AVCOMM Industrial Ethernet Firewall
S2104
User Manual

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

AVCOMM Technologies Inc.

Industrial Ethernet Firewall
S2104

User Manual

About This Manual

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

NOTE:

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

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 info@avcomm.us. if you encounter any problems.

Table of Contents

Document Introduction

First of all, thank you for using AVCOMM industrial ethernet firewall!

The AVCOMM industrial ethernet firewall is a dedicated firewall device for industrial network perimeter protection with proprietary intellectual property rights, which is independently developed by AVCOMM. The device can effectively protect the information security of industrial control systems and equipment such as SCADA, DCS, PCS, PLC, and RTU. In addition to the security function of traditional firewalls, it also provides the built-in function of industrial communication protocol analysis and filtering and can adopt deep packet inspection technology and application layer communication tracking technology for industrial protocols to prevent illegal commands and block non-industrial control protocols in order to protect the controller.

This manual describes the usage of the AVCOMM industrial ethernet firewall in detail. The users could perform various management operations on the AVCOMM industrial ethernet firewall equipment according to this manual.

1 System Login and Registration

All management, configuration and monitoring of the AVCOMM industrial ethernet firewalls are completed on the WEB management platform.

1.1 Login

After the device starts, the industrial ethernet firewall without any security policy will work in the learning mode by default. In this state, the industrial ethernet firewall does not intercept any messages.

The management platform plugs the network cable into the MGMT port. The default management port IP address of the device is 192.168.4.2 for delivery. To access the industrial ethernet firewall through the management address https, the users need to log into the WEB management platform with the correct user credentials. The login interface and instructions are shown in Figure 1:

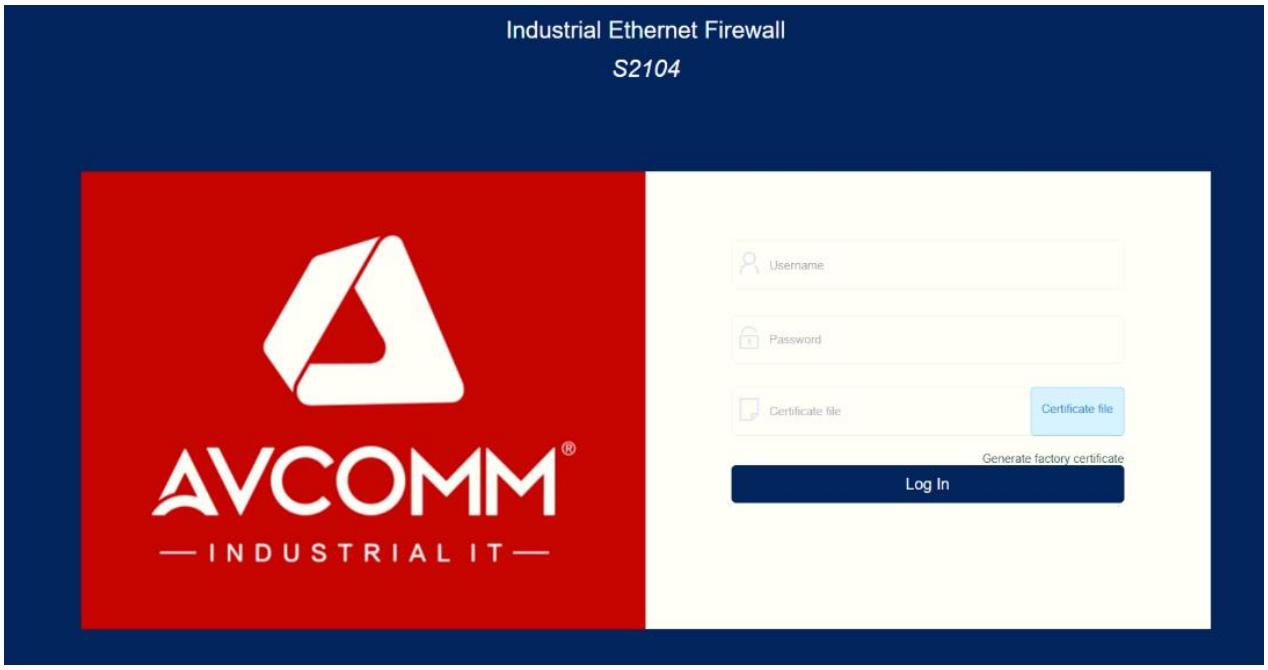


Figure 1

Name	Description
User name	A unique identifier used to distinguish user identities, created and maintained by a user with user management authority (such as sysuser, secuser, and loguser).
Password	User access password which can be modified by the user after correct login
Certificate file	The default users of the system need to import the factory certificate file to log into the system.

Generate factory certificate	Click to generate the factory certificate

Note: The default user names and passwords of the system are as follows:

- System administrator user name: sysuser, password: talent123
- Security administrator user name: secuser, password: talent123
- Audit administrator user name: loguser, password: talent123

The users can complete the first login using the "generate factory certificate" on the login interface and can use their own login certificates to log into the device. For details, refer to 8.5. The first login success interface of the WEB management platform is shown in Figure 2.

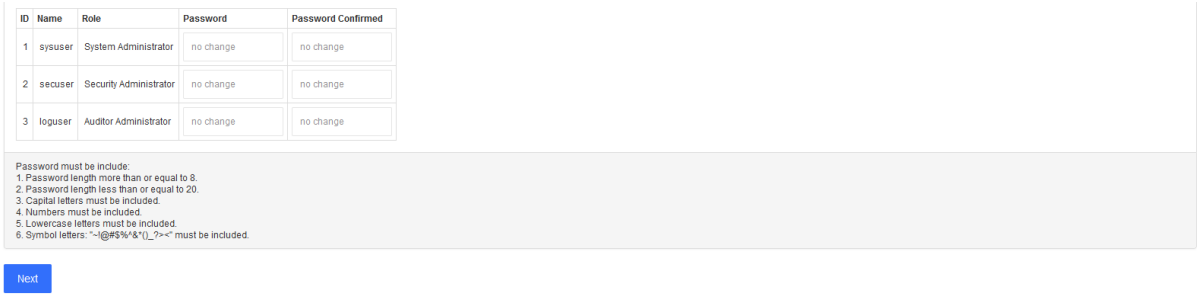


Figure 2

1.2 System setting wizard

The first login success interface of the industrial ethernet firewall is shown in Figure 2. It is recommended to modify the default administrator password in time after entering the system setting wizard. After the password is modified, click on the next page to enter the device setting. There are four working modes, and the default is the learning mode, as shown in Figure 3.

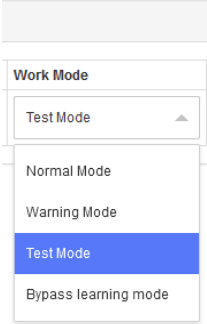


Figure 3

Name	Description
Learning mode	All packets can pass
Warning mode	All packets can pass, but a warning log will be recorded for abnormal packets matching the rules.
Protection mode	The packets are enabled and blocked according to rule matching, and those without rule matching are discarded
Bypass learning mode	Analyze the data packets mirrored to the interface

After completing the device setting, please click the next to enter the time setting, and directly click the next page if the system time is correct, as shown in FigureFigure 4.

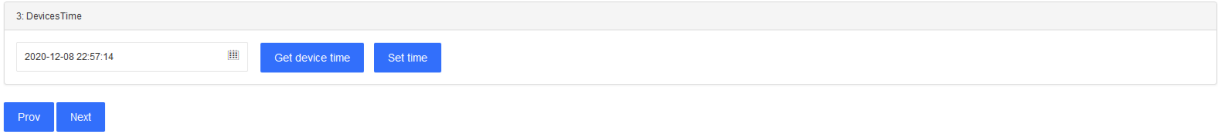


Figure 4

Click on the next page to enter the Syslog server setting. The users can choose to enable the Syslog server setting according to their needs. It is recommended that the users choose to enable the setting to monitor the industrial ethernet firewall's exception notifications and other details at any time, as shown in Figure 5:

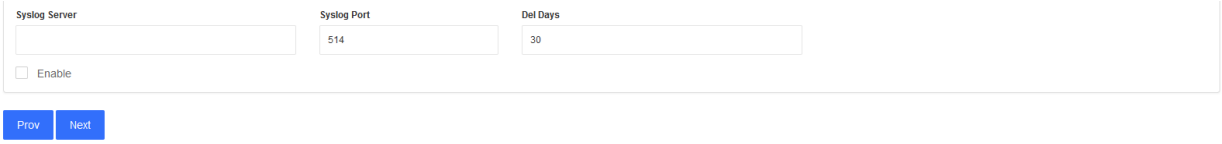


Figure 5

After completing the setting, enter the next page and click the exit wizard button to complete the configuration. The interface is shown in Figure 6:

Figure 6

1.3 Function area description

All business functions of the industrial ethernet firewall are selected through the function list of the interface, and the corresponding operations are performed in the main function operation area.

Taking this account as an example, the interface after logging into the system is shown in Figure 7:

- Operating area: Area module under current operation
- Function list: Module navigation bar

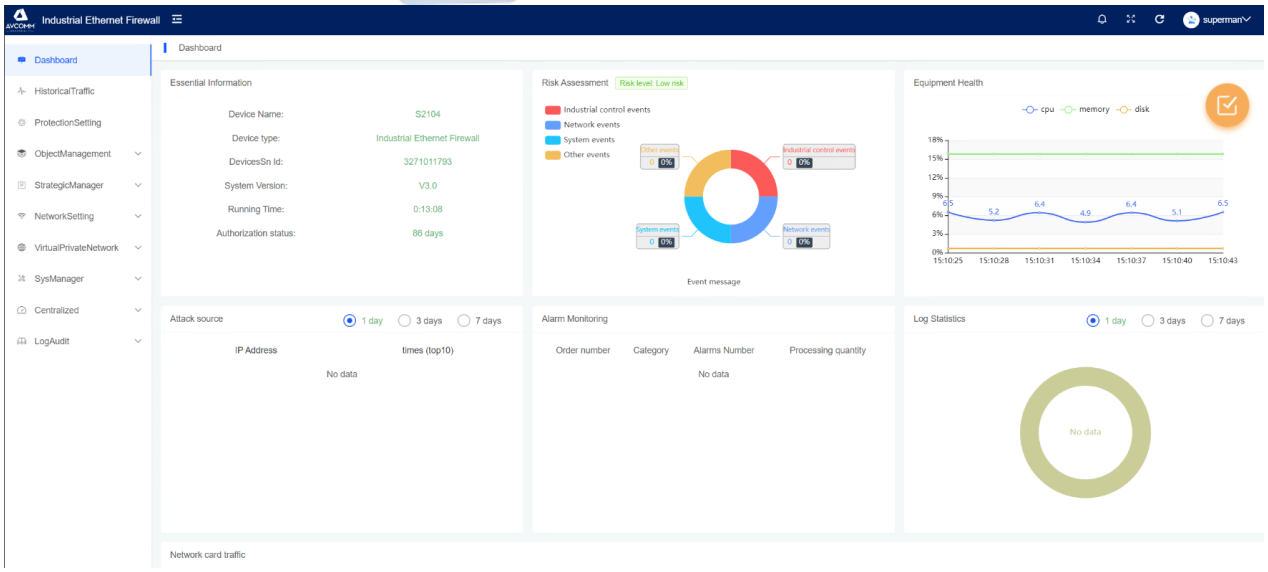


Figure 7

Click button of displayed modules to customize the modules for display, select the corresponding option and click Save to display the content of the selected option, as shown in Figure 8:

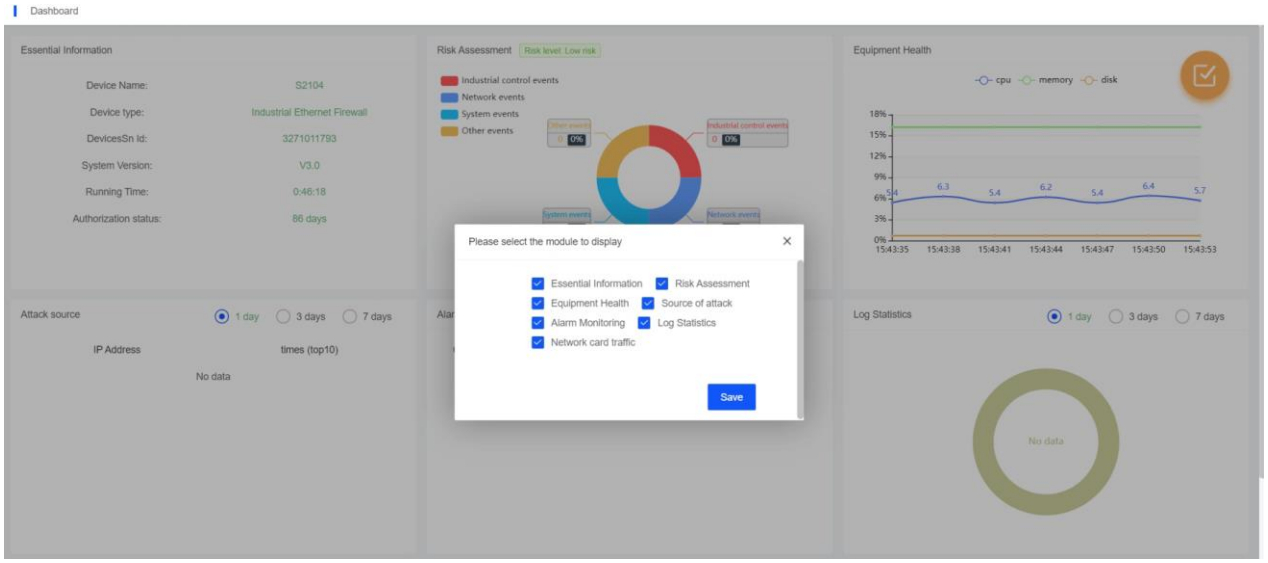


Figure 8

Name	Description
Network card traffic	Display real-time network data flow, data packets and bytes passing through the system
Essential Information	Display the name, model, serial number, system version, run time and remaining authorized days of the device
Risk assessment	Display the number and risk level assessment of industrial control events, network events, system events and other events
Equipment health	Display the usage status of the device's CPU, memory and disk

Source of attack	Display the statistical result of top10 blocked source IPs
Alarm monitoring	Real-time display of the alarm quantity and processing quantity of today's industrial control events, today's network events, today's other events as well as all industrial control events, all network events and all other events of the system
Log statistics	Count and display the percentage of warnings, prompts, and errors generated in the system with a pie chart

1.4 Log out

Click on the user name in the status bar and select logout to log out.

2 Historical Traffic

The system administrator (sysuser) can view the statistics of interface traffic in a day, the number of sessions in a day, the proportion of protocol traffic in a day, and the total device traffic statistics in a day, as shown in Figure 9:

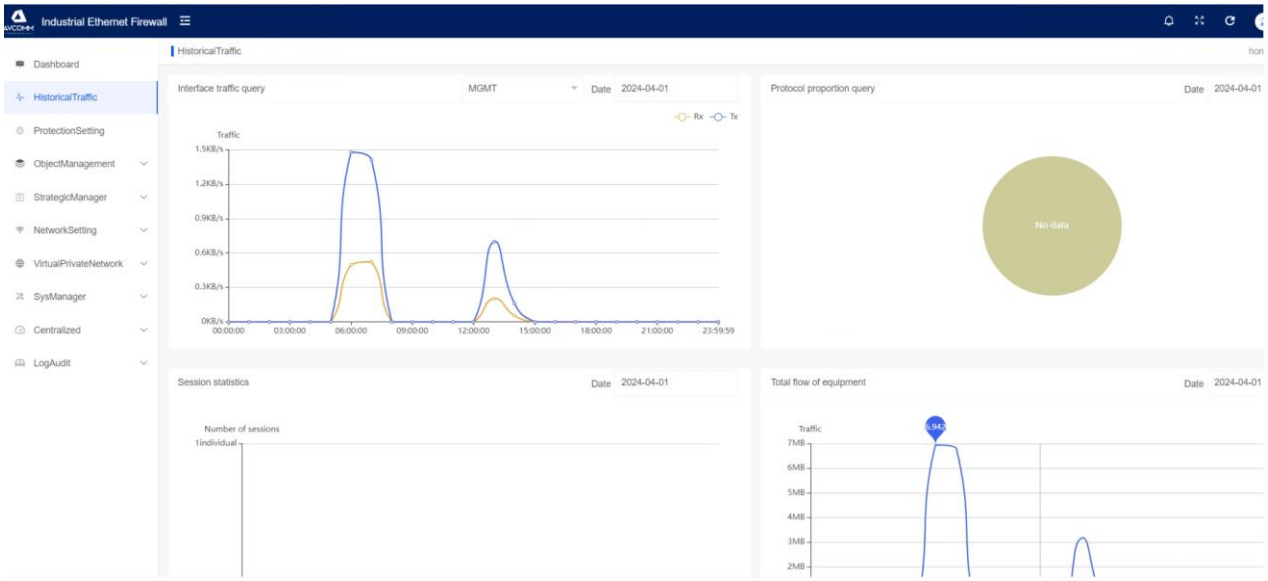


Figure 9

Name	Description
Interface traffic query	Make statistics on the traffic data of each interface within a day, and query the statistical results of historical dates
Protocol proportion query	Make statistics on the proportion of protocol traffic within a day, display it with a pie chart and query the statistical results of historical dates
Session statistics	Make statistics on the number of sessions generated by the system within a day and query the statistical results of historical

	dates
Total flow of equipment	Make statistics on the total traffic of all device interfaces within a day, and query the statistical results of historical dates

3 Protection setting

The protection setting includes three parts, namely Dos/DDos attack protection, abnormal data packet attack protection and scanning protection. It is enabled by default, as shown in Figure 10:

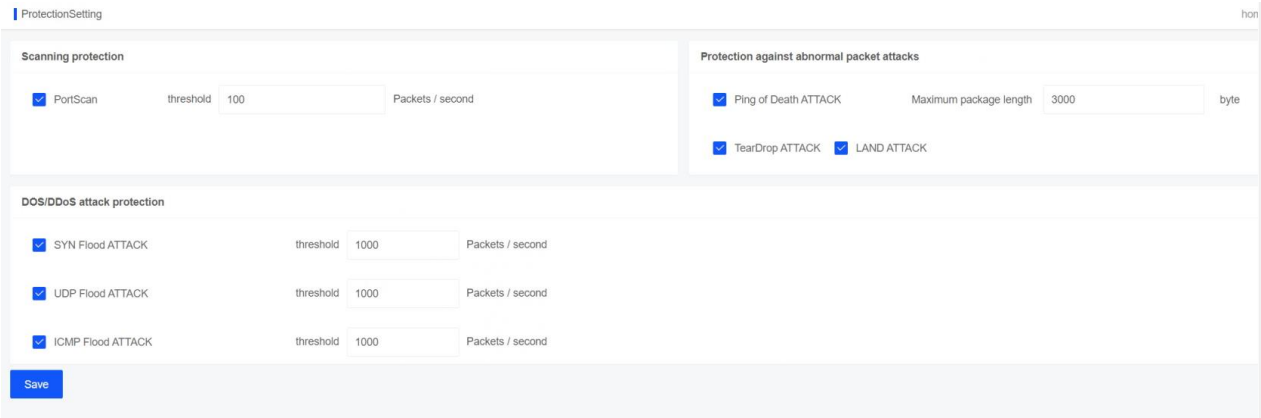


Figure 10

Name	Description
Dos/DDos attack protection	Support SYN Flood, UDP Flood and ICMP Flood attack protection, as well as setting thresholds
Protection against abnormal packet attacks	Support Ping of Death attack protection, and setting of packet length threshold; support TearDrop and LAND attack protection
Scanning protection	Support port scan protection and threshold setting

4 Object Management

The object management involves address objects, application objects, area objects, and time objects, which can be referenced by policies. When an object is referenced by industrial ethernet firewall policies, it cannot be deleted but can be edited.

4.1 Address object

The security administrator (secuser) manages the address resources which support the configuration of address objects and address groups. The input formats compatible with the address objects are host addresses, address fields, address ranges or their combinations. The operations such as adding, editing, deleting and bulk deletion can be performed on the page, as shown in Figure 11:

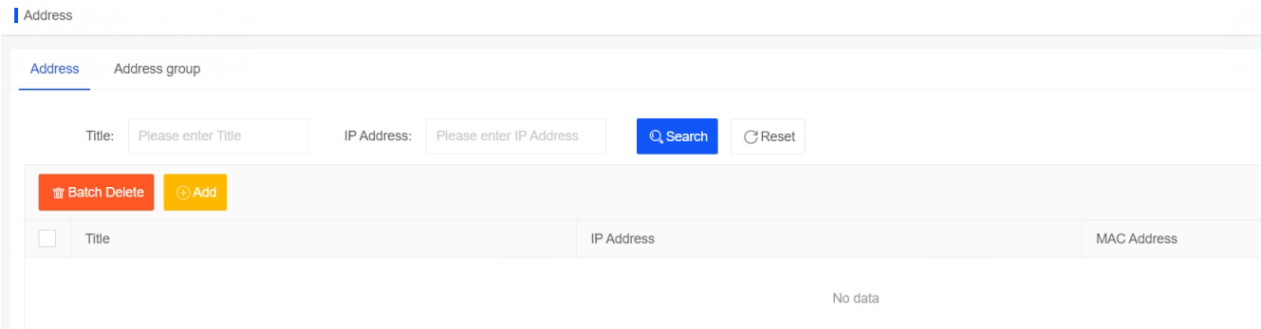


Figure 11

Click the Add button to add address resources and enter the address name. For the address object, simultaneously enter multiple IP addresses, IP address fields, or their combinations, as shown in Figure 12:

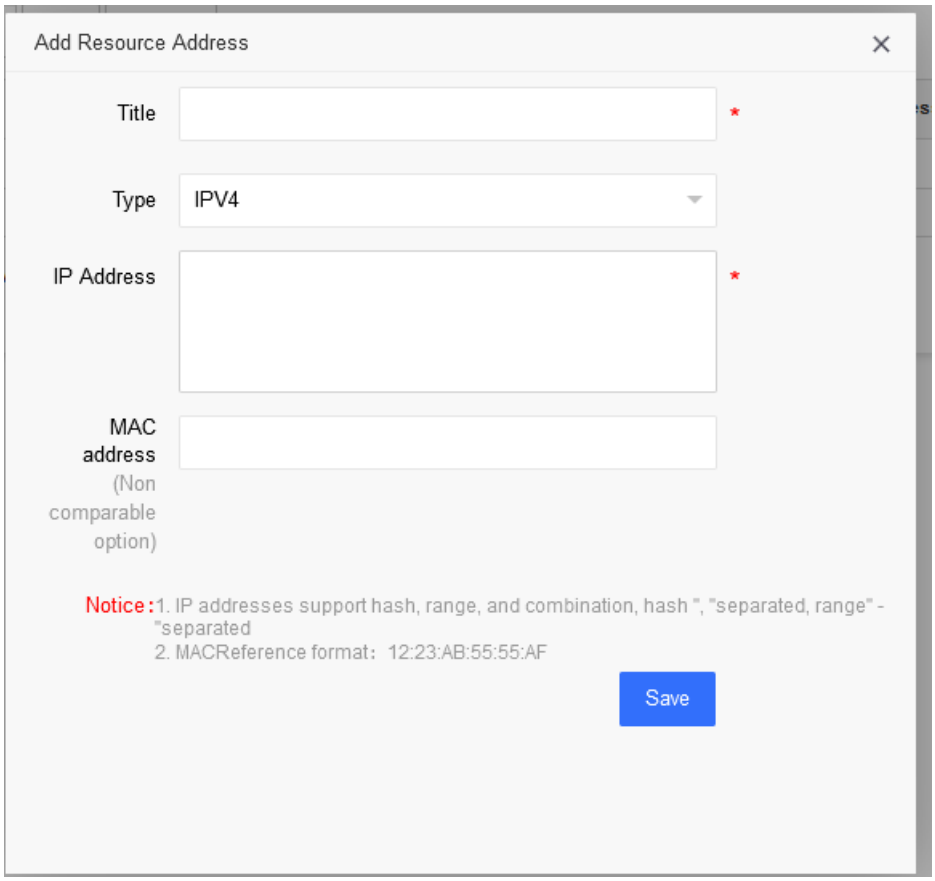


Figure 12

In addition, the administrator can also manage the address group. In the address group configuration interface, click Add to combine multiple address resources into one address group, as shown in Figure 13:

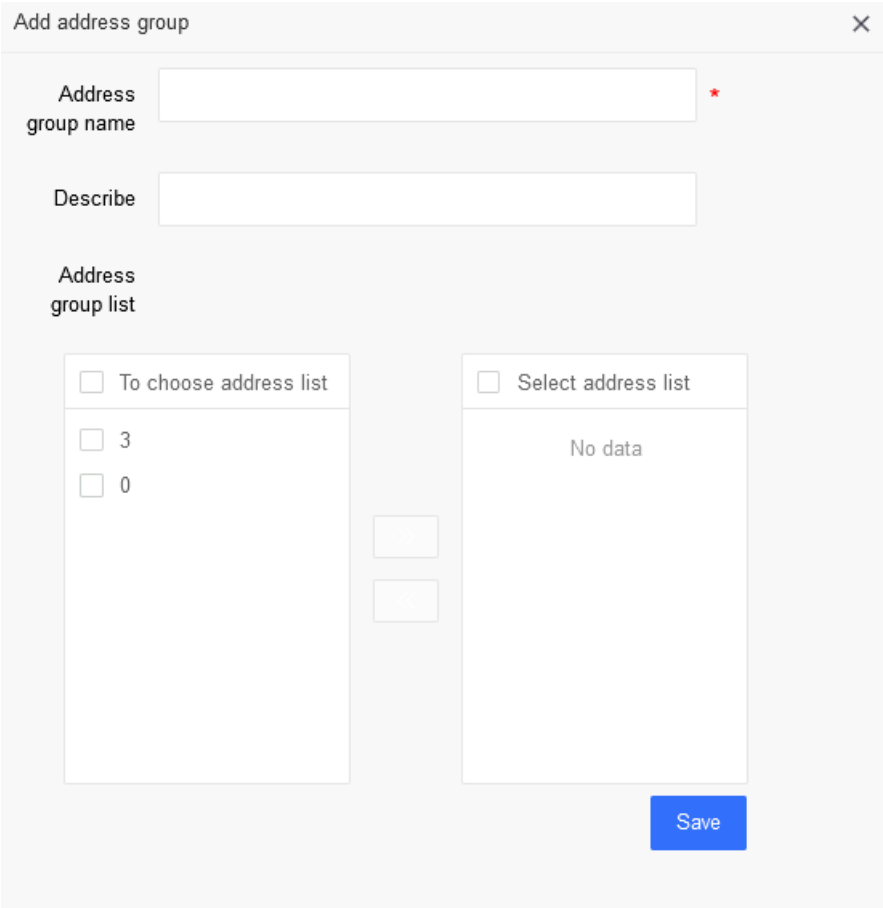
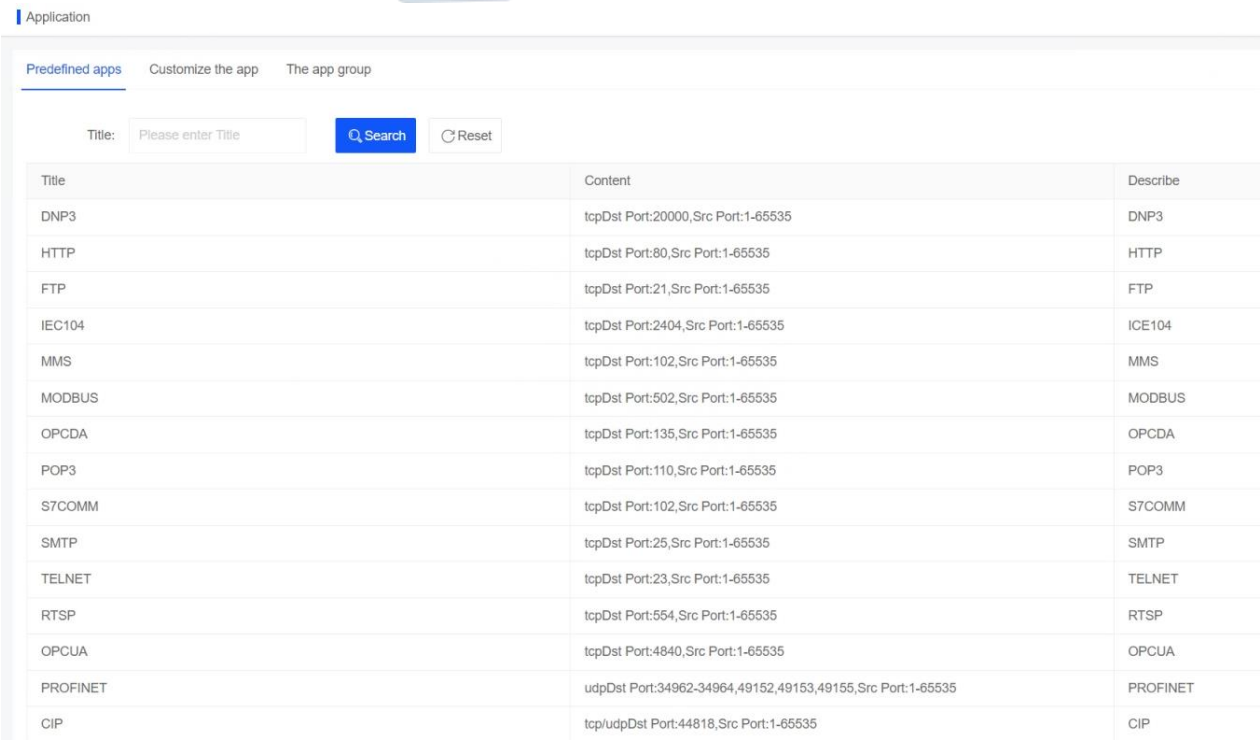


Figure 13

4.2 Application object

The application object supports the configuration of predefined applications, custom applications and application groups. The security administrator (secuser) can view the system's predefined application resources (which cannot be edited or deleted) in the predefined applications, and the operations such as add, edit and delete can be performed on the custom applications and application groups, as shown in Figure 14.



Title	Content	Describe
DNP3	tcpDst Port:20000,Src Port:1-65535	DNP3
HTTP	tcpDst Port:80,Src Port:1-65535	HTTP
FTP	tcpDst Port:21,Src Port:1-65535	FTP
IEC104	tcpDst Port:2404,Src Port:1-65535	ICE104
MMS	tcpDst Port:102,Src Port:1-65535	MMS
MODBUS	tcpDst Port:502,Src Port:1-65535	MODBUS
OPCDA	tcpDst Port:135,Src Port:1-65535	OPCDA
POP3	tcpDst Port:110,Src Port:1-65535	POP3
S7COMM	tcpDst Port:102,Src Port:1-65535	S7COMM
SMTP	tcpDst Port:25,Src Port:1-65535	SMTP
TELNET	tcpDst Port:23,Src Port:1-65535	TELNET
RTSP	tcpDst Port:554,Src Port:1-65535	RTSP
OPCUA	tcpDst Port:4840,Src Port:1-65535	OPCUA
PROFINET	udpDst Port:34962-34964,49152,49153,49155,Src Port:1-65535	PROFINET
CIP	tcp/udpDst Port:44818,Src Port:1-65535	CIP

Figure 14

Click the custom application to display the application list according to the custom rules, and click the Add button to add custom application resources, as shown in Figure 15:

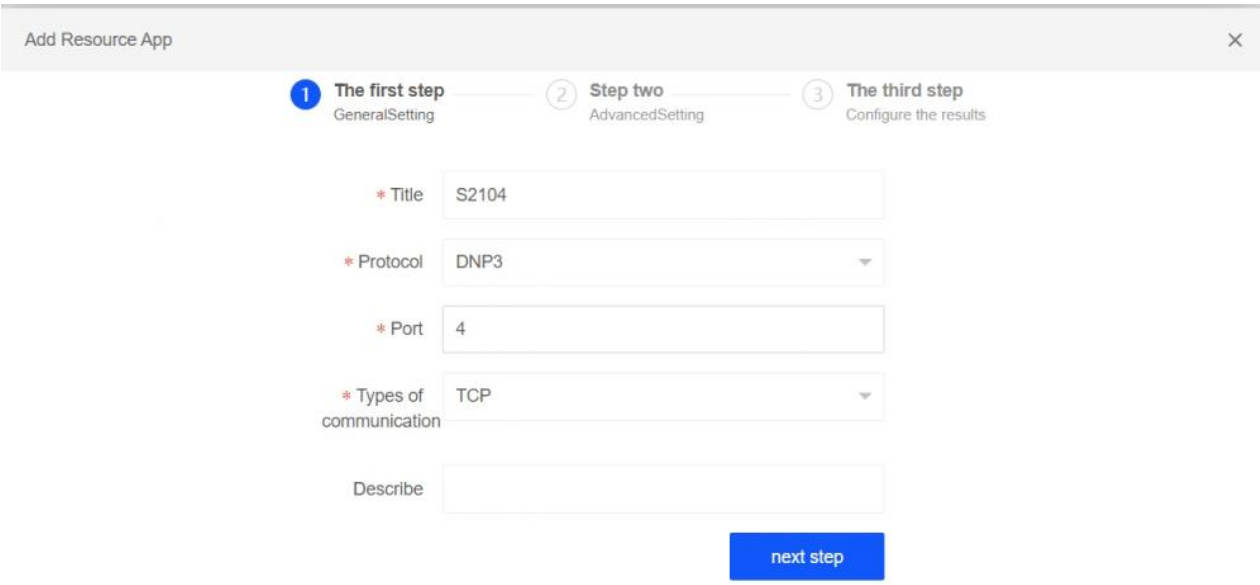


Figure 15

Name	Description
Title	Name of custom application
Protocol	Protocol types, such as MODBUS, DNP3, OPCDA and other protocols
Port	Custom port with a value ranges from 1 to 65535

Type of communication	TCP and UDP
Description	Description information of custom application with 1 to 32 characters in length

With respect to the configuration of MODBUS, complete the previous configuration and click the Next button to enter the advanced settings and configure in-depth analysis control of MODBUS application. The control supports the method, source address, destination address, etc., as shown in Figure 16:

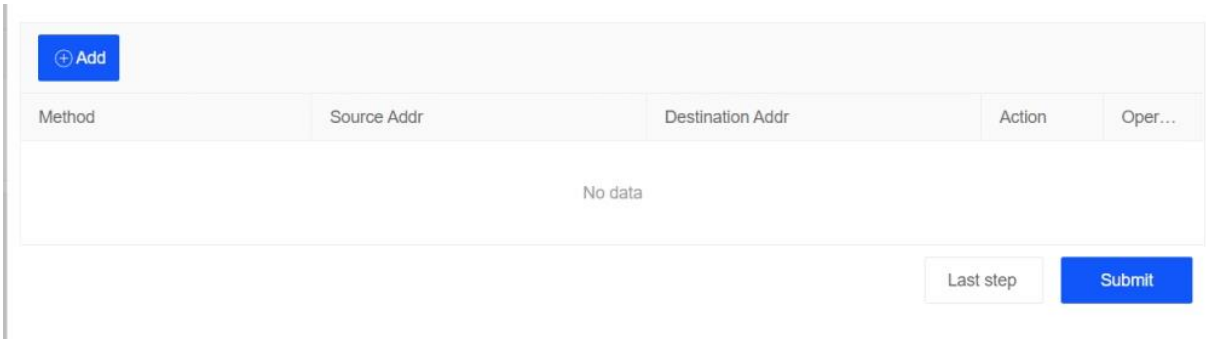


Figure 16

For configuring the service of a custom port, add a custom application, select "Custom Service" for the protocol, and click the Next button to configure the source and destination ports, as shown in Figure 17:

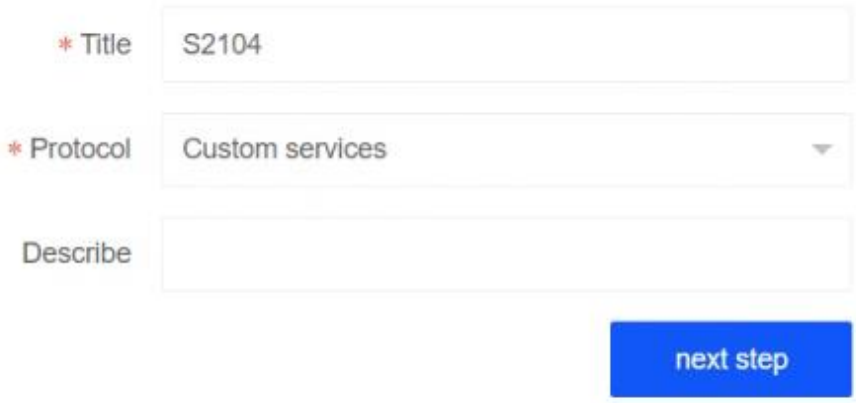


Figure 17

The user can customize TCP and UDP ports and configure the ICMP protocol. The port number is compatible with hash input, range input or combined format input, as shown in Figure 18:

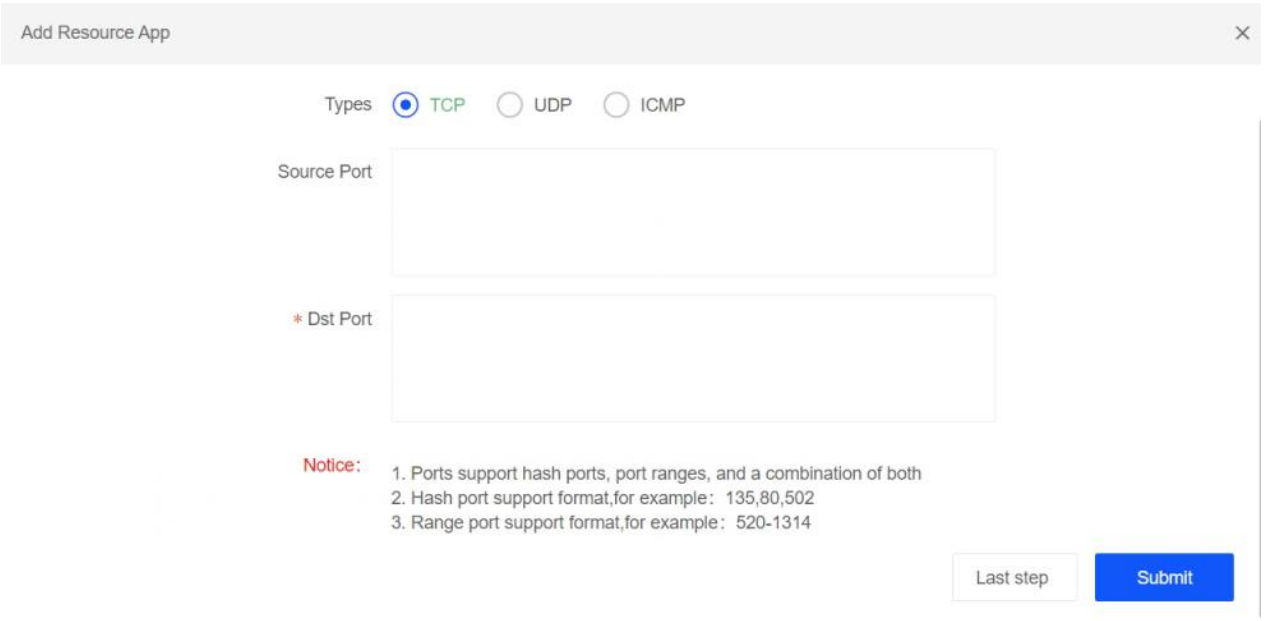


Figure 18

In addition, the administrator can also perform the operations such as adding, editing, and deleting application groups. Click the Add button to combine multiple application resources into an application group. Up to 10 applications can be added to an application group, as shown in Figure 19:

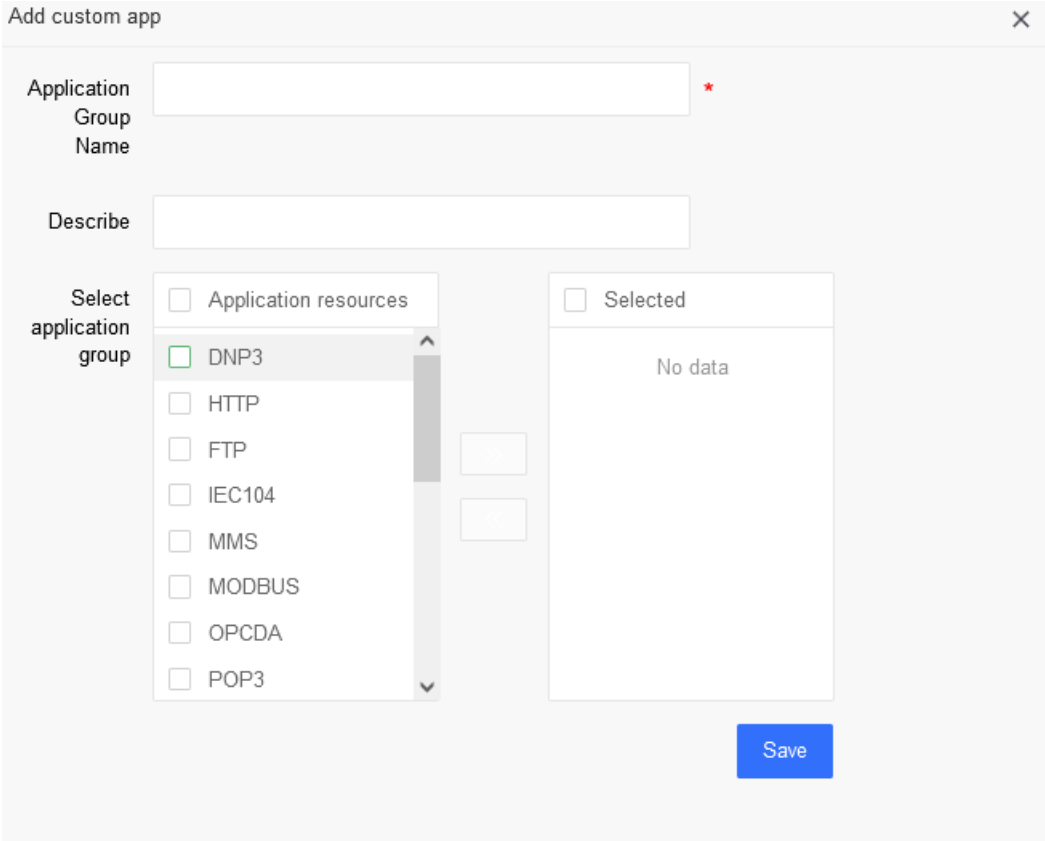


Figure 19

4.3 Regional object

The security administrator (secuser) manages area resources and can perform the operations such as editing, modifying, deleting, adding and so on. For ease of operation, the interfaces except the management port are added to the area by default, and the device has one interface per area. As shown in Figure 20:

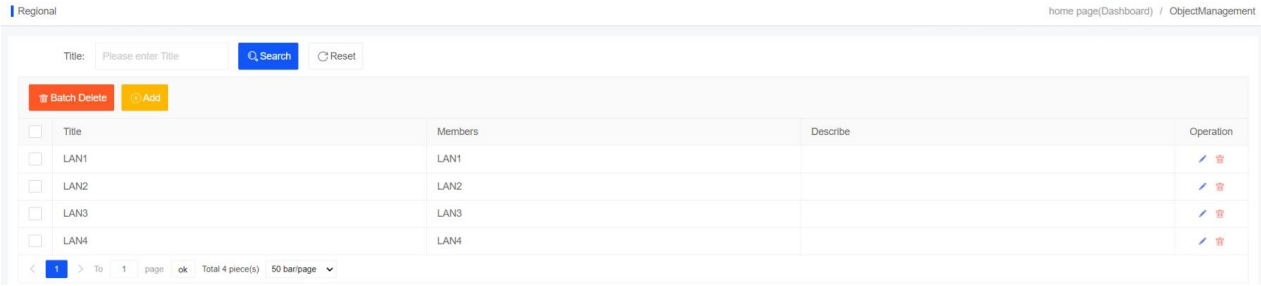


Figure 20

Note: For the area subject to policy references, the source and destination area objects are not allowed to be configured consistently

4.4 Time object

The security administrator (secuser) can manage the time resources and perform the operations such as editing, deleting, adding and so on. By default, the device has two-time objects, including an arbitrary time object "always" and a weekly cycle time object "weekly", which cannot be edited or deleted, as shown in Figure 21:

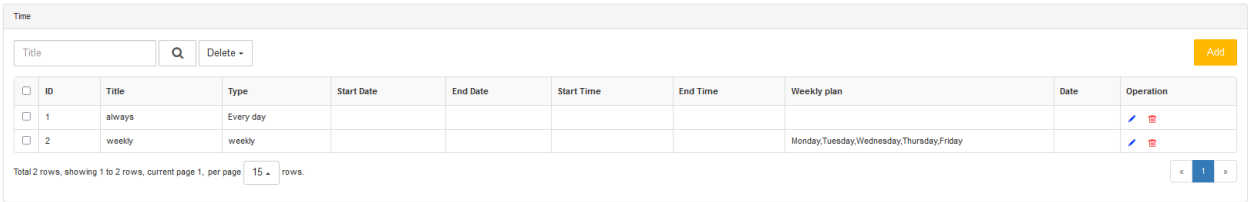


Figure 21

Click the Add button to pop up the add page and add custom time resources. Available time types for input include fixed time and periodic time. The periodic time can be configured to daily, weekly and monthly cycle, as shown in Figure 22:

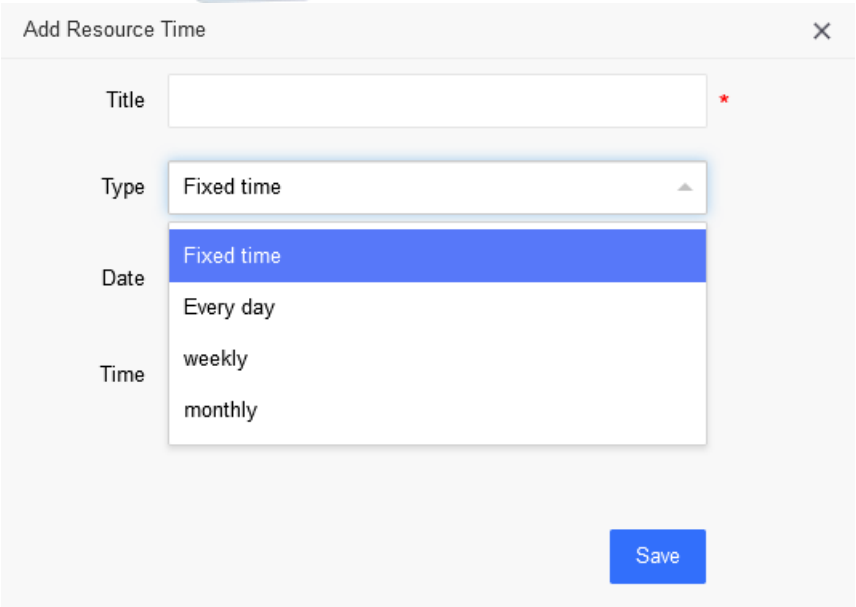


Figure 22

5 Policy Management

5.1 Policy configuration

The security administrator (secuser) can perform policy configuration management, and can perform the operations such as adding, editing, deleting, and moving. The configured policy is only available when the device works in the "protection mode".

In the protection mode, a policy can be selected for the data packet according to the application, source and destination address, source and destination area, and time object. When the policy action is blocking, the data packet will be discarded; when the policy action is allowing, the data packet will be accepted and forwarded.

Click the Add button to pop up the Add Strategy interface, edit the name, application, action and other configuration items of the policy, and click Save after finishing the configuration, as shown in Figure 23:

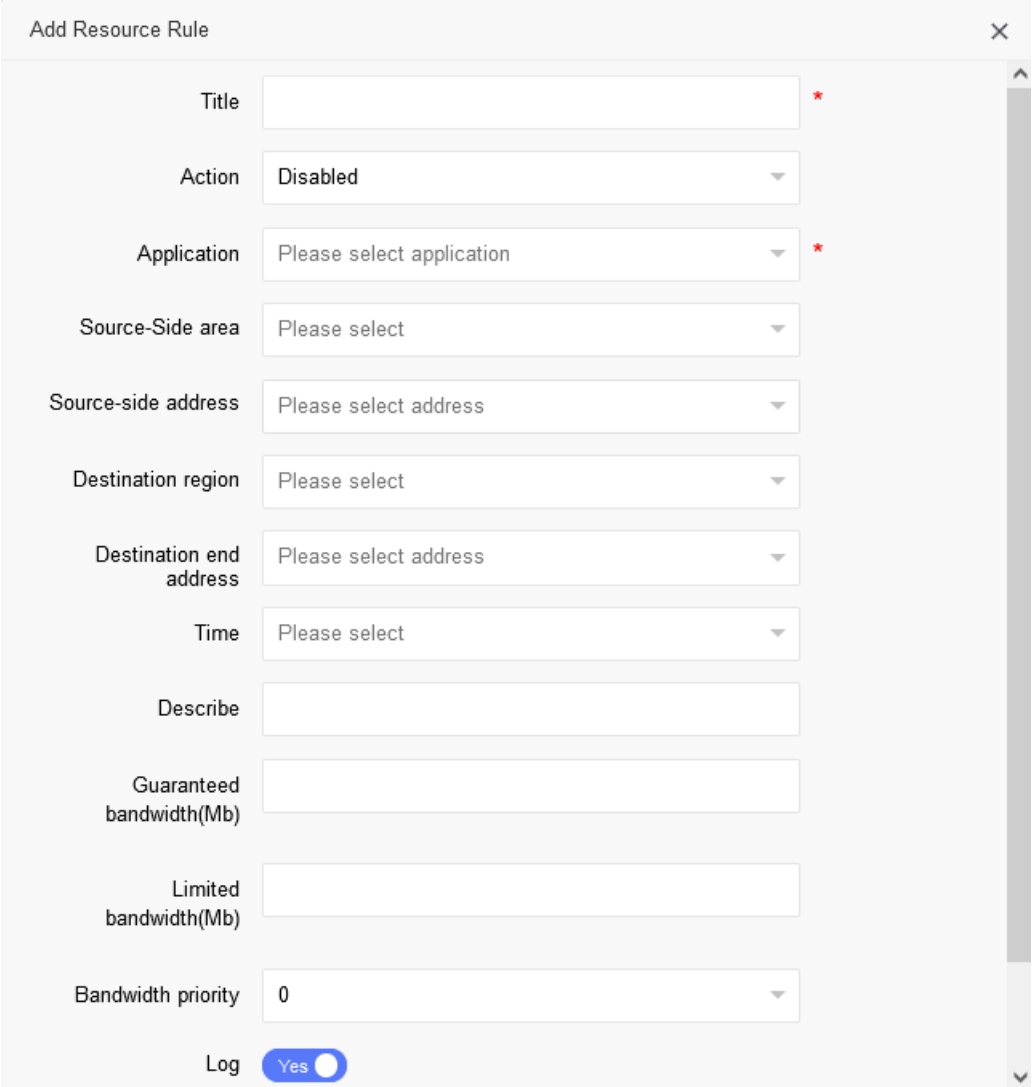


Figure 23

Name	Description
Name	Policy name, required
Action	Policy actions, including accepting, discarding, and disabling
Application	The application object matched by the policy supports the configuration of predefined applications. Required
Source-side area	Source area object for policy matching
Source-side address	The source-side address object matched by the policy can be the address object or address group
Destination region	Destination region object for policy matching
Destination end address	The destination end address object matched by the policy can be the address object or address group
Time	Time object for policy matching
Description	Description information of policy
Guaranteed bandwidth	Minimum guaranteed bandwidth of the policy

Limited bandwidth	Limited bandwidth of the policy
Bandwidth priority	It is available from 0 to 7
Log recording	Whether the policy records the log is on or off

Policy matching is subject to priority, that is, the one at the top is higher than that at the bottom, that is, the one with the larger priority number is higher. The priority of the policy can be adjusted through the button, or the upper and lower positions of the rule can be moved by dragging the policy to determine the priority of the rule, as shown in Figure 24:

Priority	Rule name	Application	Src Zone	Dst Zone	Source IP Address	Dest IP Address	Act Time	Action	Log	Describe	Operation
5	S7STOP	S7						Drop	Yes		
4	ddd	S7COMM						Accept	Yes		
3	modbus	MODBUS						Accept	Yes		

Figure 24

The configured policy supports export and import. Click Rule Export to exported policy, as shown in Figure 25:

Figure 25

Click Policy import to pop-up policy import interface (as shown in Figure 26), click to select the policy to be imported, click Import Rules to import the policy, as shown in Figure 27:

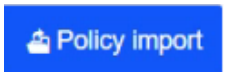


Figure 26

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

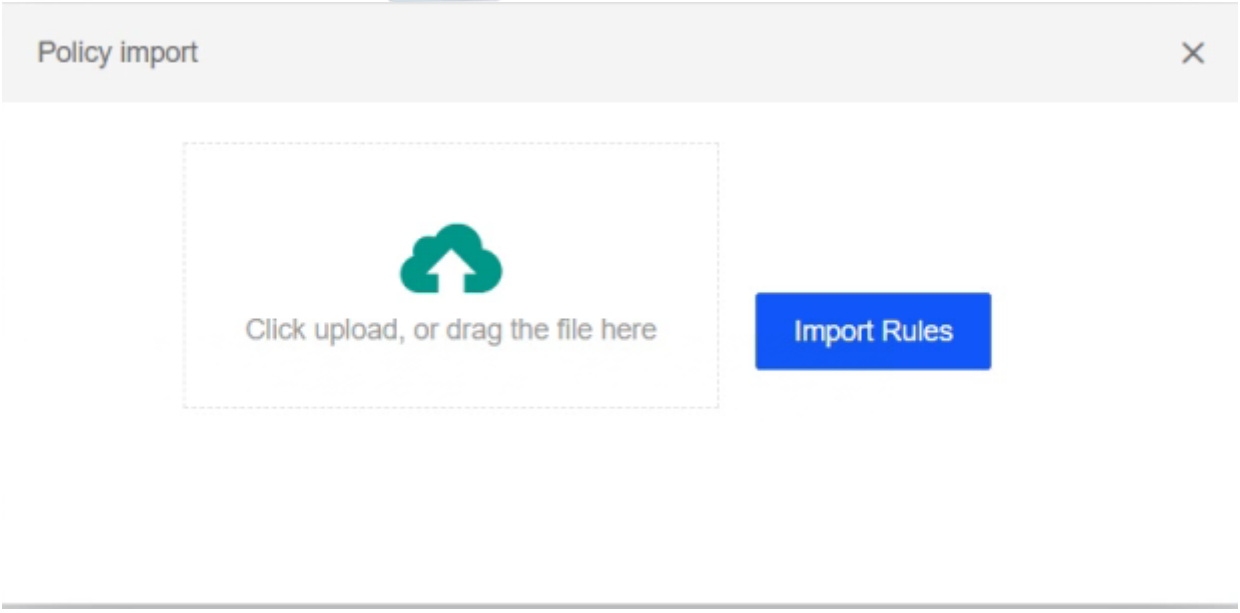


Figure 27

5.2 Policy learning

After logging in the industrial ethernet firewall, the policy administrator (secuser) can choose to enter the learning mode through the "System Management—Work Mode" module, that is, to learn the specific protocol type and detailed protocol data independently and intelligently from the network environment data stream and automatically generate protocol rules at the same time.

Select the start time, learning duration, and protocol type of learning, and click Start to start learning, as shown in Figure 28:

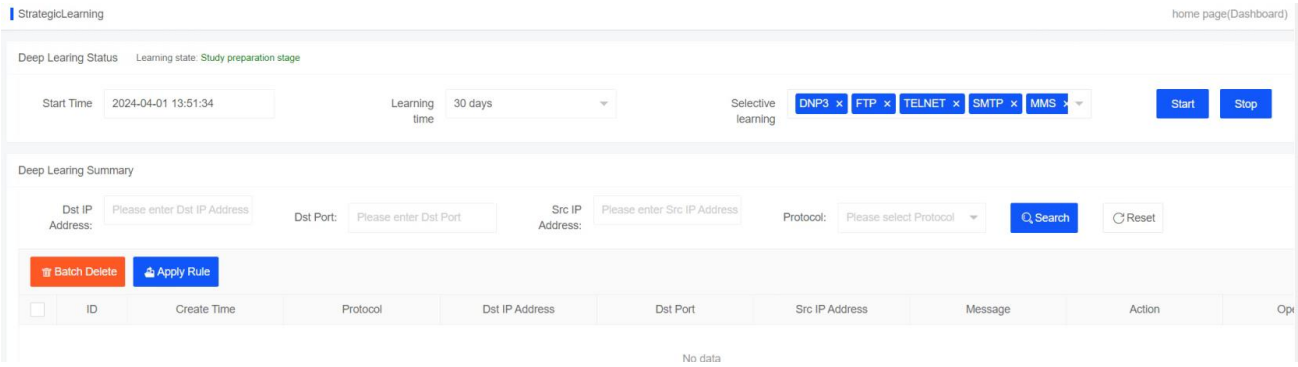


Figure 28

The learned rules can be queried by selecting the protocol and entering the destination IP, destination port, source IP address, etc., as shown in Figure 29:

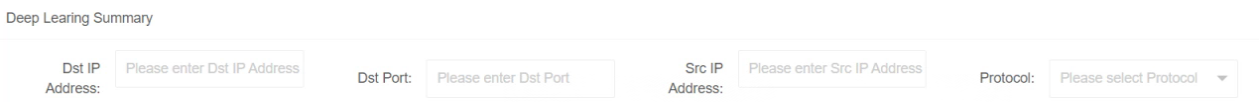


Figure 29

6 Network Configuration

6.1 Interface management

The interface types supported by interface management include physical interface, bridge interface, VLAN interface and aggregation interface.

6.1.1 Network interface

The system administrator (sysuser) can manage the device interface, view the interface connection status, and add, edit, delete and view the IP address and subnet mask of the device interface, as shown in Figure 30:

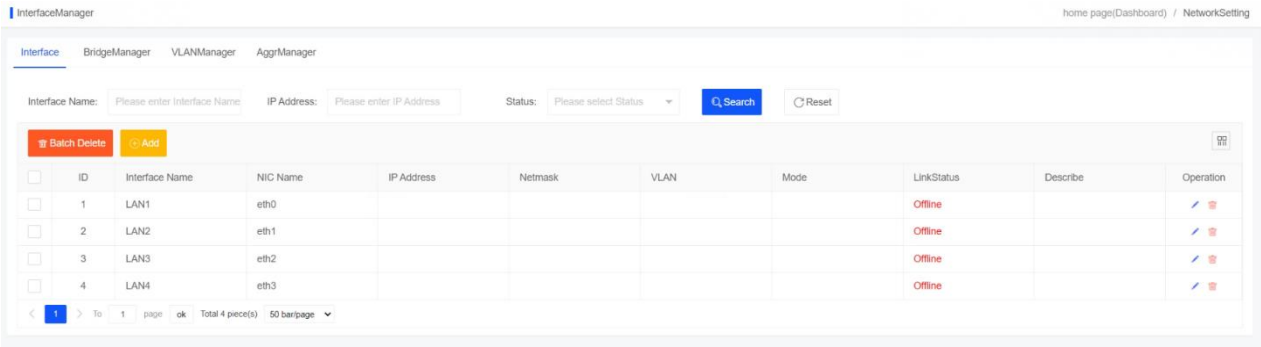


Figure 30

Click to enter the edit network interface. According to the actual environment, configure the IP address, mask and VLAN tag of the interface, as shown in Figure 31:

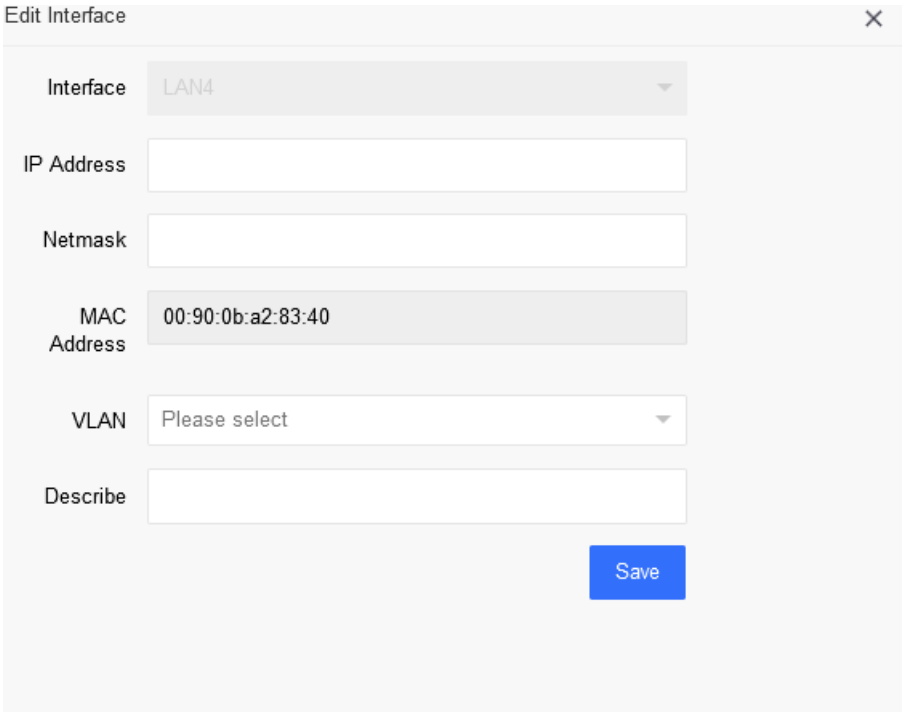


Figure 31

Click the Add button to add a virtual network interface, namely sub-interface, as shown in Figure 32:

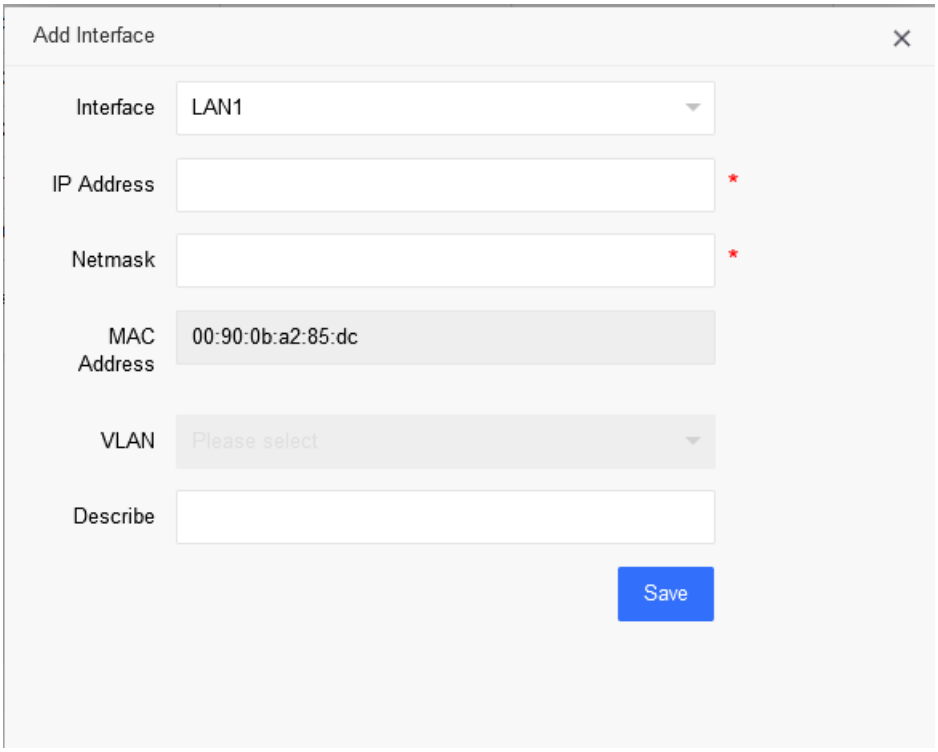


Figure 32

Note:

- Only the added virtual network interface can be deleted. The real network interface only can clean up the information related to the IP address and VLAN
- Each interface can only be added to one interface attribute;

Example: If the eth0 interface is added to the VLAN, it cannot be added to the bridge or aggregation

6.1.2 VLAN management

The system administrator (sysuser) manages the VLAN and can perform the operations such as adding, editing, and deleting. Create a new VLAN tag and click Add to enter the add interface. The VLAN tag fill-in range is 1 to 4094, as shown in Figure 33:

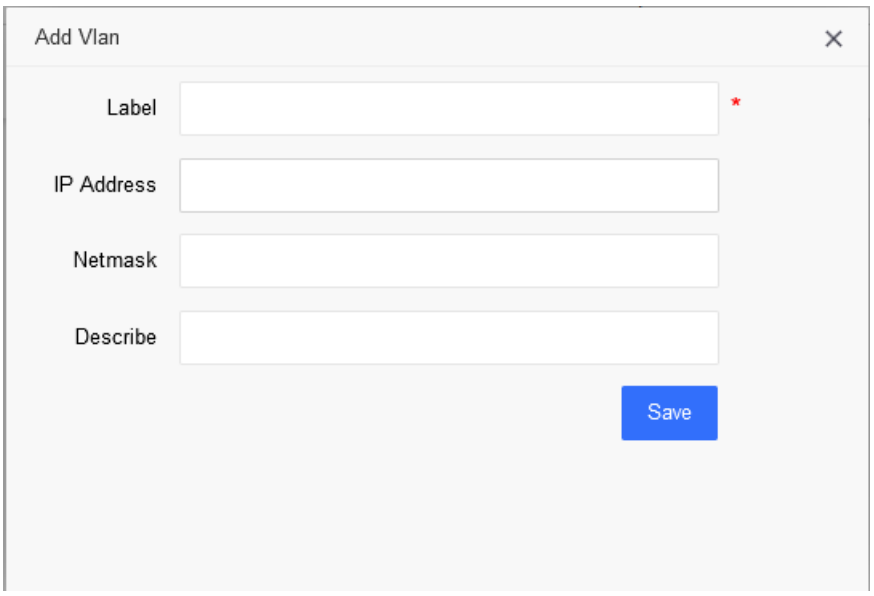
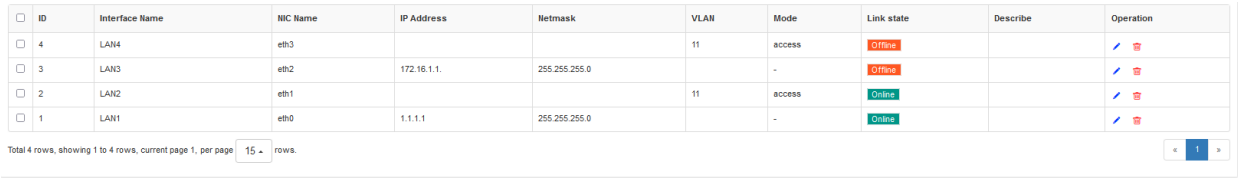


Figure 33

After configuring the VLAN tag, configure the VLAN interface, click the Edit button on the network interface, and select the VLAN tag for the interface. When configuring a single VLAN tag, the interface mode is access; when configuring two or more VLAN tags, the interface mode is trunk, as shown in Figure 34:



ID	Interface Name	NIC Name	IP Address	Netmask	VLAN	Mode	Link state	Describe	Operation
4	LAN4	eth3			11	access	Offline		
3	LAN3	eth2	172.16.1.1.	255.255.255.0		-	Offline		
2	LAN2	eth1			11	access	Online		
1	LAN1	eth0	1.1.1.1	255.255.255.0		-	Online		

Total 4 rows, showing 1 to 4 rows, current page 1, per page 15 rows.

Figure 34

6.1.3 Network bridge management

The system administrator (sysuser) manages the network bridge and can perform the operations

such as adding, editing, deleting, etc., click the Add button to enter the interface for adding a network bridge, edit the bridge interface name, and select the network interface and other information. The interface IP address of the bridge is used for bridge interface management, as shown in Figure 35:

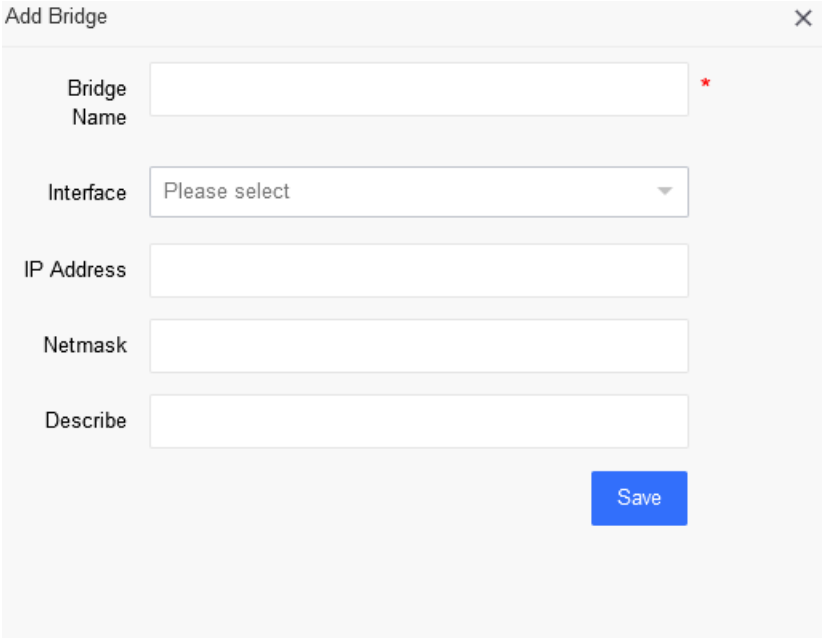


Figure 35

Note: An interface can only be added to one bridge interface, and cannot be added to another bridge interface again

6.1.4 Aggregation management

The system administrator (sysuser) manages the aggregation and can perform the operations such as adding, editing, and deleting. The aggregation interface supports five modes. The commonly used modes include one primary backup policy mode and four dynamic link aggregation modes. Click Add Aggregate Interface to enter the add interface, as shown in Figure 36:

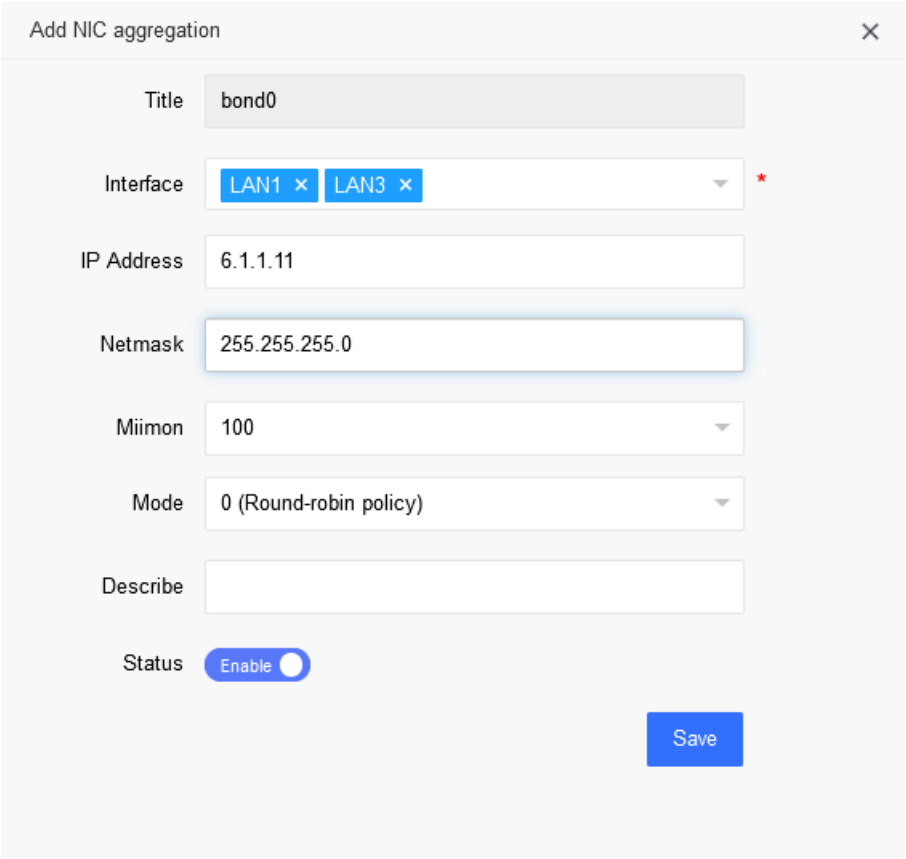


Figure 36

6.2 DHCP server

The system administrator (sysuser) manages the DHCP server. The interfaces that support the enabling of the DHCP service include physical interfaces, VLAN interfaces, and bridge interfaces. The DHCP server can be added, edited and deleted. It also supports configuring static binding of IP addresses and assigning fixed IP addresses to designated clients.

Create a new DHCP server, click the Add button to pop up the interface for adding DHCP domain, select the interface to enable the DHCP service, configure the network address/mask, address range, lease period, etc., and click Save after finishing the configuration, as shown in Figure 37:

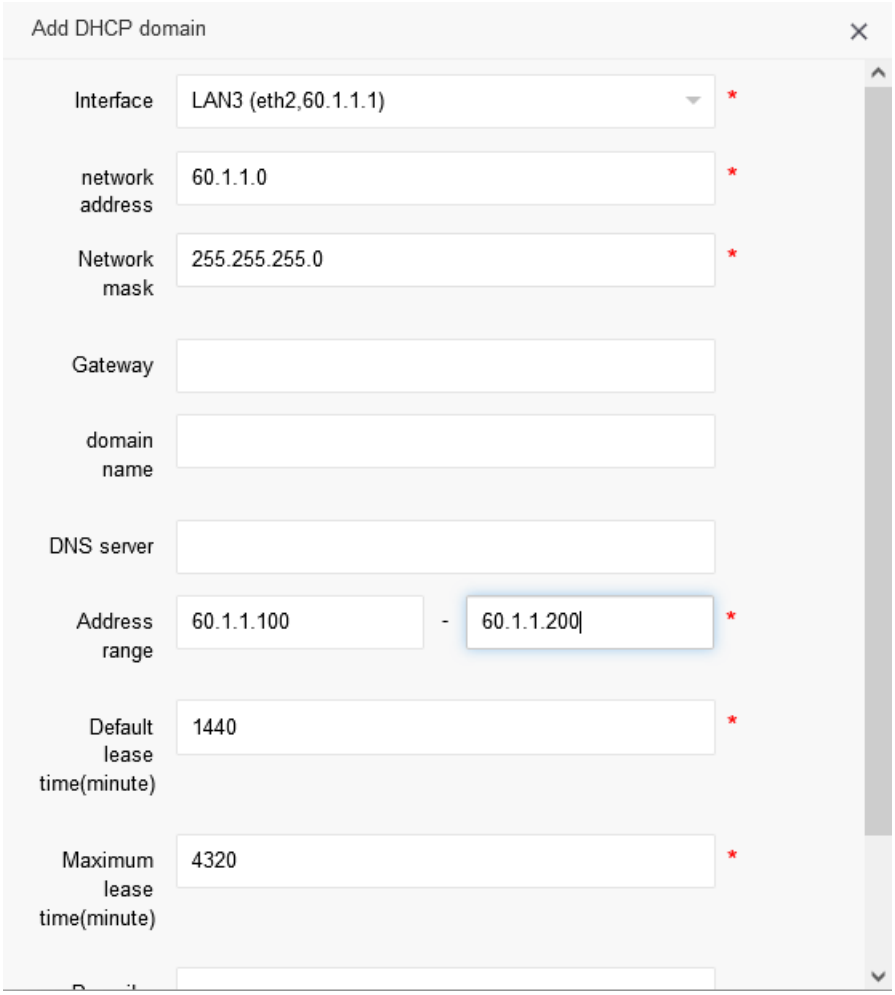


Figure 37

Name	Description
Interface	Interface with enabled DHCP service
Network address	Specified network used with the mask, required
Network mask	Mask of specified network address, required
Gateway	Set default gateway for the client
Domain name	Set DNS domain name for DHCP client
DNS server	Set the DNS server IP address for the client
Address range	Address range allocated for the DHCP client, valid within the network address/mask range, required
Default lease time	Lease time after the client obtains the address, 1 day by default
Maximum lease time	The maximum lease time is the longest time that the IP address can be used when the client has exceeded the lease time but has not updated the IP address, and it is 3 days by default.

For static binding of DHCP, enter the DHCP static IP configuration interface, and click Add to assign a specified IP address to a host, as shown in Figure 38:

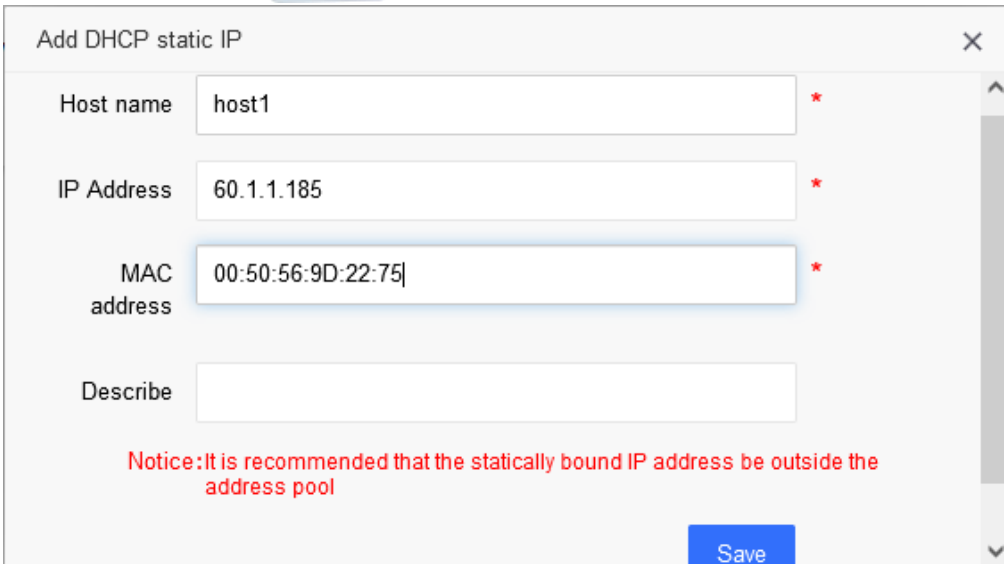


Figure 38

6.3 Static route

The system administrator (sysuser) manages the static route and can perform the operations such as adding, editing, and deleting. Click Add Route, as shown in Figure 39:

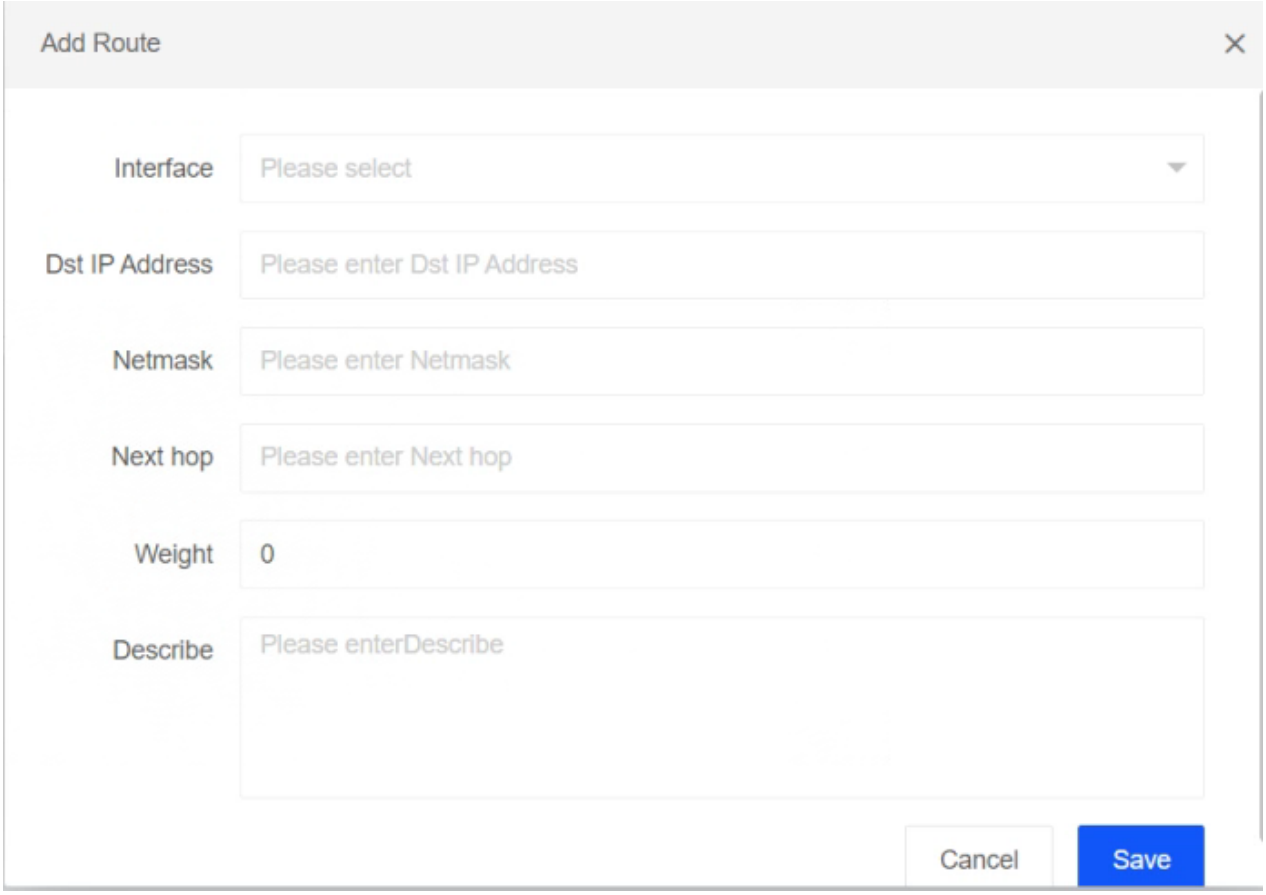


Figure 39

6.4 NAT

The system administrator (sysuser) manages the NAT, which is classified into SNAT and DNAT. With respect to NAT configuration, the user can perform address translation for specific applications. For SNAT, the user can transit the source address and perform the operations such as editing, deleting, adding and searching.

Create a new SNAT, click Add to enter the SNAT add interface, add the source IP address, destination IP address, and converted IP address of the device, etc., and enable the policy, as shown in Figure 40:

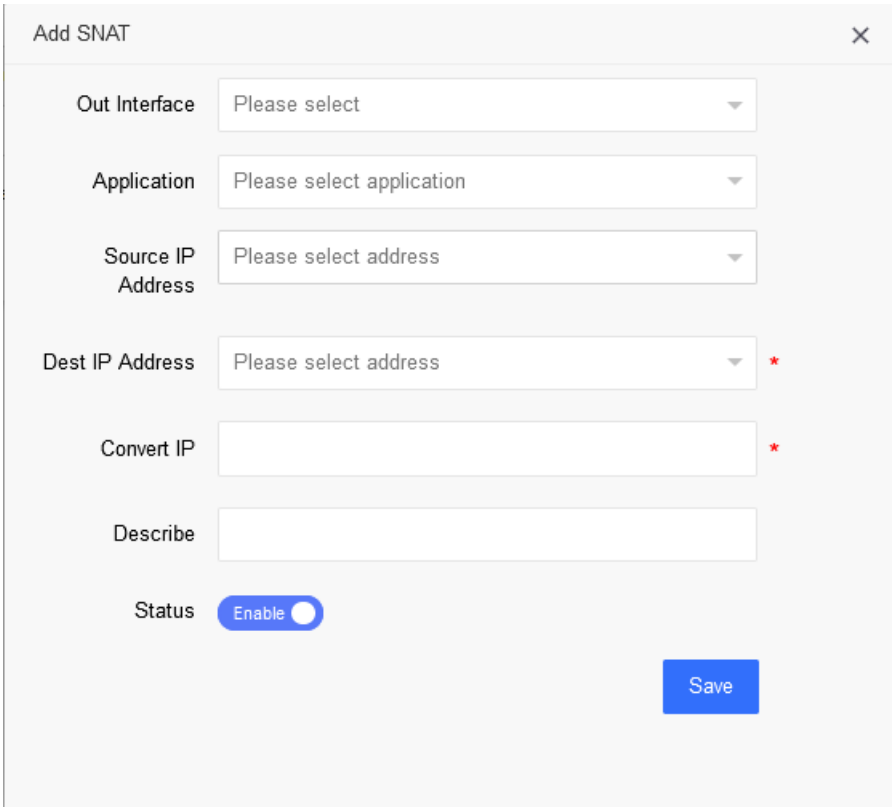


Figure 40

The user can enter the converted IP address, click Search to perform search for inquiries, which can be fuzzy search, as shown in Figure 41:

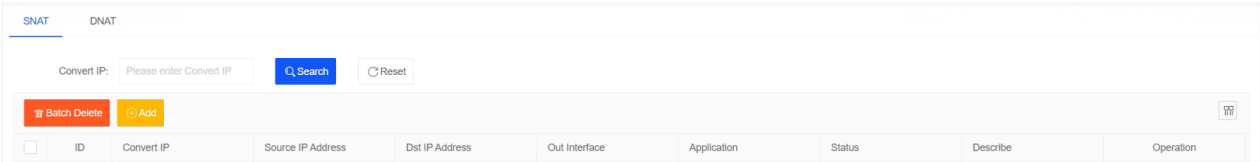


Figure 41

The DNAT can convert the destination address and destination port, and support the operations such as adding, editing, deleting, and searching.

Create a new DNAT policy, click Add to enter the NAT add interface, add the source IP address,

destination IP address, and converted IP address of the device, etc., and enable the policy, as shown in Figure 42:

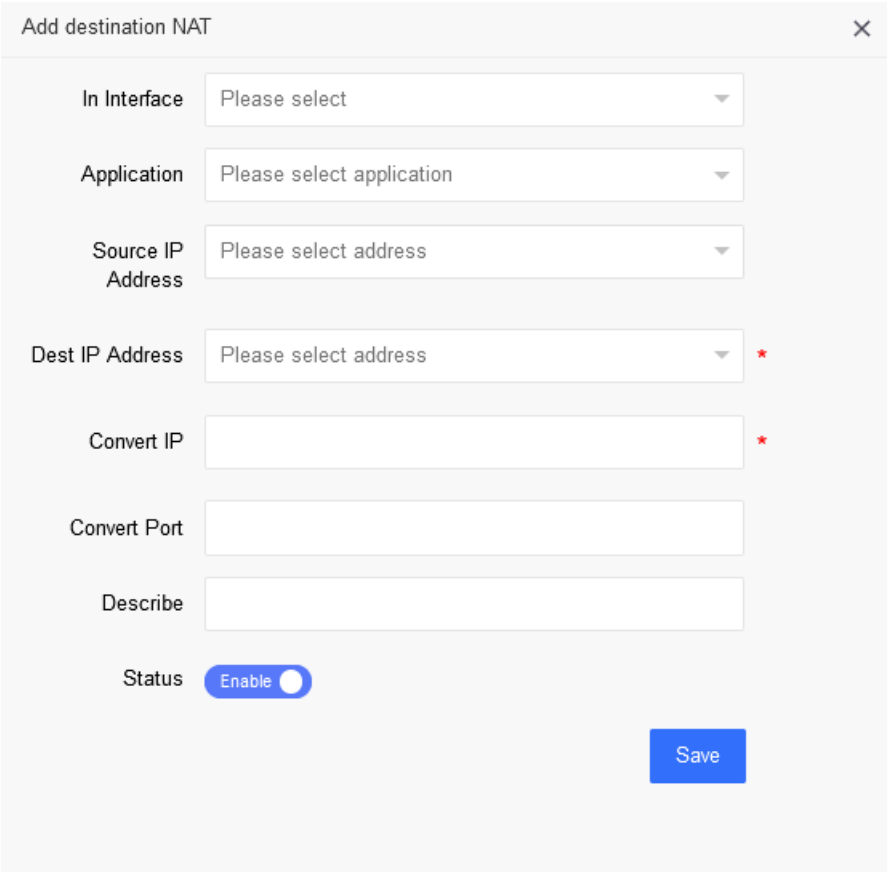
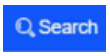


Figure 42

The user can enter the converted IP address, click  to perform search for inquiries, which can be fuzzy search, as shown in Figure 43:

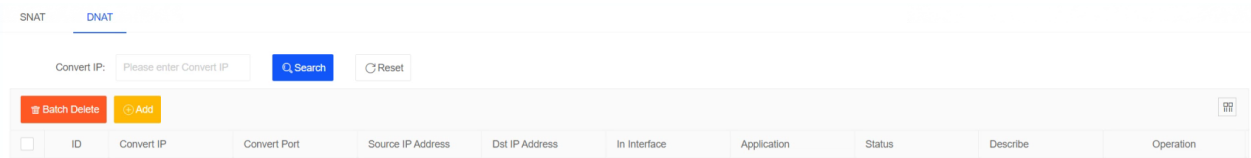


Figure 43

7 Virtual Private Network

The policy administrator (secuser) configures the VPN and encrypts the transmitted data to ensure the security of data transmission. VPN configuration supports two authentication methods, including pre-shared key and national secret certificate. The national secret certificate authentication requires authorization, and the authorization documents need to be obtained from relevant personnel.

7.1 Tunnel management

1) Policy management

The security administrator (secuser) performs the operations on policy management, such as adding, editing, deleting, and viewing.

Create a VPN policy, and first click Add Policy Configuration. The add interface is shown in Figure 44:

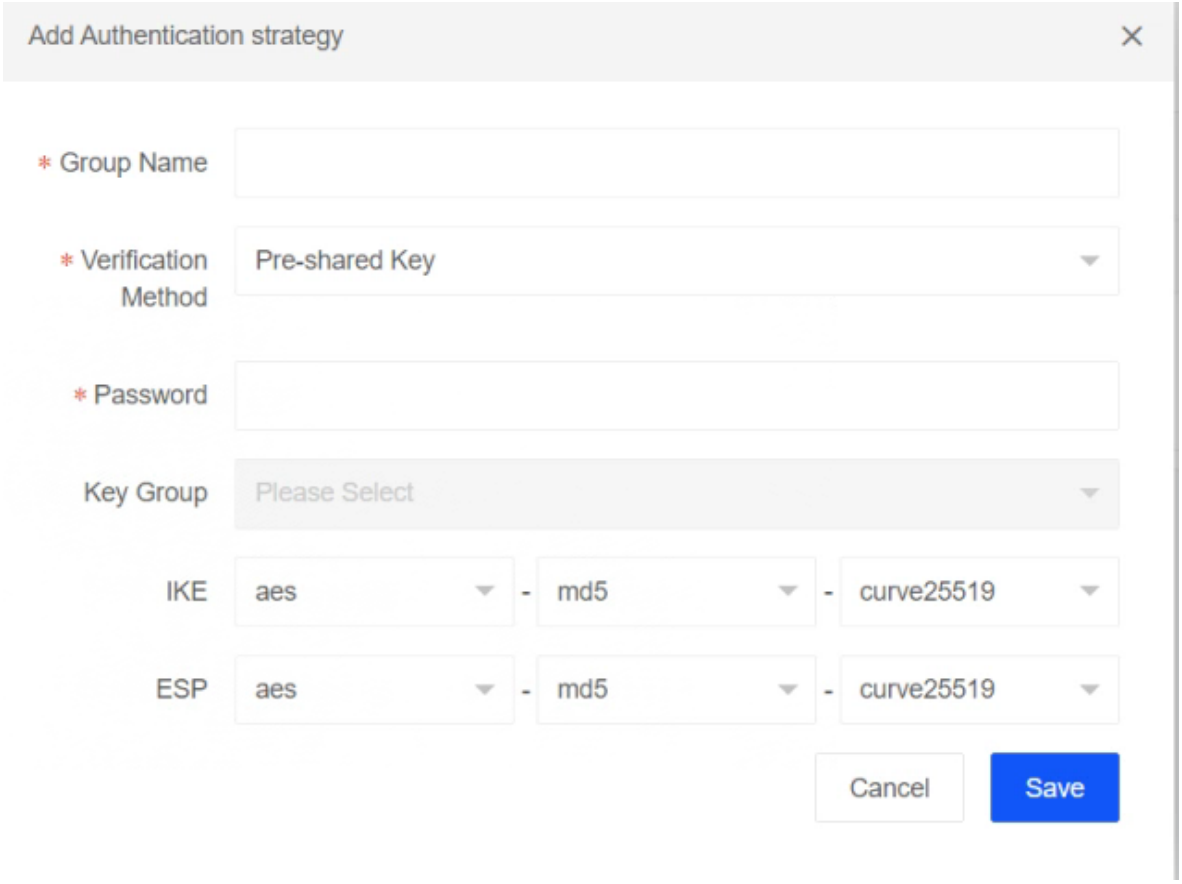


Figure 44

Name	Description
Group name	Group name of policy management
Verification method	Pre-shared key and certificate authentication, for which both ends need to have the same configuration
Password	Pre-shared key, for which both ends need to have the same configuration
IKE	IKE SA parameters exchanged and negotiated for the first time, including encryption algorithm, authentication algorithm, and DH algorithm. The successful negotiation requires the same configuration at both ends.
ESP	It is the security protocol used by the message. The firewall currently only supports the ESP mode, and it also needs to negotiate the encryption algorithm and authentication algorithm. Similarly, the successful negotiation requires the same configuration at both ends.

2) Strategic management

The security administrator (secuser) performs the operations on strategic management, such as adding, editing, deleting, and viewing.

After configuring the policy management, add the strategic management, reference the configured authentication group, configure the gateways at both ends of the VPN and the traffic to be protected (interest traffic), and check the automatic start, as shown in Figure 45:

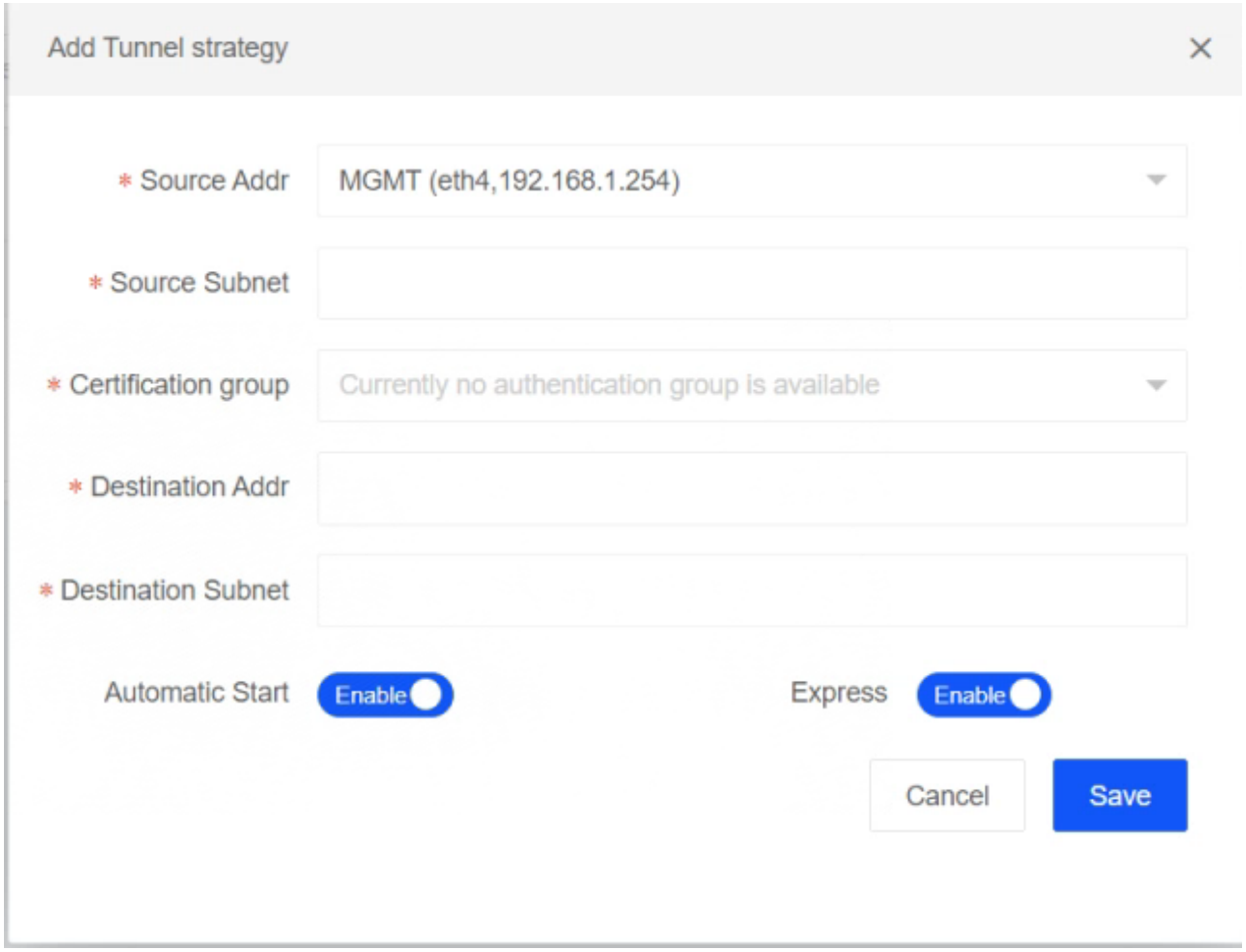


Figure 45

Name	Description
Source address	Source addresses at both ends of the VPN tunnel
Source subnet	The source subnet of the traffic protected by the VPN tunnel
Certification group	Certification group used by VPN (policy management)
Destination address	Destination address at both ends of the VPN tunnel
Deatination subnet	Deatination subnet of the traffic protected by the VPN tunnel
Automatic start	Check Enable to actively establish a VPN connection
Express	Enable the Express to issue and run the policy for protecting the traffic after the VPN negotiation is successful.

3) National secret VPN authorization

When using the national secret certificate authentication, obtain the VPN authorization first, and then configure the national secret certificate to set up the VPN. Configure the policy management first, and then conduct the strategic management. The policy management supports adding, editing and deleting.

When the authentication method is national secret authentication, the user need to obtain authorization first, click VPN>Tunnel Management>National Secret VPN Authorization, and export the national secret VPN information; after obtaining the authorization file, click Import national secret Vpn Authorization to update the authorization status of VPN synchronously, as shown in Figure 46:

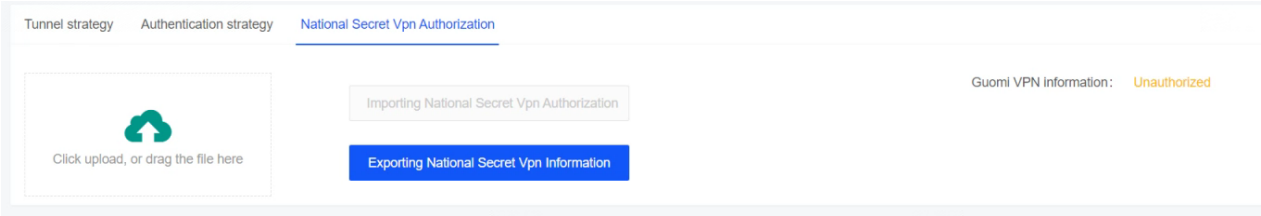


Figure 46

7.2 Certificate management

After obtaining the relevant certificate, click Add CA Certificate, as shown in Figure 47:

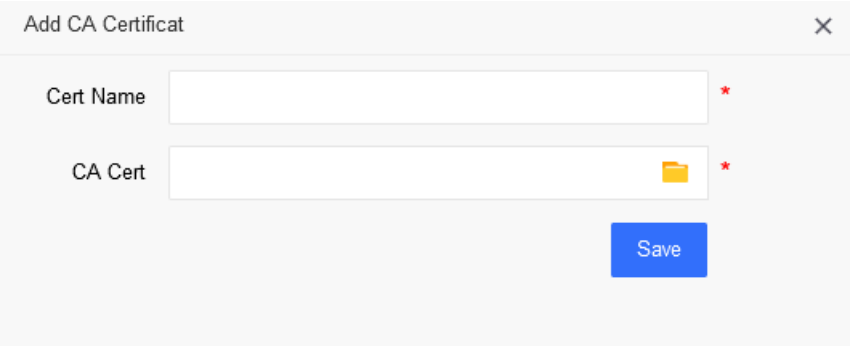


Figure 47

To add an IPSEC certificate, click Add. The signature certificate, encryption certificate and other related information are required, as shown in Figure 48:

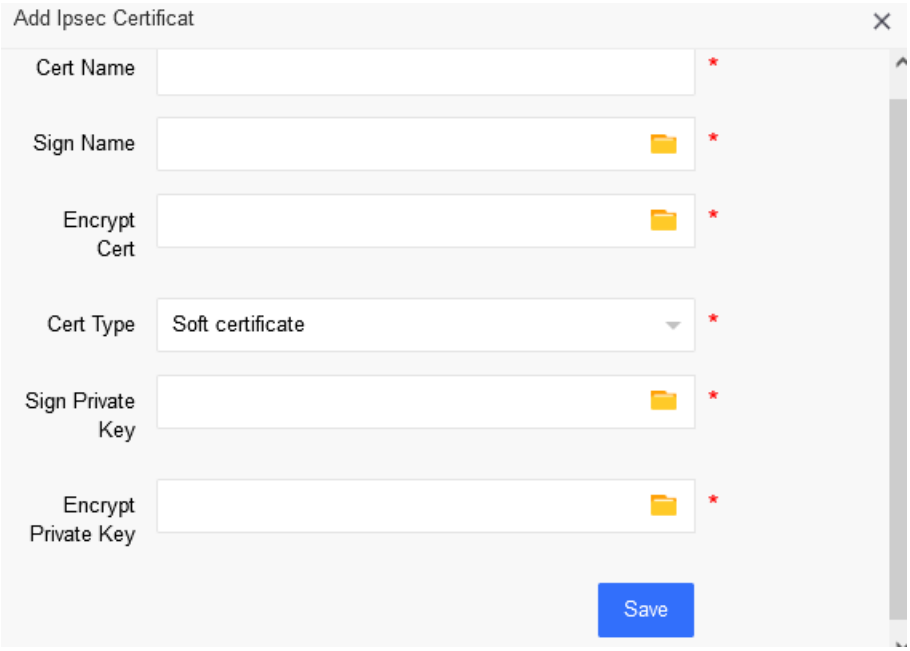


Figure 48

8 System Management

8.1 Basic setting

8.1.1 Management setting

The system administrator (sysuser) can perform management settings in the basic settings, mainly including management port configuration, SNMP setting, SSH setting, and access security setting, as shown in Figure 49:

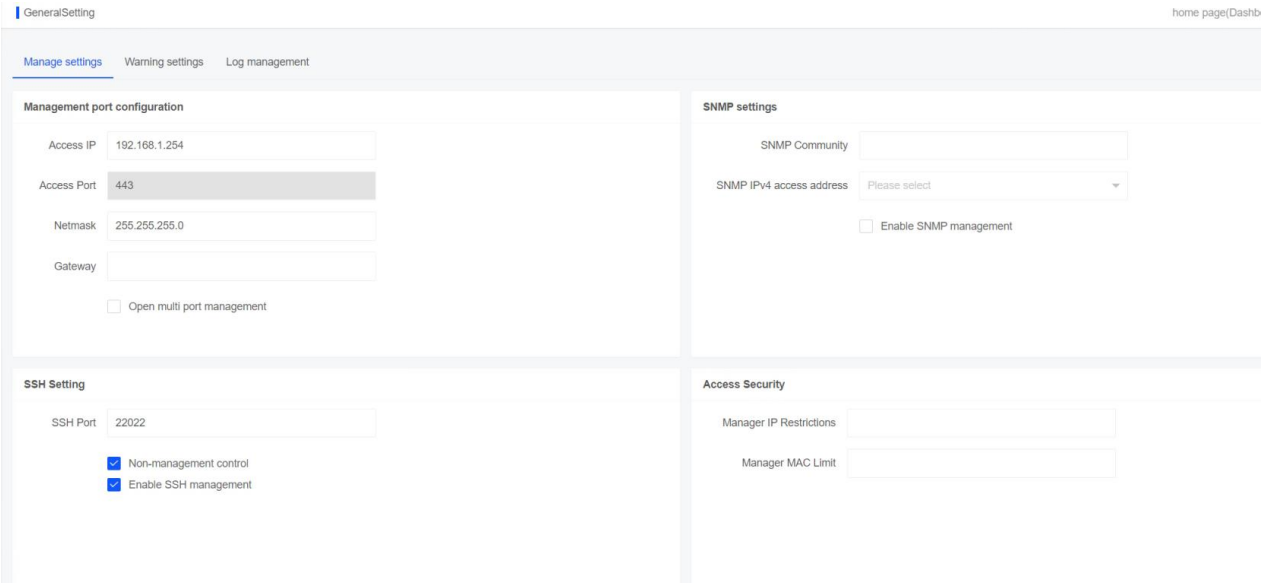


Figure 49

Name	Description
Management port configuration	Device management port configuration supports multi-port management and the port is the gateway by default
SNMP settings	SNMP service enabling, disabling and configuration
SSH setting	SSH service enabling and disabling. The SSH service of the management port and the service port can be enabled.
Access security	Support the configuration of manager access security binding

8.1.2 Warning setting

The system administrator (sysuser) can perform warning setting in the basic settings, namely warning criterion for industrial ethernet firewall CPU usage, memory usage, hard disk usage and network usage. When the device condition reaches the warning value, send a warning email through "Email Settings" to the administrator's mailbox for notification, as shown in Figure 50:

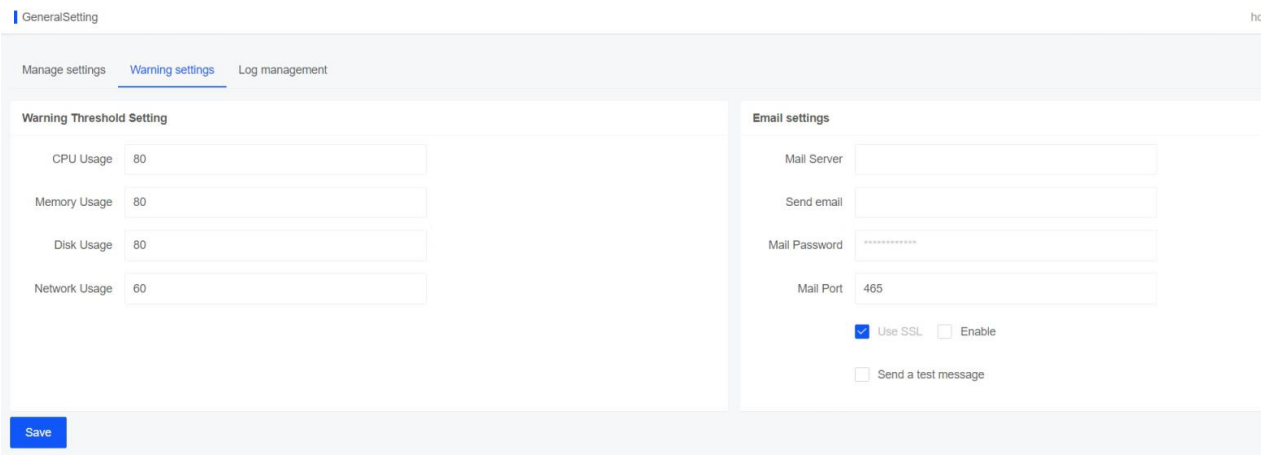


Figure 50

8.1.3 Log management

The system administrator (sysuser) can perform log management in the basic settings, mainly including log storage time management and Syslog setting. After the Syslog server is enabled, the log information will be synchronized and backed up to the Syslog server, as shown in Figure 51:

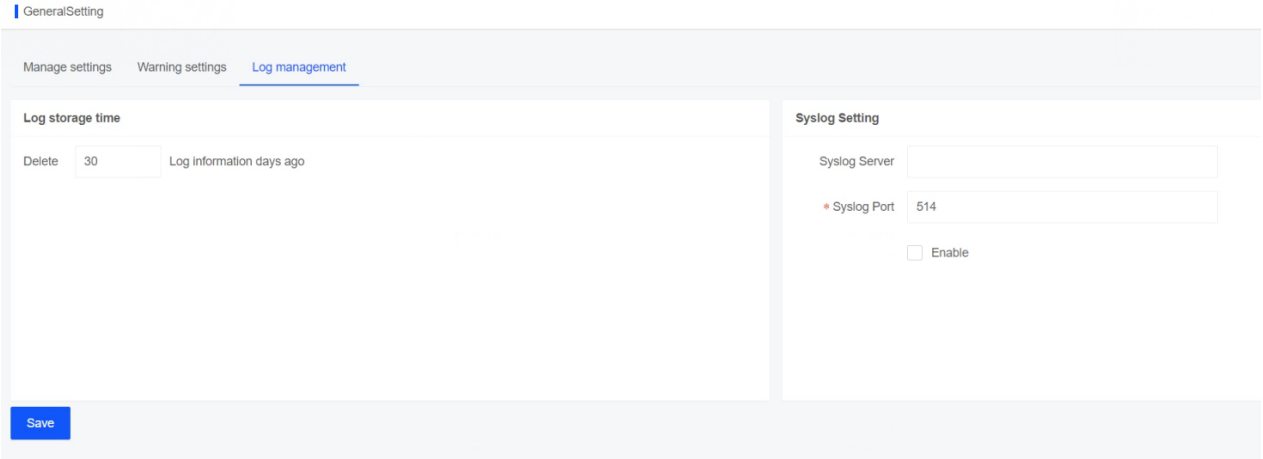


Figure 51

8.2 Assets management

8.2.1 Asset security

Asset security is divided into three parts, asset summary, asset list, and asset introduction, as shown in Figure 52:

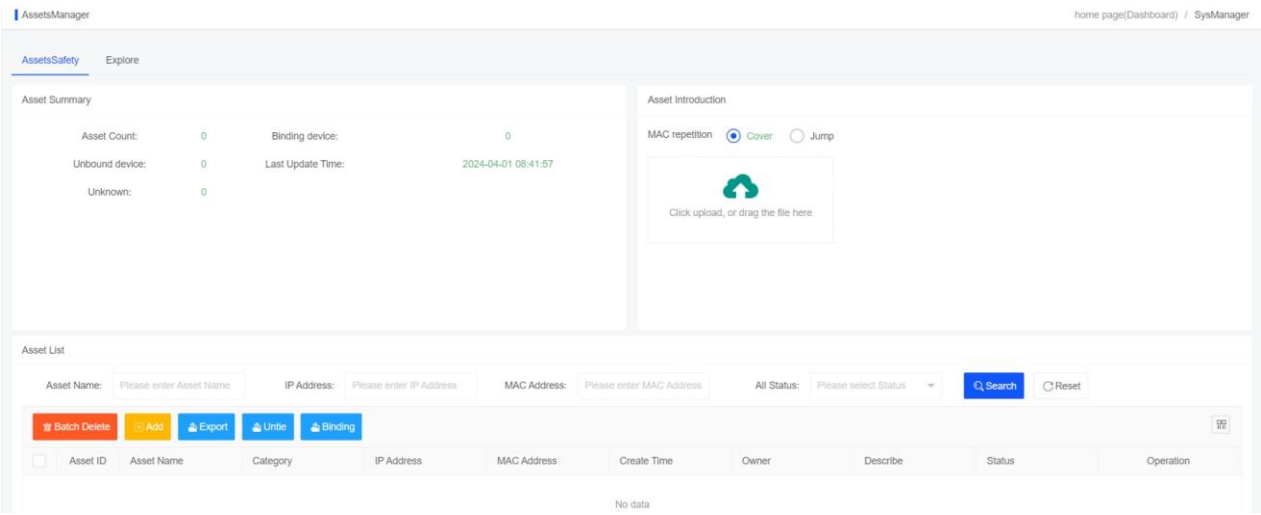


Figure 52

The policy administrator (secuser) manages the asset list, and can perform the operations such as editing, deleting, adding, unbinding and binding. Figure 53 shows the unbinding and binding:

Asset ID	Asset Name	Category	IP Address	MAC Address	Create Time	Owner	Describe	Status	Operation
		Network Switch	192.168.6.66	98:fA:9B:2C:E1:DA	2021-09-17 14:16:43			Already bound	

Figure 53

There are many options for adding asset lists. The user can also set categories manually, as shown in Figure 54:

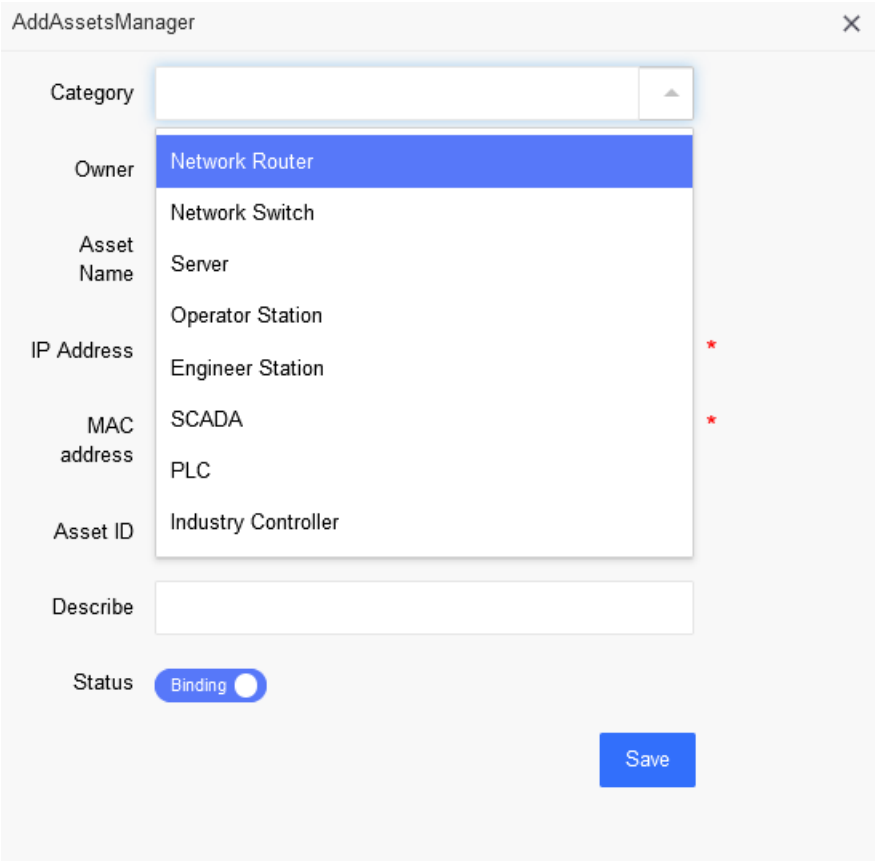


Figure 54

Asset import only supports text import in csv format, as shown in Figure 55:

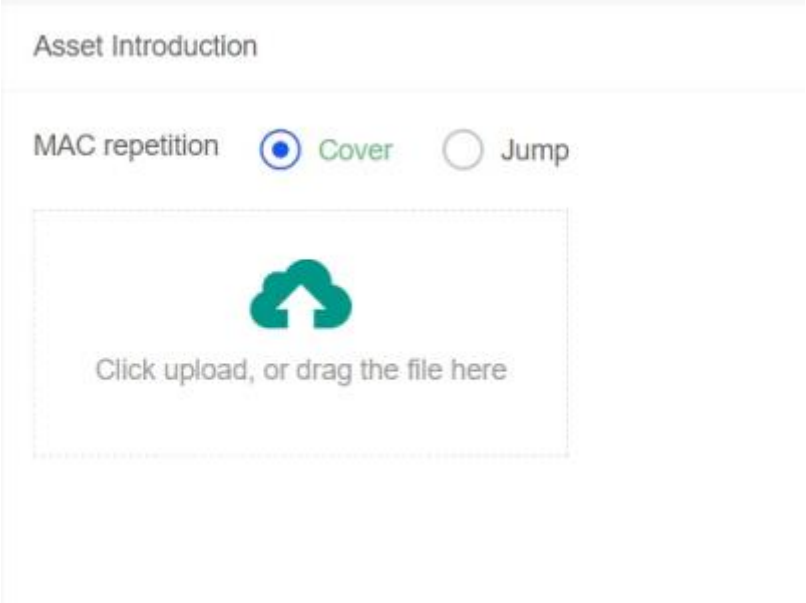


Figure 55

Name	Description
Cover	If an asset in the asset list duplicates the imported asset, remove the asset from the asset list and add the imported asset.

Jump	If an asset in the asset list duplicates the imported asset, do not handle the asset from the asset list or add the imported asset.

8.2.2 Detection

The detection can be performed through the device interface, and the detected IP and MAC can be bound.

1. Detection: Each detection lasts for 2 minutes. Select the interface and click Detection to enter the detection interface, as shown in Figure 56:

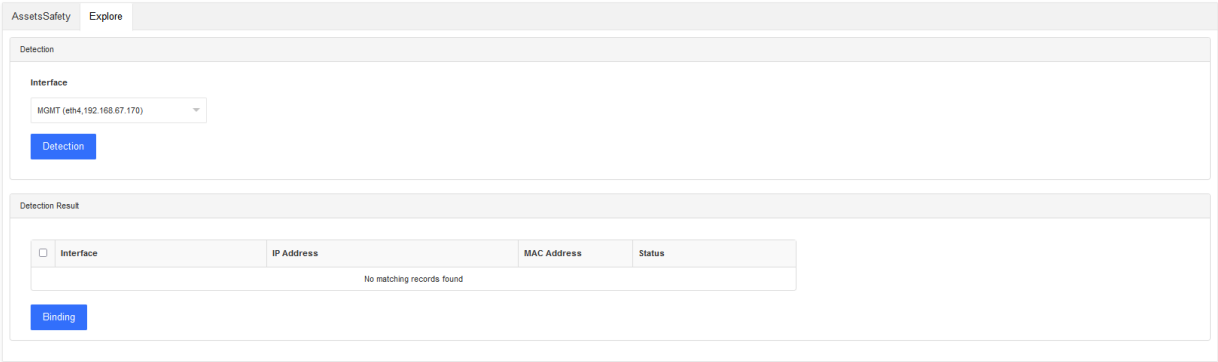


Figure 56

Note: If all results are detected within two minutes, no further detection will be performed; if no results are detected, it will wait for 2 minutes to time out and exit.

2. Binding: Bind the detected IP address with the MAC address. If the user does not want to bind or handle the detection result, select the result to be bound and click Bind, as shown in Figure 57:

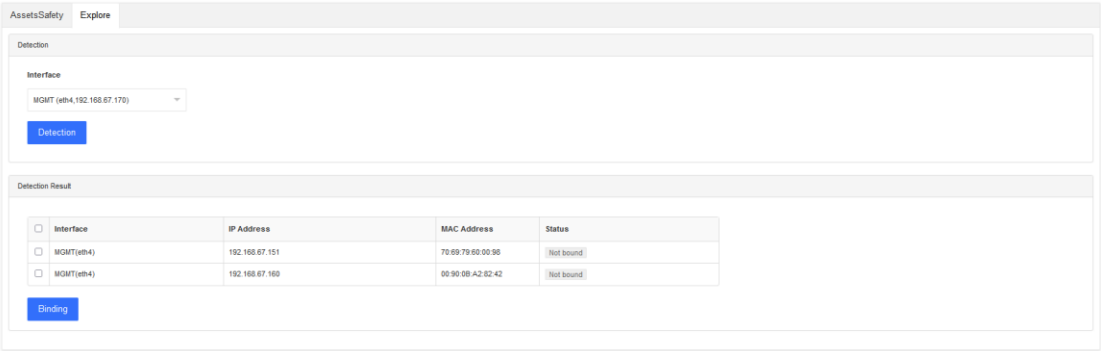


Figure 57

View the binding result of asset security, as shown in Figure 58:

Figure 58

8.3 Diagnostic tool

The diagnosis tool involves two parts: diagnosis and packet capture:

1. Diagnostic tool: it is used to detect network communication, and compatible with PING, TELNET and TRACEROUTE, as shown in Figure 59:

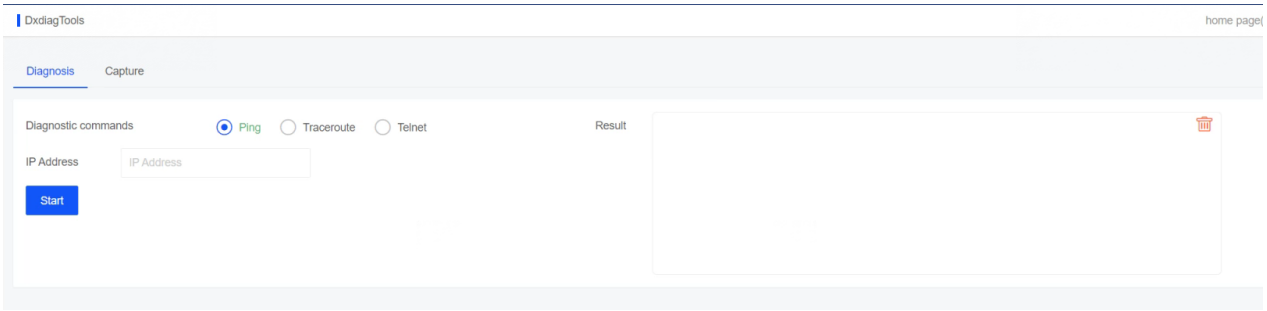


Figure 59

2. Packet capture: Packet capture conditions can be filtered by device, network interface, protocol, source IP address, destination IP address, and destination port, and the number of captured packets can be configured.

The device name and status can be used to filter the capture records. The above is shown in Figure 60:

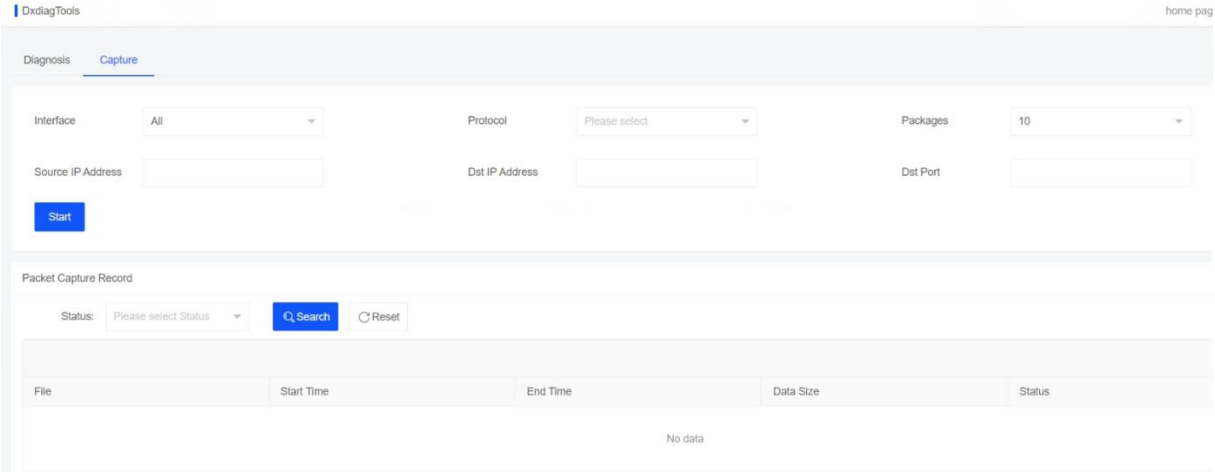


Figure 60

8.4 Control of connections

The policy administrator (secuser) can configure the maximum number of connections for an IP address and control the connection rate. It supports the operations such as add, edit and delete.

Create a maximum connection control, and click the Add button to enter the add interface. The setting range of maximum connections is 100 to 65535, and the setting range of connections per second is 10 to 10000. The above is shown in Figure 61:

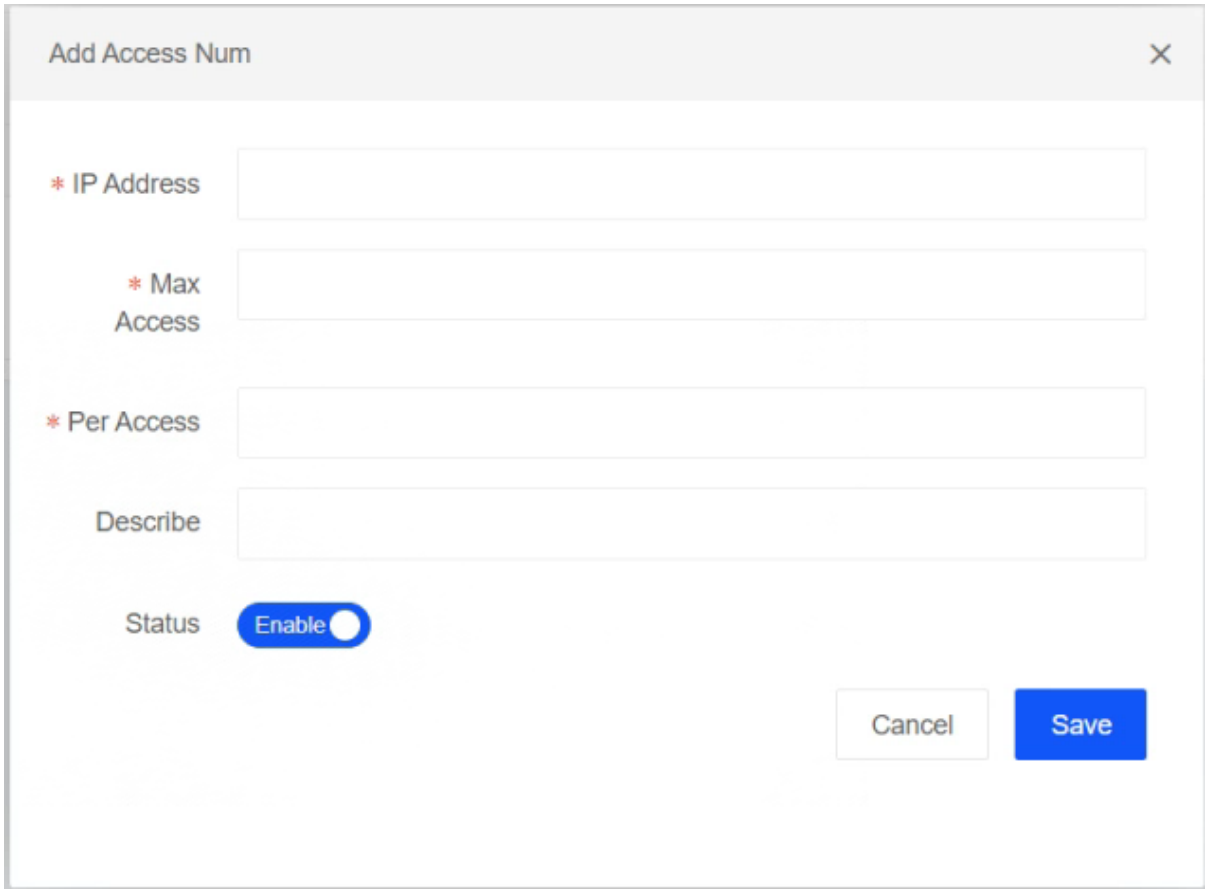


Figure 61

8.5 Account setting

8.5.1 Account setting

The industrial ethernet firewall system is a multi-user system. The administrators (sysuser, secuser, loguser) with user management authority can perform the maintenance for the users, as shown in Figure 62:

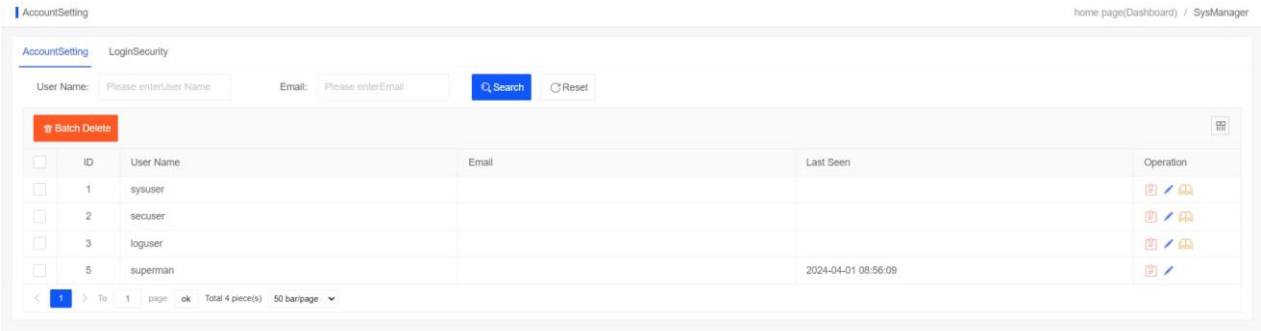
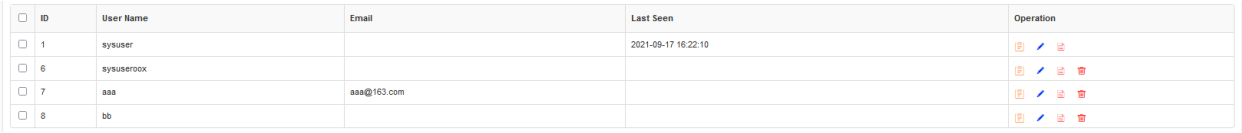


Figure 62

Administrator users (such as the sysuser system administrator) can delete sub-users, but cannot

delete themselves and other administrator users (secuser security administrator and loguser audit administrator), as shown in Figure 63:



ID	User Name	Email	Last Seen	Operation
1	sysuser		2021-09-17 16:22:10	
6	sysuseroox			
7	aaa	aaa@163.com		
8	bb			

Figure 63

Click Details to view the user's detailed information, add user permissions and take sysuser as an example, as shown in Figure 64:

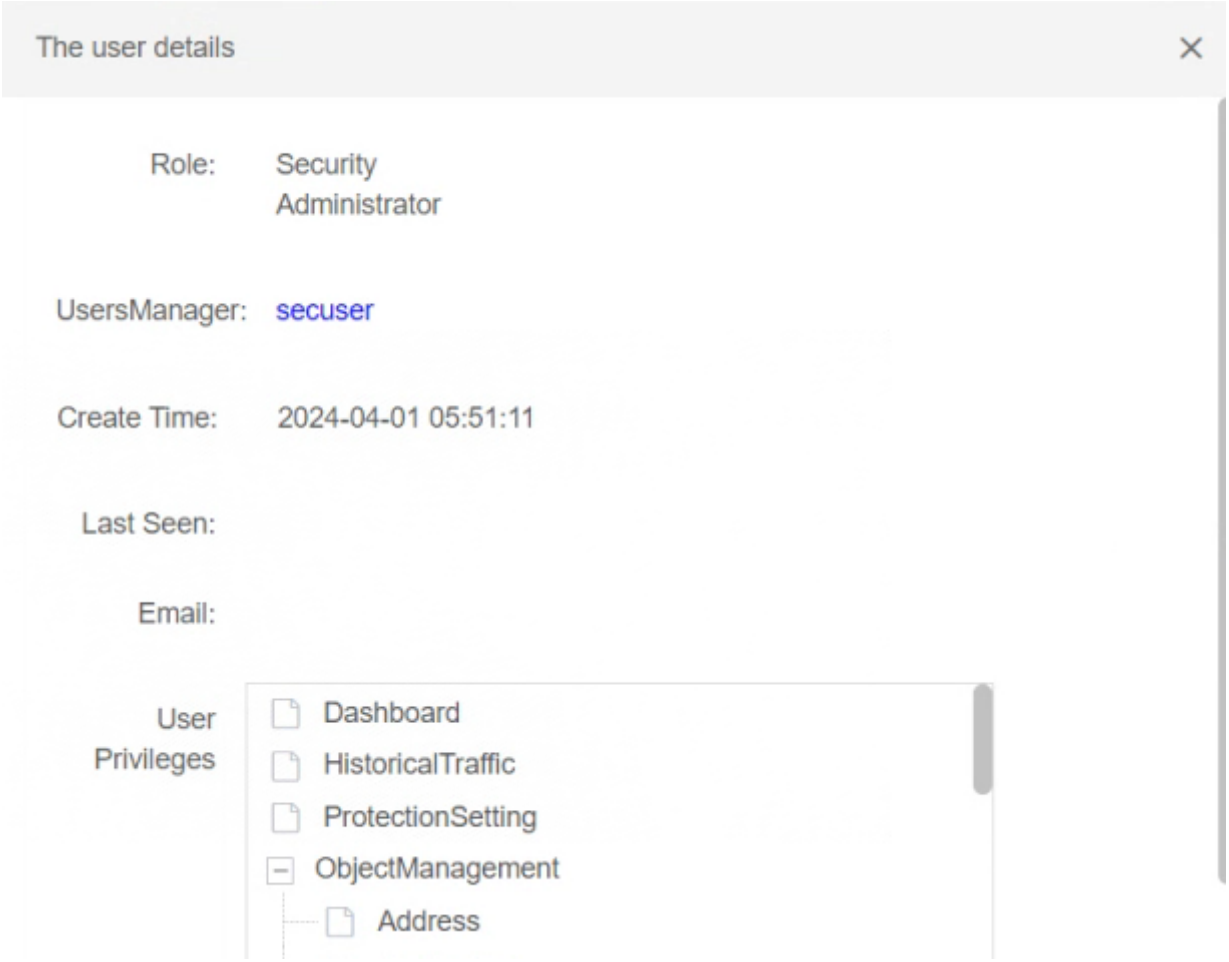


Figure 64

Click Add to add sub-users and add permissions to the sub-users. The permissions of the sub-user are less than or equal to those of the parent user, as shown in Figure 65:

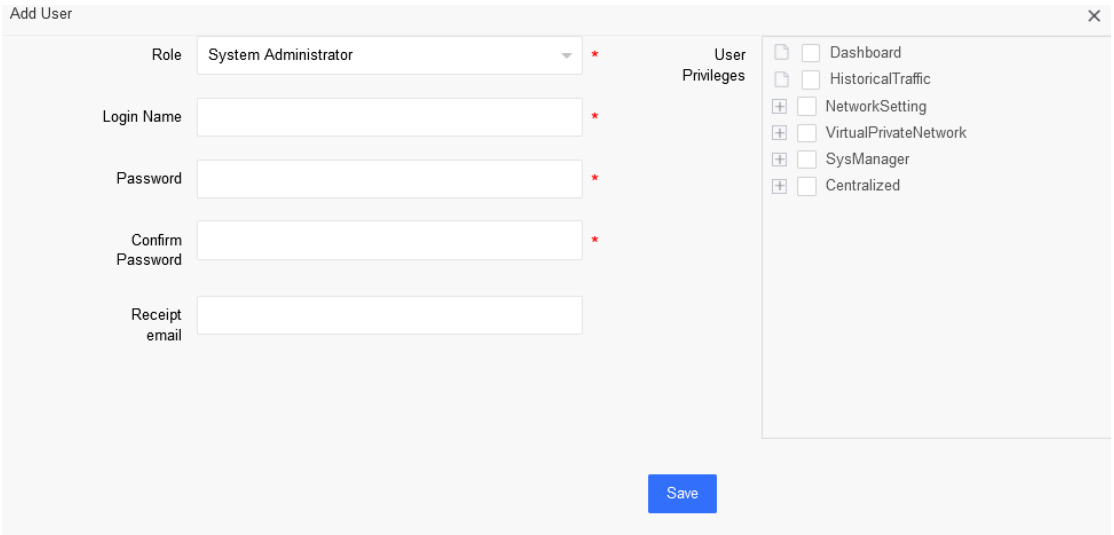


Figure 65

A certificate file is required for user login. Click to generate a certificate file and import the certificate file on the login interface to log in.

8.5.2 Login security

The policy administrator (secuser) can set the password format and password validity period through the security settings, as shown in Figure 66:

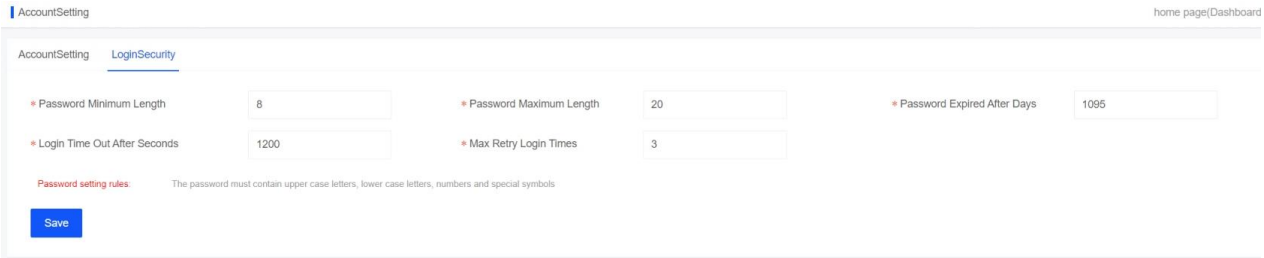


Figure 66

Name	Description
Password setting	Password limitation can be set, including password length
Password expired after days	The user password must be modified at regular intervals, that is, it has a password validity period
Login time out seconds	If the user does not operate the interface for a certain period of time after logging into the WEB management interface, it needs to log in again, and the period is the login timeout.
Max retry login times	It is the number of retries for incorrectly entering the login user name or password. If the number is exceeded, it will be prohibited to log into the system (locked for 10 minutes)

Note: The password complexity cannot be changed.

8.5.3 Separation of powers

The industrial ethernet firewall adopts the user management method with separate permissions to set the administrators in 3 roles: sysuser/secuser/loguser, respectively corresponding to the system administrator, the security administrator, and the audit administrator.

The system administrator (sysuser) is mainly responsible for the maintenance of the overall industrial ethernet firewall operation.

The security administrator (secuser) is mainly responsible for the rule setting and policy management of the industrial ethernet firewall.

The audit administrator (loguser) is mainly responsible for auditing the behavior of the industrial ethernet firewall and analyzing the system status.

Different administrators can only add or edit their own role user information but cannot modify other types of role user information.

The administrator can log into the system to create a sub-administrator under its permission and assign industrial ethernet firewall devices to the sub-administrator. The sub-administrator can only view or modify the devices assigned to it.

8.5.4 Permission assignment

The functional modules that the system administrator (sysuser) and its sub-administrators can operate include:

- Dashboard (Monitoring center)
- Historical traffic
- Network setting
- Virtual private network
- System management
- Centralized

The functional modules that the security administrator (secuser) and its sub-administrators can operate include:

- Dashboard (Monitoring center)
- Historical traffic
- Object management
- Policy management
- Protection setting
- System management
- Centralized
- Log audit

The functional modules that the audit administrator (loguser) and its sub-administrators can operate include:

- Dashboard (Monitoring center)

- Historical traffic
- System management
- Centralized
- Log audit

Note: The sub-administrator can only modify its own information in the user function module.

8.5.5 Application of configuration

After adding or modifying a rule, the rule will not be automatically applied to the corresponding industrial ethernet firewall device, but the user needs to manually click 

"Waiting for Confirmation" in the upper right corner of the page to view all pending events, as shown in Figure 67:

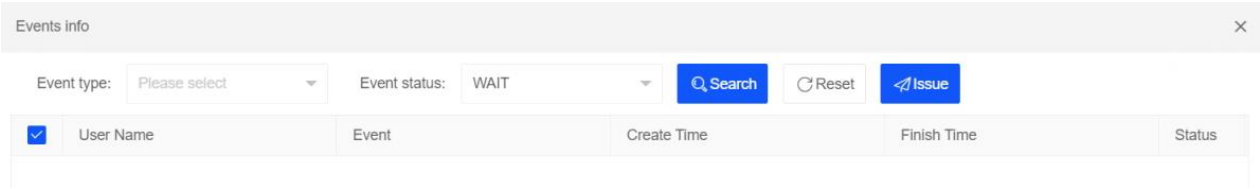


Figure 67

Check the events that need to be submitted, click the "Issue" button, and wait for the display of "Configuration Successful", which means that the configuration is successfully applied, as shown in Figure 68:

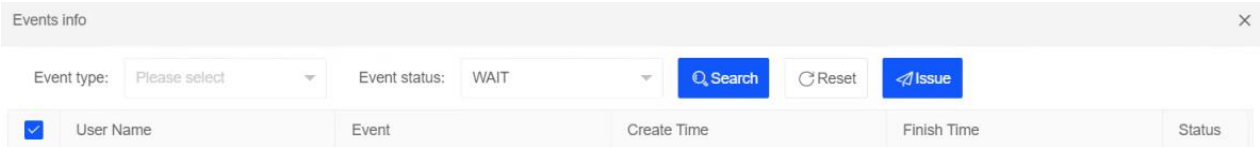


Figure 68

8.6 System setting

8.6.1 Regular choice

The system administrator (sysuser) can edit and modify the authorization information, device information, and working mode, and support system upgrades and full device backup operation, as shown in Figure 69:

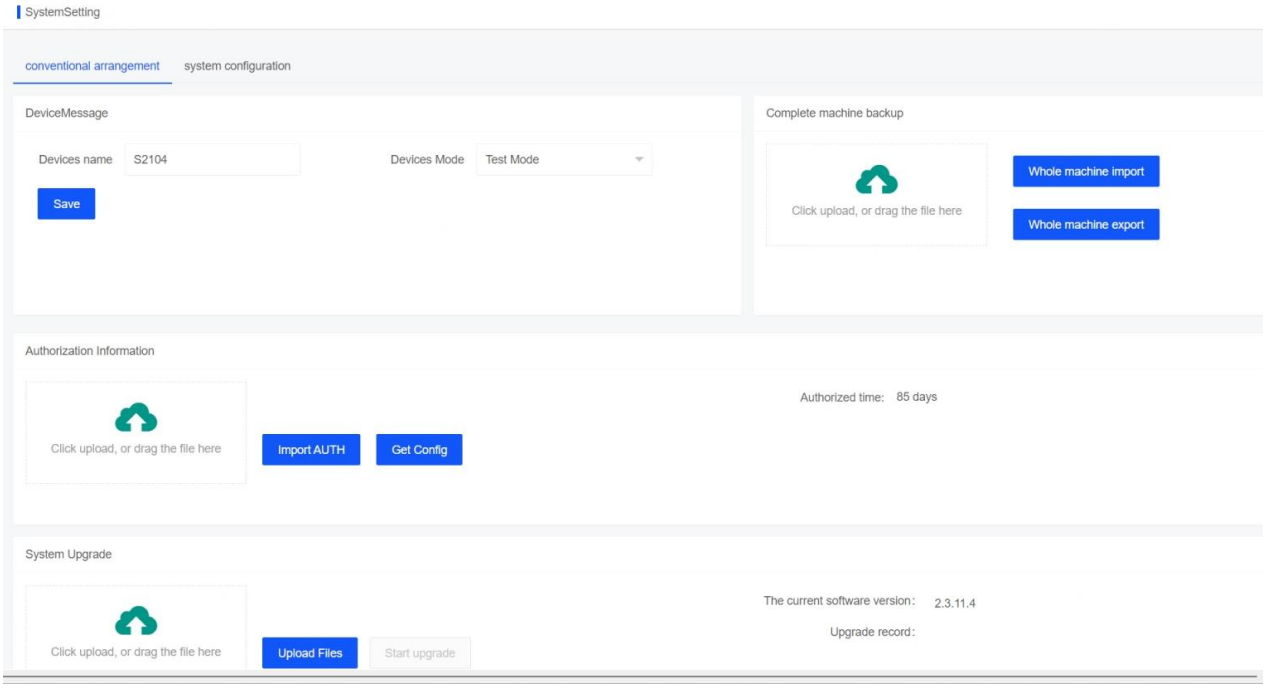


Figure 69

Name	Description
Authorization information	The authorization configuration can be obtained, and the authorization can be imported. In addition, the user can view the remaining days of authorization
Device Message	Set a device name
Device mode	Four available working modes, including protection mode, warning mode, learning mode and bypass learning mode
System upgrade	The user can view the current system version and upgrade records, and perform version upgrades
Complete machine backup	The whole device can export and import the backup file

8.6.2 System configuration

The system administrator (sysuser) can configure the system for Bypass, time server, restart, shutdown, factory reset and setup wizard, as shown in Figure 70:

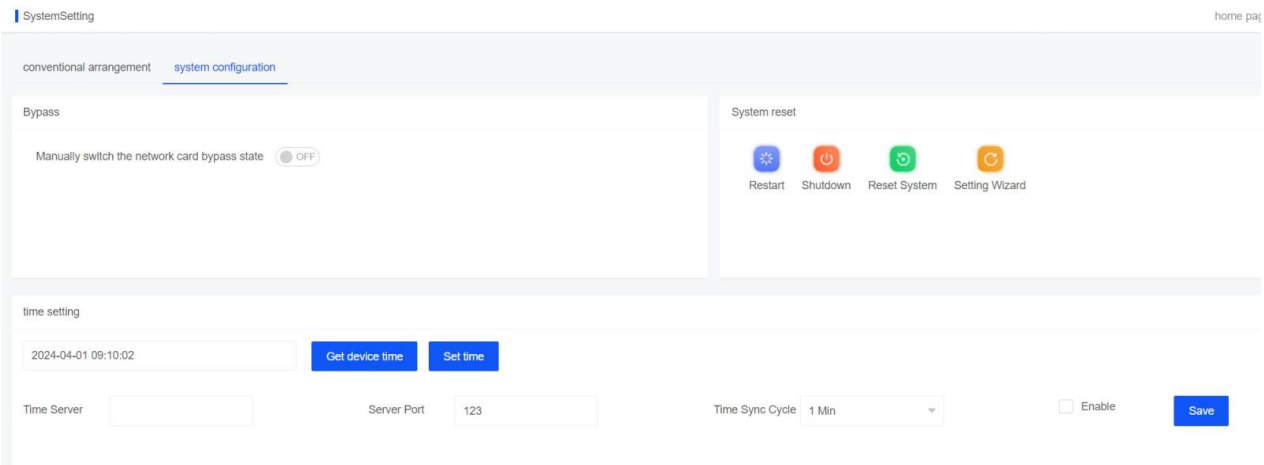


Figure 70

Name	Description
Bypass	The user can manually switch the Bypass state through settings and choose to turn on or off Bypass. Manual switching will not be allowed when the bypass is turned off
Time setting	The user can set the time, get the device time, and configure the time server, service port, time synchronization period and whether to enable
Restart	Click it to restart the industrial ethernet firewall
Shutdown	Click it to shut down the industrial ethernet firewall
Reset system	Click it to reset the device. Except for the management port address, the rest of the configuration is reset
Setting wizard	Click it to enter the initialization wizard

9 Centralized Management

9.1 Registration list

The centralized management function of industrial ethernet firewall means that firewall can be used as a centralized management terminal and the devices deployed in other areas can be registered on the centralized management platform so as to realize the control of the subordinate devices by the centralized management platform.

The functions of the centralized management platform are as follows:

1. View the basic information of the client device

After successful registration, the centralized management platform can view the basic information of the bound client device, including the device IP address, device name, serial number, authorization status, working mode, bypass status, etc.

2. Perform basic operations on the client device

For successfully registered devices, the centralized management terminal can manually switch the bypass mode and perform the operations such as authorization and de-registration of the devices.

In the device asset list of the centralized management terminal, the user can also log in to access the client device without password. In the alarm list of the show center, the user can directly jump to the data statistics page of the client device through the counted number of unprocessed alarms.

3. Monitor the operation and event information of client devices

For successfully registered devices, the centralized management terminal can view top5 device traffic conditions, alarm events and top5 attack information in real time in the show center, as well as the online and offline status of the devices. When the devices are offline, there will be an offline reminder and an offline prompt sound.

- **Manually add registration for centralized management terminal device**

In the registration list interface, the user can manually add registered assets, as shown in Figure 71:

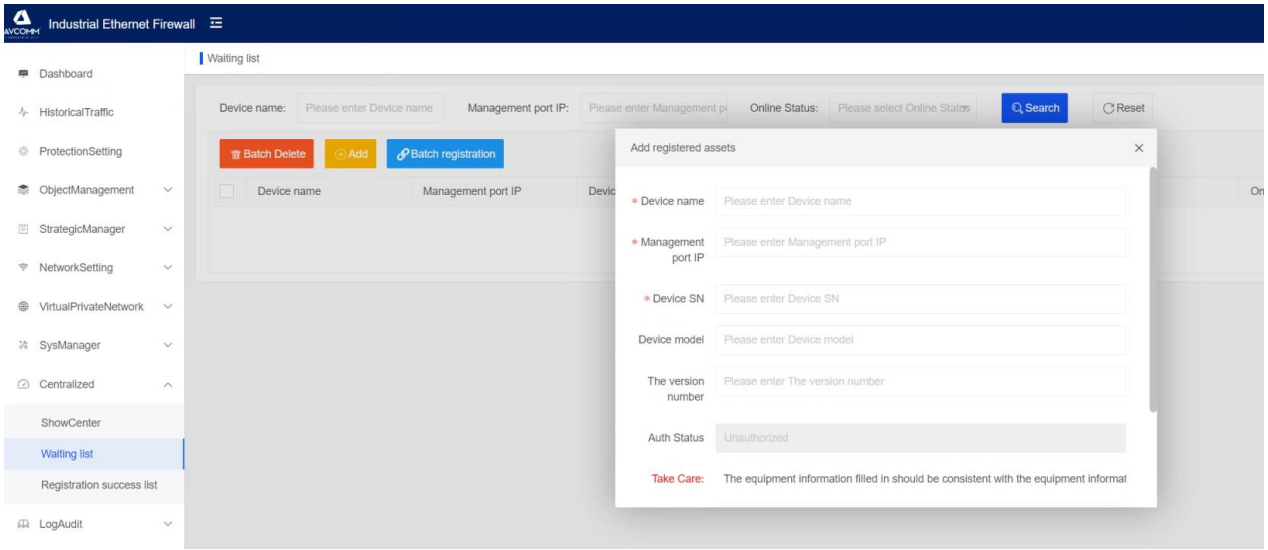


Figure 71

Name	Description
Device name	The name of the device requesting registration
Management port IP	IP address of management port for the device requesting registration
Device SN	The factory serial number of the device, which is the unique identification of the device
Device model	Model of the device for delivery
The version number	Version information of the device requesting registration
Auth status	Authorization status of the device requesting registration, through which the remaining license days of the device can be obtained
Online status	Online status of the device requesting registration, that is, whether the client device is still sending a registration request. If the client device no longer sends a request to this management platform, the status will be offline
Operation	The user can accept registration of the device requesting registration, and the device will be added to the successful registration list if the registration is accepted.

Note: For manually adding device asset information, the device name, management port IP and device serial number are required, and the rest are optional. The device serial number is used as the unique identifier of the device. When a device with a matching serial number requests registration, its information will be refreshed synchronously.

In the pending registration list interface, the user can query by device name, management port IP and online status, as shown in Figure 72:

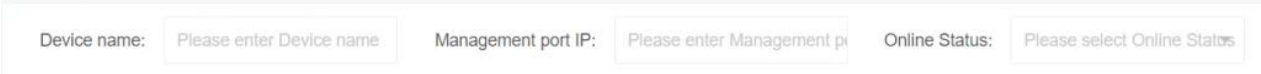


Figure 72

After registration, the user can see the successfully registered devices in the successful registration list, perform unbinding operations and view basic settings, as shown in Figure 73:

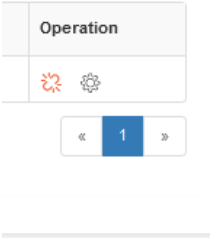


Figure 73

9.2 Show center

After the device is added to the successful registration list, the show center will display the statistical information of the device. In the device asset, the icon of this device will be displayed. In the alarm information statistics table, the alarm status of this device will be displayed. For the current risk assessment and total device traffic, the statistics on top 5 alarms of all devices and top 5 total device traffic will be taken into account, as shown in Figure 74:

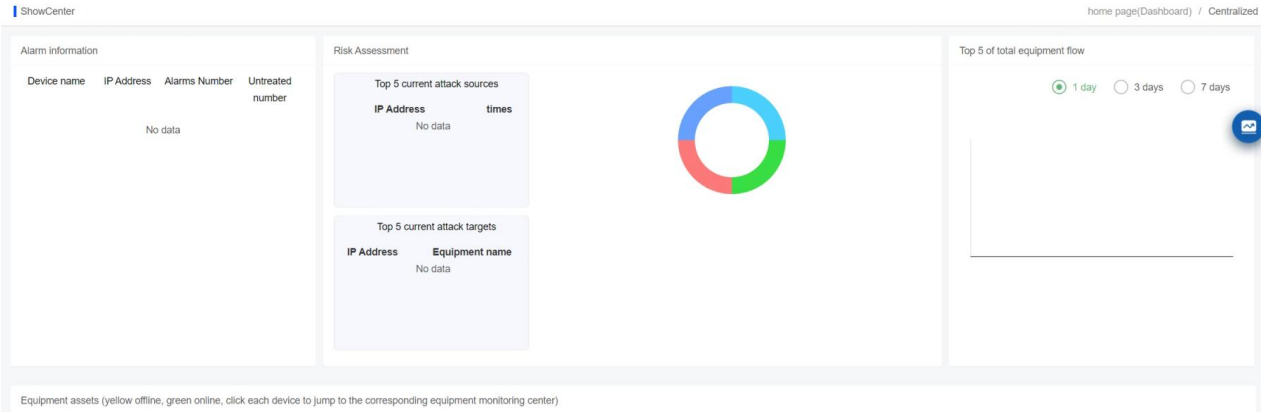


Figure 74

Name	Description
Alarm information	Collect the warning information of all successfully registered devices, including the device name, IP address, and the alarm number. Click the untreated number of the corresponding device to successfully jump to the alarm statistics page of this device
Risk assessment	For the risk assessment, the proportion of industrial protection warnings, network traffic warnings, system protection warnings, and other messages for all devices is collected. The TOP5 value of the source and purpose of the current attack is the summary of TOP5 attacks on all successfully registered devices
TOP 5 of total equipment flow	Top 5 total traffic of all successfully registered devices are collected, and the traffic information can be displayed for the last day, the last three days, and the last 7 days.
Equipment assets	After the device is successfully registered, the device information will be added to this statistics box. The green device icon indicates online and the yellow one indicates offline. When clicking on this device icon using a mouse, the user will successfully log in to the web interface of the device and operate the client device.
Offline reminder	After the successfully registered device goes offline, it will pop up an offline reminder and sound an alarm. The user can manually turn off the sound and minimize this pop-up window. The reminder will be closed when the device goes online.

10 Log Audit

10.1 Firewall log

The firewall log shows the category of protection log information recorded by the device (warning, error and prompt) and the distribution of protection log on the day (including industrial control events, network events, normal release protocols, and other events). For viewing the firewall log information, the user can filter the information to be viewed according to the source and destination IP, port and protocol type, time, log level, etc.. And the user can mark the selected item or the current page to read state. The protection log can be deleted or cleared, as shown in Figure 75:

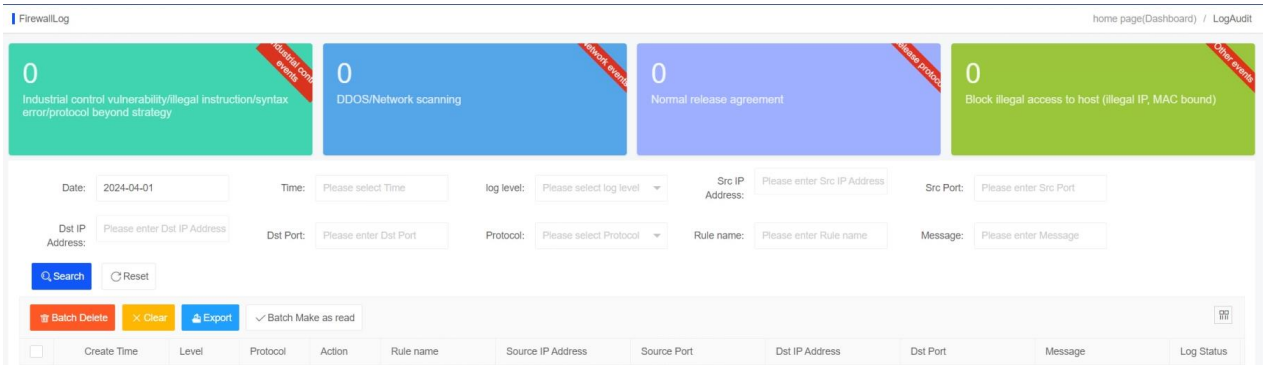


Figure 75

10.2 System log

The system log involves the query of system log information classification (warning, error and prompt) of all industrial ethernet firewall devices. The system log status can be inquired through the query time, log level, categorization information and message, and the system log can be deleted or cleared, as shown in Figure 76:

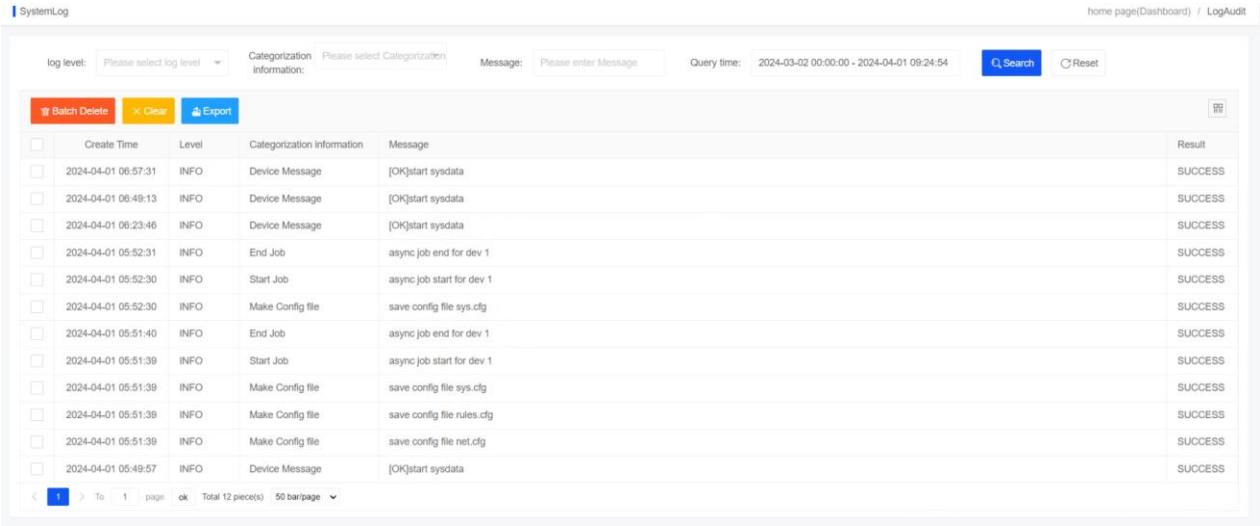


Figure 76

10.3 Admin log

The admin log involves the query of management log information classification (warning, error and prompt) of all industrial ethernet firewall devices. The admin log information can be filtered and viewed by user, IP address, log level, query time, message, etc., and the admin log can be deleted or cleared, as shown in Figure 77:

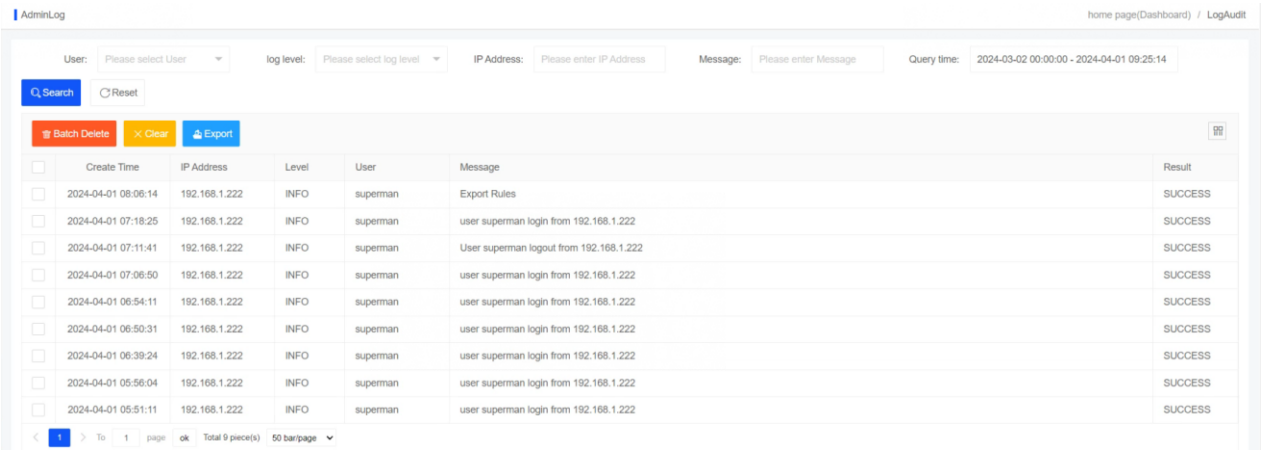


Figure 77

11 Appendix A

FAQ for AVCOMM industrial ethernet firewall:

11.1 What should I do if the web management page cannot be opened?

Answer: Check whether the industrial ethernet firewall device communicates with the client computer via the MAN port.

The default management address of the device is 192.168.4.2, please confirm whether the IP address for logging into the PC is in the same network segment

Ping the client computer to test whether the IP address of the WEB management interface can be pinged.

If you still cannot open the WEB management interface, please contact us info@avcomm.us.

11.2 What should I do if a white screen is displayed when opening the WEB management interface?

Answer: Change the browser used (Chrome or Firefox is preferred).

If it is still a white screen, please contact us info@avcomm.us.

11.3 What should I do if the business process is interrupted after the learned rules are applied?

Answer: Check the details of the applied rules to ensure that the communication commands are included. You can also manually add rules to ensure normal business communication.

If there is still an exception, please contact us info@avcomm.us.