3onedata



IAC8500-1GC4GT
Industrial Wireless AC
User Manual

Document Version: 04

Issue Date: 2023-06-13

Copyright © 2023 3onedata Co., Ltd. All rights reserved.

No company or individual is allowed to duplicate or transmit this manual in any forms without written permission issued by 3onedata Co., Ltd.

Trademark statement

3onedata , 3onedata and 3One data are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Note

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.



3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Nanshan District, Shenzhen, 518108 China
Technology support:	support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sale@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

Industrial wireless AC user manual has introduced the wireless AC:

- Network management method

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
″ ″	Words with “” represent the interface words. Eg: "The port number".
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.
About this chapter	The section ‘about this chapter’ provides links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

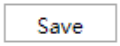
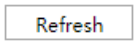
Symbols

Format	Description
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Make a necessary supplementary instruction for operation description.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Format	Description
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Button Operation Convention

Format	Description
	There is a logout button in the upper left corner of the webpage. After clicking it, the webpage returns to the login page.
	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.
	Check the line to be deleted, and then click the Delete button to delete the configuration.
	Click the Save button to submit the current configuration.
	Click “Refresh” button to refresh the current page.
	Click the switch to enable the function, as shown in figure: . Click the switch to disable the function, as shown in the figure: .

Revision Record

Version No.	Date	Revision note
01	03/15/2019	Product release
02	10/17/2019	Add USB Function
03	09/26/2022	Upgrade
04	06/13/2023	Software upgrade, add “Terminal Manage” function

Copyright © 3onedata Co., Ltd.

Contents

PREFACE 1
CONTENTS I
1 LOG IN THE WEB INTERFACE 1
1.1 SYSTEM REQUIREMENTS FOR WEB BROWSING 1
1.2 SETTING IP ADDRESS OF PC 1
1.3 LOG IN THE WEB CONFIGURATION INTERFACE 2
2 SYSTEM INFORMATION 4
3 CENTRALIZED MANAGEMENT 8
3.1 EQUIPMENT AUDIT 8
3.2 GROUP MANAGEMENT 9
3.2.1 Group Name 10
3.2.2 User Settings 11
3.2.3 Network Settings 12
3.2.4 WIFI Settings 13
3.2.5 Black and White List 21
3.2.6 Probe Settings 23
3.2.7 QoS Management 24
3.2.8 SNMP Management 26
3.2.9 User Event 27
3.2.10 Timed Restart 28
3.2.11 Configuration List 29
3.3 LOCATION MANAGEMENT 30
3.4 DEVICE LIST 31
3.5 WIRELESS TERMINAL LIST 34
3.5.1 Wireless Terminal List 34
3.5.2 Terminal Manage 35
3.6 BATCH CONFIGURATION 36
3.7 EQUIPMENT UPGRADE 38
3.8 FUNCTIONAL CONFIGURATION 39
3.9 QUERY SETTINGS 41
3.10 CONFIGURE INSTANCE: CONFIGURE AP PARAMETERS 42
4 NETWORK SETTINGS 48
4.1 LAN SETTINGS 48

Copyright © 3onedata Co., Ltd.

4.2 WAN SETTINGS 50
4.3 DHCP SETTINGS 53
4.4 VLAN SETTINGS 55
4.5 DYNAMIC DOMAIN NAME 57
4.6 ROUTING TABLE 58
5 ADVANCED NETWORK 61
5.1 UPNP SETTINGS 61
5.2 VRRP 63
5.3 RIP 67
5.4 OSPF 68
5.5 QOS 70
5.6 SLA SETTINGS 71
5.7 TRACK SETTINGS 72
5.8 SNMP MANAGEMENT 72
6 FIREWALL 74
6.1 IP ADDRESS BLACK/WHITE LIST 74
6.2 MAC FILTERING 75
6.3 URL FILTERING 76
6.4 KEYWORD FILTERING 77
6.5 PORT FORWARD 79
6.6 PORT REDIRECTION 80
6.7 DMZ SETTINGS 80
7 VPN TUNNEL 82
7.1 VPN CONNECTION STATUS 82
7.2 GRE SETTINGS 83
7.3 PPTP CLIENT SETTINGS 84
7.4 PPTP SERVER SETTINGS 86
7.5 L2TP CLIENT SETTINGS 88
7.6 L2TP SERVER SETTINGS 90
7.7 IPSEC 91
7.8 OPENVPN CLIENT SETTINGS 94
7.9 CERTIFICATE SETTINGS 98
8 SYSTEM TOOLS 100
8.1 TIME SETTINGS 100
8.2 ACCESS SETTINGS 101
8.3 TIMED RESTART 102
8.4 BACKUP RECOVERY 103
8.5 LOG MANAGEMENT 104
8.6 SYSTEM LOG 106
8.7 FIRMWARE UPGRADE 108
8.8 SYSTEM RESTART 109
9 DIAGNOSTIC TOOLS 110
9.1 PING TEST 110

Copyright © 3onedata Co., Ltd.

9.2 ROUTE TRACKING 111
10 MAINTENANCE AND SERVICE 112
10.1 INTERNET SERVICE 112
10.2 SERVICE HOTLINE 112
10.3 PRODUCT REPAIR OR REPLACEMENT 113

Copyright © 3onedata Co., Ltd.

1 Log in the Web Interface

1.1 System Requirements for WEB Browsing

The system should meet following conditions for using industrial wireless controller:

Hardware and Software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 8.0 or above
Operating system	Windows XP/7/10 or above

1.2 Setting IP Address of PC

The default management network address of the device as follows:

IP Settings	Default Value
IP Address	192.168.3.1
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Please confirm the computer has installed and enabled Ethernet network card.
- Before conducting remote configuration, please confirm the route between computer and device is reachable.
- Before making a local configuration, make sure that the IP address of the computer and the device are on the same subnet;

Note:

Copyright © 3onedata Co., Ltd.

While configuring the device for the first time, if it's the local configuration mode, first confirm the network segment of current PC is 3.

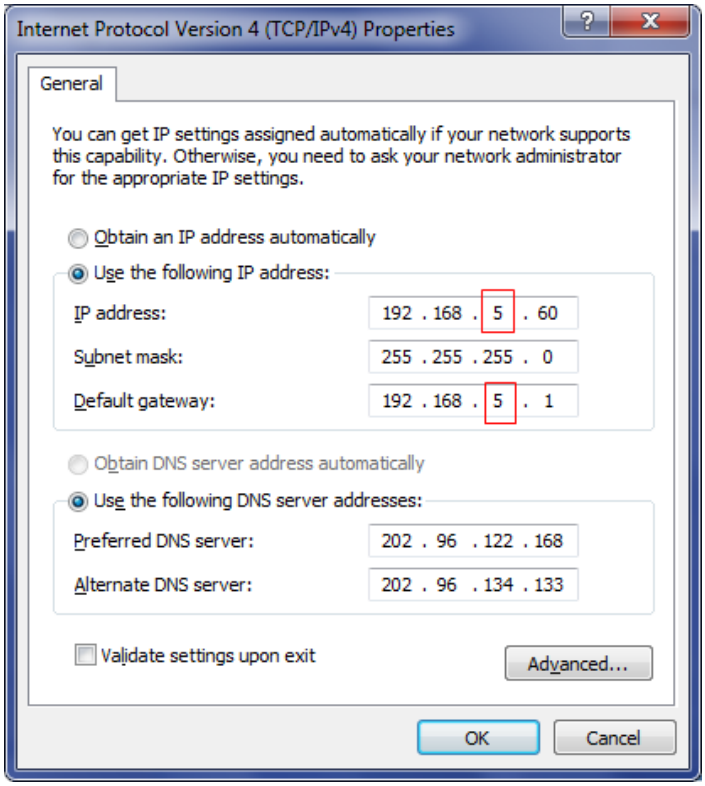
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "3".

Operation Steps

Amendment steps as follow:

Step 1 Open "Control Panel> Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2 Change the selected "5" in red frame of the picture below to "3".



Step 3 Click “OK”, IP address is modified successfully.

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

Login in the web configuration interface as follow:

Step 1 Run the computer browser.

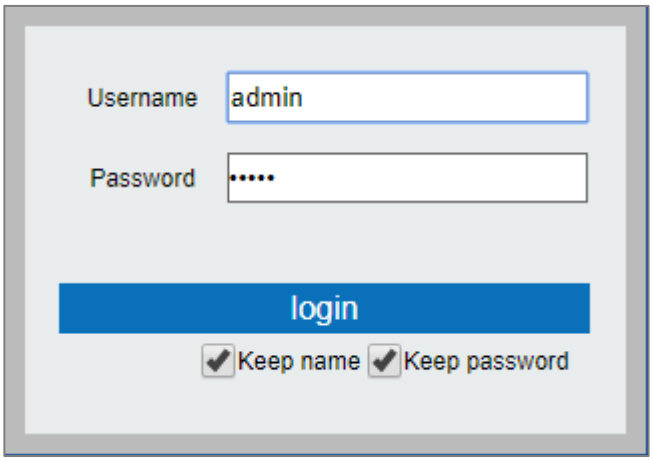
Step 2 In the address bar of browser, enter the device address "http://192.168.3.1".

Step 3 Click the “Enter” key.

Step 4 Pop-up dialog box as shown below, enter the user name and password in the login

Copyright © 3onedata Co., Ltd.

window.



Note:

The default user name and password for the serial server are "admin", which is strictly case-sensitive when typing.

Step 5 Click "Login".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.

Note:

After logging in to the device, user can modify the device IP address for convenient usage; if there is no interface operation within 10 minutes, user will need to log in to the device again.

Copyright © 3onedata Co., Ltd.

2 System Information

Function Description

You can view the following information:

- Product Information
- AP status
- Network overview
- Network status
- Network port status
- Network information
- Power status
- System overview
- Other Information

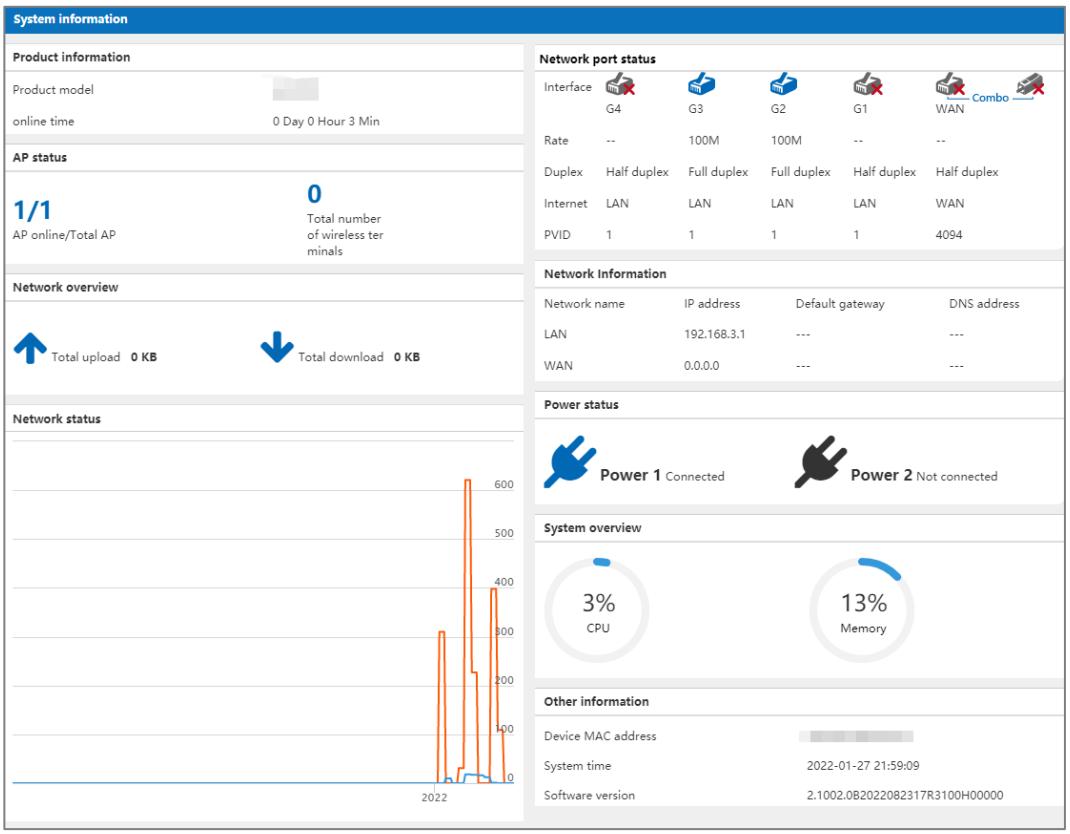
Operation Path

On the navigation bar, select "System information".

Interface Description

System information interface as follows:

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.



The main element configuration description of state information interface:

Interface Element	Description
Product Information	**The system information bar**
Product model	Display device model name
Online time	Display device running time
AP status	**AP status bar**
AP online / Total AP	Display the number of online AP device and total AP device that have been added into management
Total number of wireless terminals	Displays the total number of wireless terminal online devices that have joined the management.
Network overview	**Network overview bar**
Total upload	Total upload area. Note: Upstream traffic statistics of WAN port.
Total download	Total download area. Note: Downstream traffic statistics of WAN port.
Network status	**Network status bar**
Network state diagram	Real-time flow monitoring view: • Download: the orange line represents device's rate

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	changes of download traffic; • Upload: the blue line represents device's rate changes of upload traffic.
Network port status	**Network port status bar**
Interface	Display the connection status of each device interface: • : connected; • : disconnected.
Rate	Display the corresponding rate of the port, self-adaptive rate: • - • 10M • 100M • 1000M
Duplex	Display the corresponding duplex mode of the port: • Half duplex: the interface can only receive or send data at any time. • Full-duplex: interface can receive and send data at the same time.
Internet	Display the network type of the port: • LAN • WAN
PVID	VLAN ID number of the port
Network information	**Network information bar**
Network name	Display the connected network type of the device: • LAN • WAN
IP Address	IP address of intranet or external network.
Default gateway	Default gateway address of intranet or external network.
DNS address	DNS server address of intranet or external network.
Power status	**Power status bar**
Power status information	Display the connection status information of the power: • Not connected • Connected
System overview	**System overview bar**
CPU	The usage rate of device CPU.
Memory (%)	The usage rate of device memory. Note: The performance of the device would be affected if the application consumes too much memory.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Other information	**Other information bar.**
Device MAC address	Display device MAC address information, format is XX:XX:XX:XX:XX:XX.
System time	Display the current time of the system, format is year-month-day hour:minute:second
Software version	Display device software version information

Copyright © 3onedata Co., Ltd.

3 Centralized Management

3.1 Equipment Audit

Function Description

It displays connected AP devices. User can conduct relevant operations such as searching, managing and deleting connected AP devices.

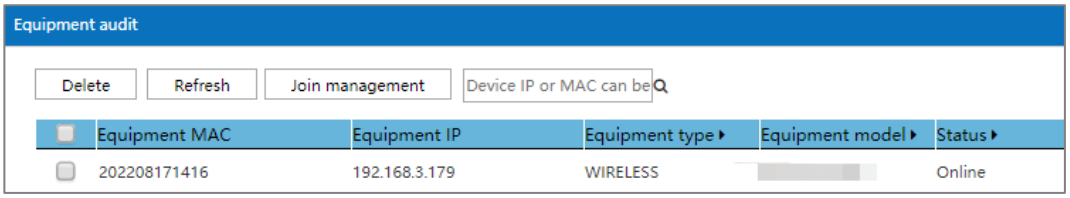
This function is not enabled by default, that is, the page will not be displayed, and the device will automatically assign groups. After it is enabled in the function configuration, this page will be displayed, at which time the device can manually assign groups.

Operation Path

Open in order: “Centralized Management > Equipment Audit”.

Interface Description

The equipment audit interface is as follows:



The main element configuration description of equipment audit interface:

Interface Element	Description
Equipment MAC	Display the MAC address of AP equipment
Equipment IP	Display the IP address of AP equipment
Equipment Type	Display the equipment type of AP equipment
Equipment Model	Display the equipment model of AP equipment
Status	Display the connection status of AP equipment: • Online

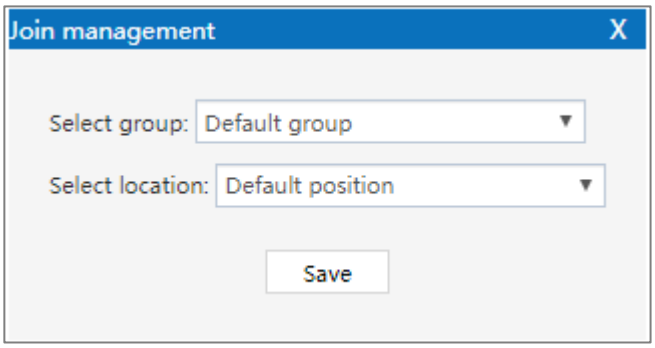
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Offline

Interface Description: Join Management

Check device information entry to join management and click “join management” button.

The join management interface is as follows:



The main element configuration description of join management interface:

Interface Element	Description
Select group	Choose group drop-down box, default to default group Note: • Default group is mainly used for equipment audit. The original configuration of equipment added to default group won’t be modified; • In general, it’s recommended to implement equipment audit and group selection operation after creating groups in group management.
Select location	Choose position drop-down box, default to default position Note: In general, it’s recommended to implement equipment audit and position selection operation after creating position in position management.

3.2 Group Management

Function Description

You can add a group to configure the devices within the group in batches, such as network settings, WIFI settings, black/white list, probe settings, QoS management, SNMP management, user events, and timed restart.

Copyright © 3onedata Co., Ltd.

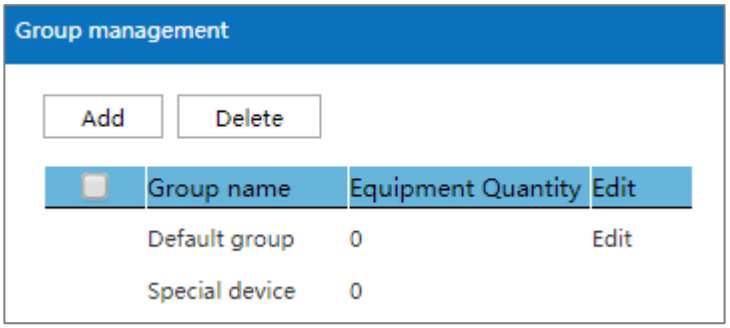
The default special device group can only see the online status of the device, and the configuration cannot be modified. It is mainly used to place devices in bridge and client mode. When a device accesses AC for the first time, if it is not AP or routing mode, it will be added to a special device group, and it can also be switched to this group through the "Device List" interface. When the work mode of the device joining the group changes, the group will not be changed, and the group can be manually switched. If the device audit function is enabled, the device connected to AC for the first time can be manually assigned to the group.

Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

The group management interface is as follows:



The main element configuration description of group management interface:

Interface Element	Description
Group name	The name of this group
Equipment Quantity	The device number of this group
Operation	Edit: modify device group information. Note: The device information in default group cannot be modified.

3.2.1 Group Name

Function Description

User can set group name.

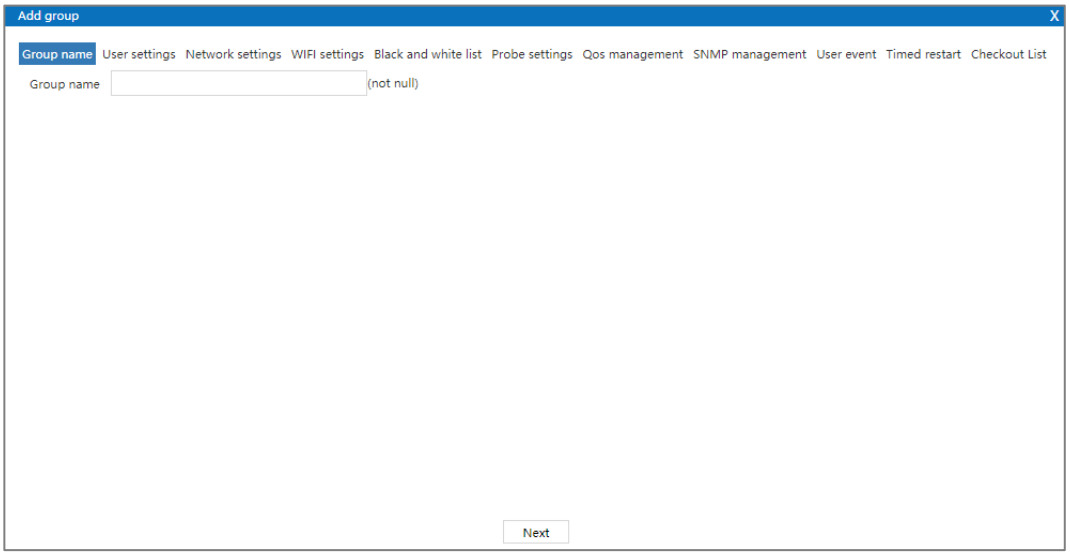
Operation Path

Open in order: “Centralized Management > Group Management”.

Copyright © 3onedata Co., Ltd.

Interface Description

Click “Add” button. The group name interface is as follows:



The main element configuration description of group name interface:

Interface Element	Description
Group name	Group name that need to be added Note: It’s recommended to use one or more types of characters, such as Chinese characters, English letters or numbers. Special characters cannot be used.

3.2.2 User Settings

Function Description

User can set username and password of AP devices.

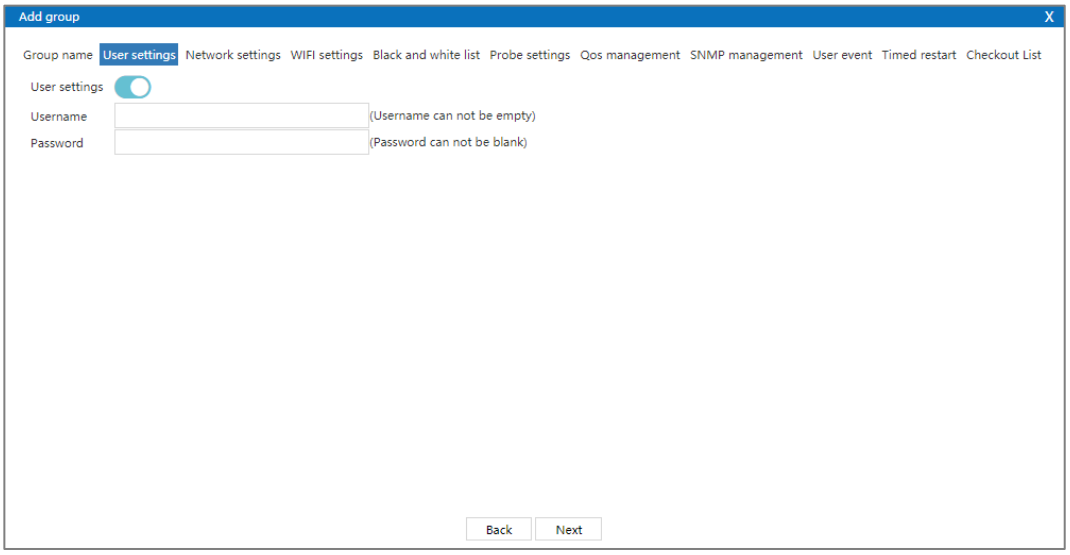
Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The user settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of user settings interface:

Interface Element	Description
Username	Set the username of AP devices in the group Note: • Both the username and password consist of uppercase and lowercase letters, as well as numbers; • The username cannot be empty if choosing setting in the user settings.
Password	Set the password of AP devices in the group Note: • Both the username and password consist of uppercase and lowercase letters, as well as numbers; • The password cannot be empty if choosing setting in the user settings.

3.2.3 Network Settings

Function Description

On the “Network Settings” page, user can set work mode and other relevant information of AP devices.

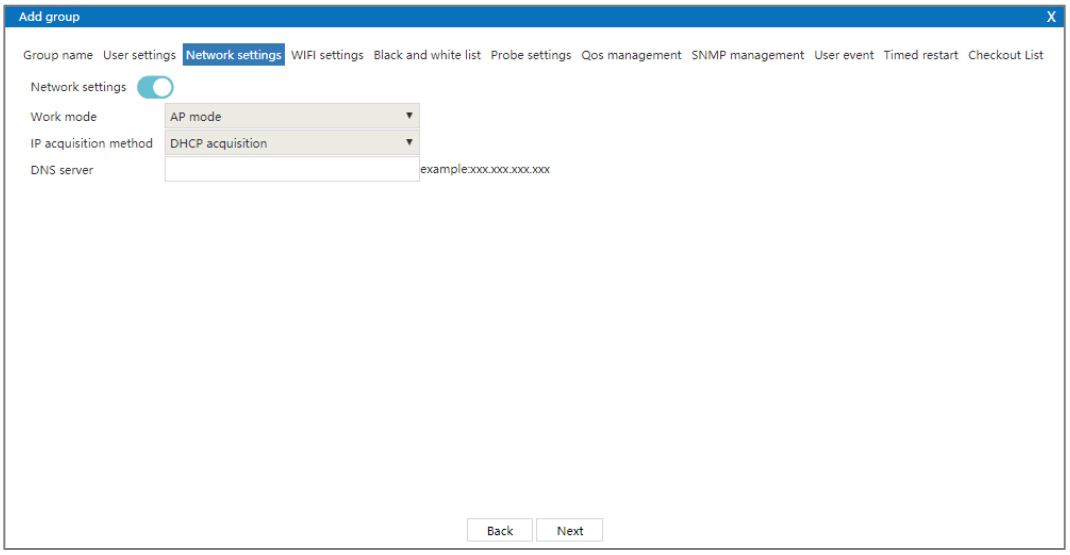
Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The network settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of network settings - routing mode interface:

Interface Element	Description
Work mode	AP mode
IP acquisition method	In AP mode, IP of default AP is dynamically acquired.
DNS server	IP address of DNS server, format xxx.xxx.xxx.xxx.

3.2.4 WIFI Settings

Function Description

User can set WIFI and other relevant information of AP devices.

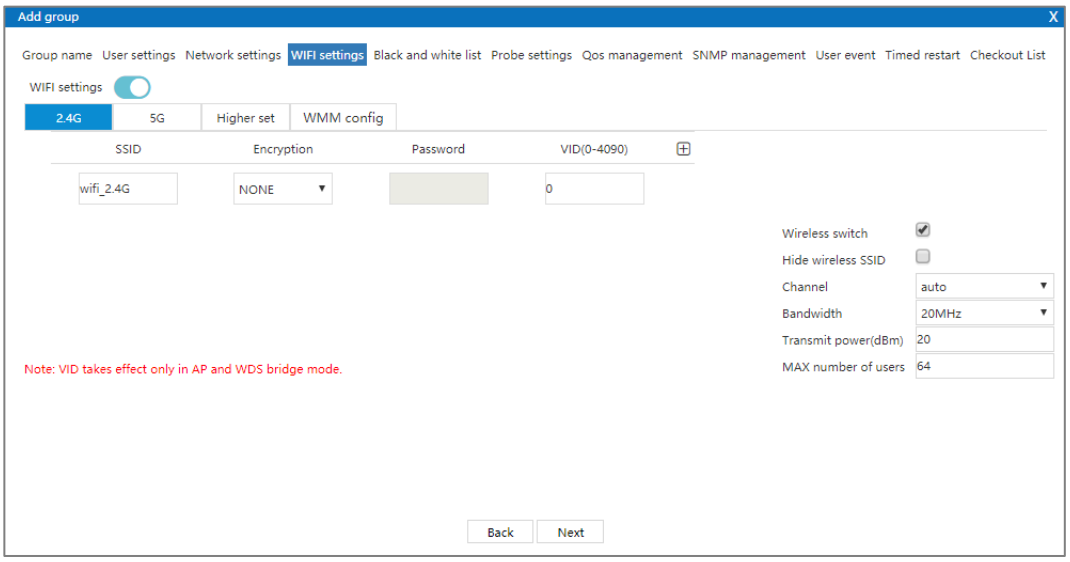
Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The WiFi settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of WIFI settings interface:

Interface Element	Description
2.4G	**2.4G configuration bar**
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Password	Password of wireless network, it supports 8-63 valid characters.
VID	Wireless network VLAN ID. Note: VID configuration is supported only in AP mode and bridge mode using WDS bridging.
Wireless switch	2.4G wireless Network function enable checkbox, check to enable wireless network function.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Hide wireless SSID	Hidden SSID function enable checkbox, check to enable hidden SSID function. SSID name of the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal manually while connecting hidden wireless signal.
Channel	Working channel of 2.4G wireless network, default to "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 1: main frequency band 2412Hz, frequency range 2401~2423Hz; • 2: main frequency band 2417Hz, frequency range 2406~2428Hz; • 3: main frequency band 2422Hz, frequency range 2411~2433Hz; • 4: main frequency band 2427Hz, frequency range 2416~2438Hz; • 5: main frequency band 2432Hz, frequency range 2421~2443Hz; • 6: main frequency band 2437Hz, frequency range 2426~2448Hz; • 7: main frequency band 2442Hz, frequency range 2431~2453Hz; • 8: main frequency band 2447Hz, frequency range 2436~2458Hz; • 9: main frequency band 2452Hz, frequency range 2441~2463Hz; • 10: main frequency band 2457Hz, frequency range 2446~2468Hz; • 11: main frequency band 2462Hz, frequency range 2451~2473Hz; • 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in America, so it's temporarily unavailable; • 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in America, so it's temporarily unavailable; Note: In order to improve the network performance, please choose unused channel in the device working environment.
Bandwidth	Channel bandwidth of wireless network, it defaults to 20MHz, options as follows:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 20MHz; • 40MHz.
Transmit power	Transmit power of 2.4G wireless signal. Value range is 1~30dBm. Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is. • Different device has different transmitting power range.
Max number of users	Maximum user number of 2.4G wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected user number.
5G	**5G configuration bar**
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Password	Password of wireless network, it supports 8-63 valid characters.
VID	Wireless network VLAN ID. Note: VID configuration is supported only in AP mode and bridge mode using WDS bridging.
Wireless switch	5G Wireless Network function enable checkbox, check to enable wireless network function.
Hide wireless SSID	Hidden SSID function enable checkbox, check to enable hidden SSID function. SSID name of the device wireless

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal manually while connecting hidden wireless signal.
Channel	Working channel of 5G wireless network, default to "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 36: main frequency band 5180Hz, frequency range 5170~5190Hz; • 40: main frequency band 5200Hz，frequency range 5190~5210Hz; • 44: main frequency band 5220Hz, frequency range 5210~5230Hz; • 48: main frequency band 5230Hz, frequency range 5210~5250Hz; • 52: main frequency band 5260Hz, frequency range 5250~5270Hz; • 56: main frequency band 5280Hz, frequency range 5270~5290Hz; • 60: main frequency band 5300Hz, frequency range 5290~5310Hz; • 64: main frequency band 5320Hz, frequency range 5310~5330Hz; • 100: main frequency band 5510Hz, frequency range 5490~5530Hz, this frequency band is not open in China, so it's temporarily unavailable; • 104: main frequency band 5520Hz, frequency range 5510~5530Hz, this frequency band is not open in China, so it's temporarily unavailable; • 108: main frequency band 5540Hz, frequency range 5530~5550Hz, this frequency band is not open in China, so it's temporarily unavailable; • 112: main frequency band 5560Hz, frequency range 5550~5570Hz, this frequency band is not open in China, so it's temporarily unavailable; • 116: main frequency band 5580Hz, frequency range 5570~5590Hz, this frequency band is not open in China, so it's temporarily unavailable; • 120: main frequency band 5600Hz, frequency range 5590~5610Hz, this frequency band is not open in China, so it's temporarily unavailable;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 124: main frequency band 5620Hz, frequency range 5610~5630Hz, this frequency band is not open in China, so it's temporarily unavailable; • 128: main frequency band 5640Hz, frequency range 5630~5650Hz, this frequency band is not open in China, so it's temporarily unavailable; • 149: main frequency band 5745Hz, frequency range 5735~5755Hz; • 153: main frequency band 5765Hz, frequency range 5755~5775Hz; • 157: main frequency band 5785Hz, frequency range 5775~5795Hz; • 161: main frequency band 5805Hz, frequency range 5795~5815Hz; • 165: main frequency band 5825Hz, frequency range 5815~5835Hz; Note: In order to improve the network performance, please choose unused channel in the device working environment.
Bandwidth	Channel bandwidth of 5Gwireless network, it defaults to 80MHz, options as follows: • 20MHz; • 40MHz; • 80MHz.
Transmit power	Transmit power of 5G wireless signal. Value range is 1~30dBm. Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is. • Different device has different transmitting power range.
Max number of users	Maximum client number of the 5G wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.
Advanced Configuration	**Advanced Configuration Bar**
Short GI	Short GI (Short Guard Interval) checkbox: • Check: enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed. • Uncheck: after disabling the function, the transmission

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	interval of data packet defaults to 800ns. Note: Under high signal strength and low latency, this function can be enabled to improve nearly 10% handling capacity.
WDS	WDS (Wireless Distribution System), this function is used for bridging multiple WLAN. Note: Please enable WDS function while bridging the device with other wireless devices.
Wireless isolate	Wireless user isolation, it's used for isolating the wireless clients connected to the device wireless network with same SSID, defaults to disabled. Note: After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.
WMM	Wireless multimedia check box, check it to enable WMM configuration.
80211r	802.11r check box, check it to enable the fast roaming function. Note: 802.11r configuration is supported only in AP mode.
RTS	Data packet RTS (Request to Send) threshold, value range 0-2347, defaults to 2347. • RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will send RTS signal; • 0 < RTS threshold < 2347: when the length of data packet surpasses RTS threshold, the device wireless terminal will send RTS signal to avoid signal conflict; • RTS threshold = 2347: the device wireless terminal won't send RTS signal. Note: • As for the wireless nodes in different wireless detection range of AP range, collision will occur when the nodes send out signals; RTS function can avoid the collision. • The device will send RTS to destination station for negotiation when the length of data packet surpasses RTS threshold. After receiving RTS frame, the wireless station will send a CTS (Clear to Send) frame to the device, which represents the two can conduct wireless communication.
Country	Applied countries and regions. Options are as follows: • China;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• USA. Note: Different country opens different channels.
Authentication method	Authentication mode of wireless network, options as follows: • Personal edition: wireless network WPA/WPA2/WPA3 uses WPA/WPA2-PSK/ WPA3-SAE encryption method and pre-shared key. Personal edition is suitable for personal and home users; • Enterprise edition: wireless network WPA/WPA2/WPA3 uses WPA-802.1X/WPA2-802.1X/WPA3-802.1X encryption method. It is necessary to install Radius server to authenticate, and suitable for enterprise users with high security requirements. Note: Authentication mode can be configured after the wireless network is encrypted, WAP2/WAP3 encryption mode does not support enterprise authentication mode for the time being.
Radius Server IP	IP address of RADIUS(Remote Authentication Dial In User Service) sever. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.
Radius Server port	The authentication port number of the RADIUS server,value range is 1-65535. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.
RADIUS Shared key	Shared key of RADIUS server. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.
WMM Configuration	**WMM Configuration Bar**
WMM Configuration Tab	• 2.4G WMM Configuration • 5G WMM Configuration
Scene	WMM scene settings, options: • No priority; • Multimedia First; • User-defined. Note: • The default scenario is no priority. At this time, data stream and video voice stream have the same priority, and no one has the priority. • After selecting WMM function, the device can process the data packet with priority level, improving the data transmission

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	performance of WMM and ensuring the service quality of voice, video and other services with high real-time requirements. • To select user-defined functions, users need to set their own parameters.
EDCA AP Parameters	WMM priority queue, options are as follows: • AC_BE (best effort streaming); • AC_BK (background streaming); • AC_VI (video streaming); • AC_VO (voice streaming);
EDCA STA Parameters	EDCA (Enhanced Distributed Channel Access) parameters of terminal device (Workstation STA) supporting 802.11 standard.
CWmin	Minimum competition window, available values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767
CWmax	Maximum contention window, available values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767. Note: The value of the maximum contention window must be greater than that of the minimum contention window.
AIFSN	AIFSN, Arbitration Inter Frame Spacing Number WMM can configure different idle waiting time for different AC. The larger the value of AIFSN, the longer the idle waiting time of users will be. Value range is 1-255.
TXOP Limit	Transmission Opportunity Limit The maximum length of time the user can occupy the channel after a successful competition The larger this value is, the longer the user can occupy the channel at a time. If it is 0, only one message can be sent after occupying the channel at a time. Note: The value of this parameter must be positive and modification is not recommended.

3.2.5 Black and White List

Function Description

User can manage the connection of wireless users, filter wireless users and other operations.

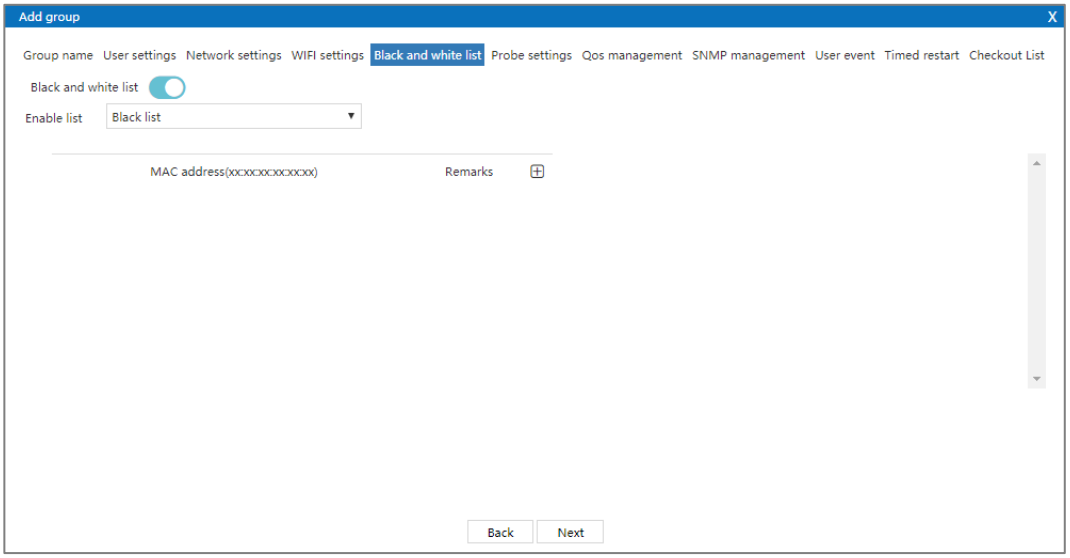
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button and finish group name settings. The black and white list interface is as follows:



The main element configuration description of black and white list interface:

Interface Element	Description
Enable list	Drop-down box of enable list: • Black list: list of wireless client forbidden to visit wireless network; • White list: list of wireless client allowed to visit wireless network; wireless clients out of white list are forbidden to visit; • Pending list: the list to be checked, which could be set to white list or black list. Note: User can only set one list of the three lists, black list, white list and pending list once.
MAC address	MAC address of wireless client, the format is XX:XX:XX:XX:XX:XX
Remarks	Remark description of the list

Copyright © 3onedata Co., Ltd.

3.2.6 Probe Settings

Function Description

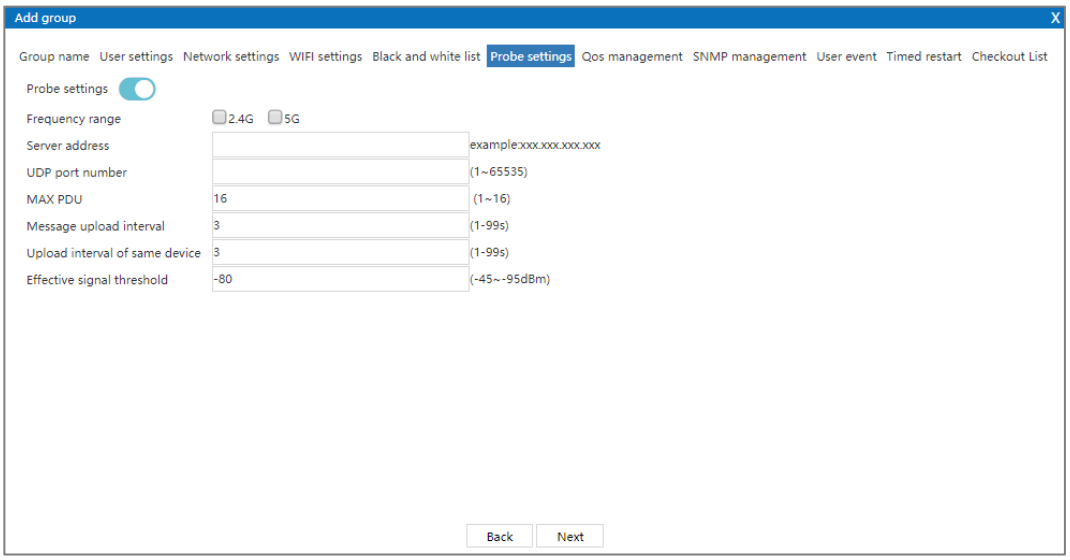
User can send the detected wireless terminal device information to the specified server.

Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The probe settings interface is as follows:



The main element configuration description of Probe settings interface:

Interface Element	Description
Frequency range	Frequency band used by wireless probe: • 2.4GHz • 5GHz
Server Address	Server address.
UDP port number	The port number of the server,value range is 1-65535.
Max PDU	Maximum device number that data transmission unit contains, valid value range 1-16.
Message upload interval	Time interval of data message upload, unit is second.
Upload interval of the same device	Time interval of the same device data upload, unit is second.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Effective signal threshold	Effective wireless signal threshold, unit is dBm, value range: -45-95. Note: If the signal strength of wireless client is less than threshold, it will be regarded as invalid signal.

3.2.7 QoS Management

Function Description

You can configure QoS policies and QoS whitelists.

- You can limit the average rate and maximum rate of data transmission for IP addresses within the policy range.
- QoS White List can set the white list of IP or MAC address. The data transmission rate in the list is not limited by the QoS policy.

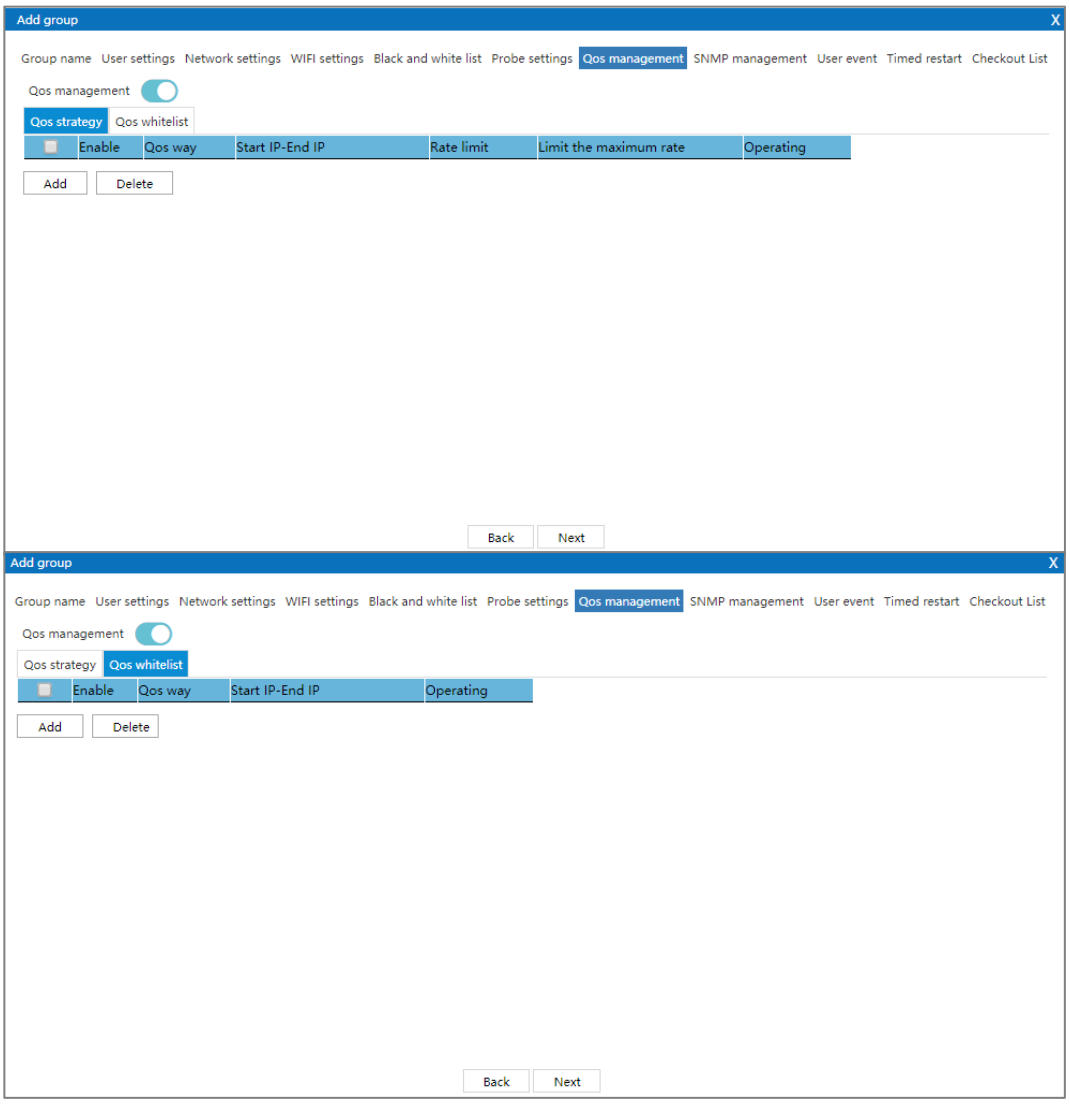
Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The QoS Management interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of QoS Management interface:

Interface Element	Description
QoS Strategy	**QoS Strategy bar**
Enable	Enable QoS strategy or not
QoS way	The method of enabling QoS strategy, available values: • IP-based speed limit • MAC-based speed limit.
Start IP-End IP	The range of the speed limit from the start IP address to the end IP address
Rate limit	The average value of limited rate.
Limit the maximum rate	The maximum value of limited rate.
Operating	Click "Edit" button to modify this QoS strategy
Add	Click "Add" button to add QoS strategy Note:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• A maximum of 3 policies is supported. • If there are multiple repeated rules for the same device, the last rule shall prevail.
Delete	Check the QoS strategy to be deleted, and click the "Delete" button to delete QoS strategy
QoS Whitelist	**QoS Whitelist Bar**
Enable	Enable QoS whitelist or not
QoS way	The method of enabling QoS strategy, available values: • IP white list; • MAC whitelist.
Start IP-End IP	The range of starting and ending IP addresses whose rate is not affected by QoS strategy.
Operating	Click "Edit" button to modify this QoS whitelist

3.2.8 SNMP Management

Function Description

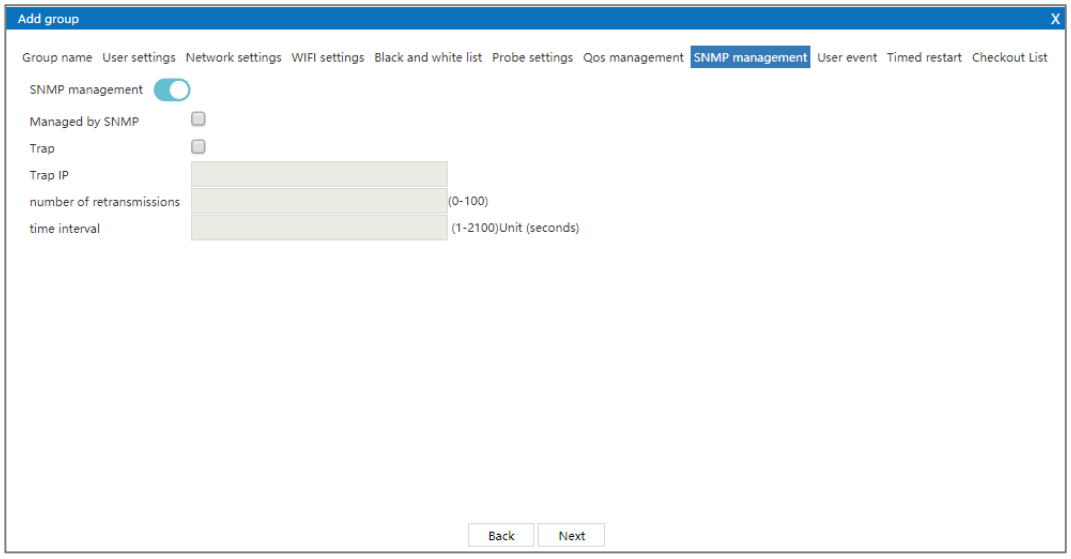
SNMP management can be enabled, and Trap can be enabled.

Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The SNMP Management interface is as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of SNMP management interface:

Interface Element	Description
Managed by SNMP	Managed by SNMP check box, check it to enable the Managed by SNMP function.
Trap	Trap check box, check it to enable Trap information, and the device actively sends the abnormal situation of the device to the management server. Note: Trap anomaly mainly include wireless client online and offline, hardware and software restarting, etc.
Trap IP	The IP address of the server receiving Trap information.
Number of retransmissions	Time of resending Trap information.
Time interval	Time interval of device sending Trap information, the unit is second.
Allow multicast transparent transmission	Allow multicast passthrough check box. When checked, multicast data is allowed to passthrough in intranet. After SNMP management is enabled, multicast passthrough is not allowed by default.

3.2.9 User Event

Function Description

You can transmit online/offline event of wireless users to designated server.

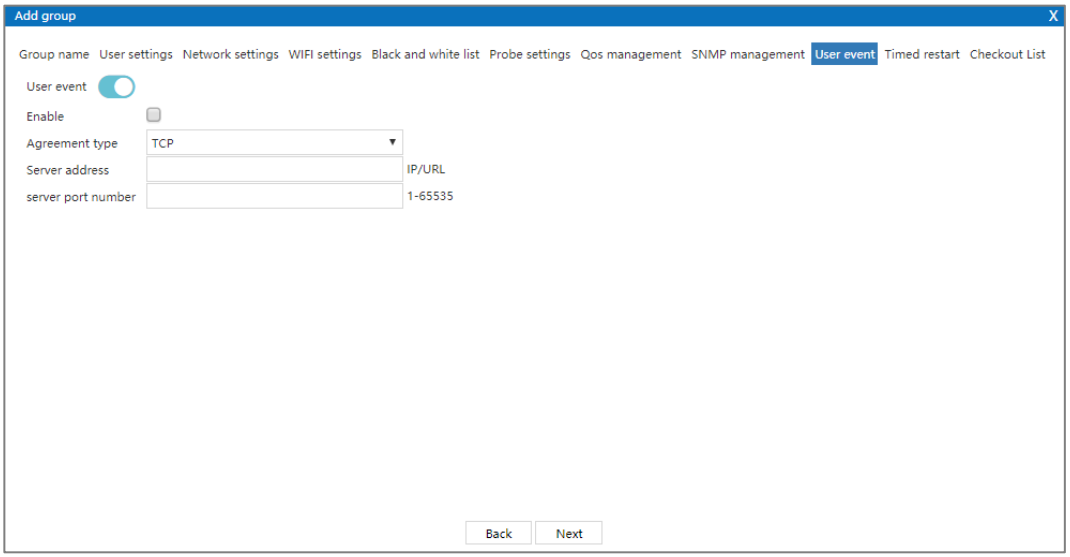
Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The user event interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of user event interface:

Interface Element	Description
Enable	Enable “User Events”.
Agreement type	Select the communication protocol that transmits user events. • TCP Protocol • UDP Protocol • HTTP Protocol
Server Address	The address of the server that receives the wireless user's online and offline events.
Server port number	The port number of the server that receives the wireless user's online and offline events.

3.2.10 Timed Restart

Function Description

You can set the periodic and timed restart of the AP device in weeks.

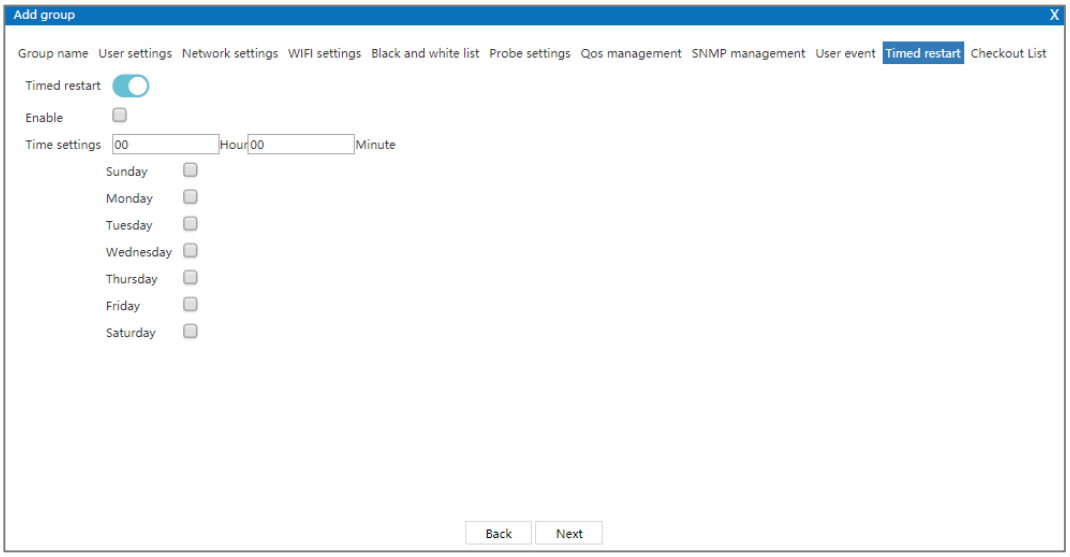
Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The Timed Restart interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of timed restart interface:

Interface Element	Description
Enable	Enable check box of timed restart.
Time settings	Set the time of timed restart.
Week settings	Check the restart date to set periodic timed restart in weeks.

3.2.11 Configuration List

Function Description

Display the list of group configurations.

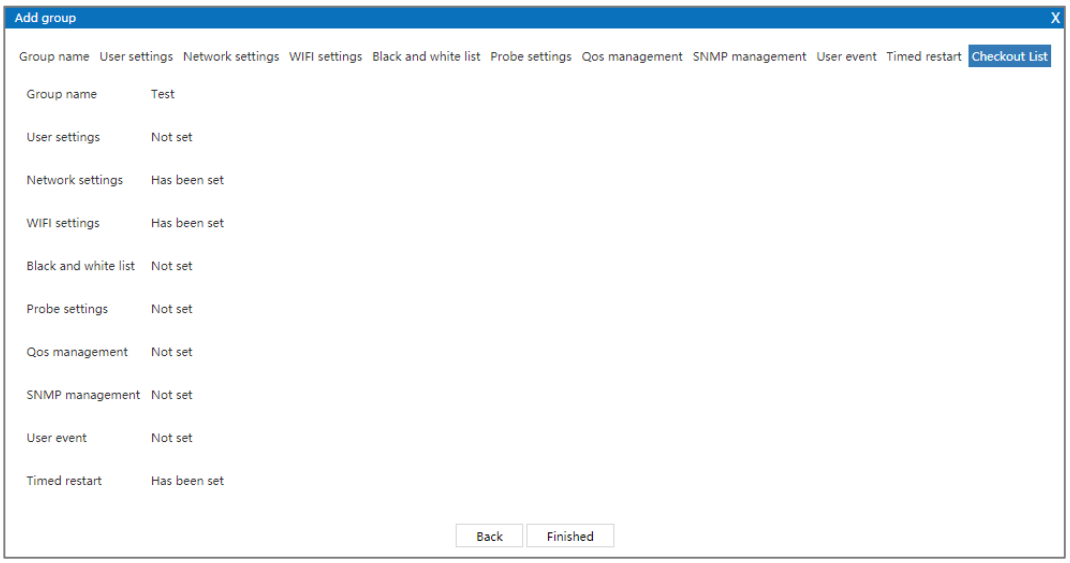
Operation Path

Open in order: “Centralized Management > Group Management”.

Interface Description

Click “Add” button to finish group name settings. The Configuration List interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of Configuration List interface:

Interface Element	Description
Checkout List	Display Group configuration information.

3.3 Location Management

Function Description

User can set the location information of the device and make remarks on the location.

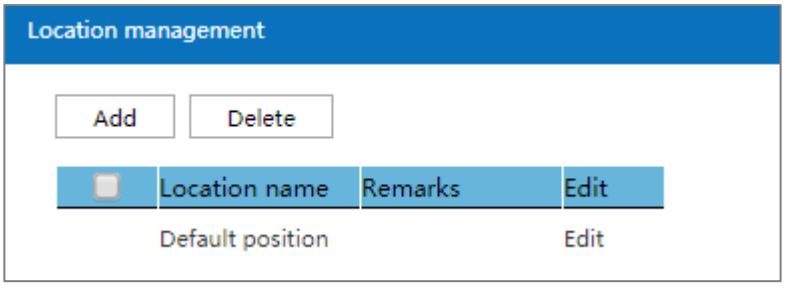
Location is for marking only, not for configuration.

Operation Path

Open in order: “Centralized Management > Location Management”.

Interface Description

The Location management interface is as follows:



The main element configuration description of location management interface:

Interface Element	Description
Location name	Location name
Remarks	Location remarks

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Operation	Edit: modify device location information.

3.4 Device List

Function Description

The current configuration and information of AP can be displayed, but with a lag of about 2 minutes. If the configuration of the device is modified, and the updated configuration can be seen by refreshing after 2 minutes, then the modification is successful.

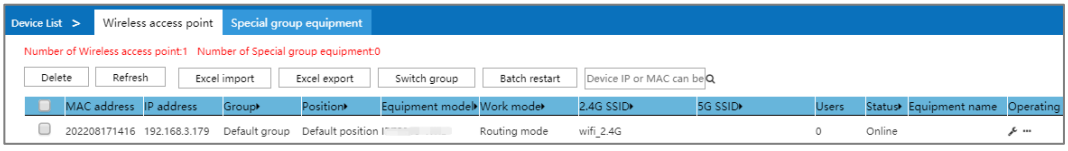
The list of devices shows AP devices that have joined the group management. The AC device and AP interactively supports protocol 1 (old version) and protocol 2 (new version). By default, AC discovers AP devices through protocol 2. When discovering AP devices of protocol 1, the information of AP devices is displayed in red letters. The AP device cannot be configured through group management (protocol 2), and it supports deletion. For this kind of AP devices, their program can be upgraded by batch upgrade function, or the AC devices can be configured as protocol 1 by function configuration. The new version of AP device is compatible with protocol 1 and protocol 2.

Operation Path

Please open in order: “Centralized Management > Device List”.

Interface Description 1: Wireless Access Point

Wireless Access Point interface as follows:



The main element configuration description of wireless Access Point interface:

Interface Element	Description
MAC address;	Display the MAC address of AP equipment
IP Address	The IP address is the IP address of AC receives the message when AP communicates with AC. If there is a cross gateway between AP and AC, it is shown as the IP address of the gateway.

Copyright © 3onedata Co., Ltd.

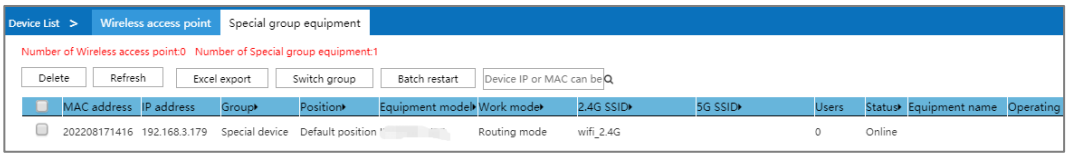
Interface Element	Description
Group	Displays the name of the group to which the AP device belongs
Position	Displays location information for AP devices
Equipment Model	Display the equipment model of AP equipment
Work mode	Display AP device working mode:
2.4G SSID	Displays the 2.4G SSID name of the AP device
5.8G SSID	Shows the 5.8G SSID name for the AP device
Users	Displays the number of wireless clients connected to the current AP device
Status	Display the connection status of AP equipment: • Online • Offline
Equipment name	Display the name of AP device, which needs to be added by the user and is equivalent to the remark of the device
Operating	• : modify the name, group, and location of the device. • : View the parameter information related to the device and group configuration. • : The old version of the device can be deleted.
Filter icon	There is a filter icon after the titles "Group", "Location", "Equipment model", "Work mode", "2.4g SSID" and "5.8g SSID". Click one or several items to select the filter operation.
Excel import	Click the import button of Excel to import xls or xlsx files to modify the device group, location and device name in batch. Note: • Older browsers such as IE8 do not support this function. • Take the xls file exported by Excel as a template, modify the device group, location or device name, and then save it as xls or xlsx file for import. • Devices whose list does not exist cannot be imported by Excel. • There is a certain lag in completing AP configuration, and it takes a certain time to take effect.
Excel export	Click the Excel Export button to export the device list information in xls format. Note: Older browsers such as E8 do not support this function.
Switch Group	Check the device information needed to switch groups, and click “Switch group” to switch groups
Batch Restart	Check the device to be restarted, and click the batch restart button to restart.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Search	Click the search icon to enter the key words in the search input box for search, mainly for the fuzzy search of equipment name, MAC address, IP address

Interface Description 2: Special Group Device

The special group equipment interface is as follows:



The main element configuration description of special group equipment interface:

Interface Element	Description
MAC address;	Display the MAC address of AP equipment
IP address	The IP address is the IP address of AC receives the message when AP communicates with AC. If there is a cross gateway between AP and AC, it is shown as the IP address of the gateway.
Group	Displays the name of the group to which the AP device belongs
Position	Displays location information for AP devices
Equipment Model	Display the equipment model of AP equipment
Work mode	Display AP device working mode:
2.4G SSID	Displays the 2.4G SSID name of the AP device
5.8G SSID	Shows the 5.8G SSID name for the AP device
Users	Displays the number of wireless clients connected to the current AP device
Status	Display the connection status of AP equipment: • Online • Offline
Equipment name	Display the name of AP device, which needs to be added by the user and is equivalent to the remark of the device
Operating	: The old version of the device can be deleted.
Filter icon	There is a filter icon after the titles "Group", "Location", "Equipment model", "Work mode", "2.4g SSID" and "5.8g SSID". Click one or several items to select the filter operation.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Excel export	Click the Excel Export button to export the device list information in xls format. Note: Older browsers such as E8 do not support this function.
Switch group	Check the device information needed to switch groups, and click “Switch group” to switch groups
Batch restart	Check the device to be restarted, and click the batch restart button to restart.
Search	Click the search icon to enter the key words in the search input box for search, mainly for the fuzzy search of equipment name, MAC address, IP address

3.5 Wireless Terminal List

3.5.1 Wireless Terminal List

Function Description

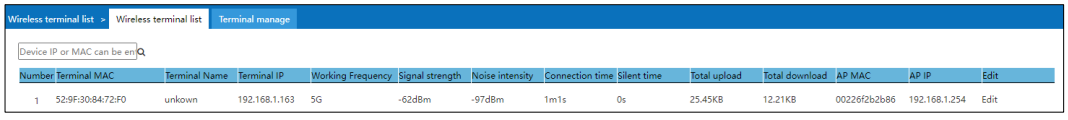
Displays the terminal information of online devices, and support terminal name modification.

Operation Path

Click: “Centralized Management > Wireless Terminal List”.

Interface Description

Wireless Terminal List interface as follows:



The main element configuration description of Wireless Terminal List interface:

Interface Element	Description
Terminal MAC	The MAC address of the accessed wireless user
Terminal name	The device name of the accessed wireless user. The terminal name can be modified via “Edit”. Support 32 characters consisting of letters, numbers and symbols.
Terminal IP	The IP address of the accessed wireless user

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Working Frequency	Frequency band accessed by wireless users
Signal strength	The signal strength of the accessed wireless user. The unit is dBm, the larger the value, the stronger the signal
Noise intensity	Signal noise intensity of accessed wireless users, unit: dbm
Connection time	Connection time of accessed wireless users
Silent time	Silence time of accessed wireless users
Total upload	Upload traffic of accessed wireless users
Total download	Download traffic of accessed wireless users
AP MAC	MAC address of AP device connected to wireless user
AP IP	IP address of AP device connected to wireless user
Search	Click the search icon to enter the key words in the search input box for search, mainly for the fuzzy search of MAC address, IP address

3.5.2 Terminal Manage

Function Description

Add and delete the terminal name of wireless device.

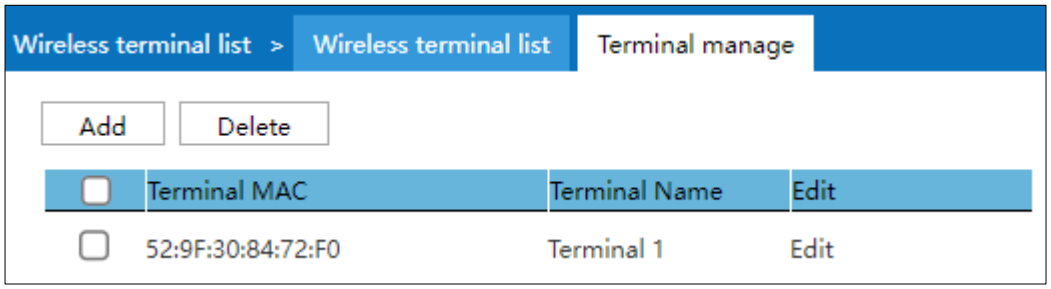
- Add the terminal name of wireless device to facilitate the device identification.
- Delete the terminal name of wireless terminal device.

Operation Path

Click: “Centralized Management > Terminal Manage”.

Interface Description

Terminal Manage interface as follows:



The main element configuration description of Terminal Manage interface:

Interface Element	Description
Terminal MAC	MAC address of terminals that need to be managed.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Terminal Name	The name of the wireless terminal device, which supports 32 characters consisting of letters, numbers and symbols.
Edit	Click “Edit” to modify the terminal name.

3.6 Batch Configuration

Function Description

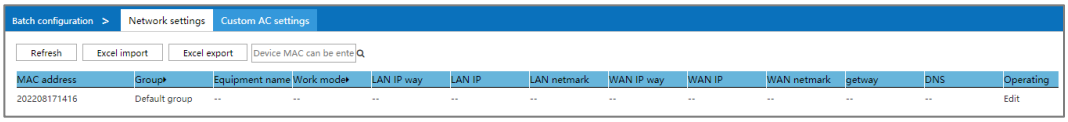
You can configure the device name, work mode, IP address, etc. of AP devices individually or in batches through importing form. Configure the AC device address of batch AP devices.

Operation Path

Click: “Centralized Management > Batch Configuration”.

Interface Description 1: Network Settings

Network setting interface as follows:



The main element configuration description of network setting interface:

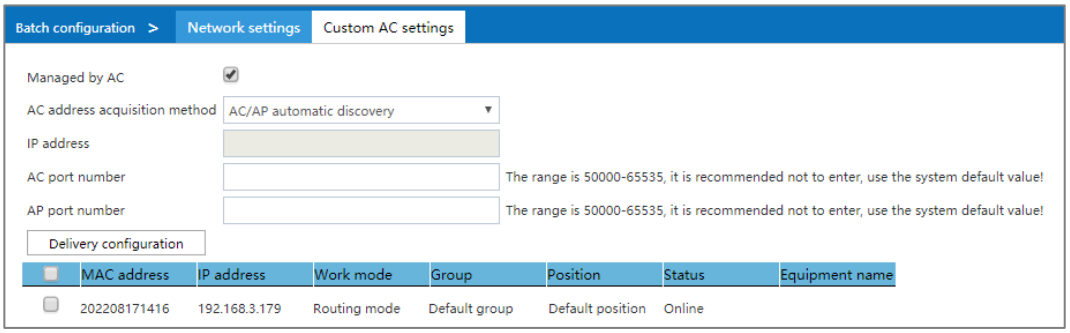
Interface Element	Description
MAC address	Display the MAC address of AP equipment
Group	Displays the name of the group to which the AP device belongs
Equipment name	Display the equipment name of AP equipment
Work mode	Display AP device working mode
LAN IP way	Displays the LAN network IP acquisition method of the AP device
LAN IP	Display the LAN network IP address of AP equipment
LAN netmask	Display the LAN network subnet mask of AP equipment
WAN IP way	Displays the WAN network IP acquisition method of the AP device
WAN IP	Display the WAN network IP address of AP equipment
WAN netmask	Display the WAN network subnet mask of AP equipment
Gateway	Display the gateway IP address of AP equipment

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Interface Element	Description
DNS	Display the DNS server IP address of AP equipment
Operating	• Edit: modify the device name, working mode, IP address, DNS, etc. • : The old version of the device can be deleted.
Filter icon	There is a filter icon after the titles "Group" and "Work mode". Click one or several items to select the filter operation.
Excel import	Click the import button of Excel to import xls or xlsx files to modify the device name, work mode, IP Address and DNS etc. in batch. Note: • Older browsers such as E8 do not support this function. • Take the xls file exported by Excel as a template, modify the device group, location or device name, and then save it as xls or xlsx file for import. • Devices whose list does not exist cannot be imported by Excel. • There is a certain lag in completing AP configuration, and it takes a certain time to take effect.
Excel export	Click the Excel Export button to export the device network settings information in xls format. Note: Older browsers such as E8 do not support this function.
Search	Click the search icon to enter the key words in the search input box for search, mainly for the fuzzy search of equipment name, MAC address

Interface Description 2: Custom AC Settings

Custom AC configuration interface as follows:



The main element configuration description of Custom AC settings interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Managed by AC	Check box of whether the AP is enabled by AC management
AC address acquisition method	The method by which the AP obtains the address of the AC device, options: • AC/AP automatic discovery • DHCP automatic acquisition • Manual configuration
IP Address	AC IP address information. This parameter needs to be set when the AC address acquisition mode is set manually.
AC port number	AC port number, value range: 50000-65535. Note: • The AC port number is not modified by default, and is only modified when the port number conflicts. • If the AC port number is empty, it indicates that the system default is used.
AP port number	AP port number, value range: 50000-65535. Note: • The AP port number is not modified by default, and is only modified when the port number conflicts.. • If the AP port number is empty, it indicates that the system default is used.
Delivery Configuration	Check the AP device whose AC address needs to be customized, and click the issue configuration button for batch configuration.

3.7 Equipment Upgrade

Function Description

The equipment model and version number of online equipment can be displayed, and batch upgrade can be conducted as needed.

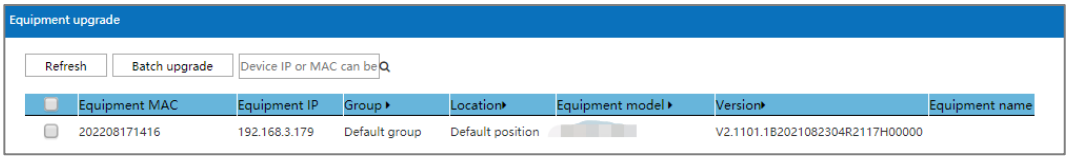
Operation Path

Open in order: “AC Management > Equipment Upgrade”.

Interface Description

The equipment upgrade interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of equipment upgrade interface:

Interface Element	Description
Equipment MAC	Display the MAC address of AP equipment
Group	Displays the name of the group to which the AP device belongs
Location	Displays location information for AP devices
Equipment Model	Displays the model name of the AP equipment
Version	Displays the software version of the AP equipment
Equipment name	Displays the name of the AP equipment
Filter icon	There is a filter icon after the titles "Group", "Location", "Device Model" and "Version ". User can select one or more items to filter.
Search	Click the search icon to search the keywords entered in the input box
Batch upgrade	Click “Batch upgrade”. Click "Select firmware" in the pop-up dialog box. After selecting firmware, click "Upgrade ".During the upgrade process, there will be a device upgrade schedule, which can be used to check the progress. Note: • In batch upgrade, only one model of equipment can be upgraded at a time. • Do not do anything else during the upgrade if there is no abnormality.

3.8 Functional Configuration

Function Description

You can enable device management, set priority, enable device audit, switch AC/AP protocol version, and set AC port number and AP port number.

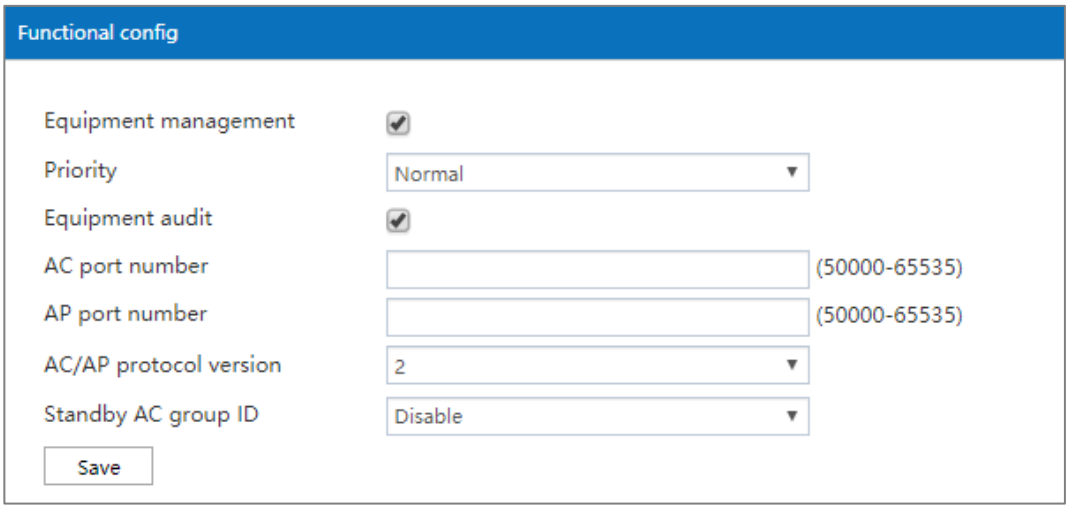
Operation Path

Open in order: “AC Management > Function Configuration”.

Copyright © 3onedata Co., Ltd.

Interface Description

The functional configuration interface is as follows:



The main element configuration description of functional configuration interface:

Interface Element	Description
Equipment management	Equipment management drop-down box: • Enable; • Close.
Priority	Priority drop-down box: • High • Normal Note: The priority is the level competition between AC and AC, and the higher priority has the right to manage. If the priority is set to the same level, the lower the MAC address, the higher the priority.
Equipment Audit	Device audit check box. When checked, the discovered AP device needs to be audited before joining the group; If it is not enabled by default, it will be unchecked, and the discovered AP devices will be automatically assigned to groups according to their work modes.
AC port number	AC port number, value range: 50000-65535 Note: • The AC port number is not modified by default, and is only modified when the port number conflicts. • The AC port number will be the default value if it is empty.
AP port number	AP port number, value range: 50000-65535 Note: • The AP port number is not modified by default, and is only modified when the port number conflicts.. • It is the default value when AP port number is empty.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
AC/AP Protocol Version	AC/AP version drop-down list, the options are as follows: • 1: the old AP is supported, and the new AP is compatible with this version. • 2. the new AP is supported, and be compatible with the discovery and batch upgrade functions of the old AP.
Standby AC group ID	The AC hot standby function supports address group and VRRP. The standby AC group ID is the mark that AC is a backup group for each other. If they are different, AC will not backup each other. Drop-down list of standby AC group ID, options as follows: • Disable • VRRP mode: VRRP mode needs to be used with VRRP protocol, and the master-standby relationship follows the master-standby relationship of VRRP. • Address group: The address group can manually add a number of different AC addresses, including the IP address of the AC device itself. The higher the rank, the higher the priority.

3.9 Query Settings

Function Description

Provide query interface for the third party, which can obtain current online device information and wireless AP online information. For the specific interface data format, please refer to The Third Party Interface document.

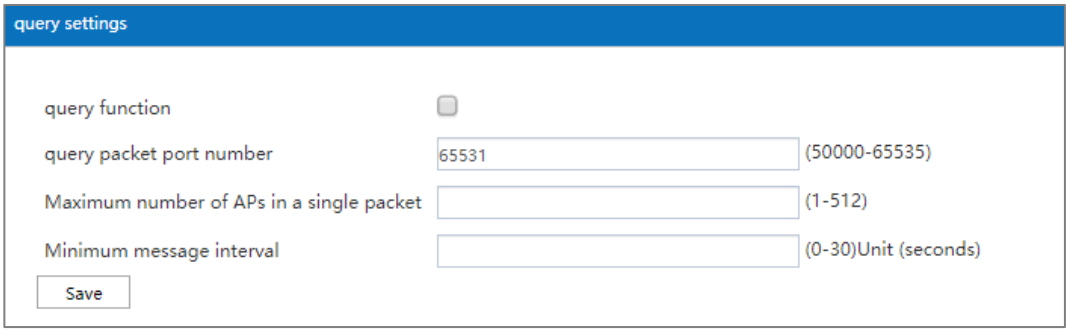
Operation Path

Click "Centralized Management > Query Settings".

Interface Description

Query Settings interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of Query Settings interface:

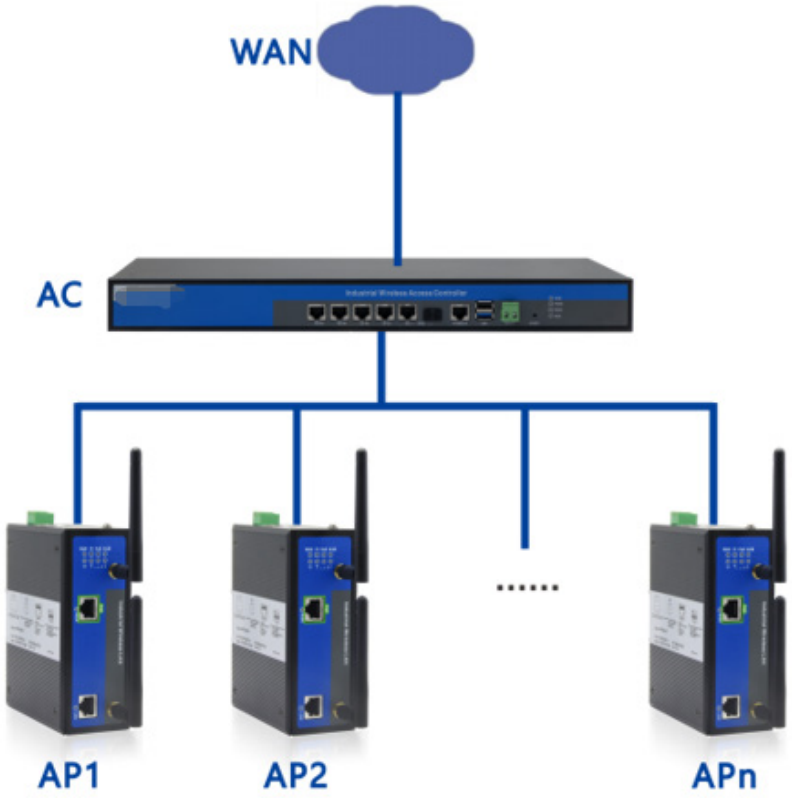
Interface Element	Description
Query function	Check box of third-party interface query function.
Query packet port number	The destination port number of the query packet, ranging from 50000-65535.
Maximum number of APs in a single packet	The maximum number of AP contained in a single message.
Minimum message interval	The minimum time interval of the message.

3.10 Configure Instance: Configure AP Parameters

Background Introduction

When users need to set parameters for multiple AP devices at the same time, they can conduct unified configuration management through AC devices. Connect the WAN ports of AC to the uplink network, while the LAN port of AC directly connects to the WAN port of AP or connects to the WAN port of AP through the switch. By operating in the web interface of AC, the parameters of multiple aps can be set uniformly.

Copyright © 3onedata Co., Ltd.



Configuration Steps

Note:
Before configuring, make sure the device is properly connected and the network is set up correctly.

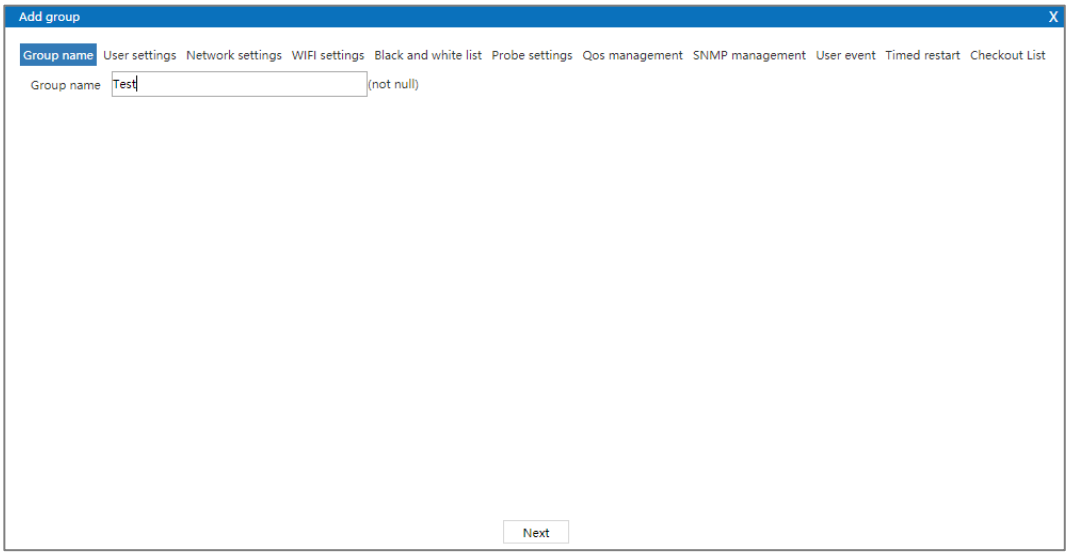
Step 1 create the group name.

1 Log in to the web configuration interface of AC and select "AC management > group management".

2 In the "group management" interface, click "add", and the "add group" interface will pop up.

3 Enter "test" in group name.

Copyright © 3onedata Co., Ltd.



4 . Click "next" to enter the "User Settings" interface.

Step 2 Set AP users.

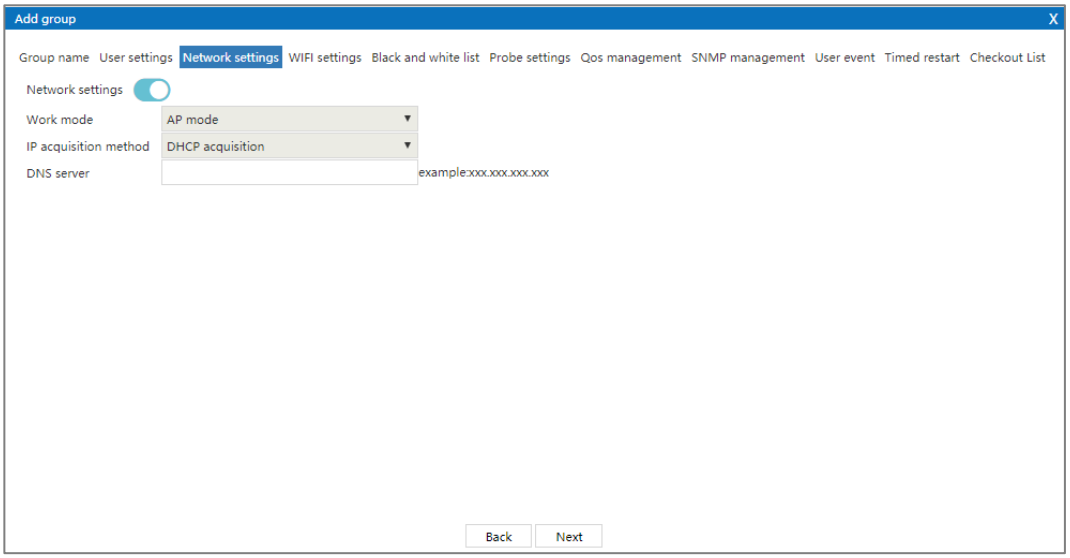
1 In the "User Settings" interface, select "do not set" from the "User Settings" switch.

2 Click "next" to enter the "Network Settings" page.

Step 3 Set AP network.

1 In the "Network Settings" interface, select "Settings" from the "Network Settings" switch.

2 Select "AP mode" in "work mode".



3 Click "next" to enter the "WIFI Settings" page.

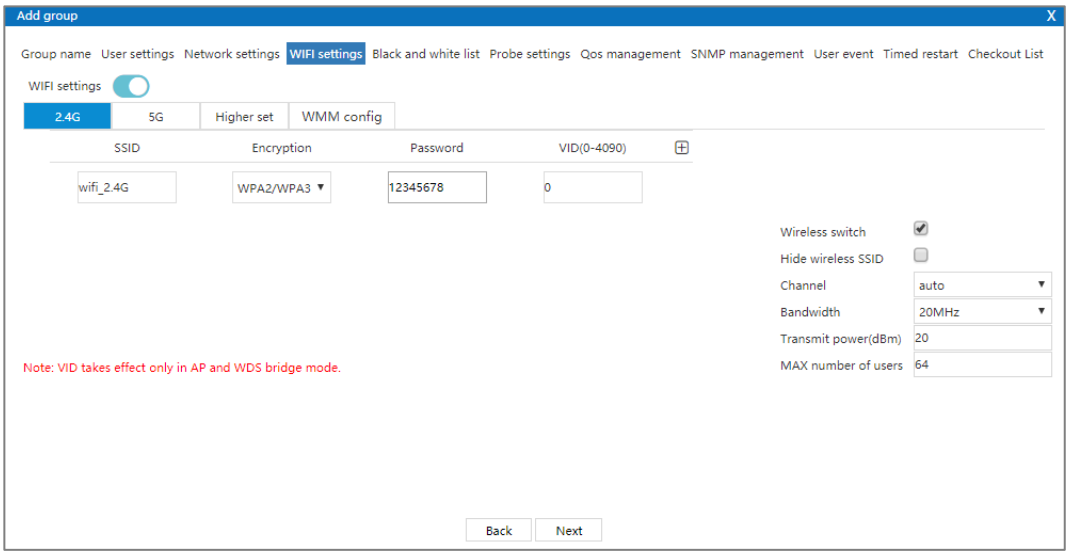
Step 4 Set AP WIFI.

1 In the "WIFI Settings" interface, select "Settings" from the "WIFI Settings" switch.

2 In the "2.4G" area, enter "wifi_2.4G" in “SSID”, select ”WPA2/WPA3" in the

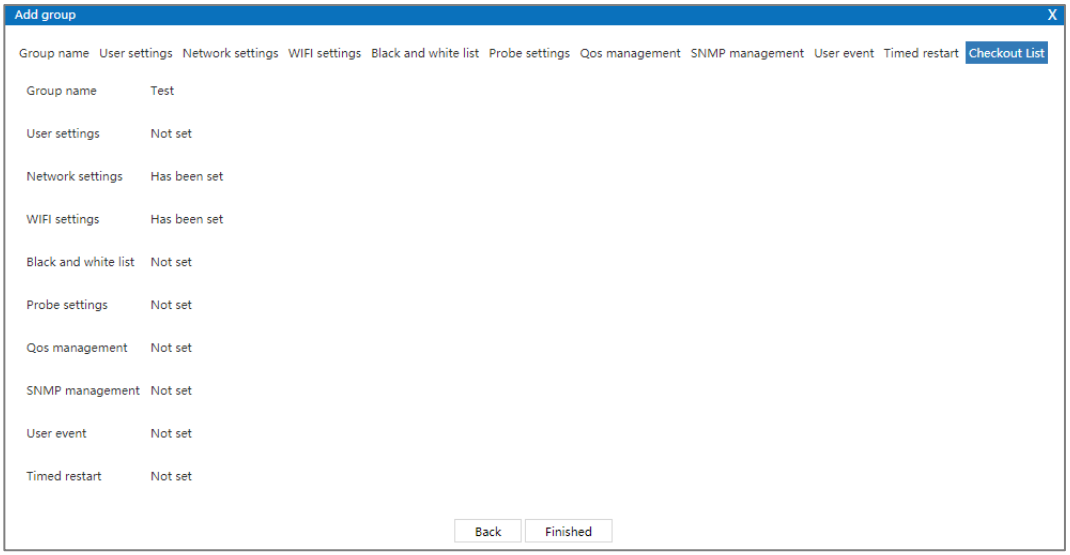
Copyright © 3onedata Co., Ltd.

"Encryption", enter "12345678" in "Password",enter "0" in "vid", enter "20" in "transmit power" and "64" in the "max number of users".



3 Click "next" to enter the "Black and white list" page.

Step 5 Click "Configuration List", view the configuration information, and click "Finish" button.



Step 6 Add the location.

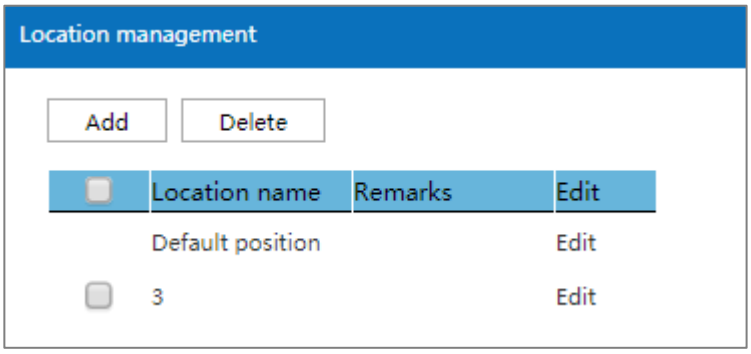
1 In the web configuration interface, select "AC Management > Location management".

2 In the "Location management" interface, click "Add" button, and the "Add location" interface will pop up.

3 Enter group name "3" in "Location name".

4 Click "Finish" and the new location information is shown below.

Copyright © 3onedata Co., Ltd.

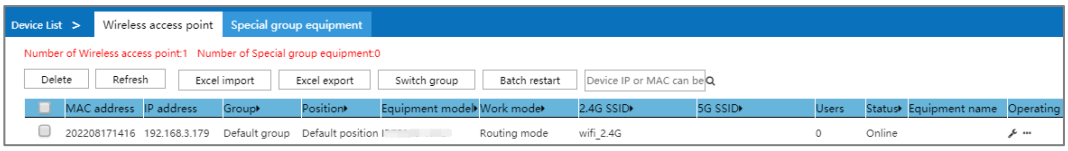


Step 7 (Single configuration) Modify the device group and location.

1 In the web configuration interface, select "AC management > Device List".

2 In the Device List interface, select the AP device to be managed, and click the icon "🔧"under Operation.

3 In the pop-up dialog box,select "Test" in "Select group", and "3" in "select location".



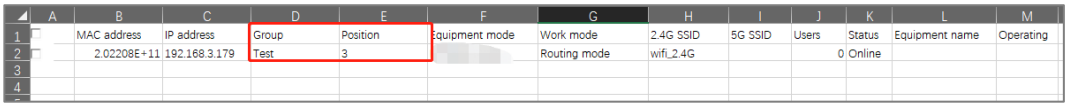
4 Save configuration

Step 8 (Batch configuration) Batch modification of device groups and locations through tables.

1 In the web configuration interface, select "AC management > Device List".

2 Click the "Excel Export" button to download the ".xls" form locally.

3 Open the table and change the "group" to "Test" and the "position" to "3" in the equipment entry.



4 Save the table in ".xls" format.

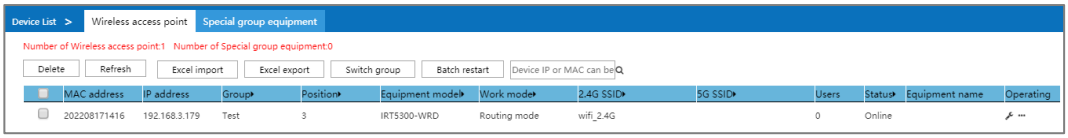
5 Click the "Excel Import" button in the WEB interface, and select the saved form file to import.

Step 9 view the configured information

1 In the web configuration interface, select "AC management > Device List".

2 In the "Device List" interface, the configured information has been displayed.

Copyright © 3onedata Co., Ltd.



Step 10 End.

Copyright © 3onedata Co., Ltd.

4 Network Settings

On the “Network settings” page, user can conduct device network settings:

- LAN settings;
- WAN settings;
- DHCP settings.

4.1 LAN Settings

Function Description

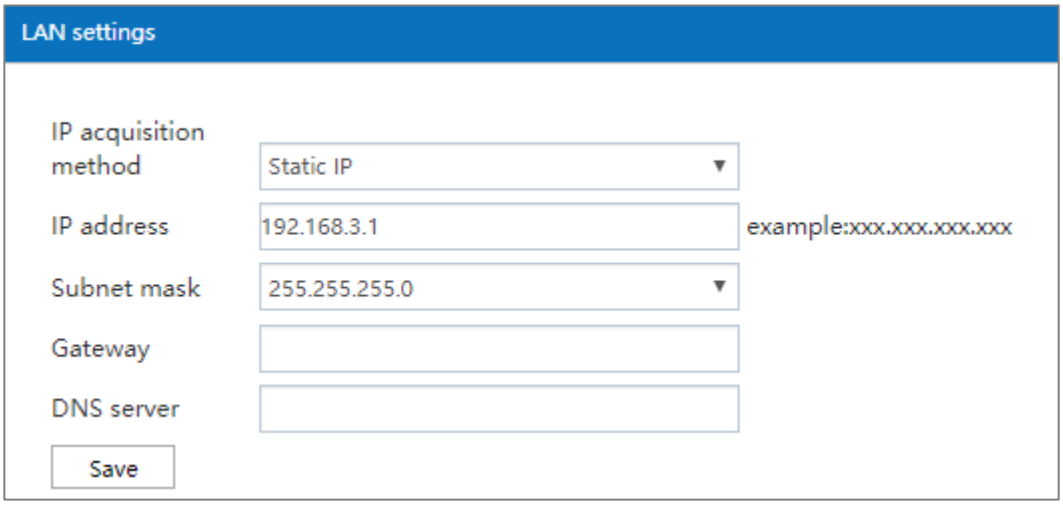
On the “LAN settings” page, user can set IP address and DNS server of the LAN, and other information.

Operation Path

Please open in order: "Network > LAN settings".

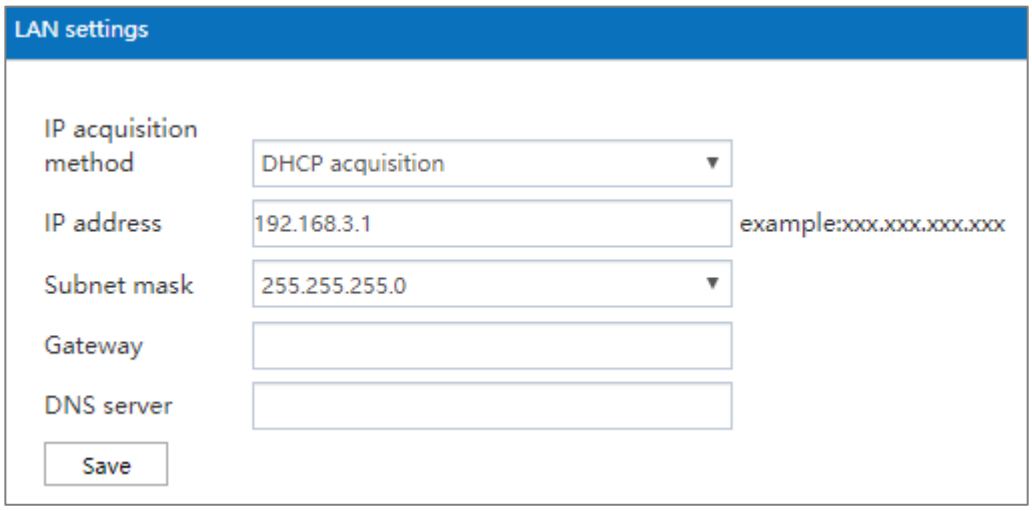
Interface Description

Choose “Static IP” in the “IP acquisition method”. The static IP interface is as follows:



Copyright © 3onedata Co., Ltd.

Choose “DHCP acquisition” in the “IP acquisition method”. The DHCP acquisition interface is as follows:



The main element configuration description of LAN settings interface:

Interface Element	Description
IP acquisition method	Shows how to get the IP of the device, options are: • Static acquisition, that is, by manually entering IP. • Under DHCP acquisition, namely through DHCP dynamic allocation acquisition, without manual input.
IP Address	The IP address of the device LAN port would be automatically acquired. Note: When "IP acquisition mode" is set to "DHCP acquisition", the item cannot be edited.
Subnet mask	Select the subnet mask from the drop-down list, which supports 32 types of class A, class B and class C subnet masks. Note: When "IP acquisition mode" is set to "DHCP acquisition", the item cannot be edited.
Gateway	The Gateway of the device LAN port would be automatically acquired. Note: When "IP acquisition mode" is set to "DHCP acquisition", the item cannot be edited.
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

Copyright © 3onedata Co., Ltd.

4.2 WAN Settings

Function Description

On the “WAN settings” page, user can set the connection type and connection parameter of the WAN. The connection types are as follows:

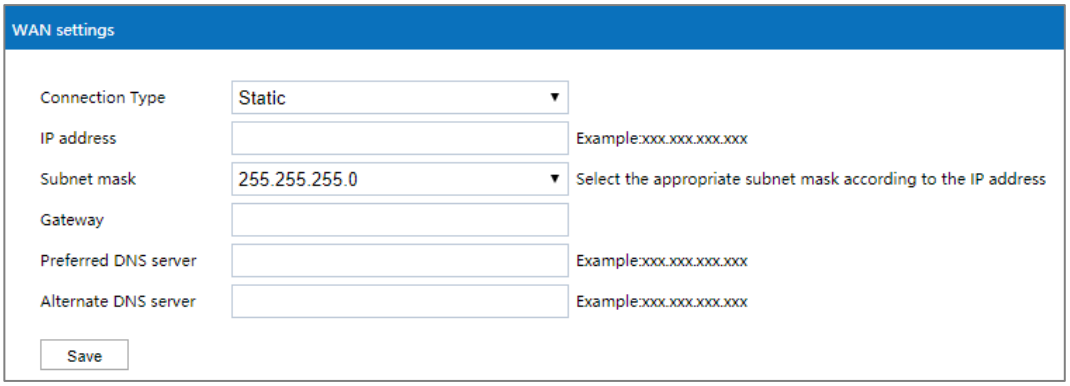
- DHCP acquisition: device WAN port acquires network address information distributed by network providers or WAN via DHCP;
- Static IP: configure device WAN port network information manually;
- PPPoE: conduct PPPoE dialing via wired network WAN port to realize Internet access.

Operation Path

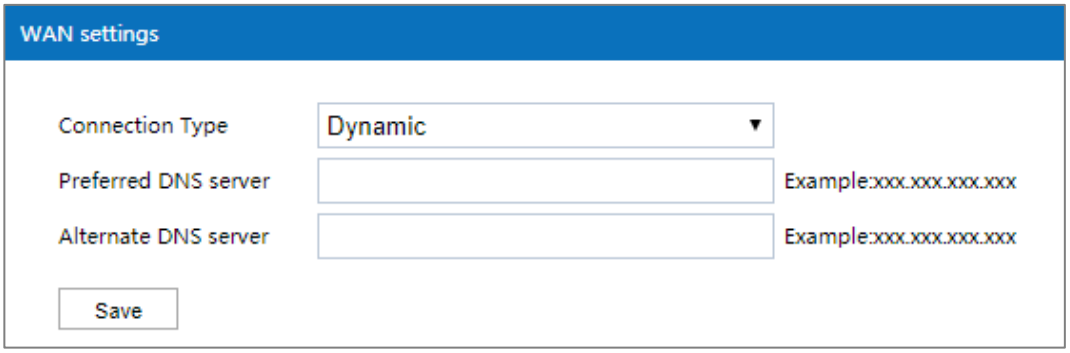
Please open in order: “Network Settings > WAN Settings”.

Interface Description 1: Static IP and DHCP Dynamic Acquisition

Choose “Static IP” in the “IP acquisition method”. The static IP interface is as follows:



Choose “DHCP acquisition” in the “IP acquisition method”. The DHCP acquisition interface is as follows:



The main element configuration description:

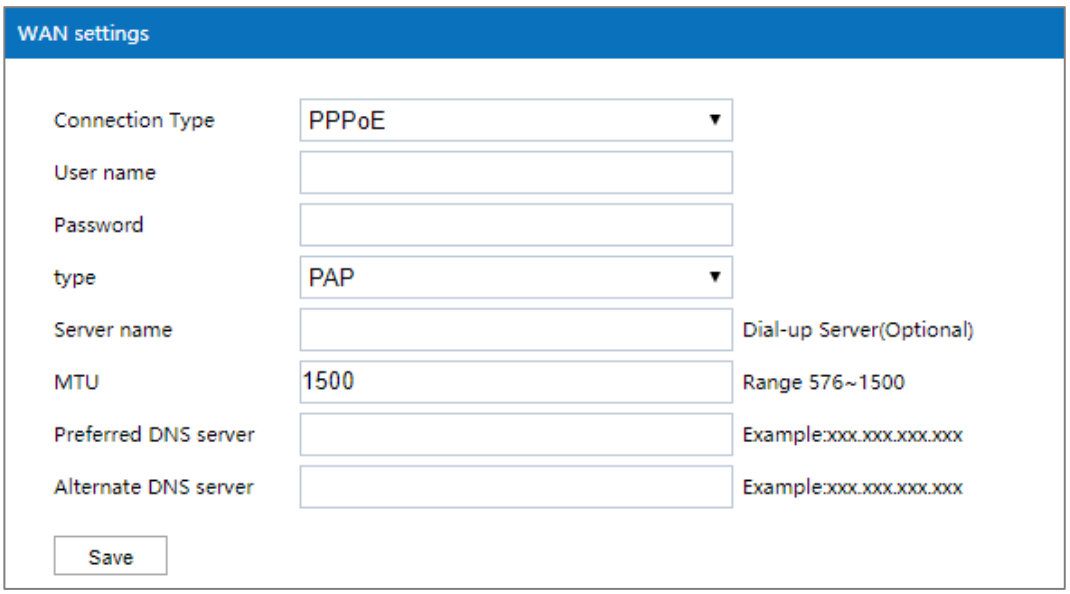
Interface Element	Description
Connection type	WAN information configuration of the equipment, options:

Copyright © 3onedata Co., Ltd.

	• Static acquisition, that is, by manually entering IP. • Under DHCP acquisition, namely through DHCP dynamic allocation acquisition, without manual input.
IP Address	The IP address of the device LAN port would be automatically acquired. Note: When "IP acquisition mode" is set to "DHCP acquisition", the item will not be displayed.
Subnet mask	Select the subnet mask from the drop-down list, which supports 32 VLSM variable subnet masks. Note: When "IP acquisition mode" is set to "DHCP acquisition", the item will not be displayed.
Gateway	The Gateway of the device LAN port would be automatically acquired. Note: When "IP acquisition mode" is set to "DHCP acquisition", the item will not be displayed.
Preferred DNS server	Address of primary DNS server.
Alternate DNS server	Address of backup DNS server. Note: • The priority level of primary DNS server address is higher than the one of backup DNS server address; • The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

Interface Description 2: PPPoE

Choose “PPPoE” in the “IP acquisition method”. The PPPoE interface is as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of PPPoE interface:

Interface Element	Description
Connection type	PPPoE tab, it supports PPPoE to achieve Internet access.
Username	User name of PPPoE connection. Note: User name, password and service name are provided by network provider.
Password	Password of PPPoE connection. Note: User name, password and service name are provided by network provider.
Type	The type of PPPoE dialing: • PAP: Password Authentication Protocol, which sends user name or password over the network; • CHAP: Challenge Handshake Authentication Protocol, it only transmits user name; • PAP/CHAP: uses Password Authentication Protocol or Challenge Handshake Authentication Protocol.
Server name	Dial-up server name, not fill if network provider doesn't supply. Note: User name, password and service name are provided by network provider.
MTU	The maximum length of a single message that can get through in PPPoE protocol dialing, with a value range of 576-1500 bytes. Note: • MTU (Maximum Transmission Unit), the device will divide the data packet into multiple small packets if the maximum length of single message exceeds the given MTU value; so reasonable setting can optimize network speed; • MTU value is recommended to be same to the one of superior router.
Preferred DNS server	Address of primary DNS server.
Alternate DNS server	Address of backup DNS server. Note: • The priority level of primary DNS server address is higher than the one of backup DNS server address; • The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

Copyright © 3onedata Co., Ltd.

4.3 DHCP Settings

DHCP (Dynamic Host Configuration Protocol) is a LAN protocol which uses UDP protocol to allocate IP address to internal network automatically and improve IP address utilization. Client in network environment can acquire dynamic IP address, Gateway address, DNS server address and other information from DHCP server.

Function Description

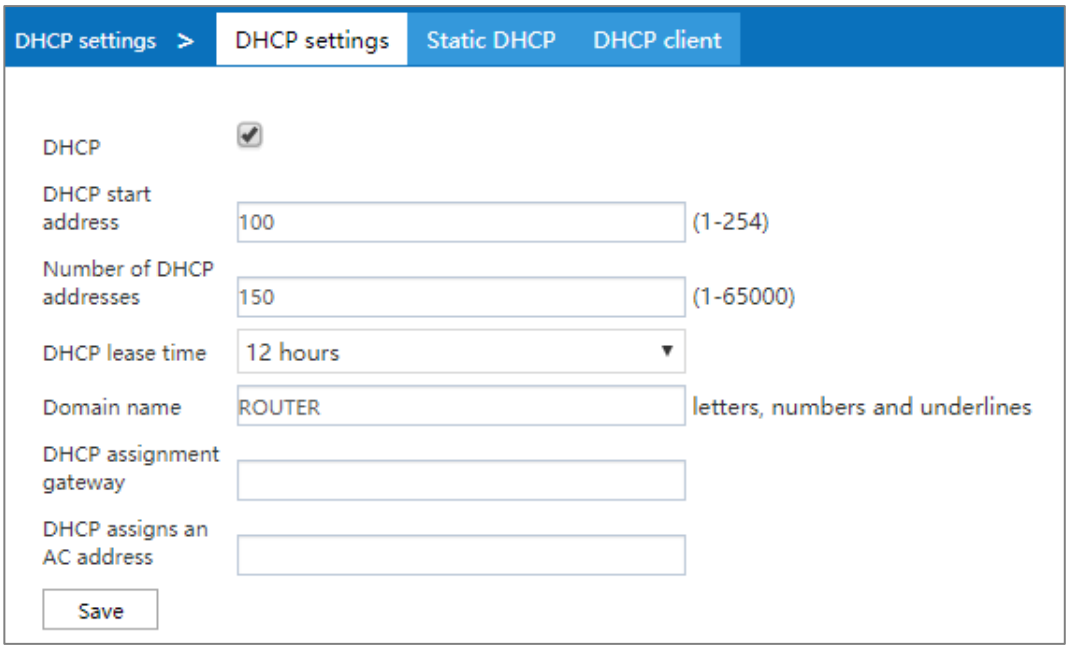
On the “DHCP settings” page, user can enable DHCP server function and set relevant parameters of gateway. It also can display relevant information such as IP address, MAC address, lease time, and remarks of the DHCP client.

Operation Path

Please open in order: “Network Settings > DHCP Settings”.

Interface description 1: DHCP settings

The DHCP settings interface is as follows:



The main element configuration description of DHCP settings interface:

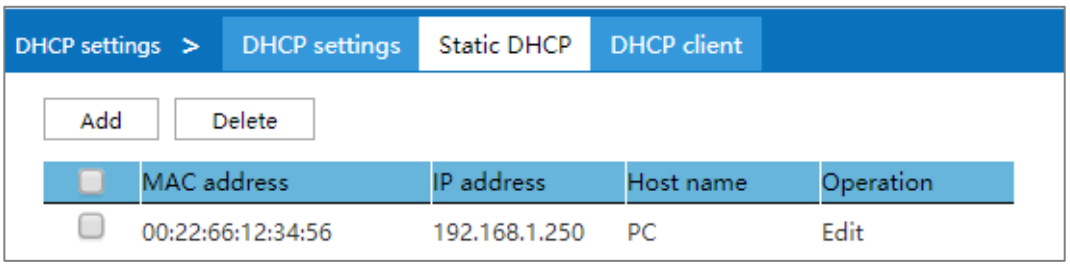
Interface Element	Description
DHCP	Enable checkbox of DHCP server.
DHCP start address	The minimum IP address host number allocated by DHCP address pool. Default to 100 and value range is 1-254.
Number of DHCP address	The maximum IP address number allocated by DHCP address pool. Default to 150 and value range is 1-65000.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
DHCP lease time	Valid time of IP address distributed by DHCP address pool, it defaults to 12 hours. Drop-down list of DHCP lease time, options as follows: • 30m • 1 hour • 6h • 12h • 1 day • 3 days • 7 days
Domain name	DHCP domain name is composed of letter, number and underline; it supports 0-32 valid characters.
DHCP assignment gateway	The gateway address assigned to client by DHCP
DHCP assigns an AC address	AC IP address assigned to AP by DHCP

Interface Description 2: Static DHCP

Static DHCP interface as follows:



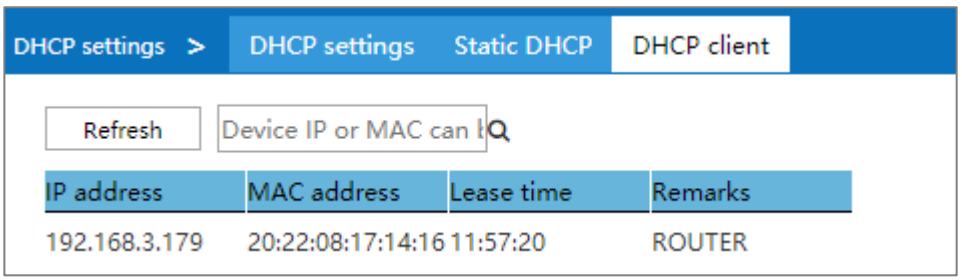
The main elements configuration description of static DHCP interface:

Interface Element	Description
MAC address;	MAC address of the device to which static IP address needs to be assigned.
IP Address	Static IP address bound to MAC address
Host name	Device name
Operation	Edit: modify the entry MAC, IP and name information

Interface Description 3: DHCP Client

Click DHCP client tab, the DHCP client interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of DHCP client interface:

Interface Element	Description
IP Address	Display IP address information of DHCP client
MAC address	Display MAC address information of DHCP client
Lease time	Display the remaining valid time after DHCP client acquires IP
Remarks	Display the remarks such as DHCP client model etc.

4.4 VLAN Settings

VLAN is Virtual Local Area Network. VLAN is the data switching technology that logically (note: not physically) divides the LAN device into each network segment (or smaller LAN) to achieve the virtual working group (unit).

VLAN advantages mainly include:

- Port isolation. Ports in different VLAN, even in the same switch, can't intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLAN can't directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. Changing the network user belongs to, don’t need to change ports or connection; only needs to change the software configuration.

That is, ports within the same VLAN can intercommunicate; otherwise, ports can't communicate with each other. A VLAN is identified with VLAN ID, and ports with the same VLAN ID belong to a same VLAN.

Function Description

The port VLAN mode is access by default, and users can configure the related parameters of VLAN.

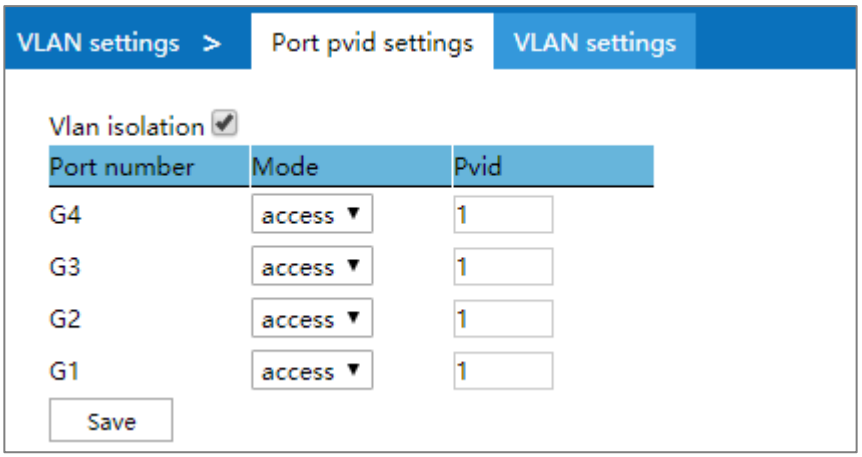
Operation Path

Open in order: "Network Settings > VLAN Settings".

Copyright © 3onedata Co., Ltd.

Interface Description 1: Port PVID Settings

Port PVID setting interface is as follows:

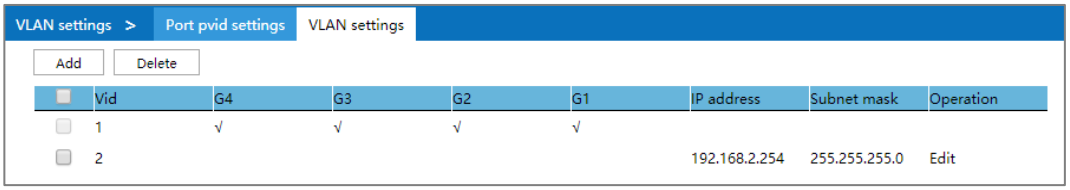


Main elements configuration description of port PVID settings interface:

Interface Element	Description
VLAN isolation	VLAN isolation function check box, check it to enable VLAN port isolation.
Port number	The corresponding port number of this device's Ethernet port.
Mode	The port link types that the device supports: • Access: Port can only belong to 1 VLAN, which is generally used to connect user device. All default ports belong to access port. • Trunk: port can belong to multiple VLAN, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices.
Pvid	Port-base VLAN ID is the port-based virtual LAN ID number. For access mode, a physical port has one and only one PVID.

Interface Description 2: VLAN Settings

VLAN settings interface is as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of VLAN settings interface:

Interface Element	Description
Vid	Displays the PVID value set for the port.
G4-G1	Displays the ports included in this VLAN, and "√" is displayed below the included ports.
IP Address	Displays the IP address corresponding to this VLAN. Note: IP addresses of different VLANs cannot be in the same network segment.
Subnet Mask	Displays the subnet mask corresponding to this VLAN.
Operation	Click "Edit" to modify the IP address and subnet mask of this VLAN. Note: When VID is 1, the corresponding IP address and subnet mask cannot be modified.

4.5 Dynamic Domain Name

If the IP address that the router Internet obtained is dynamically allocated by operator, the IP address might be different each time. In this situation, user can use dynamic domain name service. The domain name provider allows registering a domain name, which always corresponds to current dynamic IP address of the router. Therefore, user can visit the latest Internet IP address via visiting domain name.

Function Description

User can set relevant information of dynamic domain name.

Operation Path

Choose “Network Settings > Dynamic Domain” in the navigation bar.

Interface Description

The dynamic domain interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of dynamic domain interface:

Interface Element	Description
Enable	Dynamic Domain Name function checkbox, check to enable dynamic domain function.
DDNS supplier	The router supports multiple DDNS suppliers. The options in the DDNS supplier drop-down list are: • no-ip.com • 3322.org • dyndns.org • oray.com • Custom: When user chooses this item, the corresponding DDNS supplier name could be entered in the input box of DDNS supplier.
Domain name infor	The relevant information of domain name applied from DDNS supplier.
User name	The user name applied from DDNS supplier.
Password	The password applied from DDNS supplier.
Update Time	Update the time interval of dynamic DNS to server, the unit is second, the value range is 10-360.

4.6 Routing Table

Routing table is a spreadsheet or database stored in router, which has saved the paths to specified network address. The routing table includes topological information

Copyright © 3onedata Co., Ltd.

of perimeter network, which mainly aims to implement selection between routing protocol and static routing.

Function Description

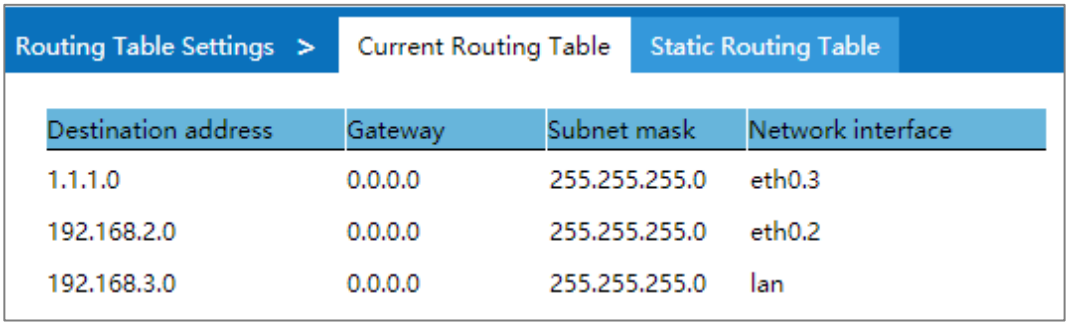
User can set relevant information of routing table.

Operation Path

Choose “Network Settings > Routing Table” in the navigation bar.

Interface Description 1: Current Routing Table

The current routing table interface as follows:

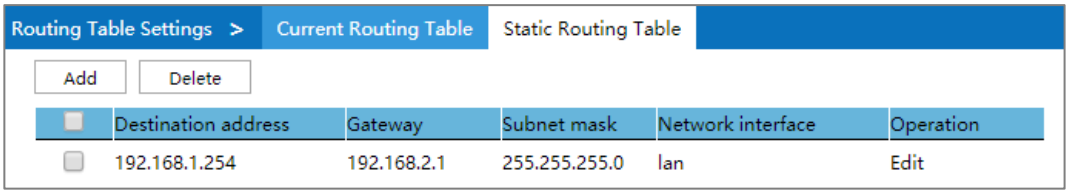


The main element configuration description of current routing table interface:

Interface Element	Description
Destination Address	The destination IP address information of current routing.
Gateway	The destination gateway information of current routing.
Subnet mask	The subnet mask information of current routing.
Network interface	The network interface information of current routing.

Interface Description 2: Static Routing Table

The static routing table interface as follows:



The main element configuration description of static routing table interface:

Interface Element	Description
Destination Address	The destination IP address information of static routing
Gateway	The gateway information of static routing
Subnet mask	The subnet mask information of static routing: • 255.255.255.255

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 255.255.255.254 • 255.255.255.252 • 255.255.255.248 • 255.255.255.224 • 255.255.255.192 • 255.255.255.128 • 255.255.255.0 • 255.255.254.0 • 255.255.252.0 • 255.255.248.0 • 255.255.240.0 • 255.255.224.0 • 255.255.192.0 • 255.255.128.0 • 255.255.0.0 • 255.254.0.0 • 255.252.0.0 • 255.248.0.0 • 255.224.0.0 • 255.192.0.0 • 255.128.0.0 • 255.0.0.0 • 254.0.0.0 • 252.0.0.0 • 248.0.0.0 • 240.0.0.0 • 224.0.0.0 • 192.0.0.0 • 128.0.0.0
Network interface	The network interface of static routing: • WAN • LAN • Manual Input
Operation	Edit: modify static routing table information.

Copyright © 3onedata Co., Ltd.

5 Advanced Network

5.1 UPnP Settings

Universal Plug and Play (UPP) is a network structure used for common peer-to-peer network connection (P2P) of computers and smart devices (or instruments). Based on Internet standards and technologies (such as TCP/IP, HTTP and XML), UPnP enables devices to automatically connect and work with each other.

When the router enables UPnP function, if the software on the user's computer also supports UPnP protocol, the router will open the corresponding virtual server port according to the requirements of user software. Based on the UPnP protocol, hosts on the LAN can request routers to perform specific ports translation, allowing external hosts to access resources on internal hosts when needed. Devices that support UPnP can be automatically discovered by the UPnP service application on the LAN. UPnP also allows supported devices to automatically leave the network without negatively impacting the device itself or other devices on the network.

Function Description

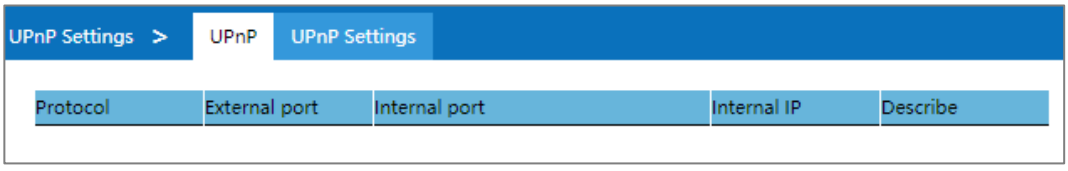
User can view internal ports translation information and configure UPnP parameters.

Operation Path

Open in order: "Advanced Network > UPnP Settings".

Interface Description 1: UPnP

UPnP settings interface as follows:



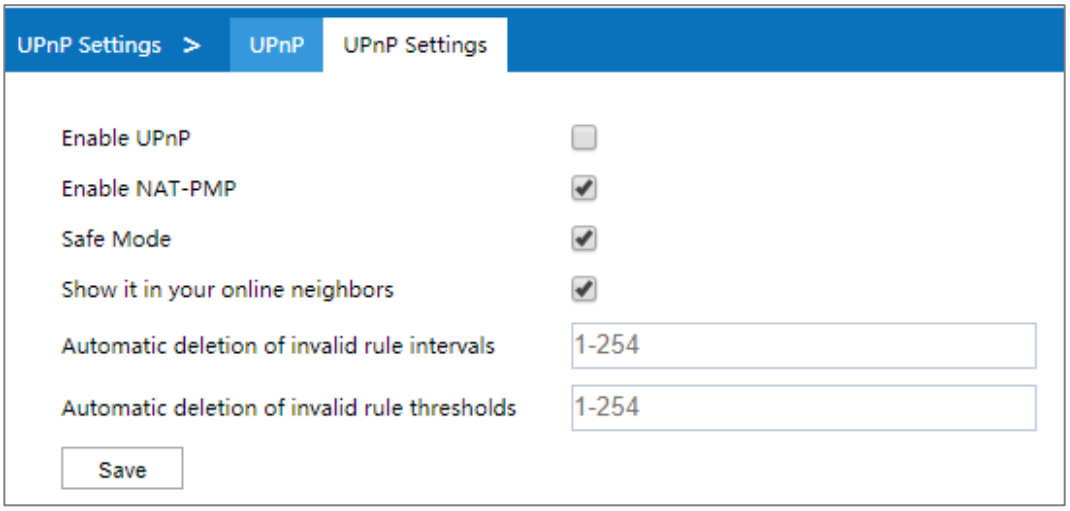
The main elements configuration description of UPnP settings interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Protocol	The type of protocol that adopts UPnP port translation, such as TCP or DUP.
External port	The router port number used for port translation is the external port number.
Internal port	The port number of local LAN host that needs to be converted.
Internal IP	The IP address of local LAN host that needs to be converted.
Describe	The description of the application when it requests port translation from the router via UPnP.

Interface Description 2: UPnP Settings

UPnP settings interface as follows:



The main element configuration description of UPnP settings interface:

Interface Element	Description
Enable UPnP	UPnP enable checkbox, check to enable UPnP function.
Enable NAT-PMP	The NAT-PMP function enable checkbox, check to enable NAT-PMP function, and the router will allow the LAN host to communicate with external devices to automate port conversion.
Safe Mode	Safe mode enable checkbox, after the safe mode is enabled, the client can only forward an input port to itself.
Show it in your online neighbors	Show the enable check box in Online neighbors, after checked, the device can be found in the PC Online

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	neighbors or network devices.
Automatic deletion of invalid rule intervals	The system automatically deletes the invalid UPnP rules list after the specified interval, unit: second.
Automatic deletion of invalid rule thresholds	The system automatically deletes the invalid UPnP rules list after the quantity of invalid UPnP rules reaches the threshold.

5.2 VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. In general, all hosts in a network will set a default route, when the destination address of the message sent by host isn't in the network segment; the message will be sent to the Router A via default router, achieving the communication between the host and external network. When the Router A breaks down, all hosts that takes Router A as default router in the network segment will disconnect communication to the outside, generating single point of failure. VRRP is proposed to solve the problem above, and it's designed for the local area network (such as: Ethernet) with multicast or broadcast capability.

VRRP organizes a set of routers (including a Master, that is the active router and several Backup, that is the standby router) in the local area network into a virtual router, which is called a backup team. The virtual router possesses its own IP address 10.100.10.1 (The IP address can be same to a router interface address in the backup team, it's called IP owner), routers in the backup team have their own IP address (such as IP address of Master is 10.100.10.2, IP address of Backup is 10.100.10.3). Hosts in the local area network only knows the virtual router IP address is 10.100.10.1, it doesn't know that the specific Master router IP address is 10.100.10.2 and Backup router IP address is 10.100.10.3. Hosts set their own default router next hop address to the virtual router IP address 10.100.10.1. Thereupon, hosts in the network start to communicate with other networks via the virtual router. If the Master router in backup team breaks down, Backup router will elect a new Master router via election strategy and provide router service for hosts in the network. Therefore, hosts in the network can uninterruptedly communicate with outside network.

Principle of realization

Copyright © 3onedata Co., Ltd.

A VRRP router has the only identification: VRID, range is 0-255. The router has only one virtual MAC address, and the address format is 00-00-5E-00-01-[VRID]. Master router is responsible for replying the ARP request by MAC address. Regardless of the switching, it's ensured to give the only consistent IP and MAC address to the terminal device, declining the switching influence to terminal device.

VRRP control message includes only one type: VRRP announce (advertisement). It's packaged by IP multicast data packet, the multicast address is 224.0.0.18, issue range can be only in the same local area network. It has ensured that VRID can be repeatedly used in different network. In order to decrease the network bandwidth consumption, only the master router can periodically send VRRP announce message. Backup router will start new VRRP election if it can't receive VRRP in three consecutive announce intervals or receives announce with 0 priority.

In the VRRP router group, the master router is elected by priority. The priority range in VRRP protocol is 0-255. If VRRP router IP address is the same to virtual router interface IP address, then the virtual router is called IP address owner in VRRP group; IP address owner automatically has the highest priority: 255. Priority 0 is usually used when IP address owner forwardly gives up the master role. Configurable priority range is 1-254. Priority configuration principle is set according to the link speed and cost, router performance and reliability, and other management strategies. In the election of master router, virtual router with high priority wins; therefore, if there exists IP address owner in VRRP group, it will appear as the master router. Candidate router with the same priority can be elected according to IP address size order. VRRP has also provided priority preemption strategy, if the strategy is configured, backup router with high priority will deprive current master router with low priority and become the new master router.

Function Description

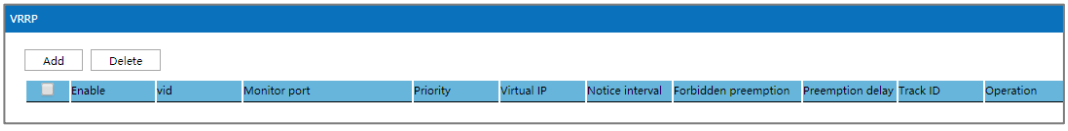
User can configure VRRP parameter.

Operation Path

Open in order: "Advanced Network > VRRP".

Interface Description

VRRP interface is as below:



Copyright © 3onedata Co., Ltd.

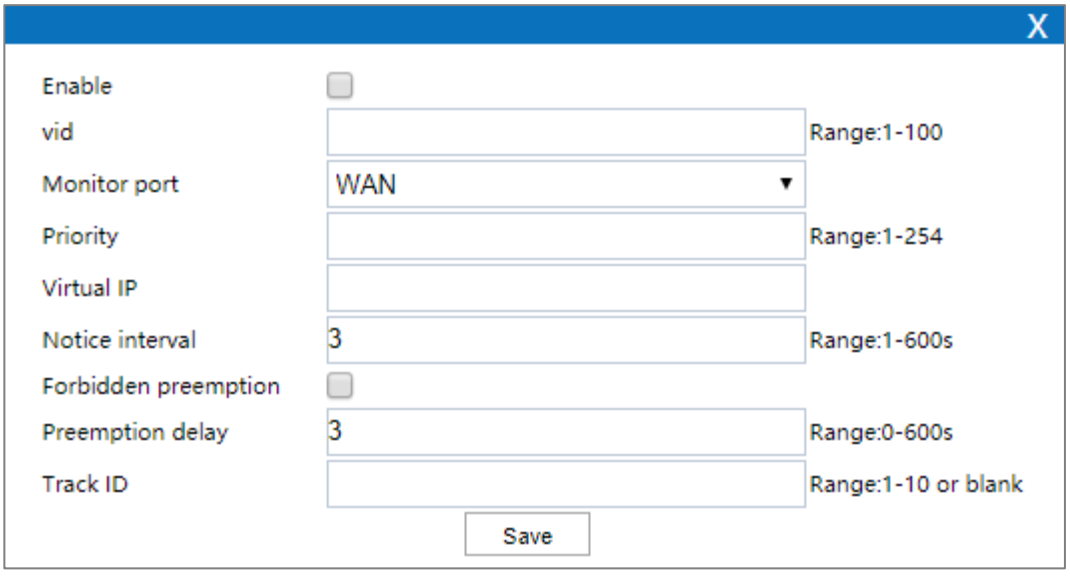
The main elements configuration description of VRRP interface:

Interface Element	Description
Enable	VRRP function status is displayed, options include: • ON Status • OFF
Vid	Identity of the virtual router is displayed.
Monitor port	Monitor ports of the device is displayed, options include: • LAN • WAN
Priority	Priority of the device. The priority is used for the election of Master device. The greater the value, the higher the priority.
Virtual IP	The IP address of the virtual router is displayed.
Notice interval	Interval at which Master device sends VRRP notice messages, unit: second.
Forbidden preemption	Status display of forbidden preemption, options include: • ON Status • OFF
Preemption delay	The delay time of switching from Backup device to Master device.
Track ID	Trace and probe Track ID.
Operation	Edit the VRRP entry.

Interface Description: VRRP-Add

Click the "Add" button to add virtual route.

The VRRP-Add interface as follows:



Copyright © 3onedata Co., Ltd.

The main elements configuration description of VRRP-Add interface:

Interface Element	Description
Enable	VRRP enable check box, check it to enable the VRRP function.
vid	Identity of the virtual router, the valid range is 1-100. Virtual routers consisting of one master device and multiple backup devices have the same identity.
Monitor port	Drop-down list of VRRP monitor port, options as follows: • LAN: LAN port as the listening port; • WAN: WAN port as the listening port.
Priority	Priority of the device. The priority is used for the election of Master device. The greater the value, the higher the priority. The more likely it is to become Master device; the valid range is 1-254.
Virtual IP	IP address of the virtual router, such as 192.168.1.1. A virtual router can have one or more IP addresses.
Notice interval	• Notice interval, valid range is 1-600 seconds. Master device periodically sends VRRP notice messages to announce its operating status.
Forbidden preemption	Disable preemption check box of VRRP, check it to disable preemption. • Non-preemptive mode. When the priority of Backup device is higher than the one of Master device, Backup device won't become the Master device; • Preemptive mode. When the priority of Backup device is higher than the one of Master device, Backup device will actively switch to Master device.
Preemption delay	The delay time of switching from Backup device to Master device, the valid range is 1-600 seconds. Note: If the preemption delay time is too short, the device status will be frequently switched; so increasing the preemption delay time can effectively solve this problem.
Track ID	Trace and probe Track ID, the ID range is 1-10, optional.

Copyright © 3onedata Co., Ltd.

5.3 RIP

RIP (Routing Information Protocol) is a simple Interior Gateway Protocol (IGP) and mainly used in small network, such as Campus Network and Local Area Network with simple structure. RIP isn't used in more complex environment and large network.

RIP is simple to achieve and easier in configuration and maintenance than OSPF or IS-IS, so it's widely used in actual networking.

Function Description

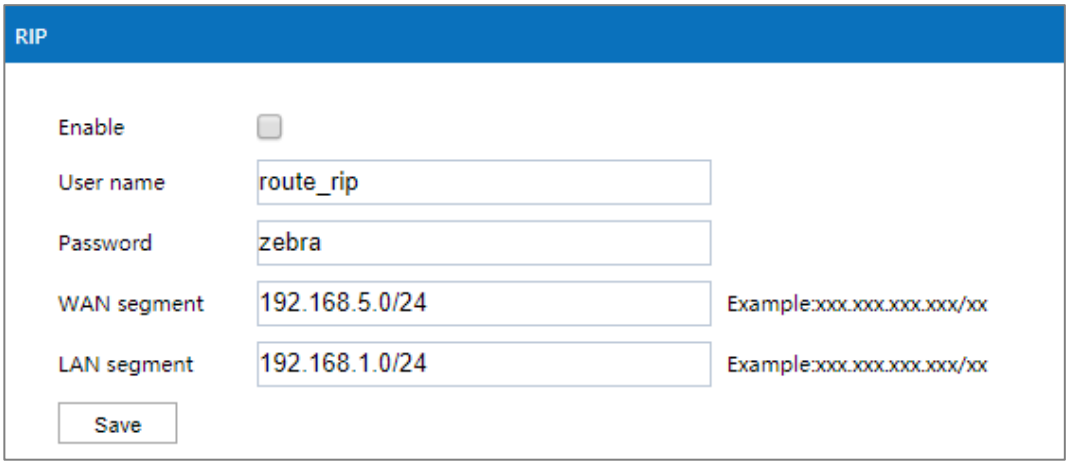
User can configure the RI related parameters.

Operation Path

Open in order: "Advanced Network > RIP".

Interface Description

The RIP interface as follows:



The main elements configuration description of RIP interface:

Interface Element	Description
Enable	RIP Enable checkbox, check to enable the RIP default configuration.
Username	User name used to log in to the RIP command line configuration.
Password	Password used to log in to the RIP command line configuration.
WAN segment	WAN segment information.
LAN segment	LAN segment information.

Copyright © 3onedata Co., Ltd.

5.4 OSPF

OSPF (Open Shortest Path First), its characteristics include:

- It's a kind of routing protocol of link status and adopts the metric value based on bandwidth;
- It adopts SPF algorithm to calculate the route, and the SPF algorithm can avoid routing loop.
- Maintain routes through neighbor relationship to avoid the consumption of bandwidth by regular updates;
- The routing update is efficient with fast network convergence, which is suitable for large and medium-sized networks.

Function Description

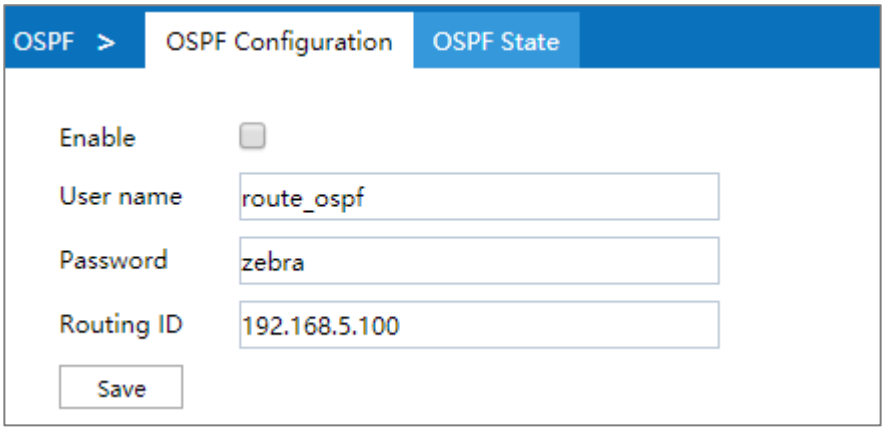
User can configure the OSPF parameters.

Operation Path

Open in order: "Advanced Network > OSPF".

Interface Description 1: OSPF Configuration

OSPF configuration interface is as follows:



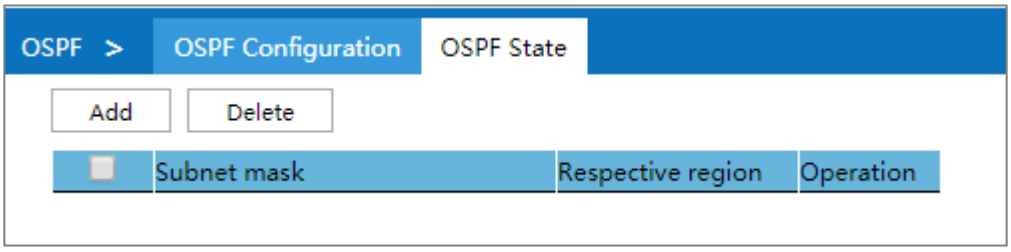
The main element configuration description of OSPF configuration interface:

Interface Element	Description
Enable	OSPF enable checkbox, check to enable OSPF protocol.
Username	User name used to log in to the OSPF command line configuration.
Password	Password used to log in to the OSPF command line configuration.
Routing ID	The router ID number, similar to the IP address format, is the unique identification of router in the autonomous system.

Copyright © 3onedata Co., Ltd.

Interface Description 2: OSPF State

OSPF State interface as follow:

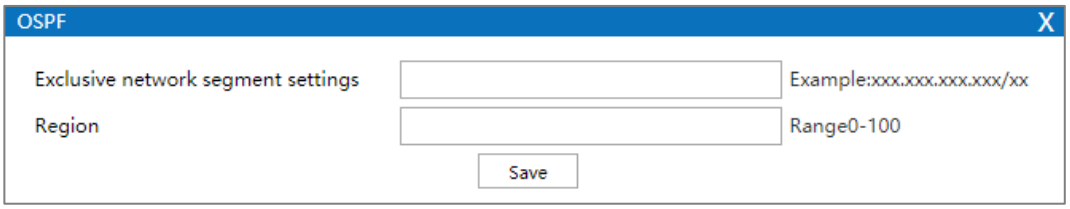


The main elements configuration description of OSPF State interface:

Interface Element	Description
Subnet mask	The network segment where the IP address of interface running OSPF protocol is located. A network segment can only belong to one area.
Respective region	The area number of the device. OSPF protocol divides the autonomous system into different areas.
Operation	Edit the OSPF network segment and region information.

Interface Description 21: OSPF State-Add

The OSPF State-Add interface as follows:



The main elements configuration description of OSPF State-Add interface:

Interface Element	Description
Exclusive network segment settings	The network segment where the IP address of interface running OSPF protocol is located. A network segment can only belong to one area, such as 10.1.1.1/24.
Region	The area number of the device. OSPF protocol divides the autonomous system into different areas, the valid range is 0-100.

Copyright © 3onedata Co., Ltd.

5.5 QoS

Function Description

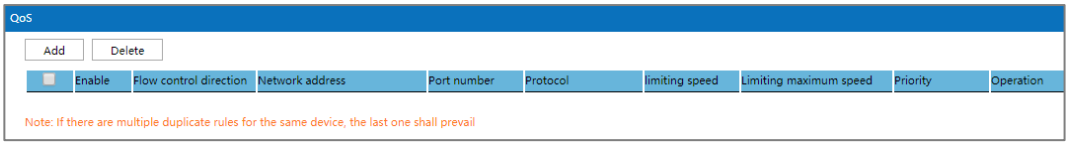
Users can configure QoS policy to limit the rate and priority of specified IP data.

Operation Path

Open in order: "Advanced Network> QoS".

Interface Description

The QoS Strategy interface as follows:



The main element configuration description of QoS classification interface:

Interface Element	Description
Enable	Enable QoS strategy or not.
Flow Control Direction	Flow control direction, such as upload and download.
Network address	Source IP address and subnet mask of the packet.
Port number	Corresponding network port number of the network address.
Protocol	Protocols used by IP data scheduling. • TCP • UDP. • BOTH
Limiting speed	Limit average rate value, the value range of the threshold is 1-1024000Kbps.
Limiting maximum speed	The maximum Limit rate value, the value range is 1-1024000Kbps.
Priority	The priority of IP data scheduling, a smaller value indicates a higher priority. The value range is 0-10.

Copyright © 3onedata Co., Ltd.

5.6 SLA Settings

Function Description

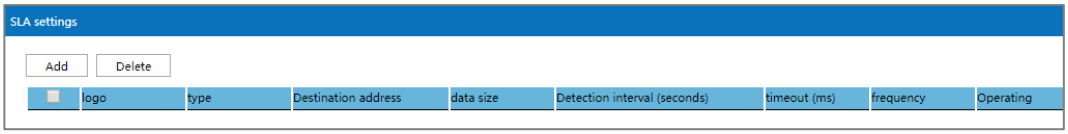
Track objects can be defined by tracking and probing one or more targets through SLA.

Operation Path

Open in order: "Advanced Network > SLA Settings".

Interface Description

SLA Settings interface as follows:



The main element configuration description of SLA settings interface:

Interface Element	Description
Logo	SLA ID number, value range is 1-10.
Type	Display SLA probe type, the default is icmp-echo. The device sends an ICMP request to the specified target, and if the ICMP response from the target is received, the target is online.
Destination Address	Destination IP address of ICMP probe packet.
Data size	The data size of the probe packet, it value range is 56-1000 bytes.
Detection interval (seconds)	Time interval to send probe packets, ranging from 1 to 608400s.
Timeout (ms)	Response timeout time, the value range is 1-300000 milliseconds. If the response is received within the specified time, the probing fails and the next probing is performed.
Frequency	Time-out number of SLA probe failures, ranging from 1 to 1000. When the timeout times reach the specified value, the link failure is considered as SLA probe failure.

Copyright © 3onedata Co., Ltd.

5.7 Track Settings

Function Description

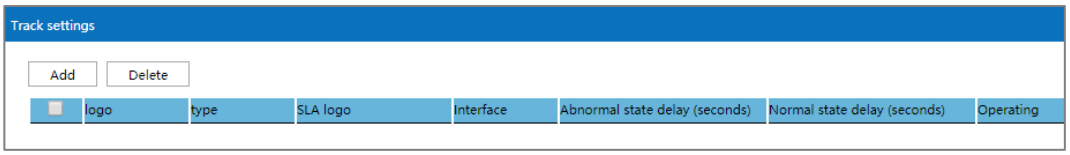
It can be configured to probe interface and link status (SLA) and realize linkage with other applications, such as VRRP.

Operation Path

Open in order: "Advanced Network> Track Settings".

Interface Description

Track Settings interface as follows:



The main element configuration description of Track Settings interface:

Interface Element	Description
Logo	Track ID number, value range is 1-10.
Type	Display track probe type, it can be displayed as follows: • sla: Tracking and probing according to SLA settings. • interface: Tracking and probing according to interface status.
SLA logo	SLA ID number, value range is 1-10.
Interface	Port number of the device.
Abnormal state delay (seconds)	When the interface or SLA is in abnormal state(interface DOWN or SLA probe fails), the delay time of Track becoming abnormal, the value range is 0-180 seconds.
Normal state delay (seconds)	When the interface or SLA is in normal state(interface UP or SLA probe normal), the delay time of Track becoming normal is 0-180 seconds.

5.8 SNMP Management

Function Description

SNMP management can be enabled, and Trap can be enabled.

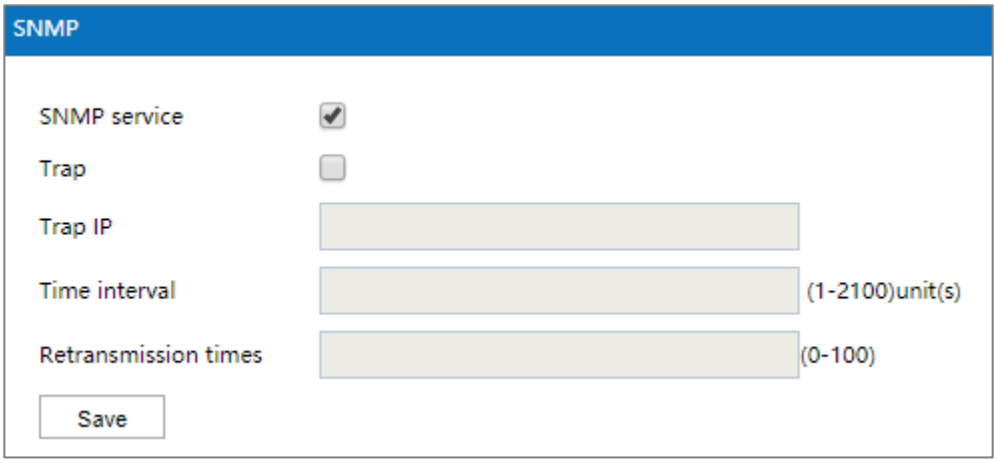
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Advanced Network > SNMP Management".

Interface Description

The SNMP management interface is as follows:



The main element configuration description of SNMP management interface:

Interface Element	Description
SNMP service	The check box of SNMP service, check it to enable SNMP management.
Trap	SNMP Trap check box, check it to enable Trap information, and the device actively sends the abnormal situation of the device to the management server. Note: Trap anomaly mainly include wireless client online and offline, hardware and software restarting, etc.
Trap IP	The IP address of the server receiving Trap information.
Time interval	Time interval to send Trap information, ranging from 1 to 2100s.
Retransmission times	The number of times to resend Trap information, ranging from 0 to 100.

Copyright © 3onedata Co., Ltd.

6 Firewall

6.1 IP Address Black/White List

Function Description

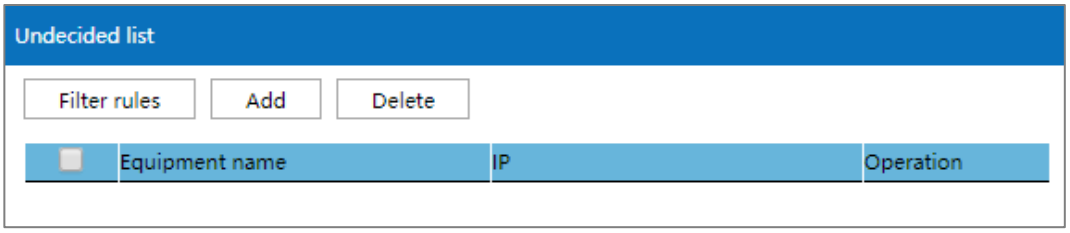
You can control the communication between the client with the specified IP address in the LAN and the WAN according to the filter list.

Operation Path

Open in order "Firewall > IP Address Black and White List".

Interface Description

IP Address Black/White List interface is as follows:



The main element configuration description of black/white list of IP address interface:

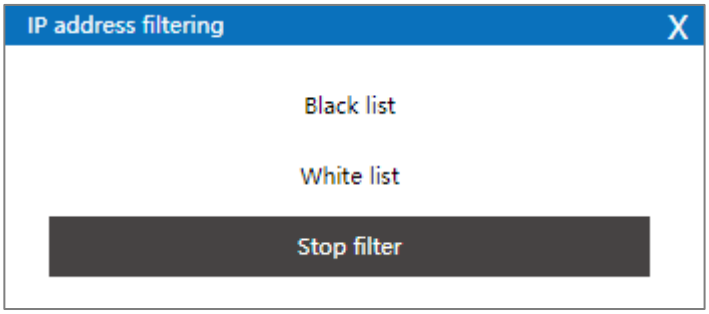
Interface Element	Description
Equipment name	The device name of client in the list. Note: • Click “add” to add device to list manually. • Click “Filters rule” button, you can switch current list between black List, white List and undecided list, to filter the Client device.
IP	IP address of client in the list.

Copyright © 3onedata Co., Ltd.

Interface Description: Filter Rule

Click "Filter rules" button for list switching.

The filter rules interface as follows:



The main element configuration description of filter rules:

Interface Element	Description
Black List	The client is prohibited from accessing the WAN list.
White List	The client is allowed to access the WAN list.
Stop filter	The pending list of client visiting WAN.

Note
Only the current list takes effect after switching the list via filter rules.

6.2 MAC Filtering

Function Description

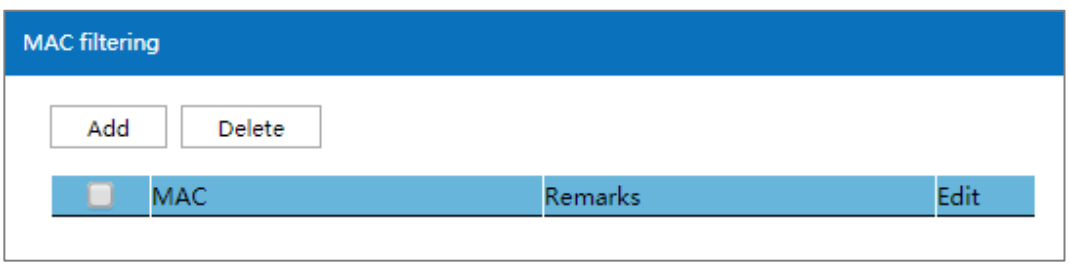
User can check or add MAC filter to forbid the communication between the clients in LAN and WAN; it can effectively control the WAN access rights of user in LAN.

Operation Path

Open in order: "Firewall > MAC Filtering".

Interface Description

MAC filter interface as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of MAC filter interface:

Interface Element	Description
MAC	MAC address of LAN client filtered by the device.
Remarks	Remarks of MAC filter entries.

Interface Description: Add MAC Filter Entry

Click "Add" to increase MAC filter entry.

MAC filter interface as follows:



The main element configuration description of MAC filter interface:

Interface Element	Description
MAC	MAC address of LAN client filtered by the device, such as: 00:22:6F:00:00:01.
Remarks	Remarks of MAC filter entries support 32 valid characters or 10 Chinese characters, optional.

6.3 URL Filtering

URL (Uniform Resource Locator) is the brief expression of access method and location of resources gained from Internet; it's the address of standard Internet resources. Each Internet file has a unique URL, which refers to the network address.

Function Description

User can check or add URL filter to prohibit the client in LAN from accessing URL address in WAN and prevent user from accessing some of the websites.

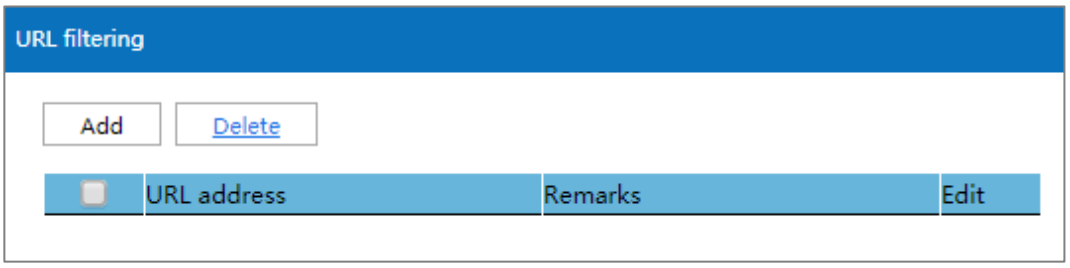
Operation Path

Please open in order: "Firewall > URL Filtering".

Interface Description

URL filter interface as follows:

Copyright © 3onedata Co., Ltd.



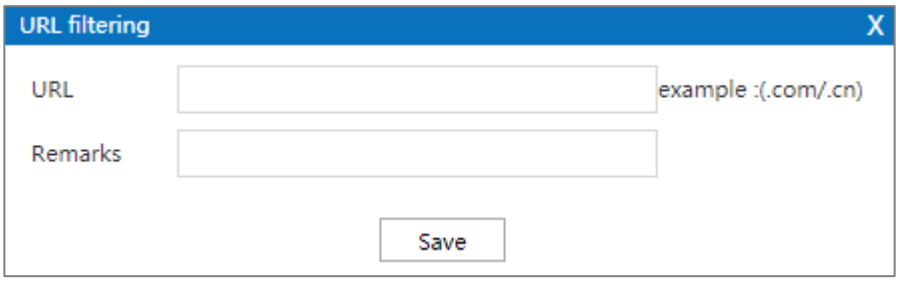
The main element configuration description of URL filter interface:

Interface Element	Description
URL	URL address in LAN filtered by the device.
Remarks	Remarks for URL addresses filter entries.

Interface Description: Add URL Filter List

Click "Add" to increase URL filter list.

URL filter interface as follows:



The main element configuration description of URL filter interface:

Interface Element	Description
URL	URL address in WAN filtered by the device, ending with ".com", ".cn" and so on. Such as: sina.
Remark	Remarks for URL addresses filter entries.

6.4 Keyword Filtering

Keyword filtering refers to the pre-programming filtering of transmitted information in the network application, detecting the specified keywords and intelligently identifying whether there exists any violation of the specified policy in the network.

Copyright © 3onedata Co., Ltd.

Function Description

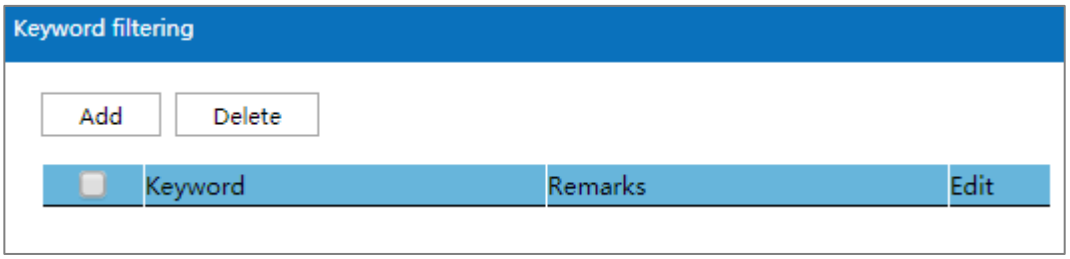
User can view or add keyword filtering entries to prevent clients on the LAN from accessing to the network address corresponding to the keywords in the WAN.

Operation Path

Open in order: "Firewall > Keyword Filtering".

Interface Description

Keyword filter interface as follows:



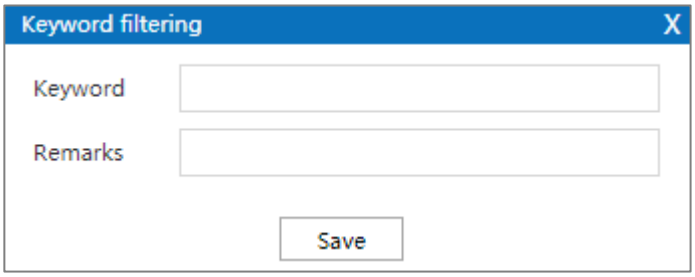
The main elements configuration description of keyword filter interface:

Interface Element	Description
Keyword	Keywords in the WAN filtered by this device.
Remarks	Remarks for keyword filtering entries.

Interface Description: Add keyword filtering entry

Click the "Add" button to add the keyword filtering entry.

Keyword filter interface as follows:



The main elements configuration description of keyword filter interface:

Interface Element	Description
Keyword	Keywords in the WAN filtered by this device.
Remarks	Remarks of the keyword filtering list; it supports 10 Chinese characters or 32 valid characters, and can be left blank.

Copyright © 3onedata Co., Ltd.

6.5 Port Forward

The Port Forward function enables user to set public service on his own network, such as Web server, FTP server, E-mail server or other applications that run only through internet. When user sends those types of requests to your network via internet, the router would forward them to the corresponding client via port forward function.

Function Description

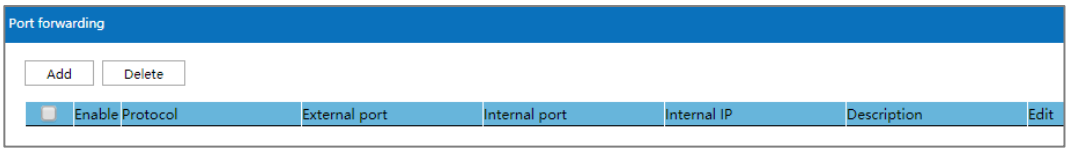
User can check or add port forward entry. It allows outer network client to visit specified device via specified port.

Operation Path

Please open in order: "Firewall > Port forward".

Interface Description

The port forward interface as follows:



The main element configuration description of port forward interface:

Interface Element	Description
Enable	Enable port forward or not: • ON Status • OFF
Protocol	The protocol type used by port forward data package: • TCP • UDP. • TCP/UDP
External port	The external port number used by external network
Internal port	The internal port number used by internal network
Internal IP	The IP address of device specified by internal network
Description	The remark information of port forward entry

Copyright © 3onedata Co., Ltd.

6.6 Port Redirection

Function Description

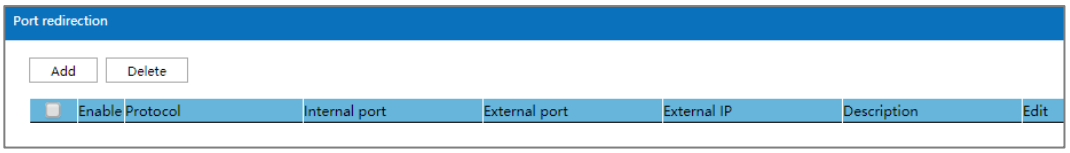
User can check or add port redirection entry, which allows client in LAN to visit the specified port of device with IP address specified by external network via specified port.

Operation Path

Please open in order: "Advanced Network > Port Redirection".

Interface Description

The port redirection interface as follows:



The main element configuration description of port redirection interface:

Interface Element	Description
Enable	Enable port redirection or not: • ON Status • OFF
Protocol	The protocol type used by port redirection data package: • TCP • UDP. • TCP/UDP
Internal port	The internal port number used by internal network
External port	The external port number used by external network
External IP	The device IP address specified by external network
Description	The remark information of port redirection entry

6.7 DMZ Settings

DMZ(Demilitarized Zone) is a buffer zone built between non-safety system and safety system for solving the problem that visitor from external network cannot visit internal network server after the firewall is installed.

Copyright © 3onedata Co., Ltd.

Function Description

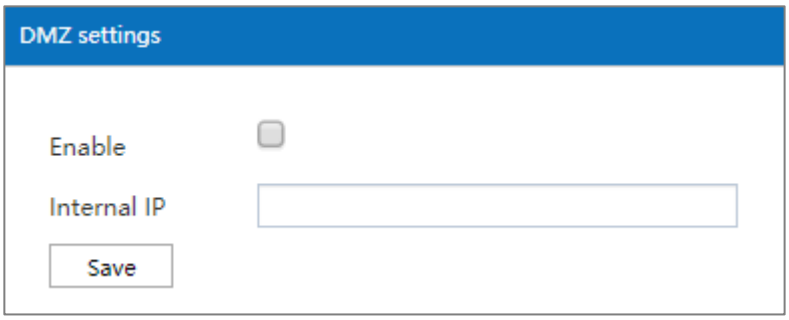
User can enable or disable DMZ function. The client can visit the specified LAN client via WAN.

Operation Path

Please open in order: "Firewall > DMZ Settings".

Interface Description

The DMZ setting interface as follows:



The main element configuration description of DMZ setting interface:

Interface Element	Description
Enable	DMZ enable check box, check it to enable the DMZ function.
Internal IP	The IP address of LAN client, for example: 192.168.1.123.

Copyright © 3onedata Co., Ltd.

7 VPN Tunnel

VPN (Virtual Private Network) is a temporary, secure connection established through a public network (usually the Internet). It is a secure and stable tunnel passing through a chaotic public network. Adopting this tunnel to encrypt data can ensure the secure use of Internet.

7.1 VPN Connection Status

Function Description

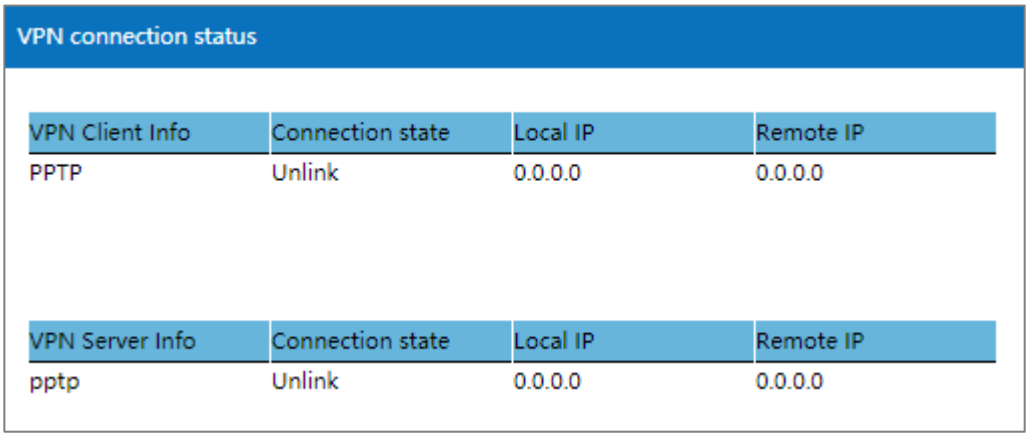
You can view VPN connection status.

Operation Path

Open in order: "VPN Tunnel > VPN Connection Status".

Interface Description

VPN Connection Status interface as follow:



The main element configuration description of VPN Connection Status interface:

Interface Element	Description
VPN Client Info	Display VPN client information.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Connection state	The connection state of client.
Local IP	The IP address of local client.
Remote IP	Display IP address of remote server.
VPN Server Info	Display VPN server information.
Connection state	Display the connection state of the server.
Local IP	Display IP address of local server.
Remote IP	Display the IP address of remote client.

7.2 GRE Settings

Generic Routing Encapsulation (GRE) protocol encapsulates data packets of certain network layer protocols (such as IP and IPX), so that these encapsulated data packets can be transmitted in another network layer protocol (such as IP). GRE adopts tunnel technology, which is the layer 3 tunnel protocol of VPN (Virtual Private Network).

Function Description

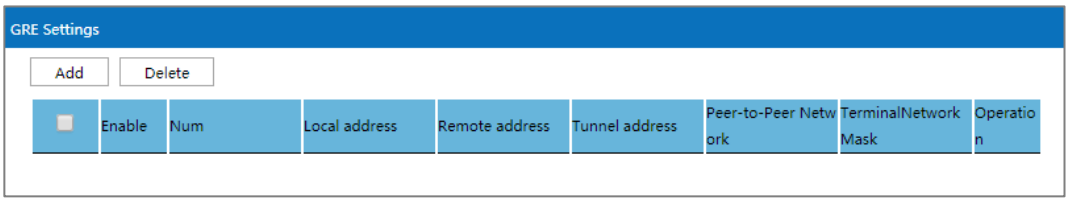
User can configure the relevant parameters of GRE.

Operation Path

Open in order: "VPN tunnel > GRE Settings".

Interface Description

GRE settings interface as follows:



The main elements configuration description of GRE settings interface:

Interface Element	Description
Enable	GRE settings is enabled or not: • ON Status • OFF
Num	The serial number of GRE settings.
Local address	Local IP address.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Remote address	End IP address.
Tunnel address	IP address of local GRE tunnel.
Peer-to-Peer Network	Subnet IP of the end GRE, for example: 192.168.1.0.
Terminal Network Mask	Subnet mask of end GRE.

7.3 PPTP Client Settings

Point to Point Tunneling Protocol (PPTP) is an enhanced security protocol. It supports multi-protocol virtual private network (VPN), which can enhance security through password authentication protocol (PAP), extensible authentication protocol (EAP) and other methods, and provide encrypted communication between PPTP client and server.

Function Description

User can configure the parameters related to PPTP client.

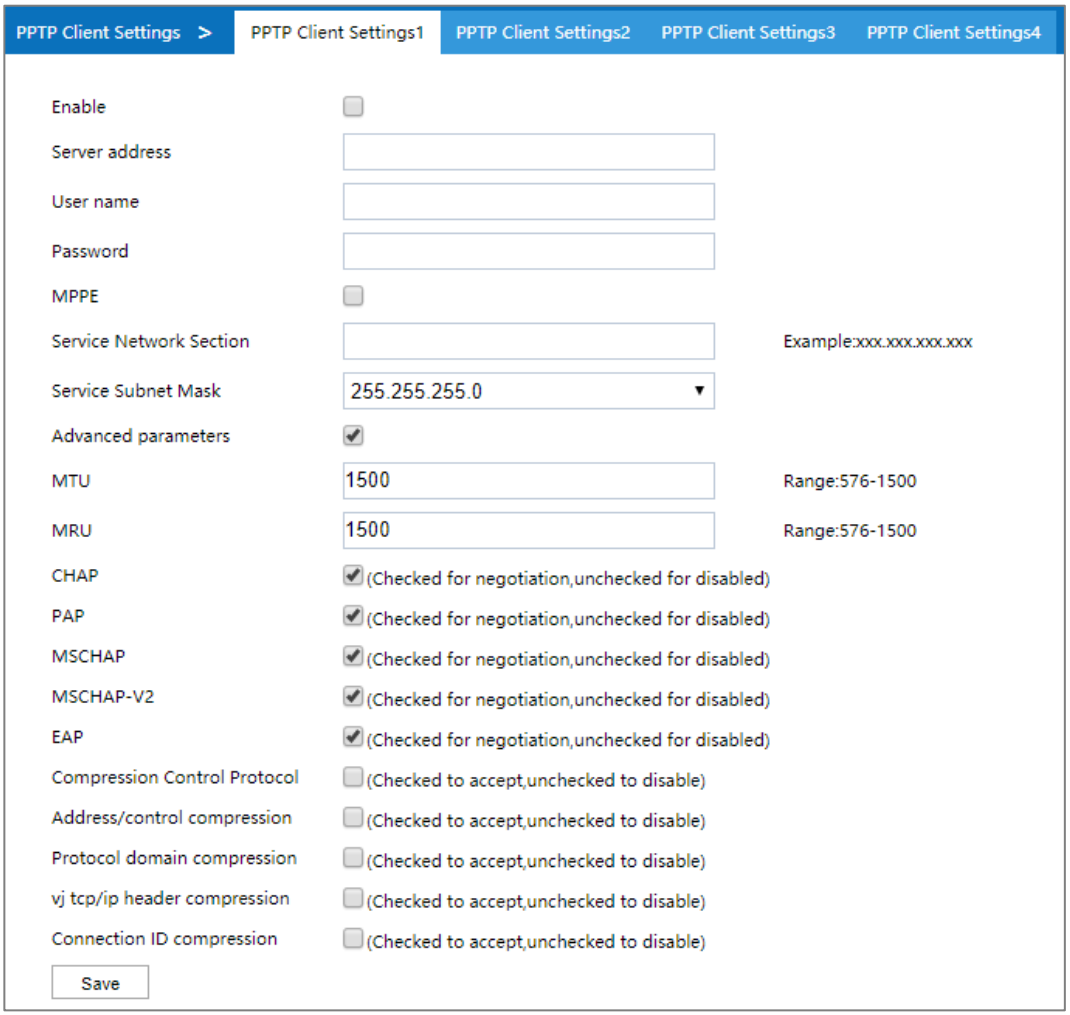
Operation Path

Open in order: "VPN tunnel > PPTP Client Settings".

Interface Description: PPTP Client 1-4

The PPTP client 1-4 settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of PPTP client 1-4 settings interface:

Interface Element	Description
Enable	PPTP Client Settings enable checkbox, check to enable the PPTP client settings function.
Server Address	IP address of PPTP server.
Username	User name allowed by PPTP server
Password	Password corresponding to the user name allowed by PPTP server.
MPPE	Functional enablement checkbox of MPPE (Microsoft Point-to-Point Encryption) protocol, click to enable MPPE encryption function.
Service Network Section	Subnet segment of the PPTP server.
Service Subnet Mask	Drop-down box of subnet mask of the PPTP server.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Advanced Parameters	Click advanced parameters checkbox, the advanced parameters configuration will be displayed.
MTU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.
MRU	Maximum Receive Unit (MRU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.
CHAP	Authentication allows the use of Challenge Handshake Authentication Protocol (CHAP).
PAP	Authentication allows the use of unencrypted keyword (PAP).
MSCHAP	Authentication allows the use of Microsoft CHAP Protocol.
MSCHAP-V2	Authentication allows the use of Microsoft CHAP V2 Protocol.
EAP	Authentication uses the Extensible Authentication Protocol (EAP).
Compression Control Protocol	Compression Control Protocol (CCP) is responsible for configuring and negotiating which compression algorithm to use on both ends of a PPP link.
Address/Control Compression	PPTP compresses address/control field of PPP frame.
Protocol Domain Compression	PPTP compresses the upper-layer protocol fields carried by PPP frame.
Vj tcp/ip header Compression	PPTP adopts Van Jacobson TCP/IP header compression algorithm, compresses the message header of upper-layer protocol TCP/IP fields carried by PPP frame.
Connection ID compression	PPTP compresses PPP frame ID.

7.4 PPTP Server Settings

Function Description

User can configure the parameters related to PPTP server.

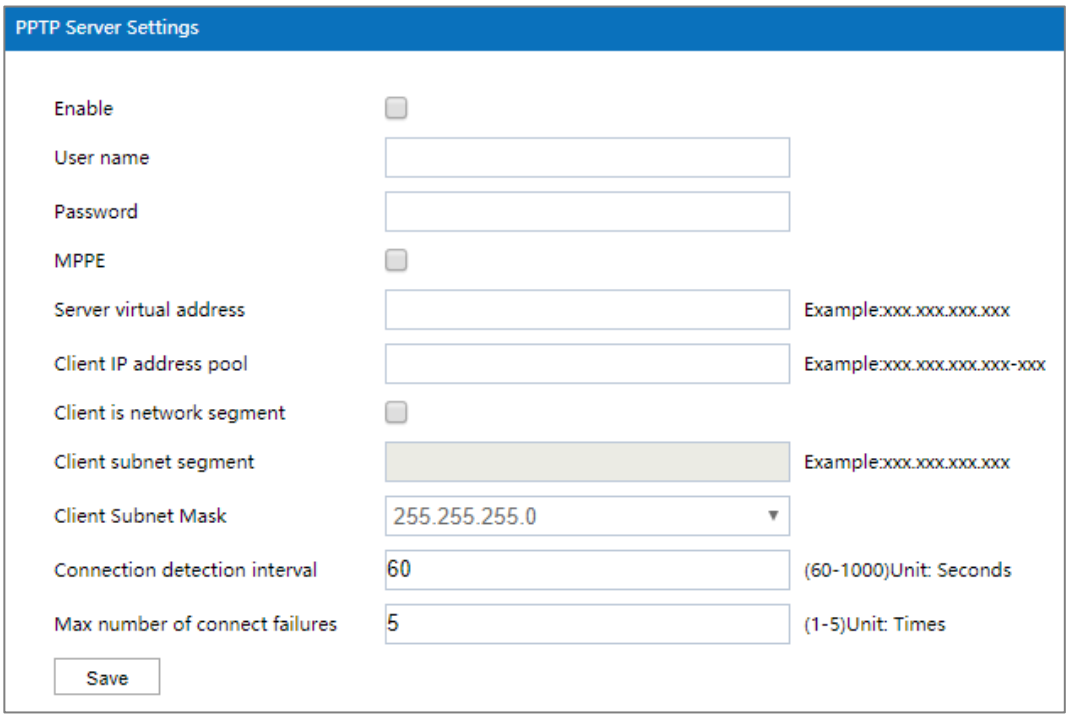
Operation Path

Open in order: "VPN Tunnel > PPTP Server Settings".

Copyright © 3onedata Co., Ltd.

Interface Description

The PPTP server settings interface is as follows:



The main elements configuration description of PPTP server settings interface:

Interface Element	Description
Enable	PPTP Server Settings enable checkbox, check to enable the PPTP server settings function;
Username	User name provided by PPTP to the client for connection.
Password	Password corresponding to the user name provided by PPTP to the client for connection
MPPE	Functional enable checkbox of MPPE (Microsoft Point-to-Point Encryption), click to enable MPPE encryption function.
Server virtual address	Virtual IP address of PPTP server.
Client IP address pool	IP address pool range assigned to the client, the format is: xxx.xxx.xxx.xxx-xxx.
Client is network segment	The client is network segment enable check box allows routers with subnets as network segments to connect and access PPTP VPN servers as clients. Check it to enable the function of the client as network segment, and input the subnet segment and mask of the client.
Client subnet segment	Set the network segment that allows the client to access,

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	and use it with the client as the network segment. Note: This input box can only be entered after enabling the function of client as the network segment.
Client Subnet Mask	Drop-down box of subnet mask of the PPTP client. Note: This input box can only be entered after enabling the function of client as the network segment.
Connection detection interval	Detect the interval of connection, the default value is 60, unit: second.
Max number of connect failures	Detect the maximum number of failed connections. The default value is 5.

7.5 L2TP Client Settings

Layer 2 Tunneling Protocol (L2TP) is an industry-standard Internet tunneling protocol. Its functions are roughly similar to those of PPTP protocol. It can also encrypt the network data flow. There are some differences between the two protocols: For example, PPTP requires the network to be an IP network, L2TP requires a point-to-point connection for data packets; PPTP uses a single tunnel, L2TP uses multiple tunnels; L2TP provides header compression and tunnel authentication, but PPTP does not support.

Function Description

User can configure the parameters related to L2TP client.

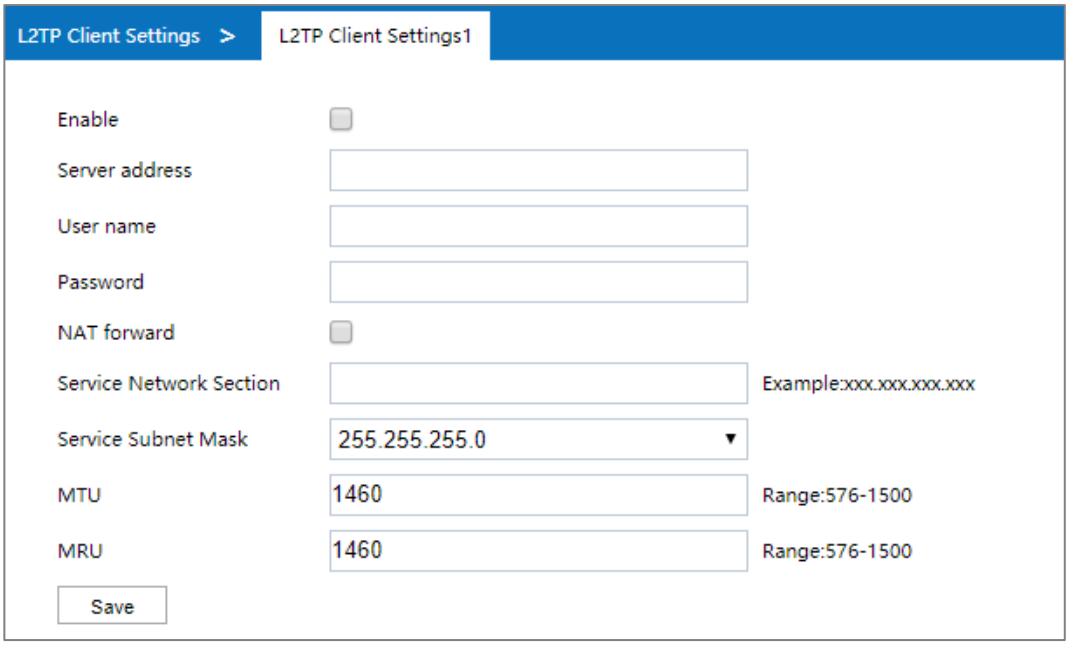
Operation Path

Open in order: "VPN tunnel > L2TP Client Settings".

Interface Description

The L2TP client settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of L2TP client settings interface:

Interface Element	Description
Enable	L2TP Client Settings enable checkbox, check to enable the L2TP client settings function.
Server Address	IP address of L2TP server
Username	User name allowed by L2TP server.
Password	Password corresponding to the user name allowed by L2TP server.
NAT forward	Enablement checkbox of NAT(Network Address Translation), check to enable NAT forwarding. All data flows of client are forwarded through the VPN server.
Service Network Section	User name provided by L2TP to the client for connection
Service Subnet Mask	Password corresponding to the user name provided by L2TP to the client for connection
MTU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.
MRU	Maximum Receive Unit (MRU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.

Copyright © 3onedata Co., Ltd.

7.6 L2TP Server Settings

Function Description

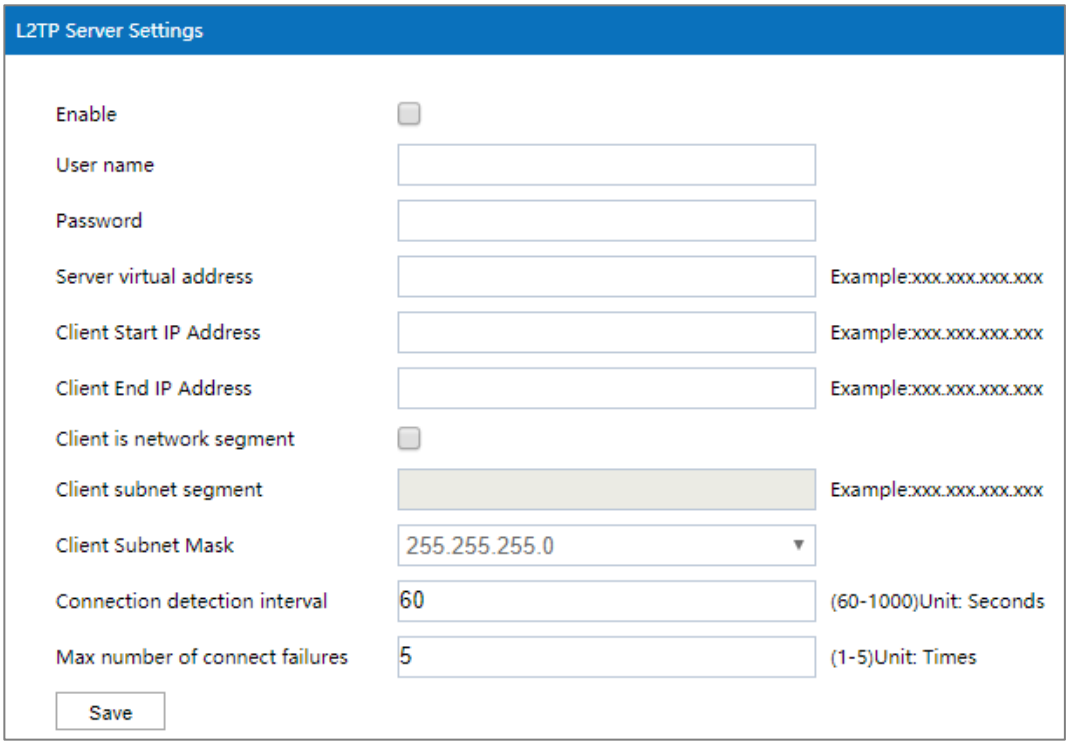
User can configure the parameters related to L2TP server.

Operation Path

Open in order: "VPN tunnel > L2TP Server Settings".

Interface Description

The L2TP server settings interface is as follows:



The main elements configuration description of L2TP server settings interface:

Interface Element	Description
Enable	L2TP Server Settings enable checkbox, check to enable the L2TP server settings function;
Username	User name provided by L2TP to the client for connection
Password	Password corresponding to the user name provided by L2TP to the client for connection
Server virtual address	Virtual IP address of L2TP server
Client Start IP address	Minimum start IP address of L2TP client
Client End IP Address	Maximum end IP address of L2TP client
Client is network	“Client subnet segment” enable checkbox. It allows the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
segment	router whose subnet is the network segment to connect as a client and access the L2TP VPN server.Click to enable the function of the client as network segment.After enabled, the subnet segment and mask of the client can be input.
Client subnet segment	Set the network segment that allows the client to access, and use it with the client as the network segment. Note: This input box can only be entered after enabling the function of client as the network segment.
Client Subnet Mask	Drop-down box of subnet mask of the L2TP client. Note: This input box can only be entered after enabling the function of client as the network segment.
Connection detection interval	Detect the interval of connection, the default value is 60, unit: second.
Max number of connect failures	Detect the maximum number of failed connections. The default value is 5.

7.7 IPsec

The Internet Protocol Security (IPsec) protocol suite is a series of protocols developed by the Internet Engineering Task Force (IETF) that provides high-quality, interoperable, cryptographic-based security for IP packets. The specific communication parties can ensure the privacy, integrity, authenticity and anti-replay of the datagram during transmission on the network through encryption and data source authentication at the IP layer.

- Confidentiality refers to the encryption and protection of user data and is transmitted in the form of cipher text.
- Data integrity refers to the authentication of received data, which can determine whether a message has been tampered with.
- Anti-replay refers to preventing an attack that malicious user repeatedly transmits captured packet, that is, the receiver rejects old or duplicate packets.

Function Description

User can configure the relevant parameters of IPsec.

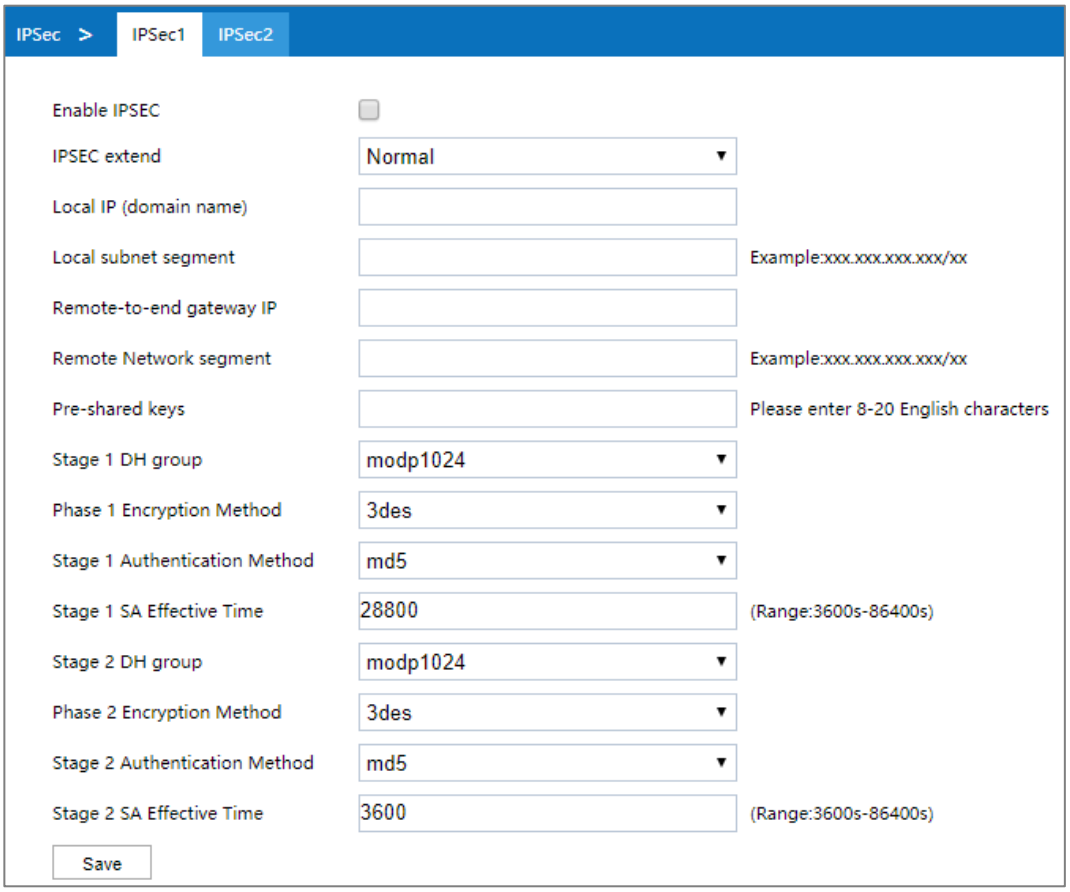
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "VPN tunnel > IPsec".

Interface Description

IPsec settings interface as follows:



The main elements configuration description of IPsec settings interface:

Interface Element	Description
Enable IPSEC	IPSec Settings enable checkbox, check to enable IPSec settings function.
IPSEC extend	Drop-down box of IPSEC extension, options as follows: • Normal: Regular IPSEC; • GRE: GRE over IPSEC, GRE encapsulation based on IPSEC encryption; • L2TP: GRE over L2TP, L2TP encapsulation based on IPSEC encryption.
Local IP (domain name)	IP address or domain name of the local external network port
Local Subnet Mask	The local subnet and mask of the router, for example: 192.168.4.0/24.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Remote-to-end gateway IP	External network port IP of the opposite end
Remote Network Mask	Protected subnet and subnet mask of the opposite IPsec end, for example: 192.168.4.0/24.
Pre-shared keys	Unicode string that verifies the IPsec connection.
Stage 1 DH group	Stage 1 DH exchange algorithm, options as follows: • modp768 • modp1024 • modp1536
Phase 1 Encryption Method	Phase 1 encryption algorithm, options as follows: • 3des • aes128 • aes192
Stage 1 Authentication Method	Stage 1 Authentication Method, options as follows: • md5 • sha • sha256 • sha384 • sha512
Stage 1 SA Effective Time	Stage 1 SA survival time, unit is second and default is 28800.
Stage 2 DH group	Stage 2 DH exchange algorithm, options as follows: • modp768 • modp1024 • modp1536
Stage 2 Encryption Method	Phase 2 encryption algorithm, options as follows: • 3des • aes128 • aes192
Stage 2 Authentication Method	Stage 2 Authentication Method, options as follows: • md5 • sha • sha256 • sha384 • sha512
Stage 2 SA Effective Time	Stage 2 SA Effective time, unit is second and default is 3600.

Copyright © 3onedata Co., Ltd.

7.8 OpenVpn Client Settings

OpenVPN is an open source encrypted tunnel construction tool. Based on the SSL/TLS protocol of OpenSSL, it can realize point-to-point SSL VPN secure connection in the Internet. OpenVPN provides two types of virtual network interfaces: TUN and TAP, which are used to establish IP tunnel and Ethernet bridge respectively. OpenVPN provides a variety of authentication methods to confirm the identities of both parties involved in the connection, including pre-shared private key, third-party certificate and user name/password combination.

By using OpenVPN, you can:

- Use specific UDP or TCP ports to realize VPN connection between two hosts.
- Realize the C/S structure and realize the interconnection of multiple Clients through server.
- Ensure the security of data transmission through TLS/SSL encryption.
- Through data compression, improve the speed of data transmission.

Function Description

User can configure the parameters related to OpenVpn client.

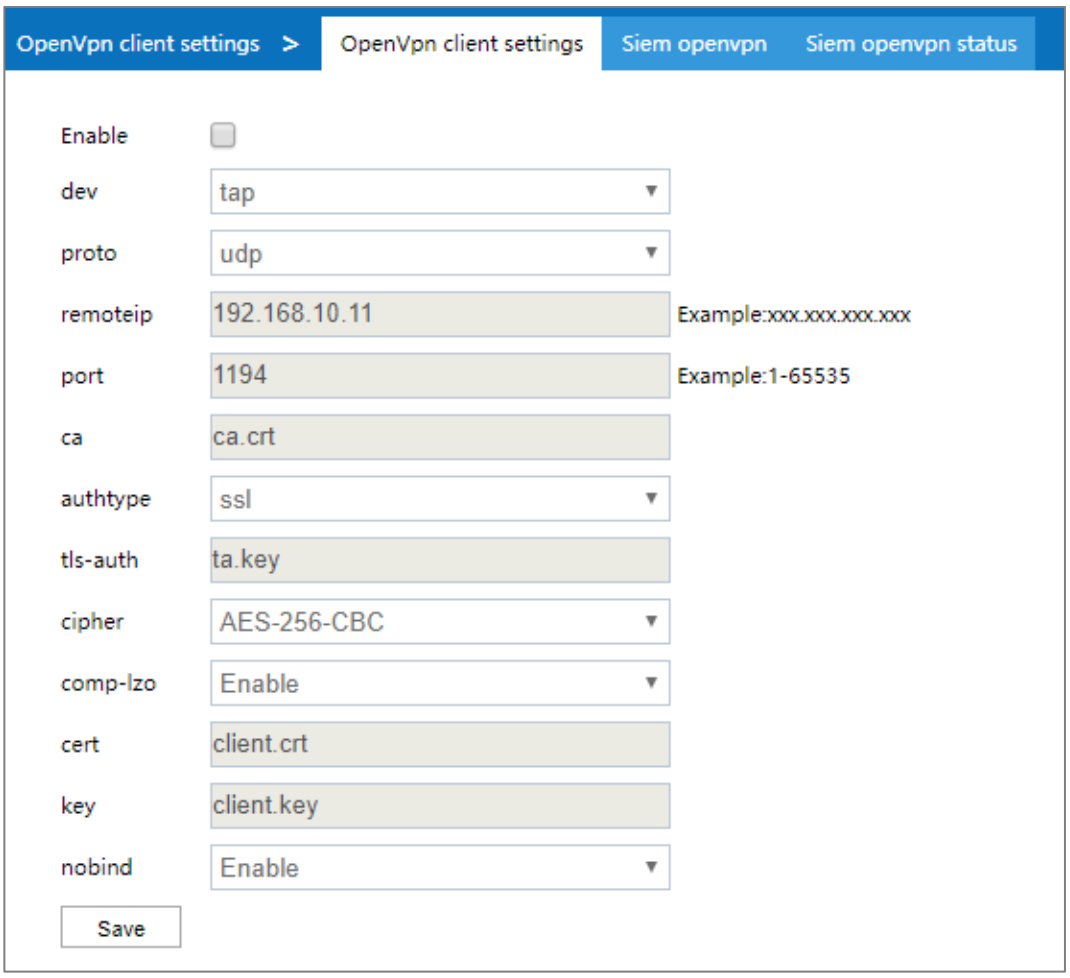
Operation Path

Open in order: "VPN Tunnel > OpenVpn Client Settings".

Interface Description 1: OpenVpn Client Settings

The OpenVpn client settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of OpenVpn client settings interface:

Interface Element	Description
Enable	Check the enable check box to enable the OpenVPN client.
Work mode	The drop-down list of OpenVpn work mode, the options are as follows: • tun: Tun mode is the routing mode, which creates an IP routing tunnel through OpenVPN. • tap: tap mode is the bridging mode, which creates a bridging network tunnel through OpenVPN.
Protocol type	The drop-down list of OpenVPN data transmission protocol type. The options are: • tcp: Transmission Control Protocol; • udp: User Datagram Protocol.
Destination Address	IPv4 address information of OpenVPN server, such as 192.168.10.11.
Destination port	The port number monitored by the OpenVPN server. The default value is 1194. The value range is 1-65535.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
ca	CA (Certificate Authority) certificate file name, which is the CA certificate used by OpenVPN client and server. It is mainly used to verify the legitimacy of server or client certificate.
Aurh type	The drop-down list of OpenVPN certificate type. The options are: • txt: use user name and password for authentication. • ssl: use SSL (Secure Sockets Layer) certificate for authentication.
tls-auth	TLS (Transport Layer Security) authentication key file name, enhanced authentication encryption, and synchronization with the server.
cipher	The drop-down list of OpenVPN encryption algorithm. The client and server are synchronized. The options are as follows: • NONE • BF-CBC • DES-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • RC2-64-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC
comp-lzo	LZO drop-down list, options are: • Enable: enable LZO algorithm to compress data, which is consistent with the server settings. • Disable.
cert	In SSL authentication mode, the certificate file name of OpenVPN client.
key	In SSL authentication mode, the key file name of OpenVPN.
txtuser	In Txt authentication mode, the user name of OpenVPN client.
txtpassword	In Txt authentication mode, the user password of OpenVPN client.
nobind	Nobind drop-down list, options are:

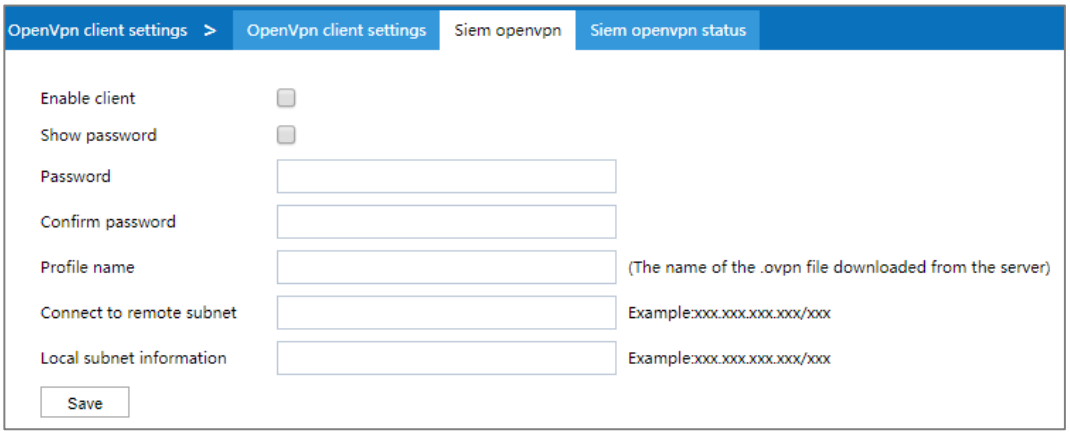
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Enable: the device does not bind any port to listen for incoming data. • Disable.

Note
CA, TLS-Auth, Cert, Key and other authentication files can be imported on the "VPN Tunnel > Certificate Settings" page.

Interface Description 2: Siemens OpenVPN

Siemens OpenVPN interface is as follows:



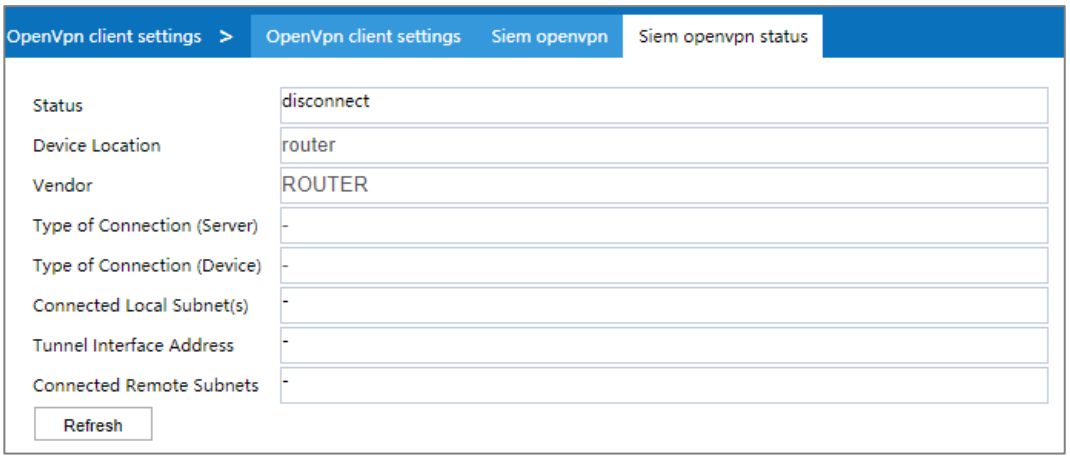
Main elements configuration descriptions of Siemens openvpn interface:

Interface Element	Description
Enable client	Enable check box to enable Siemens OpenVPN client.
Show password	Show password check box. Check it to view password information.
Password	Device password of the OpenVPN server.
Confirm password	Enter the device password of the OpenVPN server again.
Profile Name	The profile of OpenVPN server contains the configuration and authentication information of VPN server. Note The profile can be imported on the “VPN Tunnel > Certificate Settings” page.
Connect to remote subnet	IP address and subnet mask information of the remote OpenVPN server network.
Local subnet information	IP address and subnet mask information of the local subnet.

Copyright © 3onedata Co., Ltd.

Interface Description 3: Siemens openvpn State

Siemens openvpn state interface is as follow:



The main elements configuration description of Siemens openvpn state interface:

Interface Element	Description
Status	Display OpenVPN connection status.
Device location	Display the geographic location or name of the device.
Vendor	Display the supplier name.
Type of connection (Server)	Displays the connection type of the server.
Type of connection (Device)	Display the connection type of the device.
Connected local subnet	Display the information of the connected local subnet.
Tunnel interface address	Displays the tunnel interface address.
Connected remote subnet	Display the information of the connected remote subnets.

7.9 Certificate Settings

Function Description

User can add OpenVPN client authentication certificates and related configuration files.

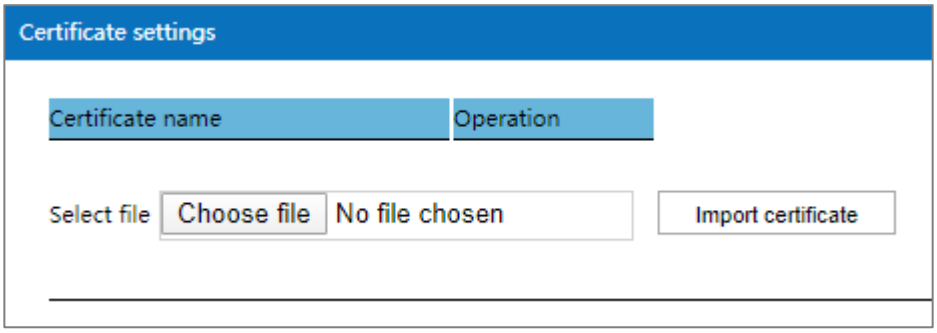
Operation Path

Open in order: "VPN Tunnel > Certificate Settings".

Copyright © 3onedata Co., Ltd.

Interface Description

Certificate Settings interface is as follows:



The main element configuration description of Certificate Settings interface:

Interface Element	Description
Certificate name	Certificate name.
Operation	Click “Delete” to delete the corresponding certificate file.
Choose file	Click “Browse” to select a local certificate file, and then click “Import Certificate” to upload the certificate file to the device. Note: Only files in ". crt", ".key" or ". ovpn" format can be uploaded.

Copyright © 3onedata Co., Ltd.

8 System Tools

8.1 Time Settings

Function Description

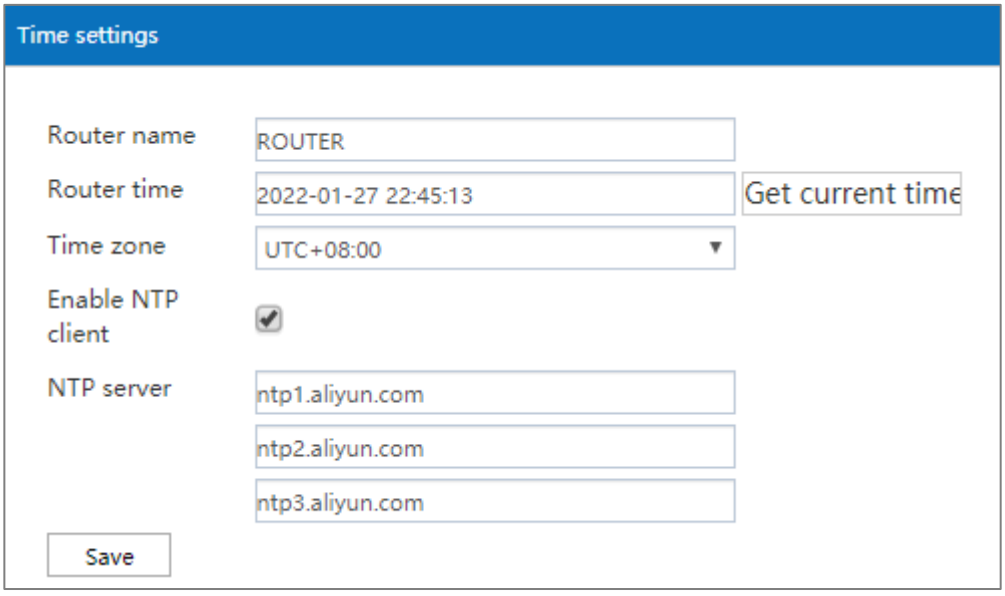
User can configure time-related parameters information.

Operation Path

Open in order: "System Tools > Time Setting".

Interface Description

Time settings interface as follows:



The main elements configuration description of time settings interface:

Interface Element	Description
Router name	The name of the router
Router time	The time of the router, the format is: year-month-day hour:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	minute: second
Time Zone	Drop-down box of time zone, user can choose according to their demands
Enabling NTP Client	NTP Client Settings enable checkbox, check to enable the NTP client function to synchronize the time of the server with the client.
NTP Server	The address of the server that needs to be synchronized Note: When there are multiple candidate NTP clients, the default is the first one. The higher the order, the higher the priority.

8.2 Access Settings

Function Description

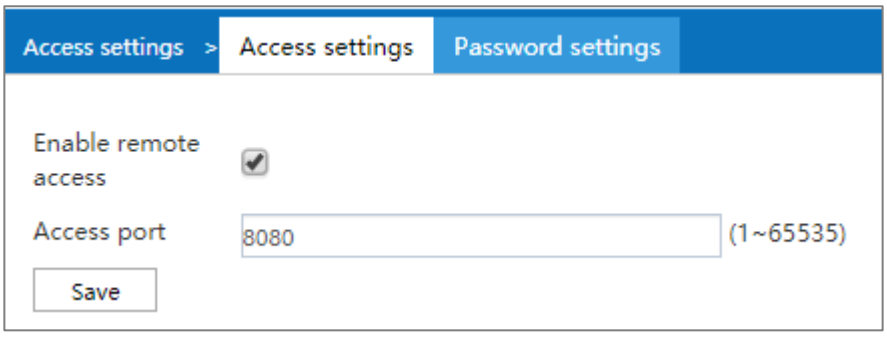
User can enable remote access and modify the username and password for accessing the device.

Operation Path

Open in order: "System Tools > Access settings".

Interface Description 1: Access Settings

Access settings interface as follows:



The main elements configuration description of access settings interface:

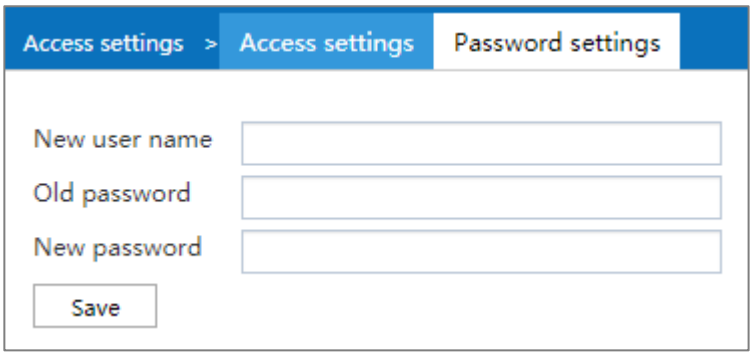
Interface Element	Description
Enable remote access	Remote access enable checkbox, check to enable remote access, the user can access the device through the HTTP/HTTPS protocol on the external network.
Access port	Port number of remote access, the port number defaults to 8080.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Note: Ensure the consistency of access port when accessing the device through a browser.

Interface Description 2: Password Settings

Password settings interface as follows:



The main elements configuration description of password settings interface:

Interface Element	Description
New username	New username settings of the device. Note: Username and password are composed of capital and lower-case letters and numbers.
Old password	The login password used by the current device. Note: The username and password of the device are both admin by default.
New password	New password settings of the device. Note: Username and password are composed of capital and lower-case letters and numbers.

8.3 Timed Restart

Function Description

User can configure the time for the device to automatically restart.

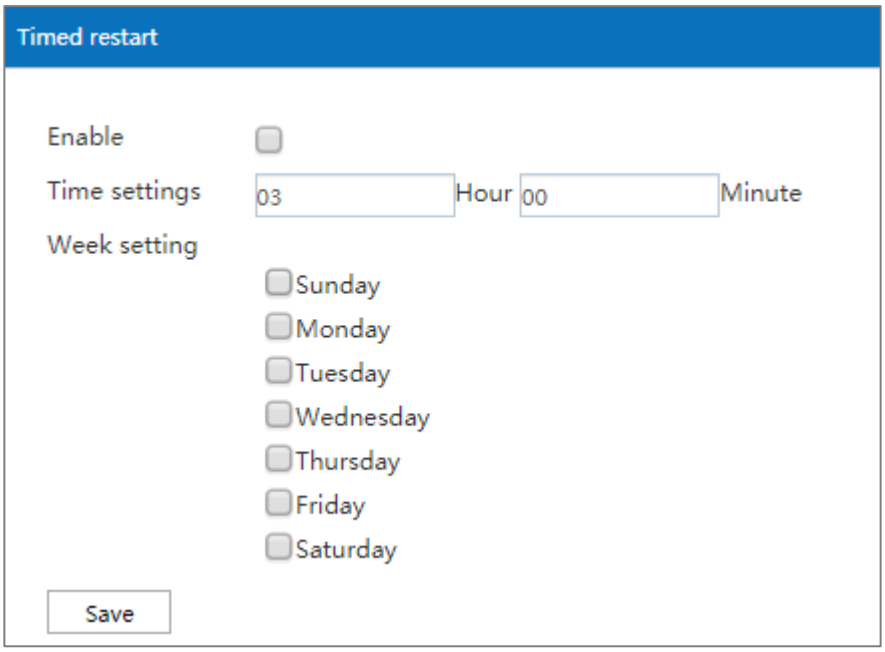
Operation Path

Open in order: "System Tools > Timed Restart".

Interface Description

The timed restart interface as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of timed restart interface:

Interface Element	Description
Enable	Timed Restart enable checkbox, check to enable Timed Restart function.
Time Settings	Device restart time and date settings. When the set time is the same as the router time, the device will automatically restart.
Week setting	Device restart week setting.

8.4 Backup Recovery

Function Description

User can select files for upload configuration, download configuration, and restore factory defaults.

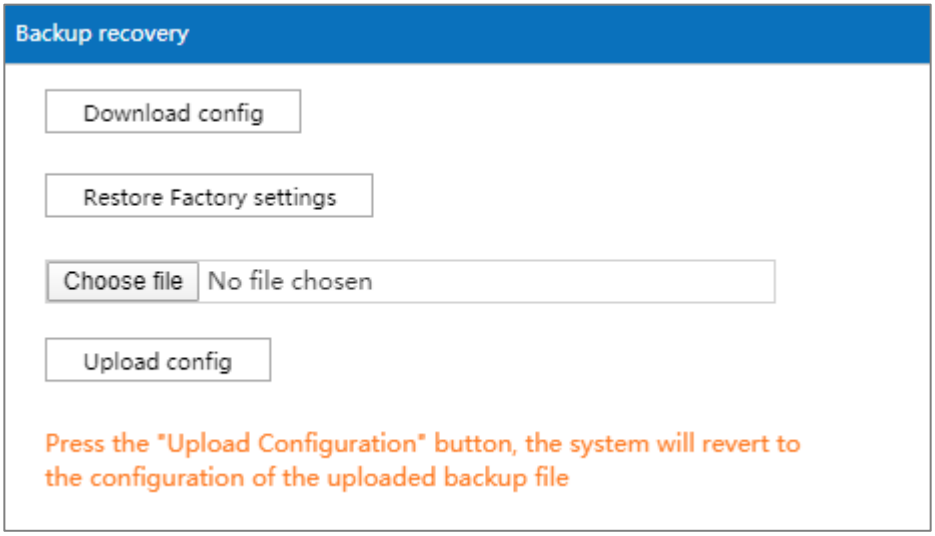
Operation Path

Open in order: "System Tools > Backup Recovery".

Interface Description

The backup recovery settings interface as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of backup recovery settings interface:

Interface Element	Description
Download config	Click the "Download" button to download the configuration file of the current device and save it in the format of ".file".
Restore factory settings	Click the button of "Restore" to restore factory defaults of the device.
Choose file	The "Choose file" button allows user to select the configuration file for the host backup.
Upload config	Click the "Upload" button to upload the backup configuration file to the current device, so that the device can restore the configuration in the backup file.

8.5 Log Management

Function Description

It can:

- record the log files to the remote server
- Clear or download USB drive log

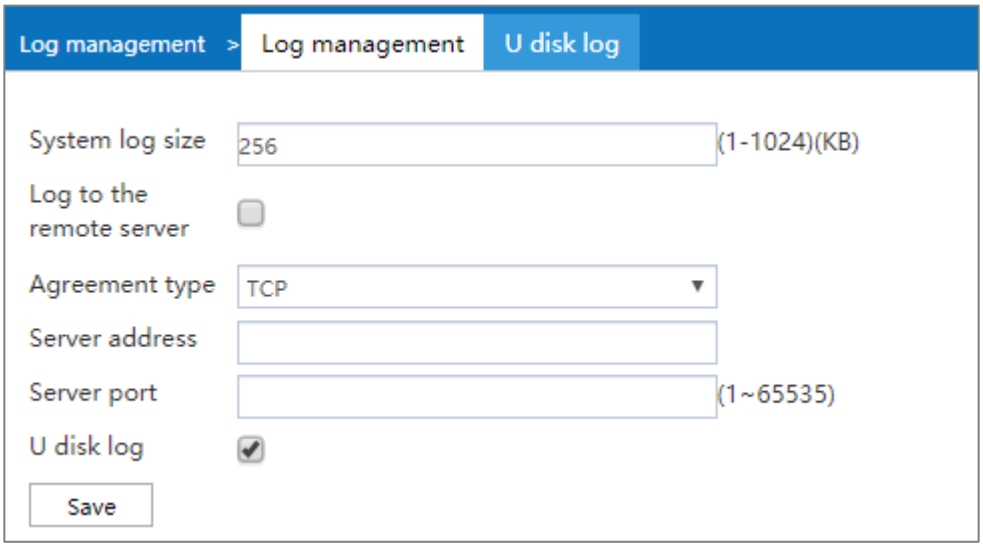
Operation Path

Open in order: "System Tools > Log Management".

Interface Description 1: Log Management

The log management interface as follows:

Copyright © 3onedata Co., Ltd.



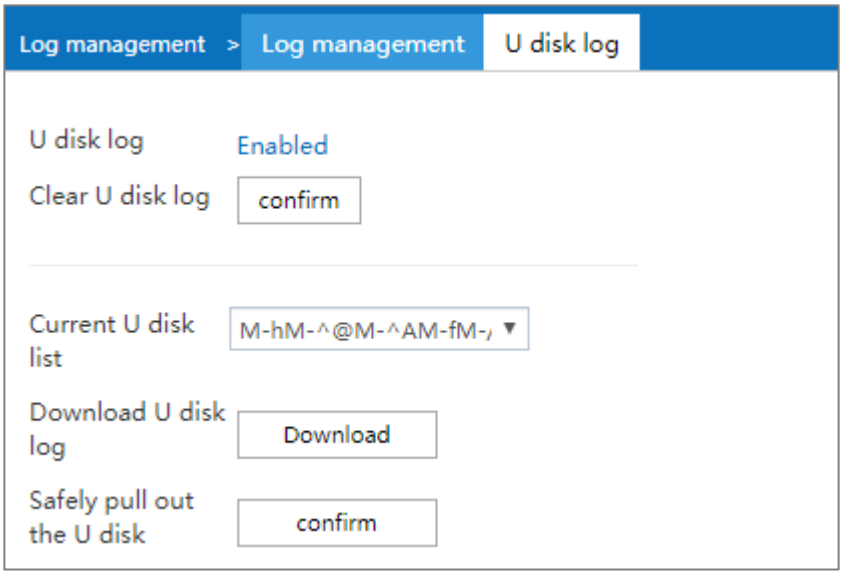
The main elements configuration description of log management interface:

Interface Element	Description
System log size	Set the size of the log file, the default is 256
Log to the remote server	Record to remote server enable checkbox, check to enable the function of recording to remote server to record log files to the remote server;
Agreement type	Drop-down box of the protocol type used by the record to remote server, options as follows: • TCP • UDP.
Server address	IP address information of the remote server
Server Port	The port number of the remote server,value range is 1~65535.
U disk log	Enable or disable the USB flash drive log: • Users can clear the U disk log or download the U disk log to the local computer when the function is disabled. • When disabled, the U disk log function is not available. Note: After the U disk log is enabled, the system will automatically write the log to the U disk.

Interface Description 2: USB Flash Drive Log

USB Flash Drive Log interface is as follows:

Copyright © 3onedata Co., Ltd.



Main elements configuration description of USB Flash Drive Log interface:

Interface Element	Description
U disk log	Display the status of U disk log function: • Enabled; • Disabled.
Clear U disk log	Clear the history log from the USB drive log file. Note: • If the USB drive saves multiple log files, all log files are cleared simultaneously. • If two USB drive are inserted at the same time, the log files on both USB sticks are cleared at the same time.
Current U disk list	Displays a list of U disk currently inserted into AC.
Download U disk Log	Download the U disk log to local computer. Notice: Before using it for the first time, make sure there is not a file with the same name as "device_history_log.log" on the USB drive to avoid changes to the log contents.
Safely pull out the U disk	Click the "Confirm" button and pull out the USB flash drive.

8.6 System Log

Function Description

User can check the log information of the device.

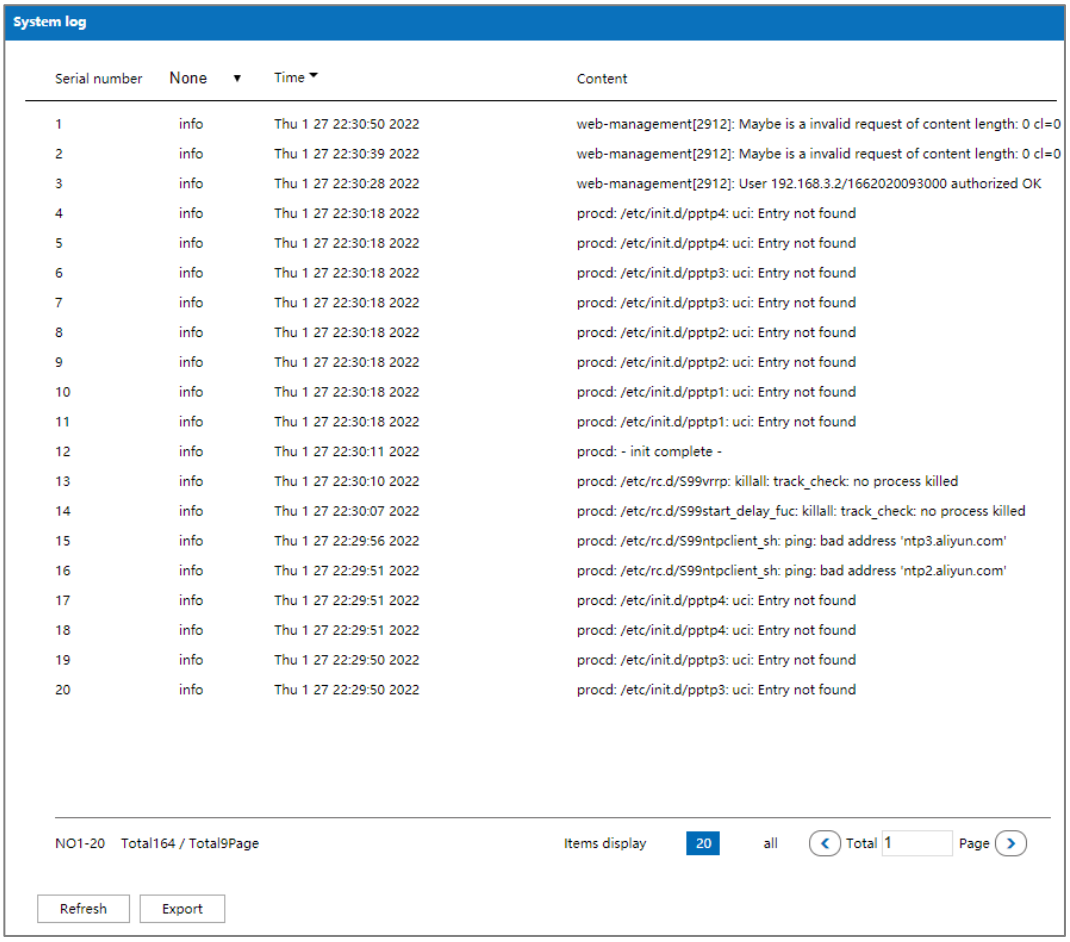
Operation Path

Please open in order: "System Tools > System log".

Copyright © 3onedata Co., Ltd.

Interface Description

The system log interface is as follows:



The main element configuration description of system log interface:

Interface Element	Description
Serial number	Log messages display sequence.
Status	Log message type, options as follows: • NONE: display all information; • Info: general messages; • Warning: alarm information; • Error: error information.
Time	The date and time filter button for log information. Note: Click the "Time" button to filter the start date and end date.
Content	A detailed description of the log contents.
Export	Click "export" to save the log messages to the local host in the format of ".txt".
Refresh	Click "Refresh" to regain the newest log messages of the device.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Note: System log can store maximum 256KB log messages of the device in the most recent period.
Items display	Log information display mode, options as follows: • 20: Display 20 log messages per page; • all: Single page displays all log information.

8.7 Firmware Upgrade

Function Description

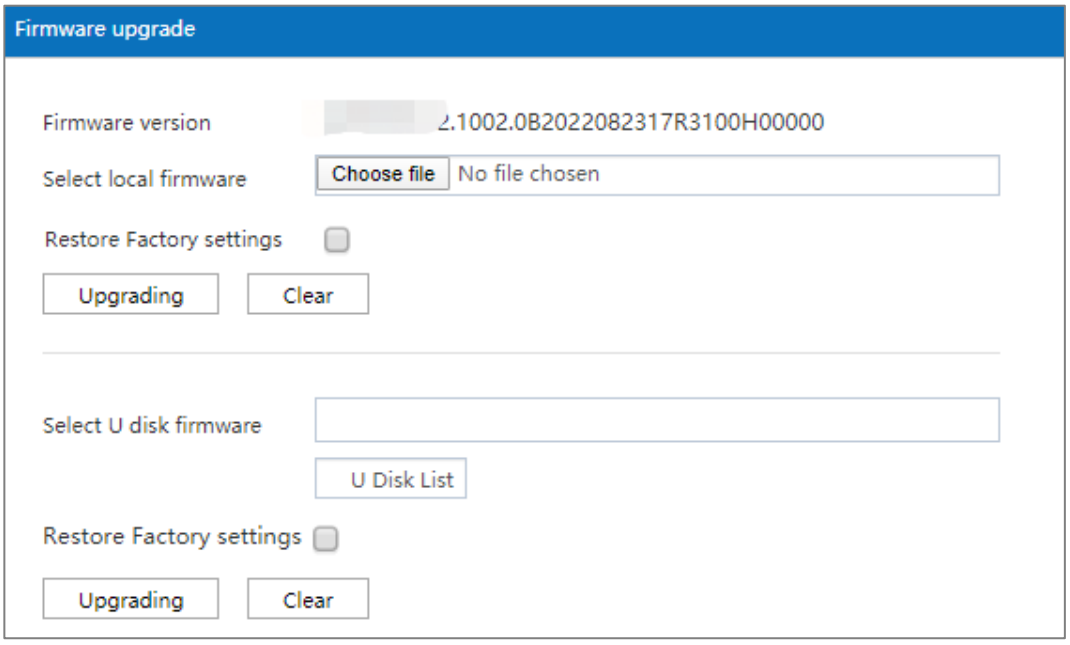
User can update the device system program via firmware upgrade.

Operation Path

Please open in order: "System Tools > Firmware Upgrade".

Interface Description

System upgrade interface as follows:



The main element configuration description of Firmware Upgrade interface:

Interface Element	Description
Firmware version	Software version used by current device.
Select local firmware	Click "Select file" to select local upgrade file of the host. Note: Please select the program version that is compatible with the current hardware during upgrading.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Restore factory settings	After upgrading, the configuration will be restored to factory settings.
Select U disk firmware	Click "Select file" to select local upgrade file in the USB flash drive. Note: Please select the program version that is compatible with the current hardware during upgrading.
Restore factory settings	After upgrading, the configuration will be restored to factory settings.
Update	Click "Updating" to upgrade the device program. Notice: • It takes a while during the upgrade process. Do not power off the device. • After a successful upgrade, the configuration of the device will remain unchanged and the firmware version information will be changed.

8.8 System Restart

Function Description

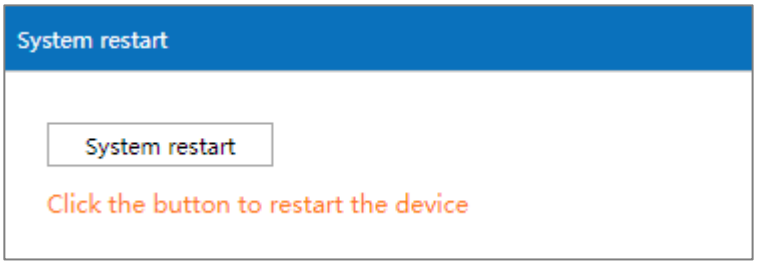
User can restart the device.

Operation Path

Open in order: "System Tools > System Restart".

Interface Description

The reboot system interface as follows:



The main elements configuration description of reboot system interface:

Interface Element	Description
System Restart	Click this button to reboot the device system. After the system restarts, it will jump back to the login interface.

Copyright © 3onedata Co., Ltd.

9 Diagnostic Tools

9.1 Ping Test

Ping belongs to a communication protocol and is part of the TCP/IP protocol. User can adopt the ping command to check whether the network is connected, which can help us analyze and determine network faults.

Function Description

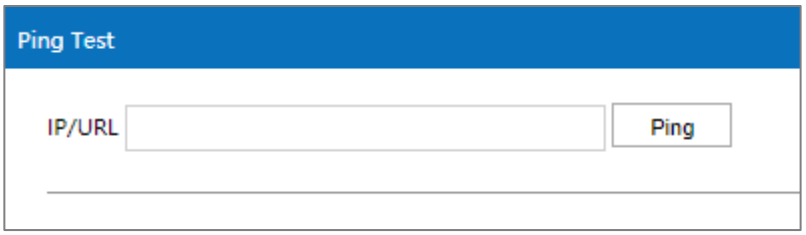
User can detect whether the target host can be connected.

Operation Path

Open in order: "Diagnostic tools > Ping test".

Interface Description

The Ping test interface as follows:



The main elements configuration description of Ping test interface:

Interface Element	Description
IP/URL	Target IP/URL address information to be detected.
Ping	Click the “Ping” button to start the test, and the test result is displayed below.

Copyright © 3onedata Co., Ltd.

9.2 Route Tracking

Route Tracking is a route-tracking utility that determines the path taken by an IP datagram to access a destination. The Route Tracking command uses the IP Time to Live (TTL) field and ICMP error messages to determine the route from one host to other hosts on the network.

Function Description

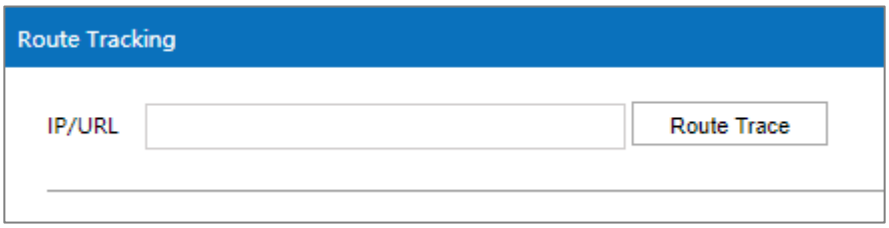
User can perform route tracking for the target host.

Operation Path

Open in order: "Diagnostic tools > Route tracking".

Interface Description

The route tracking interface is as follows:



The main elements configuration description of route tracking interface:

Interface Element	Description
IP/URL	Destination IP/URL address that requires route tracking.
Route Tracking	Click the "Route Trace" button to start tracking, and the test results are displayed below.

Copyright © 3onedata Co., Ltd.

10 Maintenance and Service

Since the date of product delivery, our company provides five-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's product, consumers can get help and solutions in the following ways:

- Internet Service;
- Call technical support office;
- Product repair or replacement;

10.1 Internet Service

More useful information and tips are available via our company website. Website: http://www.3onedata.com

10.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you solve the product or usage problems ASAP. Free service hotline: +86-4008804496

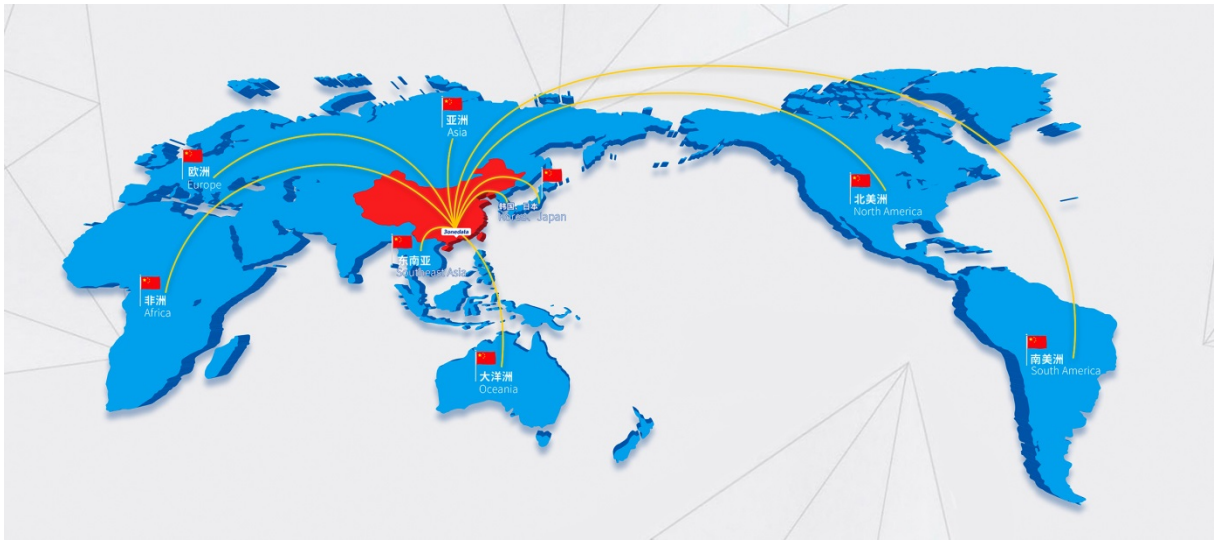
Copyright © 3onedata Co., Ltd.

10.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem. According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

3onedata



3onedata Co., Ltd.

Headquarter Address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology Support:	tech-support@3onedata.com
Service Hotline:	4008804496
Official Website:	http://www.3onedata.com