed Alarms 🕏											
F	Probe: Please select • Probe: Dst. Port: Alarm Status: All • Search											
No.	Src. IP	Dst. IP	Dst. Port	Protocol	Alarm Level	Status	No-Traffic Start Time	No-Traffic End Time	Processing Status	Probe	Probe IP	Operation
1	192.168.1.13/3 2	192.168.4.78/3 2	32	UDP	Warning	Alarming	2019-11-17 16:41:11		Closed	Probe160824084	192.168.4.98	🛃 View
2	3.3.3/32	0.0.0.0/0	32	TCP	Warning	Alarming	2019-11-17 16:41:11	-	Closed	Probe160824084	192.168.4.98	🛃 View
-	192.168.1.13/3	192.168.4.78/3			1010-010-0		2019-11-17		0	P	103.000.000	

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



5.5.4.2. Process a log.

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

Ø Probe > Logs Management > No-Traffic Alarm								
Logs Information Processing								
Probe:	Probe160824084							
Probe IP:	192.168.4.98							
Alarm Time:	2019-11-18 11:49:38							
Src. IP:	192.168.1.13/32							
Dst. IP:	192.168.4.78/32							
Transport Protocol:	UDP							
Alarm Level:	Warning							
No-Traffic Start Time:	2019-11-18 11:49:18							
No-Traffic End Time:	•							
Processing Status:	Unproce •							
Processing Time:								
Processing Opinions:								
	Save Back							

Fig.5-113 No Traffic Alarm Processing Page

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

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

5.5.4.3. Retrieve a log.

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

No-Traffic Alarm				
Probe: Please select •	Probe:	Dst. Port:	Alarm Status: All	▼ Search
		Fig.5-114		

5.5.5.Critical Event Alarm

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

Define the critical event in the system as follows:

1. Write operation of all industrial protocols:

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



5.5.5.1. Log list

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

Metwork Connection >
▲ Abnormal Traffic >
Statistical Analysis
🗟 Logs Management 🗸 🗸
Whitelist Alarm
ICS Protocol Alarm
▲ No-Traffic Alarm
Critical Event Alarm
Abnormal Traffic Logs
User-Defined Alarm
Net Session Logs
ICS Protocol Logs
Probe Run Logs
Fig.5-115 Critical Event Alarm Menu



Alarm Time Src. IP Src. Por Src. Port	1 Pro	obe > Logs Man	agement	> Critical Eve	nt Alarm											
Src. IAC: End Time Src. IP Src. Port Src. Port MAC Dst. IAC: Status Status Probe IP Operation 2015-11-16 192-158.16 . 50023 . 192-158.16 . 102 . TCP Sr7 Works Interno. Probe 10002 Probe 10002 Probe 10002 Probe 10002 . Probe 1002 . <	Critica	al Event Alarm												S	how Proces	ed Alarms
Alarm time Src. IP Device Src. Port MAC Dist. IP Device Ust. Port MAC Protocol Layer Protocol Level Status Prooe	App	Src. I	MAC:		•	Dst. MA	c:				00:00:00				9-11-18 23:59:5	9
2019-11-16 122 198.16 · 123 · 50023 · 122.168.16 · 102 · 102 · 102 · TCP S7 Product critical event allow event all	No.	Alarm Time	Src. IP		Src. Port	Dst. IP		Dst. Port			Description			Probe	Probe IP	Operation
	1			6	50023			102	TCP	\$7	protocol critical event alarm , function code : Request	Notice	Unprocessed			🛃 Process

Fig.5-116 Critical Event Alarm List Page

View all the log information on critical event alarms here, with the meaning given below: Tab.59 Instruction to Critical Event Alarm Log Display

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

AVCOMM Technologies Inc.

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



In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed. Check <Show Processed Logs> on the right side of the [Critical Event Alarm] critical event alarm list tab, view the processed log. (As shown in Fig.5-117):

Critica	I Event Alarm														s	how Process	sed Alarms
	Pr	obe: Plea	ise select	Ŧ		Probe	e:			Sr	c. IP:			Dst	IP:		
	Src. N	IAC:				Dst. MAG	:			Start 1	Time: 2019-08-05	00:00:00		End Ti	me: 2019	11-18 23:59:59	
Appl	ication Layer Prot	ocol: -Ple	ase select	٣		Sear	ch										
			0		0		D -1			T							
NO.	Alarm Time	Src. IP	Src. Device	Src. Port	Src. MAC	Dst. IP	Dst. Device	Dst. Port	Dst. MAC	Transport Protocol	Application Layer Protocol	Description	Alarm Level	Processing Status	Probe	Probe IP	Operat
	2019-11-16 16:06:04	192.168.2.2		49516		192.168.2.1		102		TCP	87	Violate S7 protocol critical event alarm , function code ;	Notice	Closed	Probe16082 4084	192.168.4.9	🛓 Vie

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

5.5.5.2. Process a log.

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

Probe > Logs Management > Critical Event Alarm > Process	
Logs Information Processing	
Probe:	Probe160824084
Probe IP:	192.168.4.98
Alarm Time:	2019-11-16 16:06:04
Src. IP:	192.168.2.200
Dst. IP:	192.168.2.1
Src. MAC:	-
Dst. MAC:	-
Description:	Violate S7 protocol critical event alarm , function code : PLC Stop
Transport Protocol:	TCP
Application Layer Protocol:	S7
Alarm Level:	Notice
Processing Status:	Closed
Processing Opinions:	999
Processing Time:	2019-11-17 17:01:18
	Back

Fig.5-118 Critical Event Alarm Processing Page

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

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

5.5.5.3. Retrieve a log.

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

Probe > Logs Management > Critical Event Alarm				
Critical Event Alarm				Show Processed Alarms 📓
Probe: Please select	Probe:	Src. IP:End Time:2019-11-18 23:59:59	Dst. IP: Application Layer Protocol:Please select	Src. MAC: Search

Fig.5-119 Retrieving a Critical Event Alarm

5.5.6.User-Defined Alarm

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

5.5.6.1. Log list

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

▲ Abnormal Traffic >
L Statistical Analysis
🗟 Logs Management 🗸 🗸
🗎 Whitelist Alarm
ICS Protocol Alarm
▲ No-Traffic Alarm
 Critical Event Alarm
Abnormal Traffic Logs
User-Defined Alarm
📋 Net Session Logs
ICS Protocol Logs
Probe Run Logs

Fig.5-120 User-defined Menu

2 Prot	be > Logs M	lanagement >	User-Defined A	Jarm													
User-D	efined Alarm															Show Pro	cessed Alarms
		Probe: Ple	ase select			Probe:			Src	. IP:		Dat IP:					
		c. MAC:				MAC:		Applic	ation Layer Prote	ocol: -Please select-	*	Start Time:	2019-11-18 00:0	00:00			
	E	nd Time: 20	19-11-18 23 59 5	9		Search											
No.	Alarm Time	Src. IP	Src. Device	Src. Port	Dst. IP	Dst. Device	Dst. Port	Src. MAC	Dst. MAC	Transport Protocol	Application Layer Protocol	Description	Alarm Level	Processing Status	Probe	Probe IP	Operation
1	2019-11-1 8 15:10:12	192.168.15.2 46		1500	192.168.15.2 37		102			TCP	\$7	Violate S7 user-defined rule alarm , Request Download	Caution	Unprocessed	Probe16082 4084	192 168 4 98	Proces s
2	2019-11-1 8 15:10:12	192.168.15.2 46		1500	192 168 15 2 37		102			TCP	S7	Violate S7 user-defined rule alarm , Upload	Caution	Unprocessed	Probe16082 4084	192 168 4 98	⊕ ^{Proces} s

Fig.5-121 User-defined Alarm List Page



View all the log information on user-defined alarms here, with the meaning given below: Tab. 60 Instruction to User-defined Alarm Log Display

Column Names	Instructions						
Alarm Time	Time when a	n alarm occurs					
Src. IP	The IP addre	ss initiating a data request, in dotted decimal format					
Src. Port	The port use	d by the machine initiating the data request					
Src. Device	The system a	automatically generates a source device name according to the					
	source IP, su	pporting custom source device name					
Dst. IP	The destinati	on IP requesting data, in dotted decimal format					
Dst. Device	The system a	automatically generates a destination device name according to					
	destination I	P, supporting custom destination device name					
Dst. Port	The port used by the requested destination machine						
Transport Protocol	The protocol type of transport layer used by the message						
Application Layer	Specific appl	lication types					
Protocol							
Src.Mac	The destinati	on MAC address requesting the data					
Dst. MAC	The destinati	on MAC address requesting the data					
Alarm Level	Warning of p	possible damage levels					
Probe	An intelliger	nt monitoring terminal name that is generated by the system or					
	named by us	ers, which is easy to remember					
Probe IP	The IP addr	ess assigned by the intelligent monitoring terminal, in dotted					
decimal format							
Operation	Process Further processing of alarm information						

In addition to displaying all unprocessed alarms, users can also view historical alarms that have been processed. Check <Show Processed Logs> on the right side of the [User-defined Alarm] user-defined alarm list tab, view the processed log. (As shown in Fig.5-122):



ser-D	Alarm															Show Pro	cessed Alarm
		c.MAC:	se select 9-11-18 23 59 56	•	Dst	Probe: MAC: Search		Applic	Sro don Layer Prob	. IP:	×	Dst. IP: Start Time:		0.00			
				Src. Port	Dst. IP	Dst. Device	Dst. Port	SIC. MAC	Dst. MAC	Transport Protocol	Application Layer	Description	Alarm Level	Processing	Probe	Probe IP	Operatio
io.	Alarm Time	Src. IP	Src. Device	SIC POIL	DOL 11						Protocol			Status			

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

5.5.6.2. Process a log.

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

Probe > Logs Management > User-Defined Alarm Logs	
Logs Information Processing	
Alarm Time:	2019-10-31 12:32:36
Src. IP:	192.168.1.101
Src. Port:	6147
Dst. IP:	192.168.3.65
Dst. Port:	502
Src. MAC:	
Dst. MAC:	
Transport Protocol:	TCP
Application Layer Protocol:	MODBUS
Alarm Level:	Caution
Probe:	Probe160824021
Probe IP:	192.168.15.194
Processing Status:	Unproci 🔻
Processing Opinions:	
Processing Time:	
	Save Back

Fig.5 -123 User-defined Alarm Processing Page

5.5.6.2.1. **Close the log.**

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

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

5.5.6.2.2. Export a message.

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



5.5.6.3. Retrieve a log.

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

Probe > Logs Management > User-Defined Alarm							
User-Defined Alarm							
Probe: Please select	Probe:	Src. IP:		Dst. IP:			
Src. MAC:	Dst. MAC:	Application Layer Protocol:	Please select v	Start Time :	2019-11-18 00:00:00		
End Time: 2019-11-18 23:59:59	Search						

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

5.5.7.Industrial Protocol Audit Log

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

5.5.7.1. Log list

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

Metwork Connection >
▲ Abnormal Traffic >
▲ Statistical Analysis >
👼 Logs Management 🛛 🗸
🗎 Whitelist Alarm
ICS Protocol Alarm
▲ No-Traffic Alarm
 Critical Event Alarm
Abnormal Traffic Logs
User-Defined Alarm
📋 Net Session Logs
🗎 ICS Protocol Logs
Probe Run Logs

Fig.5 -125 Industrial Protocol Audit Log Menu



Probe >	Probe > Logs Management > ICS Protocol Logs												
OP	c s	7	MODBUS	DNP3	IEC104	MMS	CIP	PROFINET	FINS SWIEE_T	CP SWIEE_UDP BACNE	r		
ICS Protoc	CS Protocal Loga												
Probes Probes Probes Dist. IP: Dist. IP: Dist. Prot. Dist. Prot. Probesci: Interface: Prease select ▼ Filter DCOM; No ▼ Interface: Prease select ▼ Blast Time: 2015-10-31 00 00 00 End Time:											23:59:59 Sear		
No.	Alarm Time	Src. IP	Src. Device	Src. Port	Dst. IP	Dst. Device	Dst. Port	Protocol	Interface	Operation	Probe	Probe IP	Operation
1	2019-10-31 14:01:08	192.168.10.8 7	-	1529	192.168.10.35		1042	TCP	unknown DCOM interface :0000 01430000000c000000000000 046	unknown operation code :5	Probe160824021	192.168.15.19 4	Filter Current Flow
2	2019-10-31 14:01:08	192.168.10.8 7		1529	192.168.10.35		1042	TCP	unknown DCOM interface :0000 01430000000c00000000000 046	unknown operation code :5	Probe160824021	192.168.15.19 4	Filter Current Flow
3	2019-10-31 14:01:08	192.168.10.8 7		1529	192.168.10.35		1042	TCP	unknown DCOM interface :0000 01430000000c00000000000 046	unknown operation code :5	Probe160824021	192.168.15.19 4	Filter Current Flow
4	2019-10-31 14:01:08	192.168.10.8 7		1529	192.168.10.35		1042	TCP	unknown DCOM interface :0000 01430000000c00000000000 046	unknown operation code :5	Probe160824021	192.168.15.19 4	Filter Current Flow
5	2019-10-31 14:01:08	192.168.10.8 7	-	1529	192.168.10.35		1042	TCP	unknown DCOM interface :0000 01430000000c00000000000 046	unknown operation code :5	Probe160824021	192.168.15.19 4	Filter Current Flow

Fig.5 -126 Industrial Protocol Audit Log List Page

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

Tab.61 Instruction to Industrial Protocol Audit Log Display

Column Names	Instructions					
Alarm Time	The time to generat	e a log				
Src. IP	The IP address initi	ating a data request, in dotted decimal format				
Src. port	The port initiating a	data request				
Src. device	The system automa	tically generates a source device name according to the				
	source IP, supportin	g custom source device name				
Dst. IP	The destination IP r	equesting data, in dotted decimal format				
Dst. Device	The system automatically generates a destination device name according					
	destination IP, supporting custom destination device name					
Dst. port	The port used by the requested destination machine					
Protocol	The protocol type o	f transport layer used by the message				
Interface	The operation inter	face used by OPC				
Operation	The operation meth	od used by OPC				
Probe	An intelligent moni	toring terminal name that is generated by the system or				
	named by users, wh	ich is easy to remember				
Probe IP	The IP address ass	igned by the intelligent monitoring terminal, in dotted				
	decimal format					
	Filter Current	Filter the logs, only display all logs on flows to which				
Operation	Flow	the logs belong to				
	Export Logs	Export a log to the local computer				

AVCOMM Technologies Inc.

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



5.5.7.2. Retrieve a log.

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

ICS Protocol Logs								
Probe:		Probe IP:		Src. IP:		Dst. IP:		
Src. Port:		Dst. Port:		Protocol:		Interface:	Please select 🔻	
Filter DCOM:	No V	Interface:	Please select 🔹	Start Time:	2019-10-31 00:00:00	End Time:	2019-10-31 23:59:59	Search

Fig.5 -127 Retrieving an Industrial Protocol Audit Log

5.5.8.Network Session Audit Log

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

5.5.8.1. Log list

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



Fig.5 -128 Network Session Audit Log Menu



Probe > Logs Management > Network Session Audit																	
Net Session Logs																	
Probe: [Please select] Str. (P): Dat. (P): Str. Part: Dot. Port: Pr Stat Time: 2019-11-18 000:00 End Time: 2019-11-18 23 59:59 (P Add :: Search Message Download									Protocol:								
No.	Src. MAC	Src. IP	Src. Device	Src. Port	Dst. MAC	Dst. IP	Dst. Device	Dst. Port	Protocol	Start Time	End Time	OutPackets	InPackets	OutBytes	InBytes	Probe	Probe IP
1	6c:4b:90:92: 4d:b3	192.168. 4.61	Device15740 458592112	62445	01:00:5e: 7f:ff:fa	239.255.2 55.250	Device15740 458601785	1900	UDP		2019-11-18 1 9:28:27:8429 02	4	0	864	0	Probe160824 084	192.168.4.9
2	18:68:cb:04: e0:31	192.168. 4.2	Device15740 4596631625	55347	01:00:5e: 7f:ff:fa	239.255.2 55.250	Device15740 458601785	1900	UDP		2019-11-18 1 9:28:20.5823 71	2	0	360	0	Probe160824 084	192.168.4.9
3	4c:cc:6a:42:2 a:26	192.168. 4.95	Device15740 4613319329	62050	01:00:5e: 00:00:fc	224.0.0.2 52	Device15740 458592123	5355	UDP	2019-11-18 1 9:27:59.5532 13	2019-11-18 1 9:27:59.5532 13	2	0	140	0	Probe160824 084	192.168.4.98

Fig.5 -129 Network Session Audit Log List Page

View all the log information on network session audit logs, with the meaning given below:
Tab.62 Instruction to Industrial Protocol Audit Log Display

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



5.5.8.2. Retrieve a log.

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

@ Probe > Logs Management > Network Session Audit								
	Net Session Logs							
	Probe: Please select ¥ Start Time: 2019-11-18 00:00:00 E	Src. IP: Dst. IP: End Time: 2019-11-18 23:59:59 IP Addr.:	Src. Port: Search Message Download	Dst Port: Protocol:				

Fig.5 -130 Retrieving a Network Session Audit Log

5.5.8.3. Original message download

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

VP Probe > Logs Management > Network Session Audit				
Net Session Logs				
Probe: Please select	Src. IP: Dst. IP: Dst	Src. Port:	Dst. Port:	Protocol:

Fig.5 -131 Original Message Download Button

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

Probe > Logs Management	> Network Session Audit > Original Message Download	
Original Message Download		
Device IP:	Start Time: End Time:	Search
No.	Name	Operation
1	160824006_20191010141315 pcap	Download
	Back	

Fig.5 -132 Original Message Download Page

5.5.9.Intelligent Monitoring Terminal Run Log

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

5.5.9.1.Log list

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



Metwork Connection >
▲ Abnormal Traffic >
▲ Statistical Analysis >
👶 Logs Management 🛛 🗸
Whitelist Alarm
ICS Protocol Alarm
No-Traffic Alarm
 Critical Event Alarm
Abnormal Traffic Logs
User-Defined Alarm
🗎 Net Session Logs
ICS Protocol Logs
📀 Probe Run Logs



Probe	> Logs Managemen	nt > Probe Run Logs			
Probe Ru	in Logs List				
Pr	bbe: Please select	▼ Log Type: F	Please select V SI	tart Time: 2019-10-31 00:00:00 End Time: 2019-10-31 23:59:59	Search
No.	Probe	Probe SN	Probe IP	Content	Operation Time
No.	Probe Probe160824021	Probe SN 160824021	Probe IP 192.168.15.194	Content Engine configuration packet updating successfully	Operation Time 2019-10-31 12:07:13
No. 1 2					2019-10-31

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

View the information on all intelligent monitoring terminal run logs, with the meanings given below: Tab.63 Instruction to Intelligent Monitoring Terminal Run Log Display

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

AVCOMM Technologies Inc.

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



5.5.9.2. Retrieve a log.

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

∂ Probe > Logs Management > Probe Run Logs				
Probe Run Logs List				
Probe: Please select Log Type: Please select	Start Time: 2019-10-31 00:00:00 End Time: 2019-10-31 23:59:59	Search		



5.5.10. Abnormal Traffic Log

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

5.5.10.1. Log list

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







Probe > Logs Management > Abnormal Traffic Logs										
raffic Logs List										
Device Name: Device IP: Abnormal Type: Al * Start Time: 2019-11-18 00 000 End Time: 2019-11-18 23.99 59 Saavah										
Device Name	Device IP	Abnormal Type	Upstream Baseline Value	Upstream Actual Value	Downstream Baseline Value	Downstream Actual Value	Abnormal Time Period	Processing Status	Operation	
OPS_55_192.168.4.44	192.168.4.44	Outflow	1	1095	1	0	2019-11-18 15:25:01 To 2019-11-18 15:30:01	Unprocessed	Process	
OPS_ss_192.168.4.44	192.168.4.44	Outflow	1	1314	1	0	2019-11-18 15:20:01 To 2019-11-18 15:25:01	Unprocessed	Process	
OPS_ss_192.168.4.44	192.168.4.44	Outflow	1	1241	1	0	2019-11-18 15:15:00 To 2019-11-18 15:20:00	Unprocessed	Process	
	affic Logs List arrie: 2019-11-18 00 00 00 0 Device Name OP9_58_192 168 4.44 OP9_58_192 168 4.44	affic Logs List ame:Device IP; are:Device IP; 2019-11-18 00:00:00 End Time: _2019-11-1 Device Name Device IP OPS_Ist_192:168.4.44 OPS_Ist_192:168.4.44 OPS_Ist_192:168.4.44	attr: Logs List attr: Logs List attr:	Device Name Device IP: Abnormal Type: All OPB_sti_192.168.4.44 192.168.4.44 Outfour 1 OPB_sti_192.168.4.44 192.168.4.44 Outfour 1	Device Name Device IP: Abnormal Type: Ali OPB_sti_192.168.4.44 192.168.4.44 Outflow 1 1095 OPB_sti_192.168.4.44 192.168.4.44 Outflow 1 1095	Device IP. Abnormal Type: Admormal Type: <th col<="" td=""><td>Berice IP: Anomal Type: All ** Device IP: Anomal Type: All ** Device IP: Anomal Type: All ** Device IP: Anomal Type: Ma ** Device IP: Anomal Type: Sateth Device Name Device IP Anomal Type Device Mathematic Mathematis Mathematis Mathematic Mathematic Mathematic Mathematis Mathemat</td><td>Berke IP: Abnormal Type: Adversarial Type: Adversaria Type: Adversarial Type: Adversarial Type:</td><td>Device IP Anomini Type Advorment Type Centre 12 Device IP Advorment Type Centre Centre Device IP Advorment Type Processing Status 0PEI_35_152_158_4.44 192_158_4.44 Outflow 1 1055 1 0 2019-11-119_52.011 Upprocessed 0PEI_35_152_152_158_4.44 192_158_4.44 Outflow 1 1314 1 0 2019-11-119_52.01 Upprocessed 0PEI_35_152_152_152_152_152_152_152_152_152_15</td></th>	<td>Berice IP: Anomal Type: All ** Device IP: Anomal Type: All ** Device IP: Anomal Type: All ** Device IP: Anomal Type: Ma ** Device IP: Anomal Type: Sateth Device Name Device IP Anomal Type Device Mathematic Mathematis Mathematis Mathematic Mathematic Mathematic Mathematis Mathemat</td> <td>Berke IP: Abnormal Type: Adversarial Type: Adversaria Type: Adversarial Type: Adversarial Type:</td> <td>Device IP Anomini Type Advorment Type Centre 12 Device IP Advorment Type Centre Centre Device IP Advorment Type Processing Status 0PEI_35_152_158_4.44 192_158_4.44 Outflow 1 1055 1 0 2019-11-119_52.011 Upprocessed 0PEI_35_152_152_158_4.44 192_158_4.44 Outflow 1 1314 1 0 2019-11-119_52.01 Upprocessed 0PEI_35_152_152_152_152_152_152_152_152_152_15</td>	Berice IP: Anomal Type: All ** Device IP: Anomal Type: All ** Device IP: Anomal Type: All ** Device IP: Anomal Type: Ma ** Device IP: Anomal Type: Sateth Device Name Device IP Anomal Type Device Mathematic Mathematis Mathematis Mathematic Mathematic Mathematic Mathematis Mathemat	Berke IP: Abnormal Type: Adversarial Type: Adversaria Type: Adversarial Type: Adversarial Type:	Device IP Anomini Type Advorment Type Centre 12 Device IP Advorment Type Centre Centre Device IP Advorment Type Processing Status 0PEI_35_152_158_4.44 192_158_4.44 Outflow 1 1055 1 0 2019-11-119_52.011 Upprocessed 0PEI_35_152_152_158_4.44 192_158_4.44 Outflow 1 1314 1 0 2019-11-119_52.01 Upprocessed 0PEI_35_152_152_152_152_152_152_152_152_152_15

Fig.5 -137 Abnormal Traffic Log Page

View all the log information on abnormal traffic alarms here, with the meaning given below: Tab.64 Instruction to Whitelist Alarm Log Display

Column Names	Instructions			
Device Name	The name of d	evices abnormal in traffic		
Device IP	The IP of devi	ces abnormal in traffic		
Abnormal Type	The outflow of	r inflow traffic		
Upstream Baseline Value	The amount of	upstream traffic in the abnormal traffic baseline configuration		
Upstream Actual Value	The amount of upstream traffic actually occurred to the device			
Downstream Baseline	The amount of downstream traffic in the abnormal traffic base			
Value	configuration			
Downstream Actual	The amount of	f downstream traffic actually occurred to the device		
Value				
Abnormal Time Period The time of get		enerating abnormal traffic		
Confirmed	Confirm whether abnormal traffic has been processed			
Operation	Process Further process abnormal traffic			

5.5.10.2. **Process a log.**

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



Abnormal Traffic Processing					
Device:	OPS_ss_192.168.4.44				
Device IP:	192.168.4.44				
Abnormal Type:	Outflow				
Upstream Baseline Value:	1				
Upstream Actual Value:	1095				
Downstream Baseline Value:	1				
Downstream Actual Value:	0				
Abnormal Time Period:	2019-11-18 15:25:01 To 2019-11-18 15:30:01				
Confirm:	□ Yes				
Processing Opinions:					
	Save				

Fig.5 -138 Processing Abnormal Traffic

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

Device:	OPS_ss_192.168.4.44
Device IP:	192.168.4.44
Abnormal Type:	Outflow
Upstream Baseline Value:	1
Upstream Actual Value:	1095
Downstream Baseline Value:	1
Downstream Actual Value:	0
Abnormal Time Period:	2019-11-18 15:25:01 To 2019-11-18 15:30:01
Confirm:	er Yes
Processing Opinions:	

Fig.5 -139 Confirming Abnormal Traffic

5.6. System Configuration

5.6.1. Alarm Level Settings

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







Alarm Level								
Alarm type	Emergency	Caution	Critical	Error	Warning	Notice	Information	Debugging
Whitelist Alarm	•	۲	0	0	۲	0	٥	0
ICS Protocol Alarm	0	۲	0	•	۲	0	٥	0
No-Traffic Alarm	0	0	0	0	٠	0	•	0
Critical Event Alarm	0	۲	٥	0	۲	•	0	0
User-Defined Alarm	0	٠	0	•	۲	0	0	0
Save Restore Default								



5.6.2.Instruction to Alarm Levels

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

AVCOMM Technologies Inc.

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



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

5.7. Network Connection

5.7.1.Introduction to Functions

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

5.7.2. Network Connection Baseline Configuration

5.7.2.1. Introduction to functions

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

5.7.2.2. Rule configuration

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





Fig.5-142 Network Connection Baseline Configuration Menu

Probe > Network Connection > Connection Baseline						
Prompt: IP 0.0.0	0.0 means configuring all				⊕ Add	
No.	Src. IP	Dst. IP	Dst. Port	Ope	ration	
	0.0.0.0	0.0.0.0	0		Delete	
	0.0.0.0	0.0.0.0	0		Delete	
	0.0.0.0	0.0.0.0	0		Delete	
	0.0.0.0	0.0.0.0	0	•	Delete	
	0.0.0	0.0.0.0	0		Delete	
		Save Learning Dat	ta			

Fig.5-143 Network Connection Baseline Configuration Page

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

Probe > Network Connection > Connection Baseline

Prompt: IP 0.0.0.0 means configuring all

Fig.5-144 Rule Add Button



Probe > Network Connection > Connection Baseline						
Prompt: IP 0.0.0	I.0 means configuring all			⊕ Add		
No.	Src. IP	Dst. IP	Dst. Port	Operation		
	0.0.0.0	0.0.0	0	Delete Delete		
	0.0.0	0.0.0.0	0	Delete		
	0.0.0	0.0.0	0	Delete		
	0.0.0	0.0.0	0	Delete		
	0.0.0.0	0.0.0.0	0	Delete Delete		
		Save Learning	Data			

Fig.5-145 Rule Add Page

Tab.66 Instruction to Rule Fields

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

5.7.2.3. Learning Data

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

			Probe > Network Connection > Connection Baseline							
configuring all				⊕ Add						
Src. IP	Dst. IP	Dst. Port	Ope	eration						
0.0.0.0	0.0.0	0		Delete						
0.0.0.0	0.0.0.0	0		Delete						
0.0.0.0	0.0.0.0	0		Delete						
0.0.0.0	0.0.0.0	0		Delete						
0.0.0.0	0.0.0.0	0		Delete						
	0000	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	0000 0000 0 0000 0000 0 0000 0000 0 0000 0000 0 0000 0000 0 0000 0000 0	ADDO ADDO <th< td=""></th<>						

Fig.5-146 Learning Data Button



×

Learning Data

🖲 Pro	obe >	Network Connection > Learning Data	a		
Learn	ing Da	ata Prompt: Entries added through lea	ming data are automatically saved to t	he baseline list	
Sr	c. IP:	D	st. IP:		
Dst.	Port :	Sea	Add to network baseline		
	No.	Src. IP	Dst. IP	Dst. Port	
	1	192.168.10.100	192.168.10.160	502	
	2	192.101.1.1	192.101.1.2	44818	
	3	192.115.1.1	192.115.1.2	44818	_
_		100 100 1 1	100,100,10		

Fig.5-147 Learning Data Page

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

Learning Data
Probe > Network Connection > Learning Data
Learning Data Prompt: Entries added through learning data are automatically saved to the baseline list
Src. IP: Dst. IP:
Dst. Port : Add to network baseline

Fig.5-148 Learning Data Search

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

Learning Data Src. IP: Dst. IP: Dst. Port : 0 No Src. IP Dst. IP Dst. Port 192.168.10.160 192.168.10.100 502 1 192.101.1.1 192.101.1.2 44818 2 3 192.115.1.1 192.115.1.2 44818 192.108.1.2 44818 4 192.108.1.1 192.168.15.111 239.255.255.250 1900 5

Fig.5-149 Adding the Learning Data

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



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

Fig.5-150 Deleting the Learning Data

5.7.3. Network Traffic Baseline Configuration

5.7.3.1. Introduction to functions

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

5.7.3.2. Rule configuration

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



Fig.5-151 Network Traffic Baseline Configuration Menu

			-INDUSTRIAL	1 M [®] ⊤ —	
Probe > Net	work Connection > Traffic Baseline				
Prompt: IP 0.0.0).0 means configuring all				⊖ Add
No.	Src. IP	Dst. IP	OutBytes	InBytes	Operation
1	0.0.0.0	0.0.0	0	0	Delete
			Save		

Fig.5-152 Network Traffic Baseline Configuration Page

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

Prompt: IP 0.0.0.0 means configuring all

Fig.5-153 Rule Add Button

Prompt: IP 0.0.0 means configuring all <u>O Add</u> No. Src. IP Dst. IP OutBytes InBytes Operation	4	0.0.0.0	0.0.0.0	0	0		Delete	
	No.	Src. IP	Dst. IP	OutBytes	InBytes	Ope	ration	
	Prompt: IP 0.0.0.0	rompt. IP 0.0.0 means configuring all						
Ø Probe > Network Connection > Traffic Baseline	Probe > Netwo							

Fig.5-154 Rule Add Page

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

Table 67 Instruction to Rule Fields

5.7.4. Network Connection Diagram

5.7.4.1. Introduction to functions

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

5.7.4.2. Real-Time network connection diagram

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




Fig.5-155 Network Connection Diagram Menu

$\ensuremath{\mathfrak{V}}$ Probe > Network Connection > Network Connections					
Prompt: Alter entering the time period, the static history view will be displayed					
Start Time: End Time:	Src. IP: e.g. 127.0.0.1	Dst. IP: 0.9. 127.0.0.1	Dst. Port: Port range 0-65535	Dst. MAC: e.g. กรกรรร	Search
g ⁴ Display device IP address (Double-click the IP value to view the network connect	ion details.)				
Normal Connection Abnormal Connection					

Fig.5-156 Network Connection Diagram Page

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

🖓 Probe >	Network Connection > Network Con	onnections			
Prompt: Afte	er entering the time period, the static	history view will be displayed			
Start Time: Dst. Port:		nd Time:	Src. IP: e.g. 127.0.0.1 Search	Dst IP: e.g. 127.0.0.1	
	olay device IP address (Double-click the IP value 1				
				s	

Fig.5-157 Real Time Network Connection Diagram



5.7.4.3. Historical network connection diagram

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

Start Time: End Time:	Src. IP: e.g. 127.0.0.1 Dst. IP: e.g. 127.0.0.1
Dst. Port: Port range 0-65535 Dst. MAC: e.g. ff.ff.ff.ff.ff.ff	Search
Ibipley device IP address (Double-click the IP value to view the network connection details.) Image: Normal Connection Abnormal Connection	

Fig.5-158 Historical Network Connection Diagram

5.8. Abnormal Traffic

5.8.1.Introduction to Functions

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

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

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

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





5.8.2. Baseline Configuration

5.8.2.1. Introduction to functions

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

5.8.2.2. Rule configuration

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



Fig.5-160 Baseline Configuration Menu

Baseline Configuration	Device ID	Davies MAC	OutButen	I=Dutes	Add
No. Device	Device IP	Device MAC	OutBytes	InBytes	Operation

Fig.5-161 Baseline Configuration Page

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

线配置						ut薪 ⊕
			Fig.5-162 Rule	Add Button		
Probe > A	bnormal Traffic > Baselir	e Configuration				
Baseline Con	figuration					Add
No.	Device	Device IP	Device MAC	OutBytes	InBytes	Operation
				0	0	Delete
				0	0	Delete
				0	0	🛄 Delete

Fig.5-163 Rule Add Page



Tab.68 Instruction to Rule Fields

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

5.8.3. Abnormal Traffic Monitoring

5.8.3.1. Introduction to functions

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

5.8.3.2. Traffic monitoring

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



Fig.5-165 Abnormal Traffic Monitoring Page Filter device lists by device name or IP address. (As shown in Fig.5-166):



Fig.5-166 Filtering Function

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

Probe > Abnormal Trainc > Abnormal Trainc		
Abnormal Traffic		✓ Hiding and Searching
Name: Dev(ce15708671139091 19:100.179.31.142	Name: Device15706639533781 19-159.146.1.215	Hide Ports Device name or IP address Search Device List (Drag point to canvas)
Outhytes: 0 Inflytes: 0 Open Port: Haught	OutBytes: 1925 InBytes: 0 Gynn Fart: 137,138,61668,52583,54962 50794	 Device 1570840444952 Device 15708671139292 Device 15708671139518
Name: Decical37085711613045 19:104.356,33.142 Oxf3ytes: 0 Inflytes: 0 Open Port: Inaught	Nume: YML-fest-EM IP: 192.166.77.03 Color: Source Color Color: Source Color Color: Source Color Color: Source Color Color: Source Color Color: Source Color Color: Source Color: Source	Device 157085711394814 Device 157085711394814 Device 157085711397820 Device 157085711498956 Device 1570857114149132 Device 15708571161489 Device 15708571161348 Device 15708571161348 Device 15708571161348

Fig.5-167 Monitoring Page



5.9. Statistical Analysis

5.9.1. Historical Statistics of Network Traffic Messages

5.9.1.1. Introduction to functions

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

5.9.1.2. Statistical query

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



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



Historical Traffic	
Device IP: Contrast Device IP: Search Export All	Start Time: End Time:
Device :	Contrast Device :
IP Statistics Based On Number Of Messages (Hours) Start Time:, End Time:, Device IP:	IP Statistics Based On Number Of Messages (Hours) Start Time, End Time, Device IP:
ssages (num ber) stages (num ber)	

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

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

Ø	Probe > Statistical Analysis > Historical Traffic				
Hi	torical Traffic				
[Device IP: Contrast Device IP: Search Export All		Start Time: End Time:		
	Fig	.5-170 Data St	atistics of that Day		
	Device: IP Statistics Based On Number Of Messages (Hours) Start Time, End Time, Device IP:	=	Contrast Device: IP Statistics Based On Number Of Messages (Hours) Start Timer, End Timer, Device IP:	=	Contrast Device : Device : Device : Device : Device :
ges (number)		ges (number)			
Number Of Messa		dumber Of Messa			
-	Hours	h	Hours		
	Traffic-based IP Statistics (Hours) Start Time:, End Time:, Device IP:	Ξ	Traffic-based IP Statistics (Hours) Start Time.; End Time.; Device IP:	≡	
Of Traffic (8)		of Tarfic (8)			
Number C		Number C			
	Hours		Hours		

Fig.5-171 Data Statistics Based on days.

5.9.1.3. Export a statistical graph.

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

Device:			Contrast Device :	
IP Statistics Based On Number	Of Messages (Hours)		IP Statistics Based On Number Of Messag	es (Hours) 📄
Start Time:, End Time:			Start Time:, End Time:, Device IP:	
Number OT Messages (number)		umber Of Messages (number)		Export PNG File Export VPG File Export VPG File Export PDF File

Fig.5-172 Export to a Single Statistical Graph

	- INDUSTRIAL IT -	
Probe > Statistical Analysis	> Historical Traffic	
Historical Traffic		
Device IP :	Contrast Device IP: Start Time: Search Export All	

Fig.5-173 Export All Statistical Graphs

5.9.2. Network Real-Time Traffic

5.9.2.1. Introduction to functions

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

5.9.2.2. Real-time traffic

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



Metwork Connection	
▲ Abnormal Traffic >	
🎍 Statistical Analysis 🗸 🗸	
Historical Traffic	
Traffic Compare	
♣ Live Traffic	Þ
 ✤ Live Traffic S Packet Top N 	
🕲 Packet Top N	
Packet Top N Traffic Top N	

Fig.5-174 Network Real-time Traffic Menu





Fig.5-175 Network Real-time Traffic Page

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

5.9.3.Statistics of Number of Messages

5.9.3.1. Introduction to functions

IP statistics corresponding to the number of messages passing through.

5.9.3.2. Query the number of messages.

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



Abnormal Traffic	>
🏨 Statistical Analysis	~
📓 Historical Traffic	
Traffic Compare	
-∦- Live Traffic	
🖏 Packet Top N	
Packet Top N Traffic Top N	
🕢 Traffic Top N	

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

Probe > Statistical Analysis > Pack	cket Top N	
Packet Top N		
Columns Number: 10	Start Time: 2019-10-30 End Time: 2019-10-30 Search	
All 🔻		
	IP statistics based on the number of messages	=
	Start Time:2019-10-30, End Time:2019-10-30Number of All Messages	
000	Start Time 2015-10-30, End Time 2015-10-30Number of All Messages	
Contraction	Start Time 2015-10-30, End Time 2015-10-305/umder of All Maxinges	
çəquina) səferr	Start Time 2015-16-30, End Time 2015-16-305umBer of All Waxages	
Longonnij salitetning u	Start Time 2015-16-30, End Time 2015-16-30Number of All Maxages	
aber (in Messager (number)	Start Time 2015-10-30, End Time 2015-10-305umBer of All Maxinges	

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

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

- INDUSTRIAL IT-	
Packet Top N	
Columns Number: 10 Start Time: 2019-10-30 End Time: 2019-10-30 Search	
Al IP statistics based on the number of messages Receive South Content of All Managers	=
r	

Fig.5-178 Query the Number of Messages

5.9.3.3. Export a statistical graph.

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

@ Probe > Statistical Analysis > Packet Top N	
Packet Top N	
Columns Number: 10 Start Time: 2019-10-30 End Time: 2019-10-30 Search	
All	
IP statistics based on the number of messages	=
Start Time 2019-10-30, End Time 2019-10-30Number of All Messages	
	Export PNG File Export JPG File Export SVG File
	Export PDF File

Fig.5-179 Export a Statistical Graph

5.9.4. Traffic Statistics

5.9.4.1. Introduction to functions

The corresponding traffic based on IP statistics.

5.9.4.2. Query traffic

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



Fig.5-180 Traffic Statistics Menu

Probe > Statistical Analysis > Traffic	Top N
Traffic Top N	
Columns Number: 10	Start Time: 2019-10-30 End Time: 2019-10-30 Search
All	
	Traffic-Based IP Statistics
	Traffic-Based // Statistics EXact Time 2019-10-304 Traffic Exa
8	
Traffic 68	
nex of Traffic (0)	
1 6	

Fig.5-181 Traffic Statistics Page

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

- INDUSTRIAL IT-	
Probe > Statistical Analysis > Traffic Top N	
Traffic Top N	
Columns Number: 10 Start Time: 2019-10-30 End Time: 2019-10-30 Search	

Fig.5-182 Query Traffic

5.9.4.3. Export a statistical graph.

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

Probe > Statistical Analysis > Traffic Top N	
Traffic Top N	
Columns Number: 10 Start Time: 2019-10-30 End Time: 2019-10-30 Search	
All	
Traffic-Based IP Statistics Start Time 2019-10-30, End Time 2019-10-30AII Traffic	
there of the difference of the	Export PNG File Export JPG File Export SVG File Export PDF File
ther of	

Fig.5-183 Exporting the Current Statistical Graph

5.9.5.Port Statistics

5.9.5.1. Introduction to functions

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

5.9.5.2. Query port

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

			®
.	Network Connection	>	
A	Abnormal Traffic	>	
њ	Statistical Analysis	~	
1	Historical Traffic		
I	Traffic Compare		
	I∲ Live Traffic		
(🛐 Packet Top N		
(Traffic Top N		
(Port Top N		
	Alarm Event Statistics		
Ē	Logs Management	>	
I	Fig.5-184 Port Statistics Mer	nu	

Fig.3-184 Port Statistics Menu

Of Drohe > Statistical Analysis > Bott Top N

Port Top N			
Columns Number: 10 Start Time:	End Time:	Search Expert All	
All			
		IP-Based Port Statistics Start Time:, End Time All ports	=
Cragge			
Quantity Bia			

Fig.5-185 Port Statistics Page

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

Ø Probe > Statistical Analysis > Port T	bp N			
Port Top N				
Columns Number: 10	Start Time:	End Time:	Search Export All	
All				
			IP-Based Port Statistics Start Time, End Time All ports	=
			start time, end time.All ports	
y Blancher)				
Quarte				
			2	

	AVCOMM®	
Probe > Statistical Analysis > Port Top N		
Port Top N		
Columns Number: 10 Start Time: All Y All Y Stc. Port Dot. Port	End Time: Export Ad IP-Eased Port Statistics San Time, Do Time Al ports	Ξ
Gurrenty Restances	,	

Fig.5-186 Query Traffic

5.9.5.3. Export a statistical graph.

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

Probe > Statistical Analysis > Port Top N		
Port Top N		
Columns Number: 10 Start Time:	End Time: Search Export All	
All		
	IP-Based Port Statistics Start Time:, End Time All ports	
(sequence)		Export PNG File Export JPG File Export SVG File Export PDF File
(national) years		
	Fig.5-187 Exporting a Statistical Graph	

Port To	ip N						
Columns	Number:	10	Start Time:	End Time:	Search	Export All	
	All	•					
				IP-Based Port Statistics Start Time:, End Time:All ports			=
5							
antity (Number)							
)u ant							

Fig.5-188 Exporting All Statistical Graphs

5.9.6. Alarm Event Statistics

Probe > Statistical Analysis > Port Top N

5.9.6.1. Introduction to functions

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



Fig.5-189 Menu





5.9.6.2. Query data

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







5.9.6.3. Export a statistical graph.

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

	Statistical Analysis > Ala	arm Event Statistics			
Alarm Event	Statistics				
tart Time:	2019-11-12	End Time: 2019-11-18 Search	Export All		
		Alarm Event Statistics		Alarm Event Statistics	=
20k		Start Time:2019-11-12, End Time:2019-11-18		Start Time 2019-11-12, End Time: 2019-11-18 Unar-Defined Narm	
25k	25 180		Export PNG File Export JPG File Export SVG File	No-Traffic Alarm	
o 20k			Export PDF File	Warning of Protocol Visitation	
5 5 5 15k					
in mi					
		11 58	5		
Ok	Whitelist Alarm	Warning of Protocol Violation No-Traffic Alarm	User-Defined Alarm		
		Alarm Type		Whitalist Alarm	

Fig.5-192 Exporting a Statistical Graph



Fig.5-193 Exporting All Statistical Graphs

6. System Configuration

6.1. System Overview

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







6.1.1.System Overview Display

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





6.2. System Operation Log

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





SysLog Logs

Ø Management Platform > System Operation Logs > System Operation Logs						
Operation Log List						
Operation IP		User Plea	ase select 🔻	Log Source Please set	lect • Operatio	on Type Please select v
Start Time	2019-10-31	End Time 20	19-10-31	Search	Export	
No.	Time	User	Log Source	Operation Type	Operation IP	Content
1	2019-10-31 15:52:15	admin_zpf	Management Platform	Login	192.168.1.101	Login successfully
2	2019-10-31 15:32:34	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
3	2019-10-31 15:32:24	audit_lzz	Management Platform	Logout	192.168.1.205	Exit successfully
4	2019-10-31 15:32:14	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
5	2019-10-31 15:32:01	audit_lzz	Management Platform	Logout	192.168.1.205	Exit successfully
6	2019-10-31 15:10:07	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
7	2019-10-31 15:09:58	audit_lzz	Management Platform	Logout	192.168.1.205	Exit successfully
8	2019-10-31 15:09:47	audit_lzz	Management Platform	Login	192.168.1.205	Login successfully
9	2019-10-31 15:09:38	admin_lzz	Management Platform	Logout	192.168.1.205	Exit successfully

Fig.6-7 System Operation Log Page

6.2.1.Retrieve a Log

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

Management 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 Export

Fig.6-8 Query Conditions

6.3. Hard Disk Utilization Logs

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [Hard Disk Utilization Logs/Hard Disk Utilization Logs] in the left navigation bar, click Menu (as shown in Fig.6-9), display the hard disk utilization logs page on the right (as shown in Fig.6-10):



Fig.6-9 Hard Disk Utilization Logs Menu Bar

O Menagament Districm - Librar	1 Disk Utilization Logs > Hard Disk Utilization Logs		COMM®
	LOSK OURZAUUT LOGS > Hard DISK OURZAUUT LOGS		
Hard Disk Utilization Logs			
Start Time:	End Time : Mar	agement Platform IP: Search	
No.	Time	Management Platform IP	Description
1	2019-10-30 14:22:31	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 08:00:08	192, 168, 8, 249	Data store exceeds time threshold by 1 day, start auto clean
9	2019-10-30 07:00:05	192.168.8.249	Data store exceeds time threshold by 1 day, start auto clean

Fig.6-10 Hard Disk Utilization Logs Page

6.3.1.Retrieve a Log

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

Hard Disk Utilization Logs			
Start Time:	End Time :	Management Platform IP:	Search

Fig.6-11 Retrieve Conditions

6.4. System Restart Log

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [System Restart Logs/Hard Disk Utilization Logs] in the left navigation bar, click Menu (as shown in Fig.6-12), display the system restart log page on the right (as shown in Fig.6-13):

5		AVCOM	M
	ж	Topology Management	>
	B	System Overview	>
	₽	System Operation Logs	>
	<u> </u>	Hard Disk Utilization Logs	>
	3	System Reboot Logs	~
	t	System Reboot Logs	
		Database Backup Logs	>
	ŤŤĨ	System Configuration	>
	?	Unknown Device	>
	(1-1) ;;1	SysLog Logs	>



Image Management Platform > System Reboot Logs > System Reboot Logs						
System Reboot L	System Reboot Logs					
Start Time:	End Time :	Manager	nent Platform IP: Search			
No.	Time	Management 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	16.16.13	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			
44	2010 10 17 10:33:46	102 168 / 70	Quetam rahvot			

Fig.6-13 System Restart Log Page

6.4.1.Retrieve a Log

In the list page of system restart logs, the logs can be retrieved based on the conditions. (As shown in Fig.6-14):

System Reboot Logs			
Start Time:	End Time :	Management Platform IP:	Search
	Fig.6-14 R	Retrieve Conditions	



6.5. Database Backup Log

After successfully logging in the management platform as auditor, find [System Settings] in the above menu bar, click the button, then find [Database Backup Logs/Database Backup Logs] in the left navigation bar, click Menu (as shown in Fig.6-15), display the database backup log page on the right (as shown in Fig.6-16):

×	Topology Management	>
®	System Overview	>
¢	System Operation Logs	>
	Hard Disk Utilization Logs	>
5	System Reboot Logs	>
	Database Backup Logs	~
	👔 Database Backup Logs	
	Database Backup Logs System Configuration	>
ŧŧŧ		>

Fig.6-15 Database Backup Log Menu Bar

Management F	Management Platform > Database Backup Logs > Database Backup Logs					
Database Backup	Logs					
Start Time:	End Time		Search			
No.	Backup Time	Result	Operation Time	Number of Files	Number of PCAP Files	

Fig.6-16 Database Backup Log Page

6.5.1.**Retrieve a Log**

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

Database Ba	ickup Logs	
Start Time:	End Time :	Search
	Fig. 6-17 Retrieve Conditions	





6.6. System Configuration

6.6.1. Password Management

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

🔆 Topology Management >
H System Configuration V
🔒 Password Management
🌾 Data Storage Configuration
Protocol Parameter
👷 🏟 Protocol Parsing Engine
License Management
Device Management
🔁 Trusted Hosts
SysLog Configuration
🧶 USM Upgrade
⑦ Unknown Device >

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):

🧩 Topology Management >
₩ System Configuration V
🔒 Password Management
☆ Data Storage Configuration
Protocol Parameter
Protocol Parsing Engine
License Management
Device Management
Trusted Hosts
SysLog Configuration
🧶 USM Upgrade
⑦ Unknown Device >

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):





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



Management Platform > System Configuration	n > Password Management	
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:		
Change P	assword	

Fig.6-22 Password Management Page

6.6.1.1. Reset a password.

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

6.6.1.2. Modify the PIN

Modifying the PIN code allows the user to modify the PIN code of the USBKey already associated with the user. This feature is only available to users who have correctly installed the USBKey plug-in and are associated with the USBKey.

To modify the PIN code, download and install the USBKey plug-in. See Fig.6-23 for the download link url:

Management Platform > System Configuration > Pass	word Management
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 to	he plug-in to use the following functionality. <u>USBKey Download Link</u> !
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)

Fig.6-23 Modify a PIN Code Page

To modify the PIN code, please enter the correct old PIN code. The new PIN code and the repeated new PIN code must be the same. The PIN code must meet the following conditions: the password must contain upper- and lower-case letters, numbers and special characters, with a length of less than 8 characters and up to 16 characters. Click <Modify a PIN Code> to complete the operation of modifying a PIN code.

6.6.2. User Management

The management platform supports decentralized and hierarchical management, currently supporting users of four levels: system operator, configuration administrator and audit administrator. The system operator can create different users and assign different roles. The configuration administrator can manage configurations, and auditor can view all logs.



6.6.2.1. Information view

System operator logs in, click system configuration/user management in the left navigation bar (as shown in Fig.6-24), and enter the page of user management (as shown in Fig.6-25):



Fig.6-24 user administration menu

lanagemen	Download the US	BKey plug-in first to use the function of	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	e	g Bind USBKey
3	audit	Audit Administrator				Change Password	🔁 Edit Remarks	Bind USBKey
4	hyp_admin	Configuration Administrator				Change Password	C Edt Remarks	Bind USBKey
5	hyp_audit	Audit Administrator				A Change Password	C Edit Remarks	Bind USBKey
6	zmy_admin	Configuration Administrator				Change Password	C Edit Remarks	Bind USBKey
7	zmy_audit	Audit Administrator				A Change Password	🕑 Edit Remarks	Bind USBKey
8	guest_admin	Configuration Administrator				Change Password	🕑 Edit Remarks	(3 Bind USBKey
9	guest_audit	Audit Administrator				A Change Password	C Edit Remarks	Bind USBKey
10	wjy_admin	Configuration Administrator				A Change Password	P Edt Remarks	Bind USBKey



6.6.2.2. Add user.

Log in as the system operator, click <Add> on the right side of the [System Configuration/User Management] user list tab (as shown in Fig.6-26) to pop up the user add page (as shown in Fig. 6-27):

Management Platform	n > System Configuration > User Management	
User Management	Download the USBKey plug-in first to use the function of PIN code, <u>Download link</u> !	⊕ Add

Fig.6-26 User Add Button



Unifiedsecurity managementplatform > System Configuration > User Management					
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 Administrate 🔻				
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 charact	special characters (#@! \sim %^&*), 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				
	Save Submit all information and go back to the user list display				
		page			
Operation	Back	Ignore all modifications and go back to the user list display			
	page				

6.6.2.3. Modify a password.

Log in as the system operator, click < Modify a Password> under the operation column in the [User Management] user list, open the [User Management] user basic information modify page, modify the basic information on the user (as shown in Fig.6-28):



♥ Unified Security Management Platform > System Configuration > User Management					
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				
	Save Back				

Fig.6-28 Modify a Password Page

6.6.2.4. Modify a remark.

Log in as the system operator, click <Modify a Remark> under the operation column in the [User Management] user list, open the [User Management] user basic information modify page, modify the basic information on the user (as shown in Fig.6-29):

Unified Security Management Platform > System Configuration > User Management					
Modify User Basic Information					
User Name :	admin				
User Authority:	Configure Administrator				
Remarks:					
	Save Back				



6.6.2.5. Delete a user.

Log in as the system operator, click <Delete> under the operation column in the [User Management] user list, click <Save> to delete the user that is no longer in use.

6.6.2.6. Bind a USBKey

To bind the USBKey, please download and properly install the USBKey plug-in first, and insert the USBKey to be bound before it can be used properly.

Log in as the system operator, click <Bind a USBKey> under the operation list to be bound with the USBKey under [User Management] (as shown in Fig.6-30), enter the bind a USBKey page (as shown in Fig.6-31):



inagement	Download the US	8Key plug-in first to use the function of	of PIN code. Download link!					④ Add
ŧ0.	User Name	Authority Type	USBKey Information	Remarks	Creation Time		Operation	
1	admin	Configuration Administrator				Change Password	Edit Remarks	Bind USBKey
2	sysoperator	System Operator				C Edit Remarks		Bind USBKey
3	audit	Audit Administrator				Change Password	Edit Remarks	Bind USBKey
4	hyp_admin	Configuration Administrator				Change Password	C Edit Remarks	Bind USBKey
5	hyp_audit	Audit Administrator				A Change Password	Edit Remarks	Bind USBKey
	zmy_admin	Configuration Administrator				Change Password	Edit Remarks	Bind USBKey
7	zmy_audit	Audit Administrator				A Change Password	Edit Remarks	Bind USBKey
1	guest_admin	Configuration Administrator				Change Password	Edit Remarks	Bind USBKey
)	guest_audit	Audit Administrator				A Change Password	Edit Remarks	R Bind US8Key
0	wjy_admin	Configuration Administrator				Change Password	Edit Remarks	Bind USBKey
1	wjy_audit	Audit Administrator				A Change Password	Edit Remarks	Bind USBKey
2	ld_admin	Configuration Administrator				Change Password	Edit Remarks	Bind USBKey
3	ld_audit	Audit Administrator				A Change Password	Edit Remarks	Bind USBKey
4	1 admin	Configuration Administrator				A Change Password	PI Edit Remarks	P Bind USBKev

Fig.6-30 Bind a USBKey Button

Unified Security Management Platform > System Configuration > User Management						
Modify User Basic Information Download the USBKey plug-in first to	Basic Information Download the USBKey plug-in first to use the function of this page, <u>Download link</u> !					
User Name:	audit_lzz					
User Authority:	Audit Administrator					
USBKey List:	Please select Change the Alias Refresh List					
	Save Back					

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):

N	Modify USBKey Alias							
	Unified Security Management Platform >	System Configuration > User Management						
	Modify USBKey Alias							
	New alias:	(New alias length cannot not be greater than 15 characters)						
		Save Back						

Fig.6-32 USBKey Alias Modification Page

Enter the new alias, click <Save> and make it come into effect, go back to the bind a USBKey page; click <Back> and go back to the bind a USBKey page.

6.6.2.7. Unbind a USBKey

To unbind a USBKey, only operate for a user bound with a USBKey.

Log in as the system operator, click <Unbind a USBKey> under the user operation list with the USBKey to be unbound under [User Management] (as shown in Fig.6-33):

	L	8 1(8)				
71	audit_lzz	Audit Administrator	AA05553A9400355C	2019-10-30 09:42:05	Change Pass Z Edit Rema U Unbind USB Reset FIN c Dele word ris Key te			
Fig.6-33 Unbind a USBKey Button								
AVCOMM Technologies Inc. 333 West Loop North, Suite 460 Houston, TX 77024, USA info@avcomm.us www.avcomm.us								
242								



Click <Confirm> to unbind the USBKey. Click <Cancel> to cancel the operation, (as shown in Fig.6-34):

Prompt		×				
Are you sure individualized USBKey?						
	Confirm	Cancel				

Fig.6-34 Unbind a USBKey Confirm Page

6.6.2.8. Reset a PIN code.

71

To reset a PIN code, please download and properly install the USBKey plug-in first. Insert the USBKey with the user to be reset before it can be used properly.

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



Fig.6-35 Reset a PIN Code Button

Click to display the page as shown in Fig.6-36, click <Confirm>, reset the PIN code of the user's USBKey to the initial password, click <Cancel> to cancel the operation.



Fig.6-36 Unbind a USBKey Confirm Page

6.6.3.USBKey Management

The operation page is used to change an alias and reset a PIN code for USBKey. To use the functions, download and professionally install the USBKey plug-in. Log in as the system operator, click [System Configuration/USBKey Management] in the left navigation bar (as shown in Fig.6-37), enter the [USBKey Management] page (as shown in Fig.6-38):



Fig.6-38 USBKey Management Page

6.6.3.1. Change an alias.

After selecting a USBKey in the USBKey list, click <Change an Alias>, enter the USBKey alias modification page, (as shown in Fig.6-39):

Modify USBKey Alias		×		
Unified Security Management Platform > System Configuration > User Management				
Modify USBKey Alias				
New alias:	(New alias length cannot not be greater than 15 characters)			
	Save Back			

Fig.6-39 USBKey Alias Modification Page

Enter the new alias, click <Save> and make it come into effect, go back to the USBKey management page; click <Back> and go back to the USBKey management page.

6.6.3.2. Reset a PIN code.

After selecting a USBKey in the USBKey list, click <Reset a PIN Code>, click <Reset a PIN Code> to pop up the reset PIN code confirmation box, (as shown in Fig.6-40):



Fig.6-40 Reset a PIN Code Confirmation Box

Click <Confirm>, reset the PIN code of the user's USBKey to the initial password, click <Cancel> to abandon the operation.

6.6.4. Database Storage Cycle Configuration

It is used to configure the management platform database storage and backup cycle. Log in as the configuration administrator, click [System Configuration/Database Storage Cycle Configuration] in the left navigation bar (as shown in Fig.6-41), enter the [Database Storage Cycle Configuration] page (as shown in Fig.6-42):



Fig.6-41 Database Storage Cycle Configuration


Image Management Platform > System Configuration > Data Storage Configuration			
ata 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 Single-table data will be deleted will be deleted by the single-table data reaches the set value (1~50), the data of the earliest day will be deleted			
Audit multicast and broadcast Enable • messages			
Audit host security guarding Disable • messages			
Enable storage time When it is enabled, a delete operation will be performed if either of the space and storage time conditions is met threshold			
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

6.6.4.1.**Save**

Fill in the information according to the prompts. Click <Modify> first, then click <Save> to distribute the configuration. (As shown in Fig.6-43):

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	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	
Audit host security guarding messages	
Inable 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
Save	



6.6.5. Protocol Parameter Configuration

6.6.5.1. Introduction to functions

The whitelist configuration template often needs to use custom function codes and other addable fields. At present, the CIP drop-down menu can add such fields through custom items, but only support adding. In the



industrial firewall learning process, new custom fields used by users may be learnt. In this case, it is necessary to re-modify the field description and delete user-defined fields. To this end, the industrial firewall, through a dedicated protocol parameter configuration page, facilitates users to manage the specific features of some industrial protocols.

6.6.5.2. Protocol parameter configuration

Log in as the configuration administrator, click [Whitelist Management/Protocol Parameter Configuration] in the left navigation bar (as shown in Fig.6-44), enter the [Protocol Parameter Configuration] page (as shown in Fig.6-45):



Fig.6-44 Selecting Protocol Parameter Configuration

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



Management Platform > Sys	tem Configuration > Protocol Parameter		
Dbject Configuration			● Add
No.	Object Number	Description	Operation
1	01H	Identity Object	
2	02H	Message Router Object	
3	03H	DeviceNet Object	
4	04H	Assembly Object	
ervice Configuration			⊕ Add
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 stan		
		objects	

Tab.66 Instruction to CIP Protocol Service Configuration Fields

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



	Delete	Delete user-defined CIP service, unable to delete CIP standard		
		service		
Tab.67 Instruction to CIP Protocol PCCCC Configuration Fields				
Column Names	Instructions			
CMD	The CMD number in a PCCC message embedded in the CIP protocol,			
	displayed i	n hexadecimal values		
FNC	The FNC	The FNC number in a PCCC message embedded in the CIP protocol,		
	displayed i	n hexadecimal values		
Description	The metho	od description uniquely determined by the CMD and FNC		
	combination in PCCC			
Operation	Modify Redefine the method uniquely determined by the CMD and FNC			
	combination, unable to modify the standard method defined by			
	PCCC			
	Delete Delete the user-defined method uniquely determined by the			
		CMD and FNC combination, unable to delete the standard		
		method defined by PCCC		

6.6.5.3. CIP configuration addition

Click <Add> on the right of each configuration list, <Add> in object configuration of (as shown in Fig.6-46), open the object configuration addition page (as shown in Fig.6-47):

Management Platform > System Configuration > Protocol Parameter				
CIP CIP E	EPATH IEC104			
Object Configuration				
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



E	Edit					×
	Protocol Par	ameter Con	figuration >	Edit CIF	P object	
	Object Number:	ACH				
	Description:	Vendor Specif	ic			
		Save	Back	c i		

Fig.6-47 CIP Protocol Object Configuration Addition Page

Please refer to 6.6.5.2 Protocol Parameter Configuration for the meaning of object number and description.

Click <Save> to save the added custom object to the backstage, and then skip to the protocol parameter configuration page.

Click <Back> to go back to the protocol parameter configuration page without saving the edited custom object.

6.6.5.4. CIP Configuration modification

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

6.6.5.5. CIP Configuration deletion

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

6.6.5.6. CIP EPATH Configuration addition

Click the tab and skip to the CIP EPATH configuration page (as shown in Fig.6-48), click <Add> to add a rule.

Management	Management Platform > System Configuration > Protocol Parameter					
CIP	CIP CIP EPATH IEC104					
No.	Dst.Ip	Dst.Mask	Encoding Format	Operation		
	0.0.0	0	padded v	Delete		
	Save					





6.6.5.7. CIP EPATH Configuration deletion

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

Managemer	Management Platform > System Configuration > Protocol Parameter					
CIP	CIP EPATH IEC104					
No.	Dst.lp	Dst.Mask	Encoding Format	Operation		
			с С			
	0.0.0.0	0	padded	Delete		

Fig.6-49 CIP EPATH Deletion Operation

6.6.5.8. CIP EPATH Configuration saving

m Configuration > Protocol Param

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

CIP CIP EPATH IEC104				
				Add
No.	Dst.Ip	Dst.Mask	Encoding Format	Operation
	0.0.0.0	0	padded ¥	Delete Delete
		Save		

Fig.6-50 CIP EPATH Saving operation.

6.6.5.9. IEC104 Configuration

O Manade

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

Management Platform > System Configuration > Prot	ocol Parameter	
CIP CIP EPATH IEC104		
Prompt: This is a global configuration that affects all industr	ial firewalls and audit	
Transmission Reason Length: 2 v	Public Address Length: 2 V	Message Body Address Length: 3 •



6.6.5.10. IEC104 Configuration saving

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

Management Platform > System Configuration >	Protocol Parameter			
CIP CIP EPATH IEC10	4			
Prompt: This is a global configuration that affects all in	dustrial firewalls and audit			
Transmission Reason Length: 2	Public Address Length:	2	Message Body Address Length:	3 *
		Save		
	Fig.6	5-52 IEC104 Sav	ing	

AVCOMM Technologies Inc. 333 West Loop North, Suite 460 Houston, TX 77024, USA | info@avcomm.us | www.avcomm.us 251



6.6.6. Decoding Engine Configuration

The configuration of the decoding engine allows users to conveniently and quickly define the supported private protocols, realize in-depth protocol resolving by uploading the engine configuration files, automatically generate the rule configuration interface and give an alarm.

Click [System Configuration/Decoding Engine Configuration] in the left navigation bar (as shown in Fig.6-53), enter the [Decoding Engine Configuration] page (as shown in Fig.6-54):



-INDUSTRIAL IT-						
Managen	nent Platform > System Configuration	> Protocol Parsing Engine				
Solect File Upload 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

6.6.6.1. Upload a decoding engine configuration file.

Click "Select a File" to select the preset decoding engine configuration file, click "Upload" to complete the configuration of private protocol (as shown in Fig.6-55):

Manager	@ Management Platform > System Configuration > Protocol Parsing Engine								
Se	Select File Upload								
Support Pro	otocol List : (After updating the decoding	engine inlease restart study function of a	lavicas)						
oupport inc	stocor cist . (Anter applating the decoding	engine, prease restart study function of	1011003.1						
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

6.6.6.2. Protocol parsing information display.

After successful resolving, the management platform displays the resolved private protocol information (as shown in Fig.6-56). Display fields, including protocol ID, protocol name, version number, upload time and usage status.

Soloct	File Heleod				
Select	File Upload				
port Protoco	I List : (After updating the decoding	engine, please restart study function of d	evices.)		
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

Fig.6-56 Protocol Resolving Information Display

6.6.7. Authorization Management

To authorize functions such as [Industrial Firewall], [Host Reinforcement] and [Monitoring Audit], click [System Configuration/Authorization Management] in the left navigation bar (as shown in Fig.6-57), enter the [Authorization Management] page (as shown in Fig.6- 58):







	AVCOMM [®]	
Management Platform > System Configuration > License Managemen	nt	
License Management		
Select a License File Start Uploading		
License Items :		
License Items	Status	Expiry Date
Industry Firewall	Licensed	Permanent
Host Security Guarding	Licensed	Permanent
B Host System Reinforce	Licensed	Permanent
Network Monitor and Audit	Licensed	Permanent

Fig.6-58 Authorization Management Page

6.6.7.1. Start upload.

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

6.6.8. Device Management

Device management is one of the important functions of the management platform, which provides a friendly interface to help users manage devices.

Log in as the configuration administrator, click [System Configuration/Device Management] in the left navigation bar (as shown in Fig.6-59), enter the [Device Management] page (as shown in Fig.6-60):



Fig.6-59 Device Management Menu



Managen	Imagement Platform > System Configuration > Device Management							
Device List								
Device Name:		Device IP:		Device MAC:		Device Type	Please select	▼ Search
No.	Device Name	IP Address	MAC Address	CPU(%)	Memory(%)	Traffic	Device Type	Operation
1	test1	192.168.1.11	88:88:88:88:88:88				Workstation	(ii) SNMP 🔣 View 🛛 Modify 🏢 Delete
2	Device15708671238759998	100.199.53.145	c4:ba:a3:00:09:b1		-		Unclassified	🐵 SNMP 民 View 🗹 Modify 🛅 Delete
3	Device15708671238739995	100.197.53.145	c4:ba:a3:00:09:b1		-		Unclassified	(ii) SNMP 🔣 View 🗹 Modify 🎁 Delete
4	Device15708671238729992	100.195.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	(ii) SNMP 🔣 View 🖉 Modify 🌐 Delete
5	Device15708671238709989	1.101.115.93	c4:ba:a3:00:09:b1		-	-	Unclassified	(ii) SNMP 民 View 🗹 Modify 🌐 Delete
6	Device15708671238699986	1.100.115.93	c4:ba:a3:00:09:b1		-	-	Unclassified	(ii) SNMP 民 View 🗹 Modify 🌐 Delete
7	Device15708671238679983	100.188.53.145	c4:ba:a3:00:09:b1	-	-	-	Unclassified	(ii) SNMP 民 View 🖉 Modify 🌐 Delete
8	Device15708671238659981	100.187.53.145	c4:ba:a3:00:09:b1		-	-	Unclassified	(ii) SNMP 民 View 🗹 Modify 🌐 Delete
9	Device15708671238649978	1.98.115.93	c4:ba:a3:00:09:b1			-	Unclassified	(ii) SNMP 民 View 🗹 Modify 🏥 Delete
10	Device15708671238629975	100.182.53.145	c4:ba:a3:00:09:b1		-	-	Unclassified	(ii) SNMP 民 View 🗹 Modify 🎁 Delete
11	Device15708671238619972	100.180.53.145	c4:ba:a3:00:09:b1		-		Unclassified	(ii) SNMP 民 View 🗹 Modify 🌐 Delete
12	Device15708671238599969	100.178.53.145	c4:ba:a3:00:09:b1				Unclassified	(ii) SNMP 民 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	Instruction	Instructions				
Device name	A device n	A device name that is easy to remember				
IP address	The IP add	The IP address assigned by the device, in dotted decimal format.				
MAC address	The MAC	address assigned by the device				
CPU (%)	The SNMF	P protocol obtains the device CPU utilization ratio information on				
Memory (%)	the current	IP address				
traffic	The SNMF	P 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					
	View	View more detailed information on the device				
Operation	Modify	Modify and set the device information				
Delete Delete a device						

6.6.8.1. SNMP Configuration

Click <SNMP Configuration> under the operation column in the [Device Management], display the detailed



information on SNMP configuration as shown in the following figure. (As shown in Fig.6-61):

SNMP conliguration information		
Device Name:	test1	
SNMP Version:	V1	v
Group Name:		Please fill in the group name corresponding to SNMP of the device, e.g.: public, private
Security Level:	No certification and no encrypt	tion 🔻
Certification Type:	MD5	v
Certification Key:		No certification, not editable
Encryption Type:	DES	v
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
	Test connect Save	Back

Fig.6-61 SNMP Configuration

6.6.8.2. Check a device.

Click <View> under the operation column of [device management] display list, display the detailed information on the device as shown in the following figure. (As shown in Fig.6-62):

$\ensuremath{\mathfrak{P}}$ Management Platform > System Configuration > Device Configuration	
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:	
	Back

Fig.6-62 Device Information View Page

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

6.6.8.3. Add a device.

Click <Add> on the right side of the [Device Management] device list tab to pop up the device add page. (As shown in Fig.6-63):



Management Platform > System Configuration > Device Management	
Device Basic Information	
Device Name:	*
IP Address:	
MAC Address:	· · · · · · · · · · · · · · · · · · ·
Device Type:	Unclassified T
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 T
User Name:	
Password:	
	Save Back

Fig.6-63 Device Add Page

Tab.69 Instruction to Device Add Information

Column Names	Instructions
Device name	A device name that is easy to remember
IP address	The IP address assigned by the device, in dotted decimal format
Device type	The purpose classification of the device, such as workstation and controller, etc.
Remarks	Optional, additional explanatory information

6.6.8.4. Modify a device.

Click <Modify> under the operation column in the [Device Management] device list, open the [Device Basic Information] to modify the basic information on the device (as shown in Fig.6-64):

Management Platform > System Configuration > Device Management	
Device Basic Information	
Device Name:	Device15708671238759998
IP Address:	100.199.53.145
MAC Address:	c4:ba:a3:00:09:b1
Device Type:	Unclassified T
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 T
User Name :	
Password:	
	Save Back

Fig.6-64 Device Basic Information Modification Page



6.6.8.5. Delete a device.

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

6.6.8.6. Retrieve a device.

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

$\ensuremath{\mathbb{Q}}$ Management Platform > System Configuration > Device Management			
Device List			● Add
Device Name: Device IP:	Device MAC:	Device Type: Please select	Search



6.6.9. Trusted Host

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

6.6.9.1. Information view

Log in as the configuration administrator, click [System Configuration/Trusted Host] in the left navigation bar (as shown in Fig.6-66), enter the [Trusted Host] page (as shown in Fig.6-67):





Management Platform > System Configuration > Trusted Hosts Add Add			• Add
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 AVCOMM Technologies Inc.

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



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		
	View	View more detailed information on the trusted host	
Operation	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):

Management Platform > System Configuration > Trusted Hosts		
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:		
	Back	

Fig.6-68 Trusted Host Information View Page

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

6.6.9.2. Add a host.

Click <Add> on the right side of [System Settings/Trusted Host] trusted host list tab (as shown in Fig.6-69) to pop up the trusted host add page (as shown in Fig.6-70):

Management Platform > System Configuration > Trusted Hosts	⊕ Add
Add Trusted Hosts List	
Fig.6-69 1	Frusted Host Add Button
Management Platform > System Configuration > Trusted Hosts	
Add Trusted hosts	
Hosts Name:	*
IP Address:	*
MAC Address:	□ (Verify MAC address; separate MACs with ":")
Remarks:	
	Save Back

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

6.6.9.3. Modify trusted host information.

Click <Modify> under the operation column in the [Trusted Host] trusted host list, open the [Trusted Host Basic Information] to modify the basic information on the trusted host (as shown in Fig.6-71):

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:	
	Save Back

Fig.6-71 Trusted Host Basic Information Modification Page

6.6.9.4. Delete a host.

Click <Delete> under the operation column of [Trusted Host] trusted host list to delete the trusted host that is no longer in use.

6.6.9.5. Retrieve a host.

In the [Trusted Host] trusted host list page, retrieve a trusted host according to the conditions. (As shown in Fig.6-72):

Add Trusted	Hosts List	
Hosts Name:	IP Address: Search	
Fig.6-72 Retrieving a Trusted Host		
AVCOMM Technologies Inc. 333 West Loop North, Suite 460 Houston, TX 77024, USA info@avcomm.us www.avcomm.us		



6.6.10. Syslog Configuration

6.6.10.1. Introduction to functions

Configure the IP address and port of syslog server, send the firewall alarm log and the whitelist alarm log that are generated by the industrial firewall device to the syslog server, which are divided into a common type and a grid type.

6.6.10.2. Save and enable the syslog service configuration.

Log in as the configuration administrator, click [System Configuration/syslog Configuration] (as shown in Fig.6-73), enter the syslog configuration page. (As shown in Fig.6-74):





		- INDUSTRIAL IT-
SysLog Configuration		
Server IP Address:	12	27.0.0.1
Server Port:	51	14
Syslog Type:	C	tommon type
		Save

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):

𝔅 Management Platform > System Configuration > SysLog Configuration		
SysLog Configuration		
Server IP Address:	127.0.0.1	
Server Port:	514	
Syslog Type:	Common type •	
Save		

Fig.6-75 Saving the syslog Configuration.

6.6.10.3. Save and enable the grid type syslog service configuration.

Select the grid type through syslog type, which requires a specified elect network card, select the network card and click <Save> to save and enable the syslog service. (As shown in Fig.6-76):

Management Platform > System Configuration > SysLog Configuration			
SysLog Configuration			
Server IP Address:	127.0.0.1		
Server Port:	514		
Syslog Type:	Power Grid Type		
Network card name and IP: Please select			
	Save		

Fig.6-76 Grid Type

6.6.11. Management Platform Upgrade

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

6.6.11.1. Management platform upgrade

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







6.6.11.2. Start upgrade.

After selecting the upgrade file, click <Start Upload>, check the progress of the progress bar. After successful

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



upgrade, access to the management platform. (A α shown in Fig. (80):

(As	shown	n in Fig.6-89):
pk	ease choose file]
sta	rt upload	

Fig.6-89 Start Upgrade

6.7. Topology Management

6.7.1.Introduction to Functions

Network topology management is a basis for the security management of the target system. To clarify the network topology of the customer system can not only find the existing security problems and hidden dangers of the customer system, but also have a very positive and important significance for subsequent security protection.

The management platform provides more professional device management tools and network topology management tools, which can help customers to carry out digital management of the existing device, and also allow customers to create and modify the current network topology of the system very easily.

6.7.2. Topology

The management platform provides a network topology management tool, which can easily form network topology diagram according to the current situation of the user system. Log in as the configuration administrator, display the network topology of the user system by default, click [Topology Management/Topology Management] in the left navigation bar (as shown in Fig.6-90), enter the [Topology Management] page (as shown in Fig.6-91):



Fig.6-90 Device Management Menu



Fig.6-91 Device Management Page

Log in as auditor, display the network topology of the user system by default, click [Topology Management/Topology Management] in the left navigation bar (as shown in Fig.6-92), enter the [Topology Management] page (as shown in Fig.6-93):



Fig.6-92 Device Management Menu



Ø Management Platform > Topology Management > Topology Management		
Full Screen Start Connecting Zoom Out Zoom in Mouse Zoom Save Topological Graph Export Select File Import	Please enter IP or device name!	earch All
Pay attention to "start connecting"; Click on the source device and the target device to connect them © Quadric Line	Drag point to canvas	
© Straight Line	Industry Firewall	>
Poly Line Curve	Probe	>
	Unclassified	>
EQ Protect Addition	Workstation	>
Probe168824921-Online Firew1119528083-Offline	Controller	>
	Network Device	>
Device15706571238146857	Server	>
testi		

Fig.6-93 Device Management Page

6.7.2.1. Composition of network topology

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

- Industrial firewall
- Intelligent monitoring terminal
- Workstation (including IEG)
- Controller
- Network device
- Server
- Unclassified

(As shown in Fig.6-94):

Please enter IP or device name!	Search All
Drag point to canvas	
Industry Firewall	>
Probe	>
Unclassified	>
Workstation	>
Controller	>
Network Device	>
Server	>

Fig.6-94 Topology Device List

6.7.2.2. Network topology device query

Query the device that meets the requirements according to the conditions, click <Search All> to execute the query (as shown in Fig.6-95):

192.168.1.11	Search All
Drag point to canvas	
Industry Firewall	>
Probe	>
Unclassified	>
Workstation	~
🔓 test1	
Controller	>
Network Device	>
Server	>



6.7.2.3. Edit a network topology.

It is very convenient to edit the topology.

> For the device

The user only needs to find the device to be added into the topology on the right device tree, click the small icon on the left of the device and drag it into the canvas to complete the addition of the device.

> For the connector

The user first selects the type of lines. Currently, there are the following types of connection lines:



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

Quadric Line
🔵 Straight Line
Poly Line
Curve

Zoom In

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

, but also supports zoom by mouse wheel:

Mouse Zoom

Save Topological Grap

to complete the

saving of the topology. The topology information can be normally viewed when logging in next time.

After editing the topology, the user clicks <Save Topology>, as shown:

6.7.2.4. Topology linkage

Topology management can not only view the network topology of the user system, but also view the number of alarms currently generated on the industrial firewall. Right-click and select View in the pop-up menu to view the detailed information on the device.

Right click on any device in the topology and click <Delete> in the pop-up menu to delete the device from the topology, with the corresponding connecting line deleted at the same time. Or right click on the connecting line, select <Delete> to delete the corresponding connecting line.

6.8. Unknown Device Detection

6.8.1. Unknown Device Detection Configuration

Log in as the configuration administrator, click [Unknown Device Detection/Unknown Device Detection Configuration] in the left navigation bar (as shown in Fig.6-96), enter the [Unknown Device Configuration] page (as shown in Fig.6-97):





Fig.6-96 Unknown Device Detection Configuration Menu Bar

💎 Manager	Management Platform > Unknown Device > Unknown Devices				
Unknown De	avices				
Enable®	Disable Working Mode: Lea	ming V Issue Refres	ih List		
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:tb:73:e3	2019-10-17 11:28:57		

Fig.6-97 Unknown Device Detection Configuration Page

6.8.1.1. **Distribute the configuration.**

Unknown device detection can be enabled or disabled. The working status must be selected after being enabled, which includes Learning, Detecting.

When selecting Learning, click <Distribute the Configuration> to generate the learning data, click <Refresh a List> to view the learned learning data. (As shown in Fig.6-98):



Ø Management Platform > Unknown Device > Unknown Devices				
Unknown Dev	vices			
Enable®	Ŭ.	lease select	esh List	
No.		earning NAC 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):

Manageme	nt Platform > Unknown Device > U	known Devices			
Unknown Devi	ces				
Enable®	Disable Working	Mode: Learning	▼ Issue	Refresh List	
No.	IP Address		MAC Address	Creation Time	
			Fig.6-99 Detecting	g	

Rule Edit

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

Management Platform > Unkr	nown Device > Unknown Devices				
Unknown Devices					
Enable® Disable©	Working Mode: Learning	Y	Issue	Refresh List	

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):

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

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):







😍 Manag	gement Platform > Unknown D	evice > Unknown	Devices Logs						
Unknown	Devices Log List						Show p	processed logs	
IP Address	Search	MAC Address:		Start Time:	2019-10-31 00:00:00	End Time :	2019-10-31 23:55	9:59	
No.	Access Time Invalid	IP	MAC	Ala	arm Information	Process	sing Status	Operation	
Total 0 F	Page(s) / 0 Record(s),Current Page 1						First Prev N	lext 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):

Management Platform > Unknown D	evice > Unknown	Devices Logs			
Unknown Devices Log List				Show	processed logs
IP Address: Search	MAC Address:		Start Time: 2019-10-31 00:00:00	End Time : 2019-10-31 23	59:59
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

6.8.1.2. Process a log.

Click <Process> under the operation column in the [Unknown Device Detection Logs] display list, display (as shown in Fig.6-105) the [Unknown Device Detection Logs] processing page:

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.



6.8.1.3. Retrieve a log.

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

Unknown Devices Log List			Show processed log	gs 🗆
IP Address:	MAC Address:	Start Time: 2019-10-31 00:00:00	End Time: 2019-10-31 23:59:59	
Search				

Fig.6-106 Retrieving an Unknown Device Detection Log

6.9. Syslog Log

Receive the syslog logs reported from other devices, click [Syslog Logs/Syslog Logs] in the left navigation bar (as shown in Fig.6-107), enter the [Syslog Logs] page (as shown in Fig.6-108):



Fig.6-107 syslog Log Menu



6.9.1.**Retrieve a Log**

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

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

Fig.6-109 Log Query