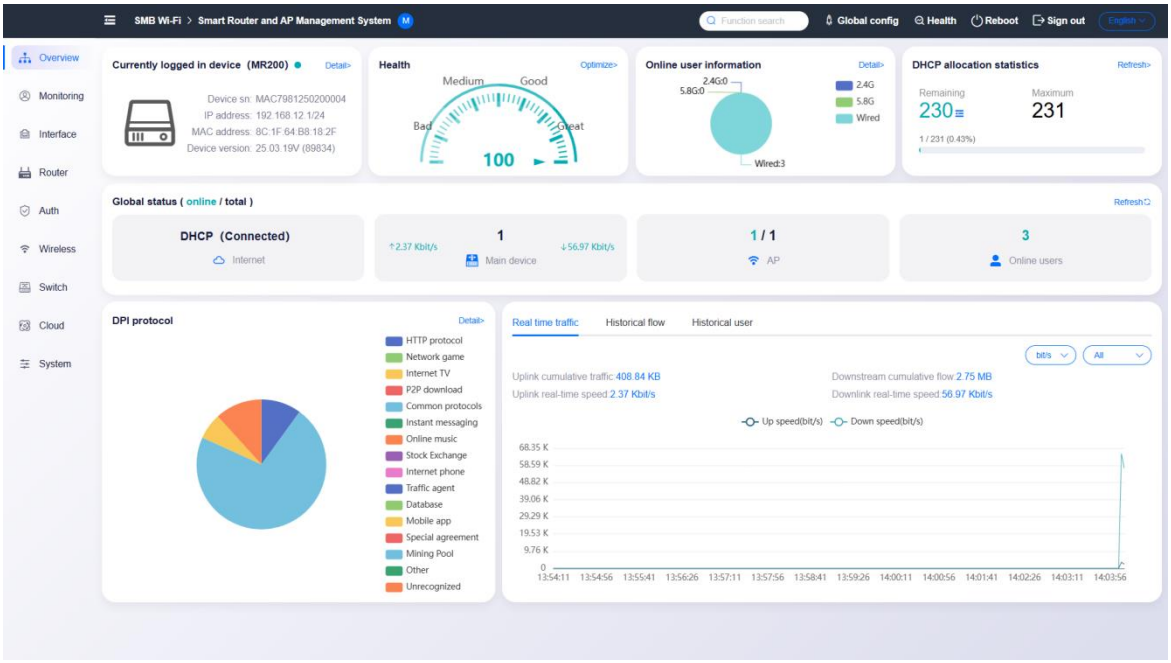
NWAC128

User manual

Gateway and AP Controller

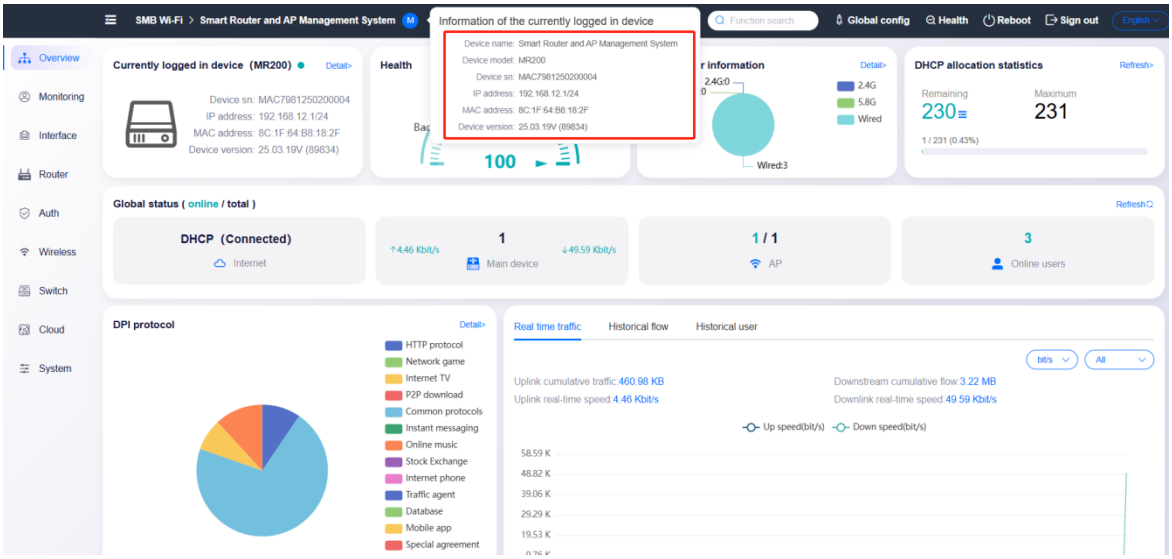
一、 Overview

The overview page of this device is mainly focused on data unification. Device information, terminals, and overall network-related functions are all displayed on this page. Most of the corresponding data statistics sections support clicking to jump to the data detail page

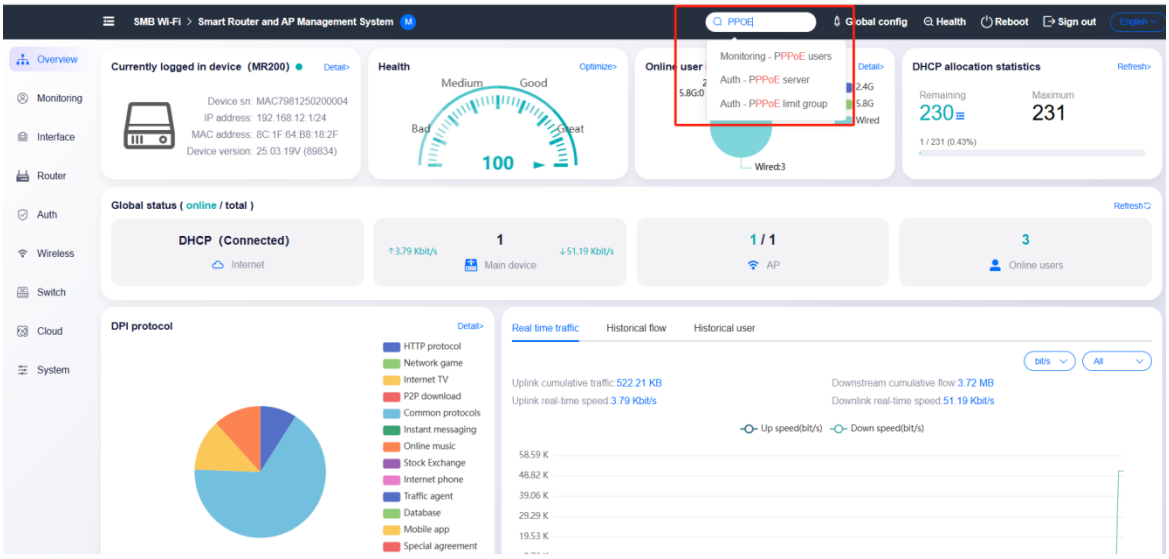


1.1 Quick Function Bar

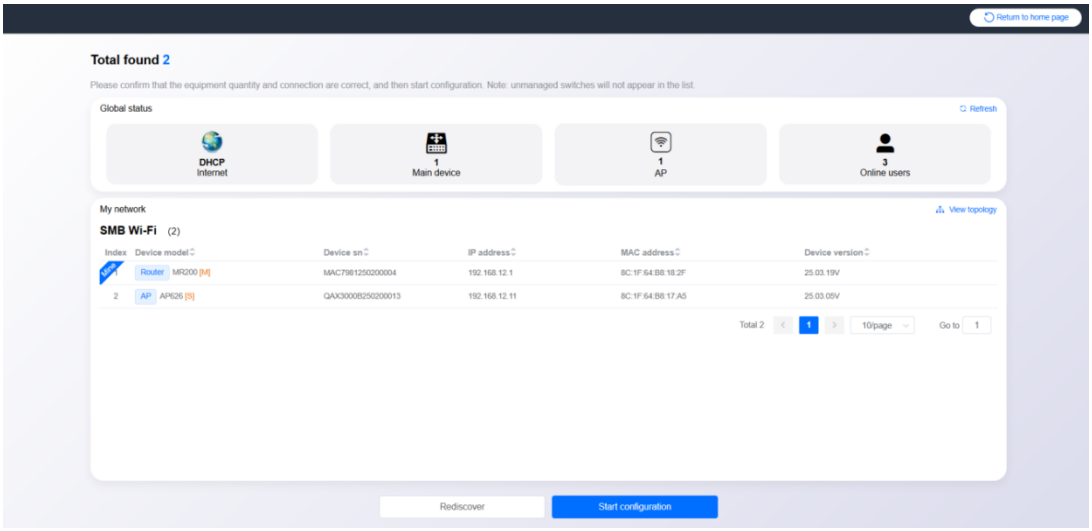
Current device login information: When the mouse hovers over the "M" (or "S" for slave devices) or "i" sub-label at the top of the page, the current device name, model, software version, serial number, current gateway address and other information are displayed.



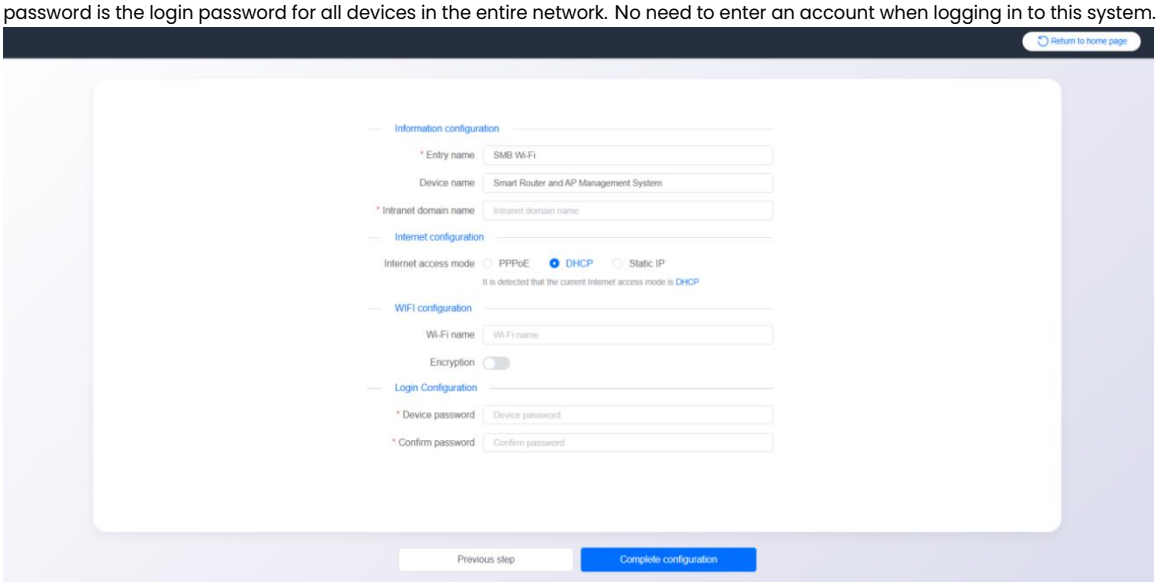
Function search: For users who are using this system for the first time and are not sure where the function is located in the menu, this function can be used. Enter the function keyword in the search function, such as "PPPoE " and the system will automatically display all related "PPPoE " functions in the current system. Click to enter the corresponding page.



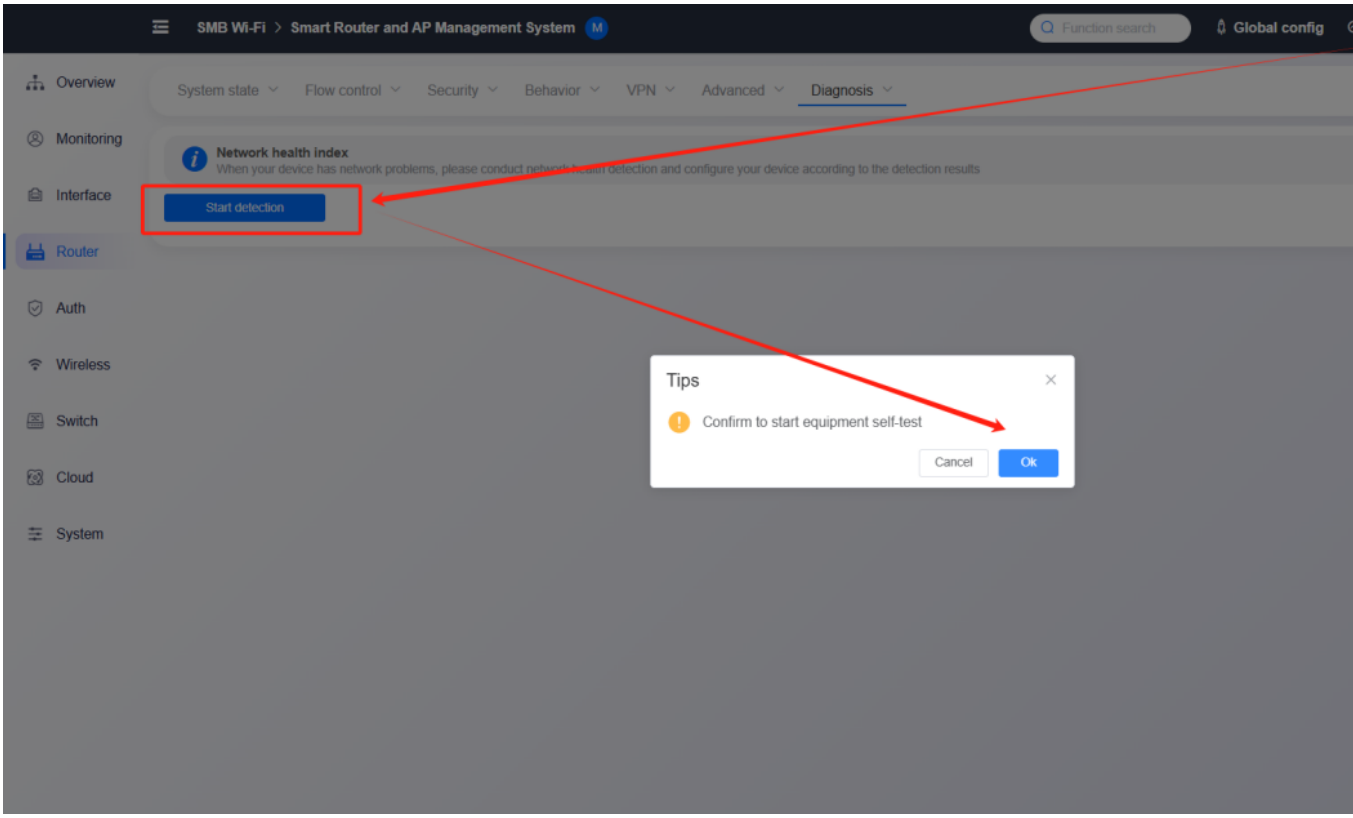
Global config: Configure the whole network information (similar to the configuration wizard, but different from the wizard). The system will automatically discover all devices in the intranet of this main device (including APs, firewalls, switches, etc. These devices need to support this system, otherwise they will not be discovered). It also supports viewing the topology. If a new device is connected to this intranet and is not displayed in the device list (including the topology), you can click "Rediscover" to update the new device online.



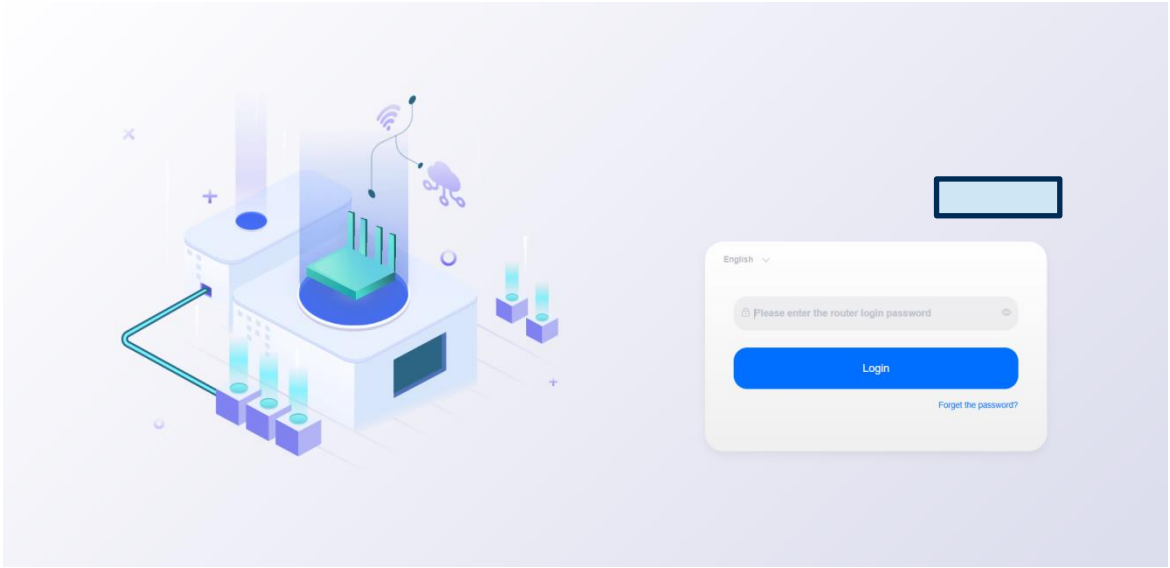
Click "Start configuration" to enter, and click "Complete configuration" after configuring as needed. Among them, the device password is the login password for all devices in the entire network. No need to enter an account when logging in to this system.



Health: Click Health to jump to the page for testing the health of the current network environment. The test conditions are set by the system defaults, and the test results will be displayed on the page. When you return to the "Overview" page, the system will automatically score according to the test results. The higher the score, the better the network health index.

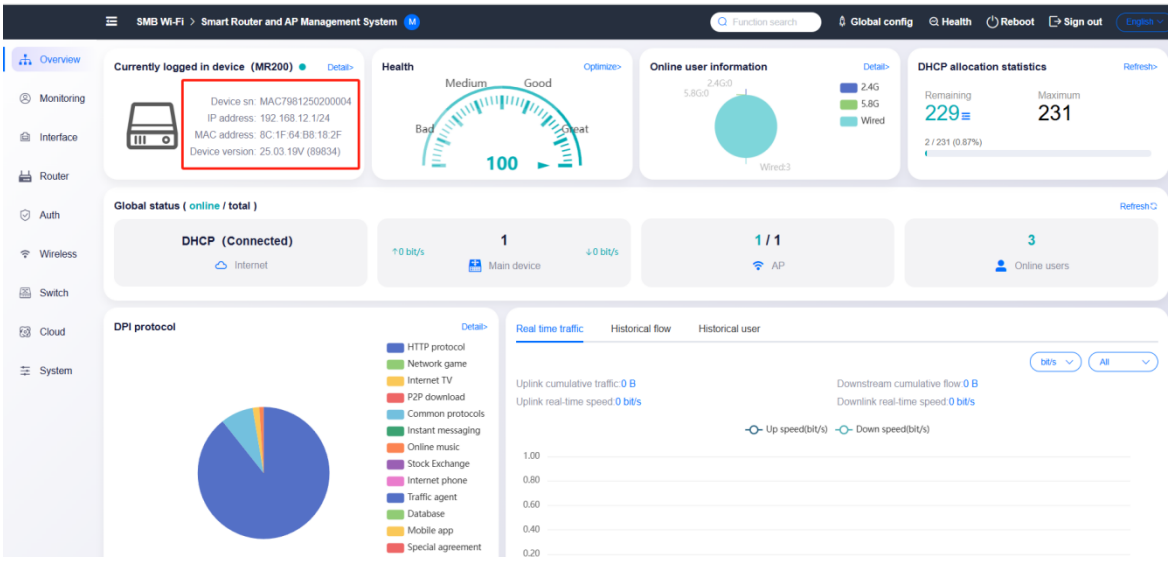


Reboot: Click to confirm restarting the device, and the device will be rebooted.
Sign out: Click it to exit the system management page and return to the login page

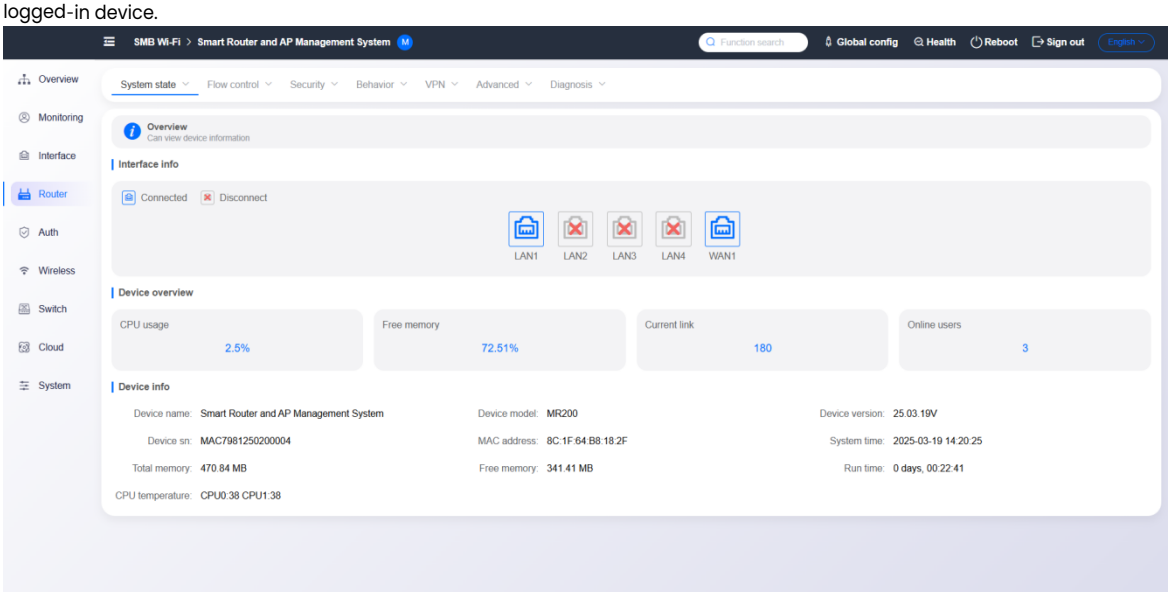


1.2 Statistics

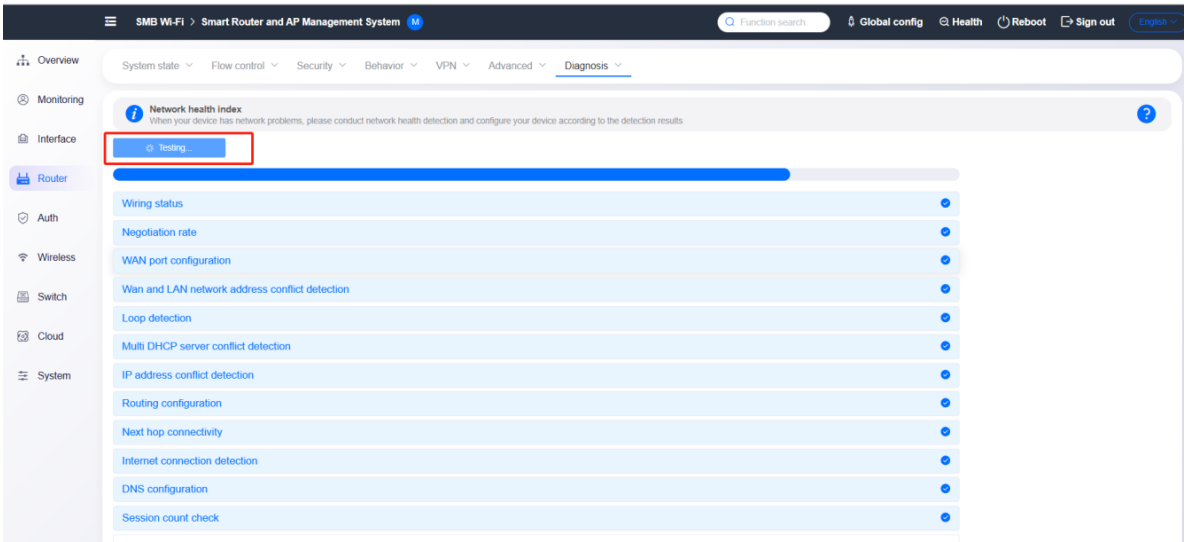
Displays the basic information of the currently logged-in device, including serial number, management IP address, MAC address and firmware version



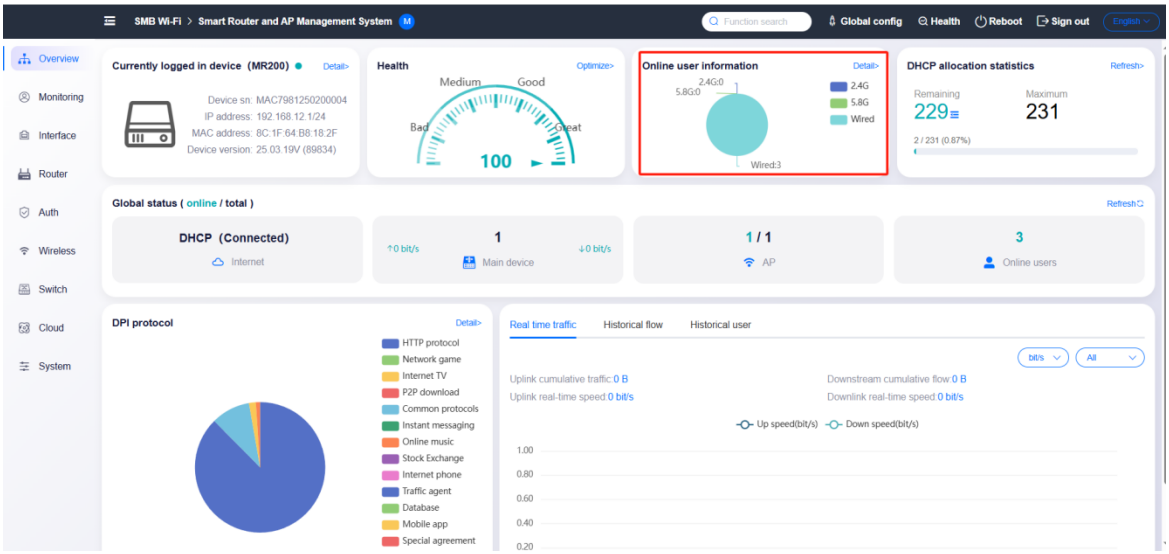
Detail: Click the "Detail" button to jump to the device system state page, which displays other information about the currently logged-in device.



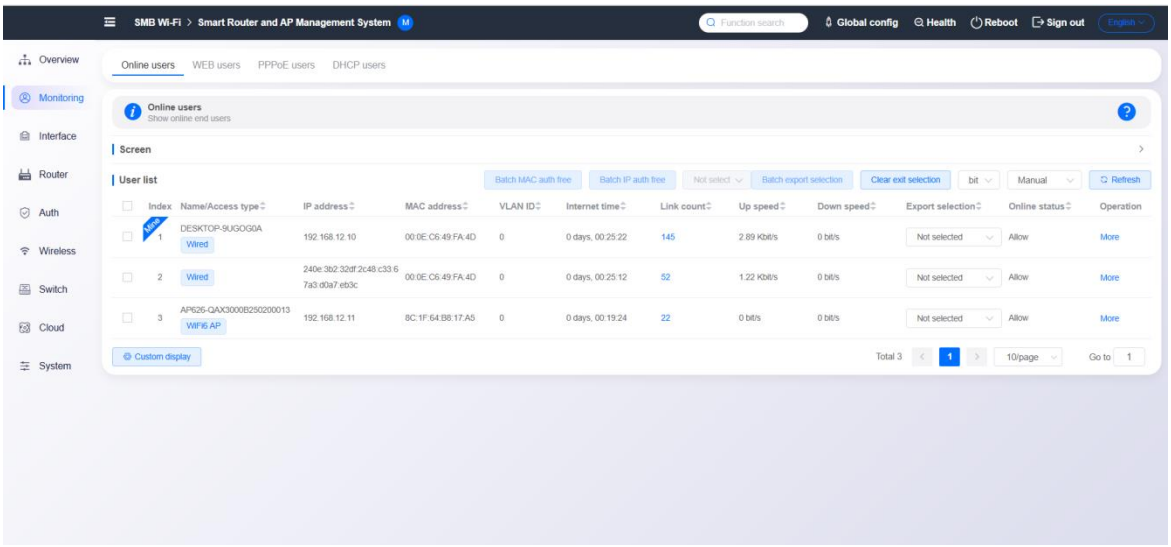
Health Index: The current device network health index. The higher the index, the healthier the device. If you click the "testing" button, the page will jump to the automatic detection page. The result provides detailed descriptions of the detection items;



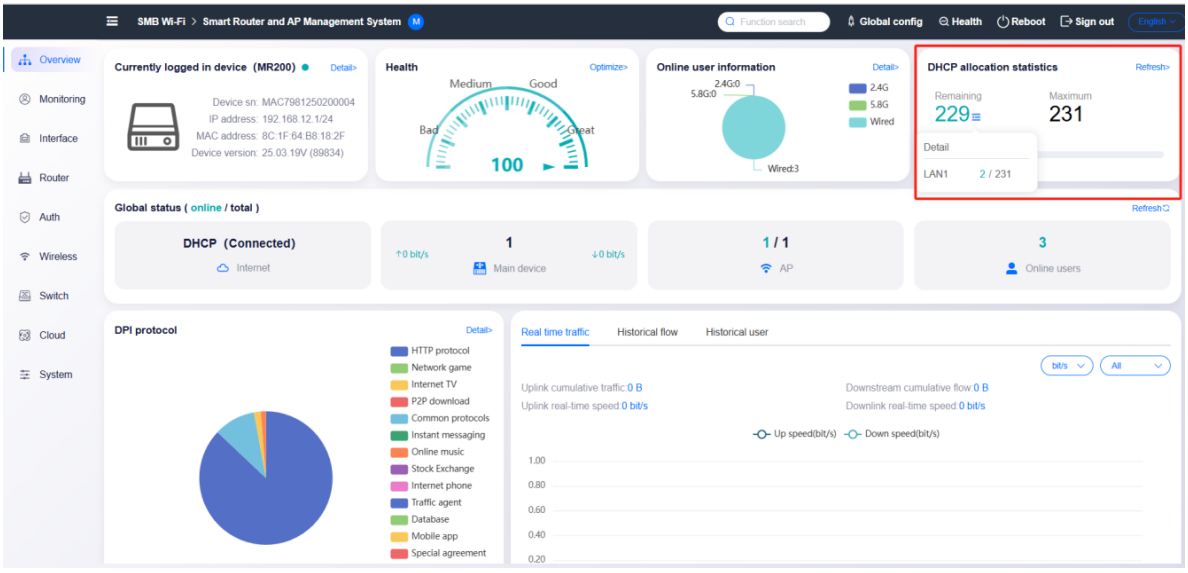
Count the number of wired users and wireless users in the current intranet, and wireless 2.4G users and 5.8G users are counted separately in the pie chart



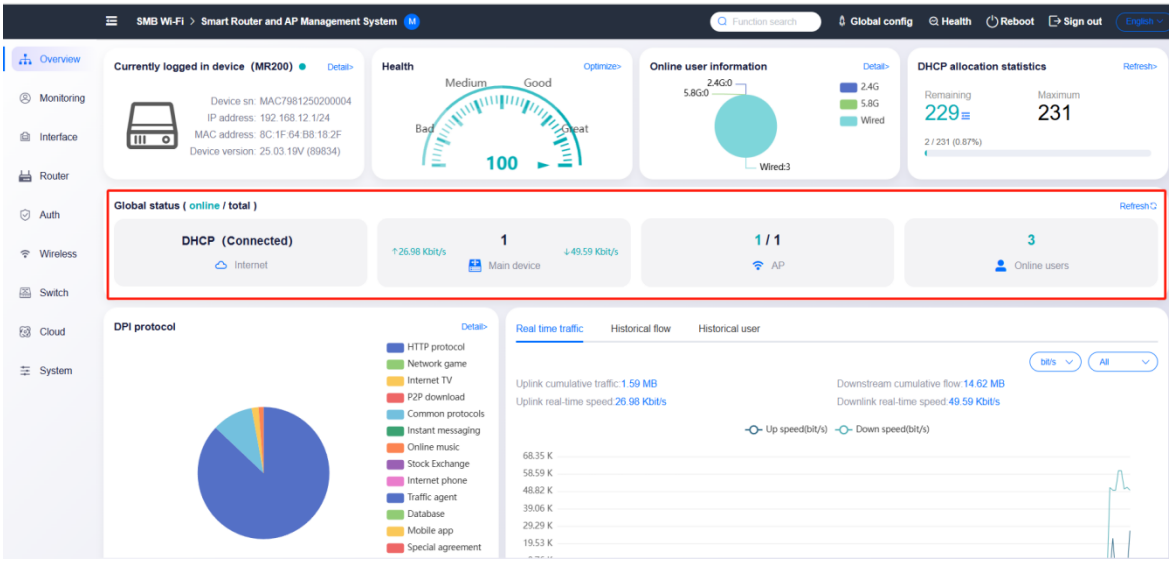
Click the "**Detail**" button to jump to the "Monitoring" , Online users will be displayed in the detailed statistics page of the online user list;



DHCP allocation statistics: Displays the current remaining and maximum number of DHCP that can be allocated . In the details, you can view the DHCP usage of different LAN ports. Click the "Refresh" button and the DHCP allocation statistics will be updated.

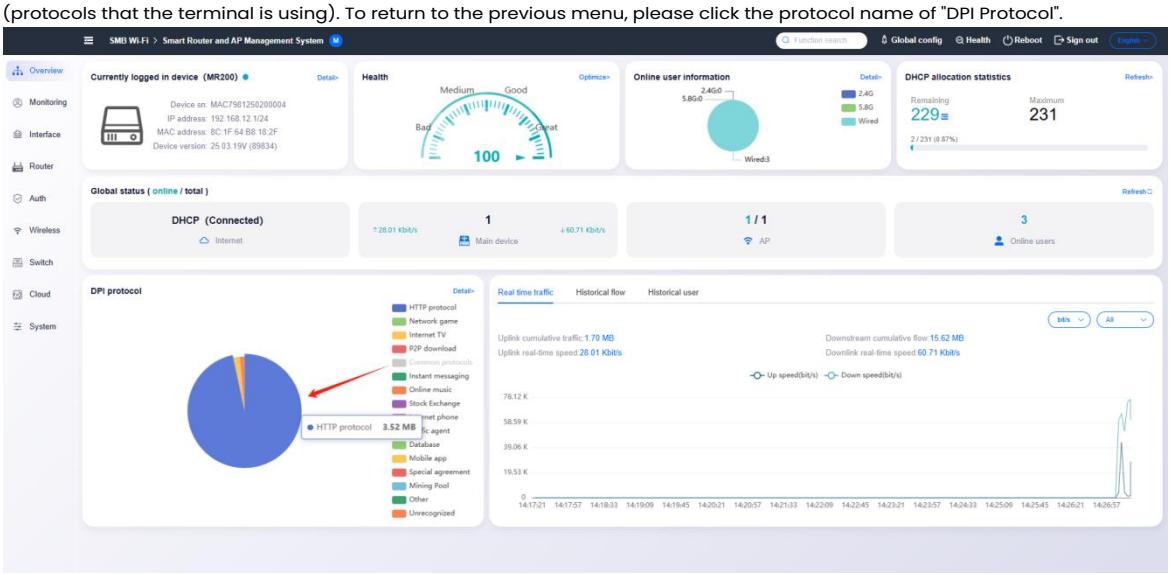


Global status (Online/total): The current device external network acquisition method and current DHCP connection status, the number of main devices and real-time external network uplink and downlink, the number of wireless AP and online users. Click the "Refresh" button to update the global network status statistics.

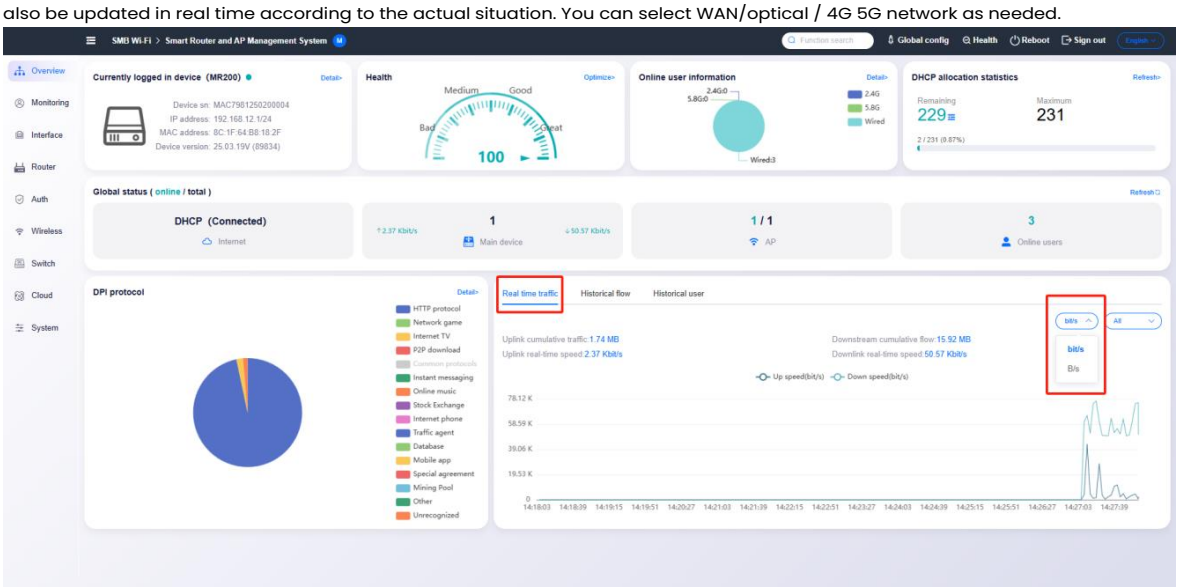

SMB Wi-Fi > Smart Router and AP Management System
Function search
Global config
Health
Reboot
Sign out
English
Overview
Monitoring
Interface
Router
Auth
Wireless
Switch
Cloud
System
Currently logged in device (MR200)
Detail>
Device sn: MAC798125020004
IP address: 192.168.12.1/24
MAC address: 8C:1F:64:B8:18:2F
Device version: 25.03.19V (89834)
Health
Optimize>
Medium
Good
Bad
Great
100
Online user information
Detail>
2.4G:0
5.8G:0
Wired:3
2.4G
5.8G
Wired
DHCP allocation statistics
Refresh>
Remaining
229
Maximum
231
2 / 231 (0.87%)
Global status (online / total)
Refresh
DHCP (Connected)
Internet
↑26.98 Kbit/s
1
Main device
↓49.59 Kbit/s
1 / 1
AP
3
Online users
DPI protocol
Detail>
HTTP protocol
Network game
Internet TV
P2P download
Common protocols
Instant messaging
Online music
Stock Exchange
Internet phone
Traffic agent
Database
Mobile app
Special agreement
Real time traffic
Historical flow
Historical user
bit/s
All
Uplink cumulative traffic:1.59 MB
Uplink real-time speed:26.98 Kbit/s
Downstream cumulative flow:14.62 MB
Downlink real-time speed:49.59 Kbit/s
Up speed(bit/s)
Down speed(bit/s)
68.35 K
58.59 K
48.82 K
39.06 K
29.29 K
19.53 K

DPI protocol: Statistic the usage percentage of DPI protocol by terminal users. DPI protocols are displayed by category and level. Different color represent different protocols. When the mouse points to the corresponding protocol, the traffic usage of the protocol will be displayed. If you click the color on the right side of the protocol, the corresponding protocol will not be displayed in the pie chart. If you need to restore the display, click the color card again.

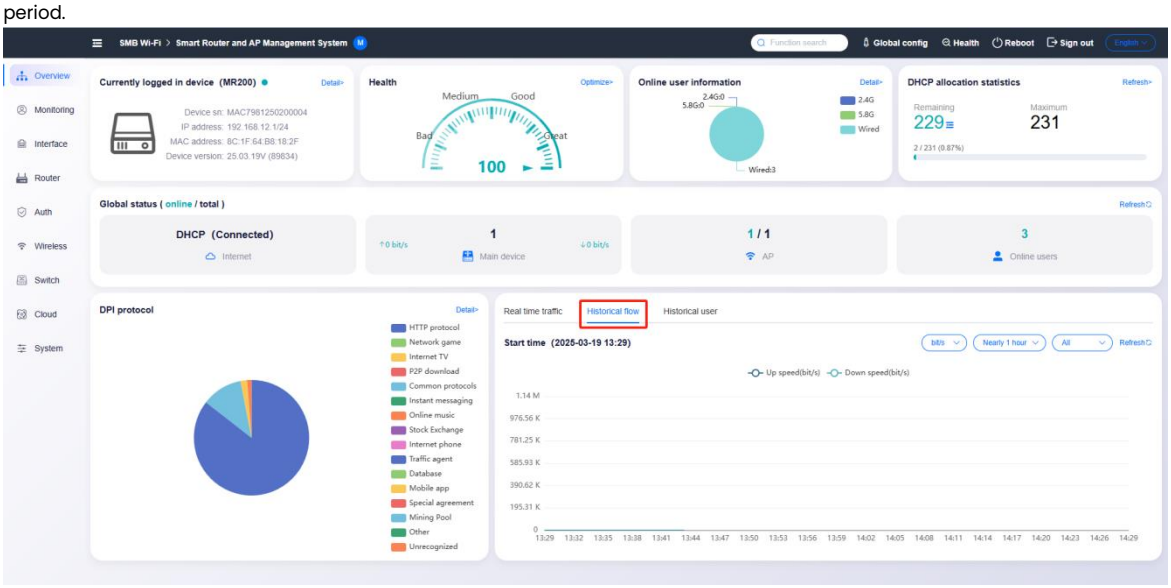
The pie chart only shows the traffic usage of the first-level menu of the protocol. Each first-level protocol also contains second-level and even third-level protocols. If you click on common protocols, it also includes https, terminal types, common office, etc. (protocols that the terminal is using). To return to the previous menu, please click the protocol name of "DPI Protocol".



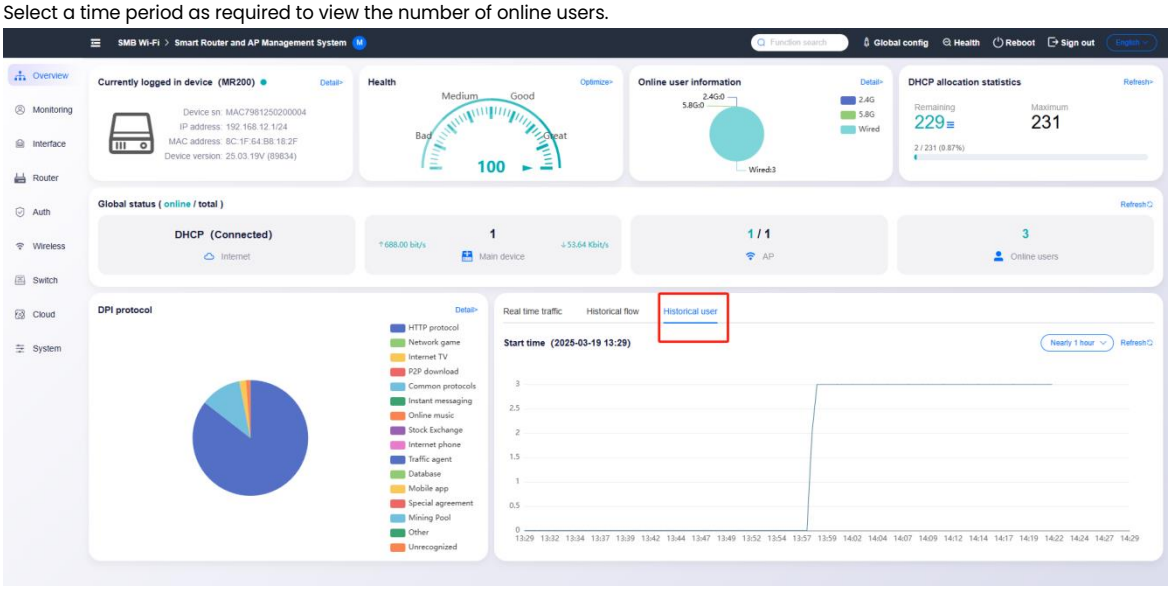
Real time traffic: This mode automatically refreshes all current external network traffic usage data, and the line chart below will also be updated in real time according to the actual situation. You can select WAN/optical / 4G 5G network as needed.



Select time period and WAN port as needed to query the traffic usage of the corresponding WAN port in the historical time period.



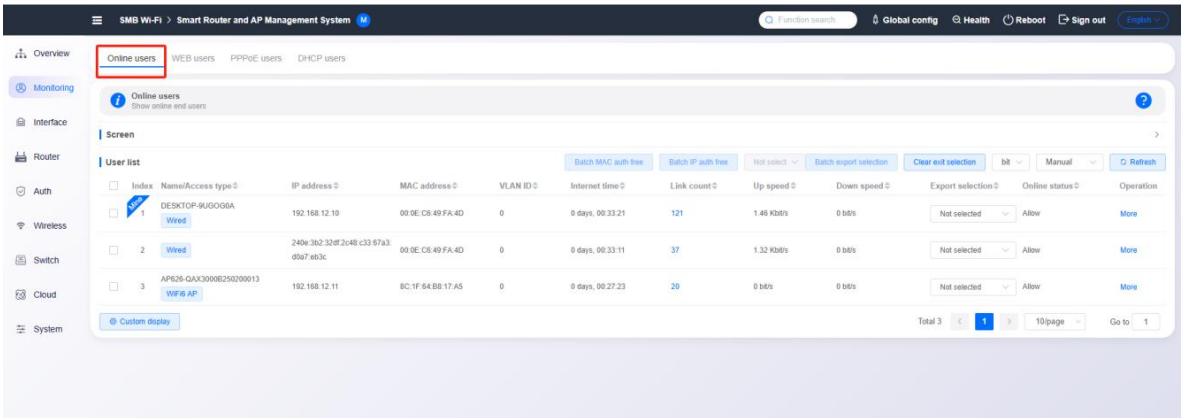
Select a time period as required to view the number of online users.



二、 Monitoring

2.1 Online users

Shows the online users status.



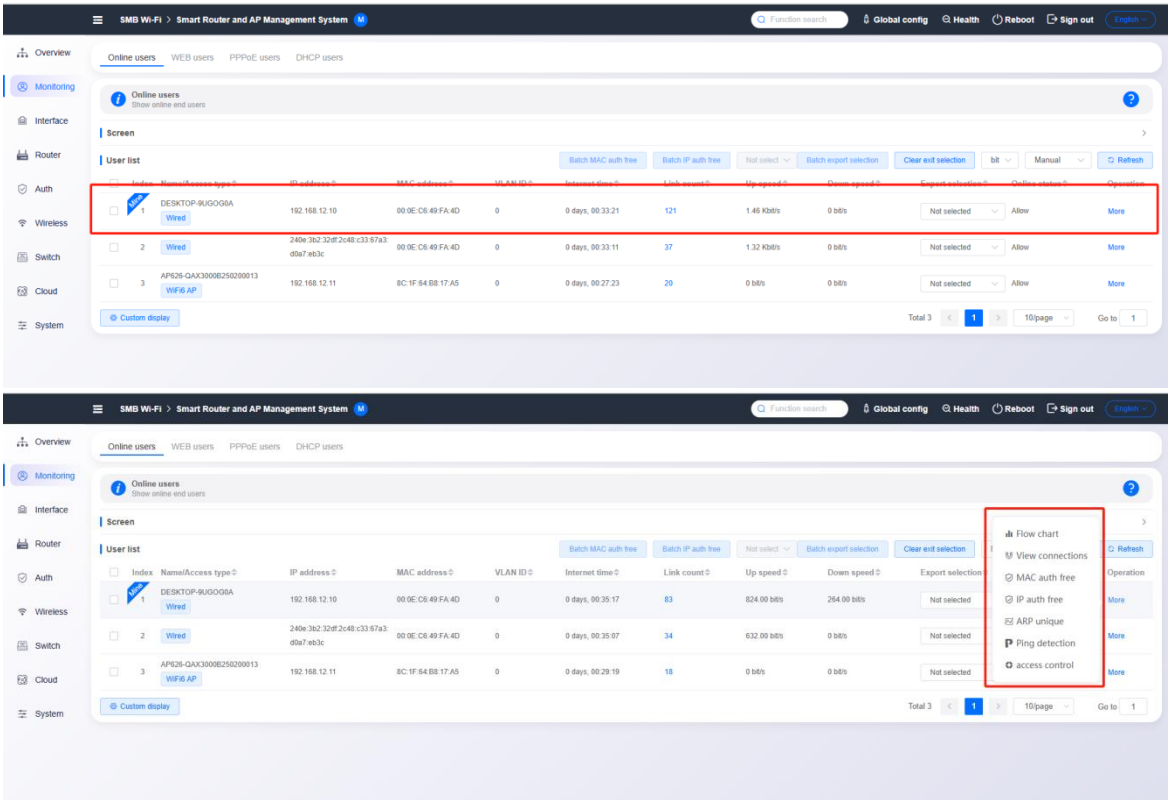
Selection

Supports conditional filtering and searching for users by name, IP address and MAC address. User information that meets the filtering conditions is displayed in the "User list".

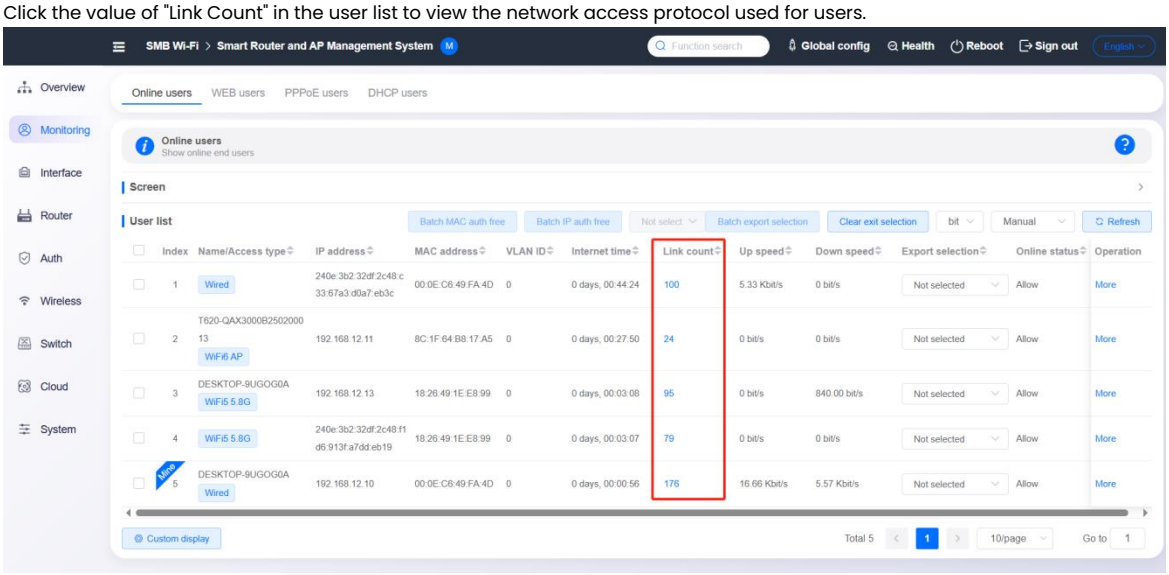
User list

Displays all online users or users who meet the filtering conditions. In the list, you can intuitively see the network conditions occupied by each terminal, basic terminal information, Internet access status, etc.

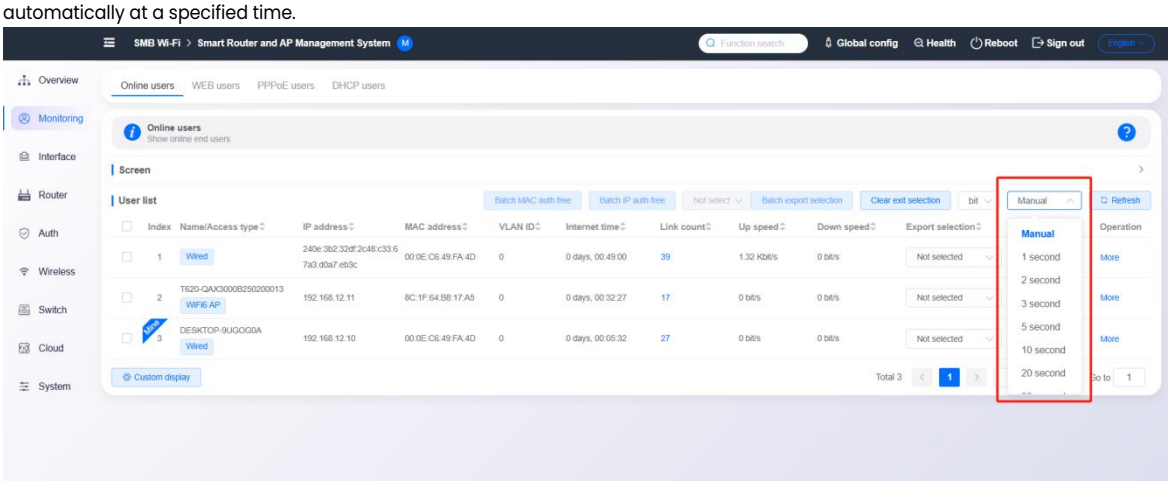
The operation bar also includes: viewing flow chart, connection, authentication-free, ARP binding (unique by default), ping detection, access control and other quick functions.



Click the value of "Link Count" in the user list to view the network access protocol used for users.

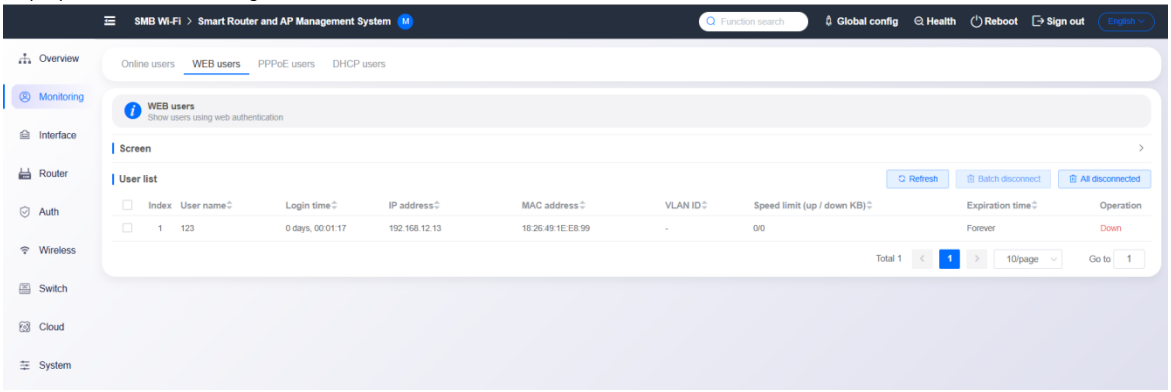


The user connection list supports returning to the host list, deleting all connections, and refreshing connections manually or automatically at a specified time.



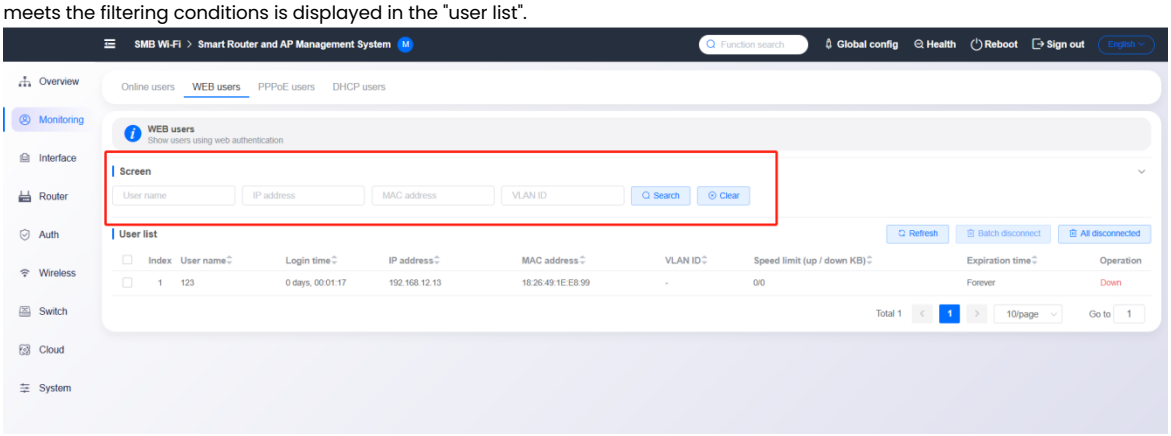
2.2 WEB users

Displays users who are using web authentication



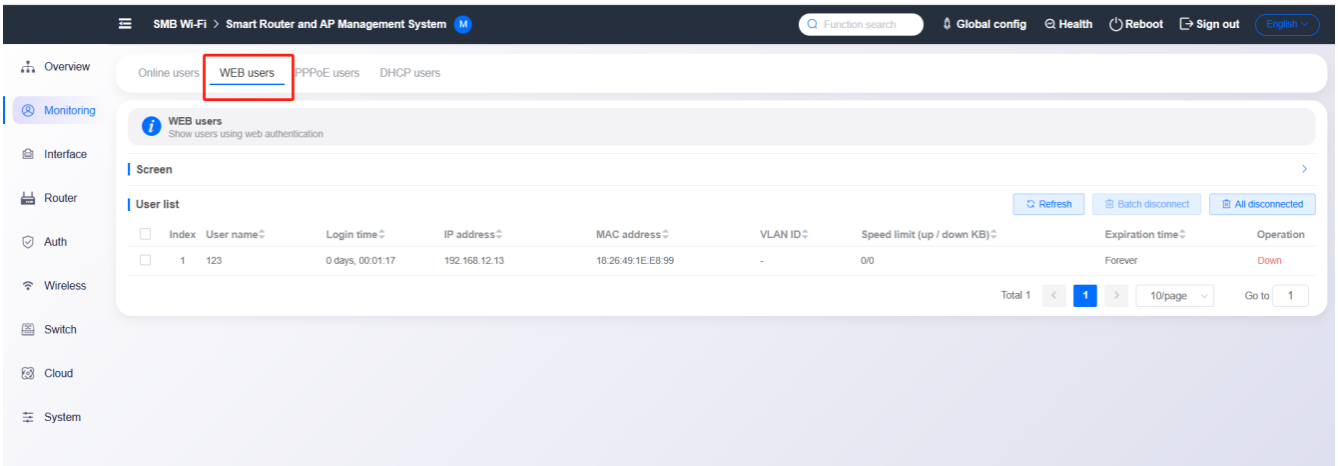
Filtering

Supports conditional filtering and searching for users by user name, IP address, MAC address and VLAN ID. User information that meets the filtering conditions is displayed in the "user list".



User list

Display all users who have successfully passed the WEB authentication or users who meet the screening conditions. You can intuitively see the network occupied by each terminal, basic information of the terminal, Internet access status, etc. The operation item supports disconnecting the terminal. If you click "Batch Disconnect", "All Disconnected" for the billing user or "Disconnect" for the terminal in the list, the authenticated terminal will exit the authentication.

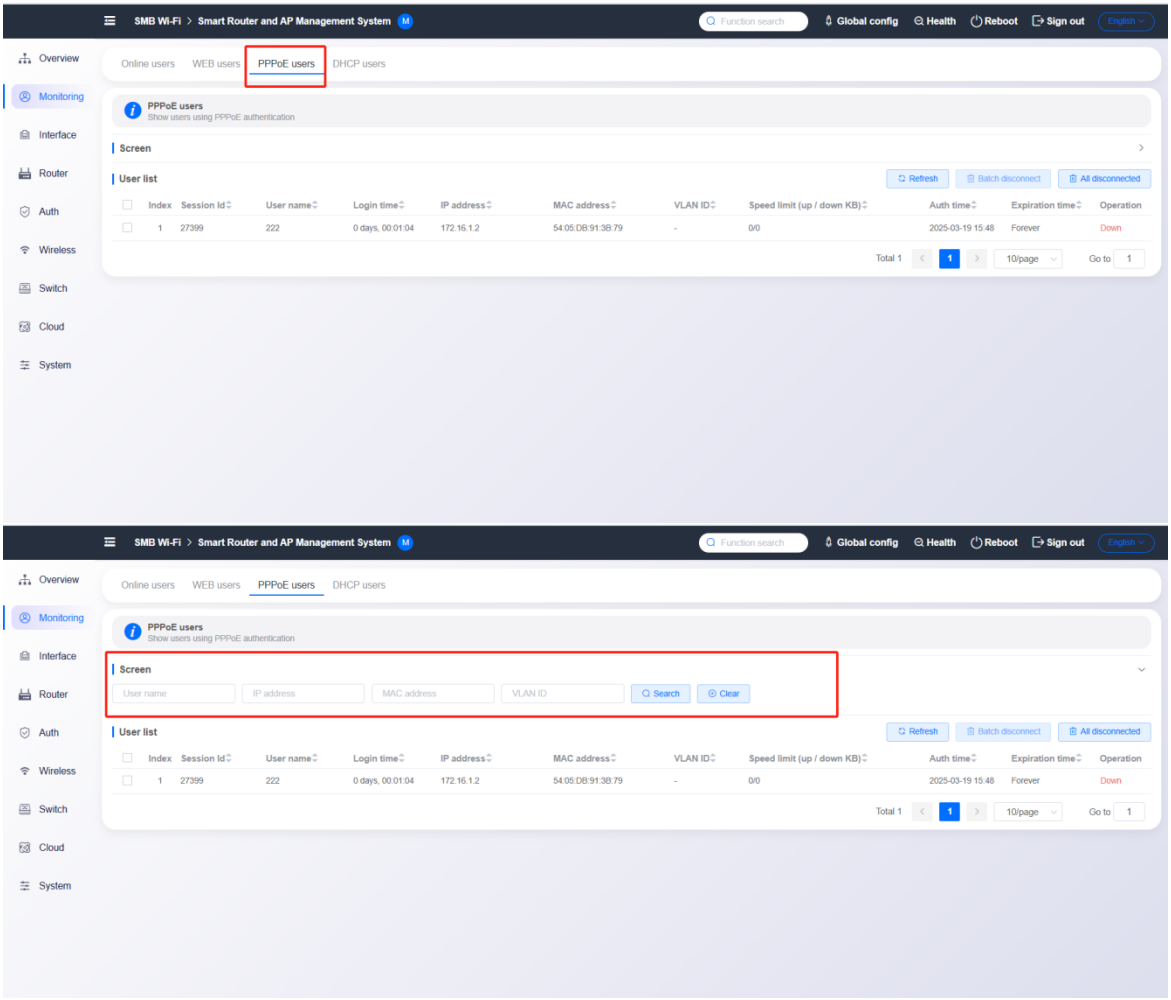


2.3 PPPoE users

Displays users are using PPPoE authentication.

Filtering

Supports conditional filtering and searching for users by user name, IP address, MAC address and VLAN ID. User that meets the filtering conditions is displayed in the "User list".

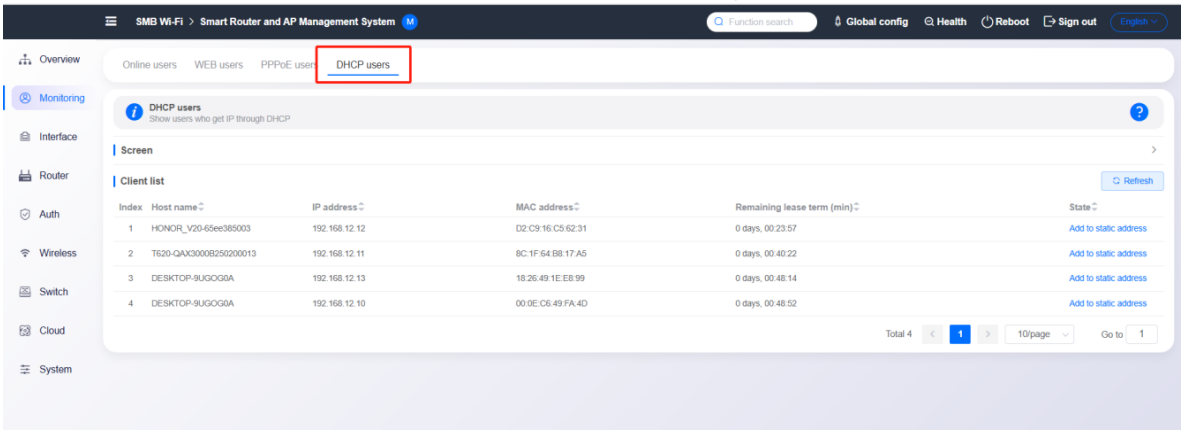


User list

Shows all users who have successfully connected via PPPOE dial-up or users who meet the screening condition. You can intuitively see the network occupied by each terminal, basic terminal information, Internet access status, etc. The operation item supports disconnecting the terminal. WEB authentication users include users who have passed billing authentication. If you click " All Disconnected" for a billing user or "Disconnect" for a terminal in the list, the authentication terminal will exit authentication.

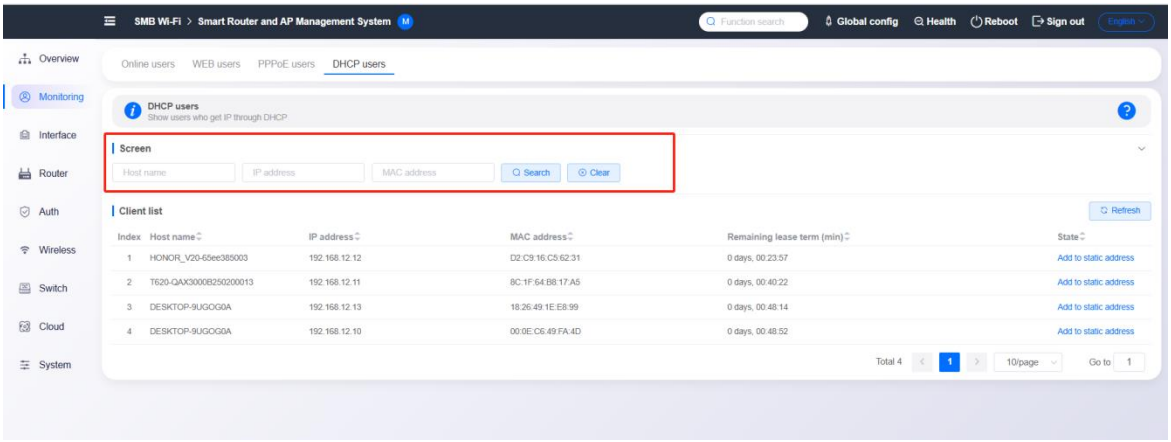
2.4 DHCP users

Displays information about all users who automatically obtain IP addresses through DHCP.



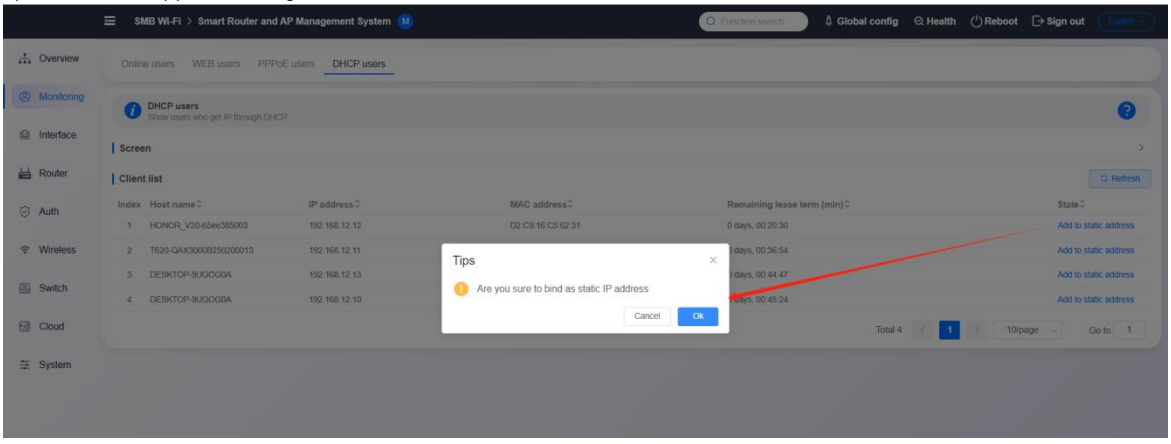
Filtering

Supports conditional filtering and searching for users by host name, IP address, and MAC address. User information that meets the filtering conditions is displayed in the "Client list".

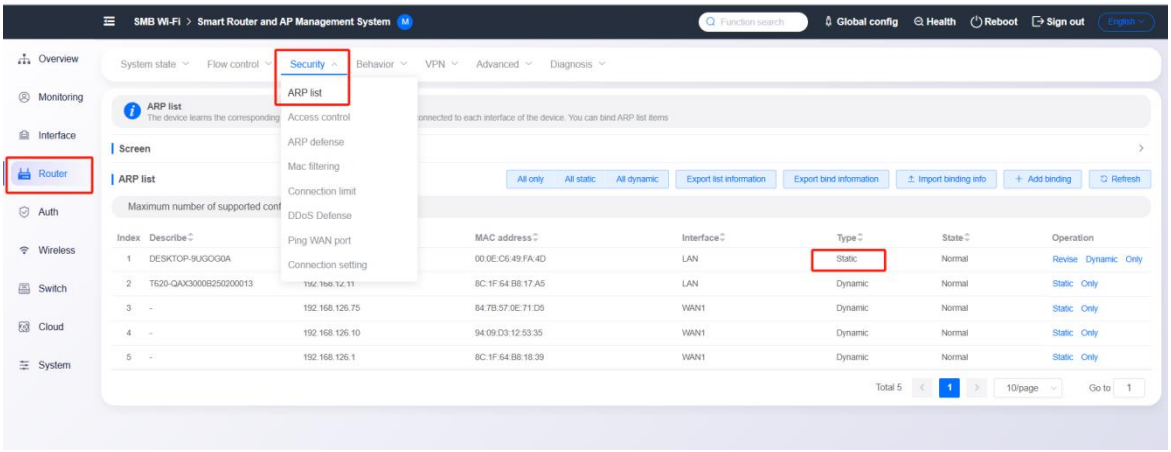


Client list

Displays all users who have successfully connected via DHCP or user information that meets the screening condition. The operation item supports binding DHCP users to "add to static address".



The results can be viewed in “ARP list”.



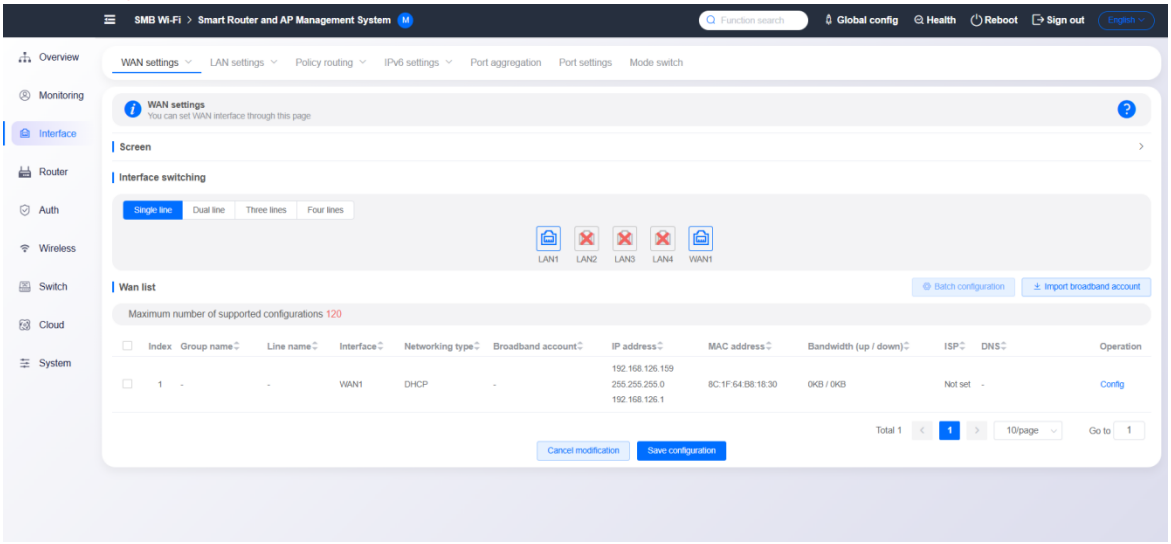
三、 Interface

3.1 WAN settings

Set the WAN port parameters, select the network line type of the device, etc. Please be sure to configure the WAN port according to your needs, otherwise it will affect the normal use of the network.

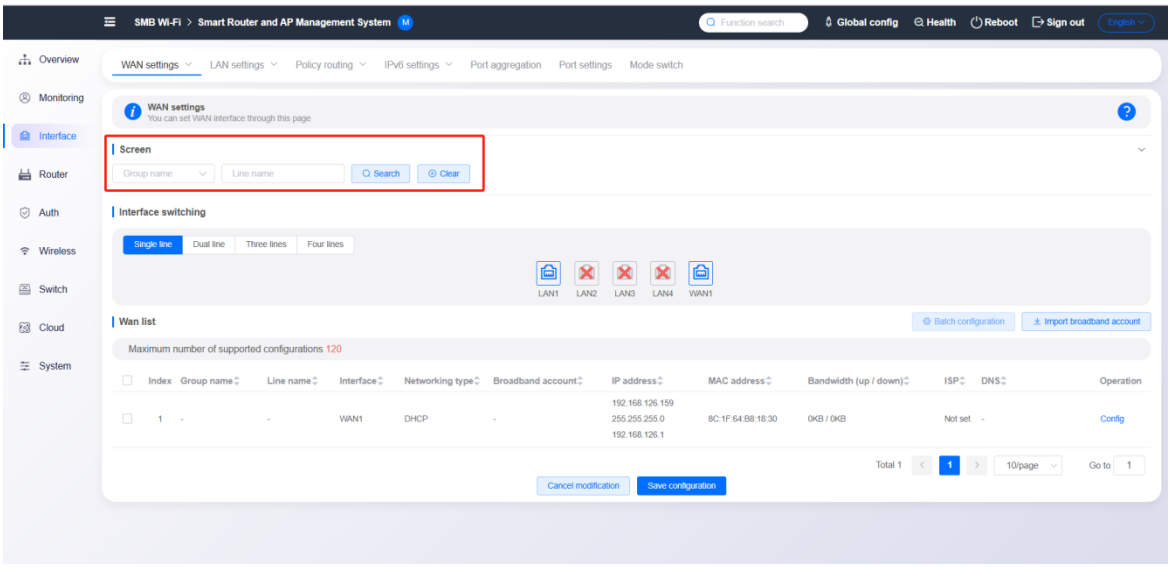
3.1.1 WAN settings

在本菜单中可以根据需要选择设备 WAN 口条数，此处的 WAN 口线路数是根据设备硬件显示的，如果需要设置更多的 WAN 口数请移至“WAN extend”菜单查看配置方法。配置 WAN 口数量的最大条数受授权 WAN 口数量影响，因此如果需要配置较多 WAN 口数，请先获取扩 WAN 授权。In this menu, can select the number of WAN ports of the device as needed. The number of WAN ports here is displayed according to the device hardware. If WAN ports will be configured, please move to the "WAN extend" menu to view the configuration method. The maximum number of WAN ports is affected by the number of authorized WAN ports. Therefore, if want to configure more WAN ports, please obtain WAN extension authorization first.



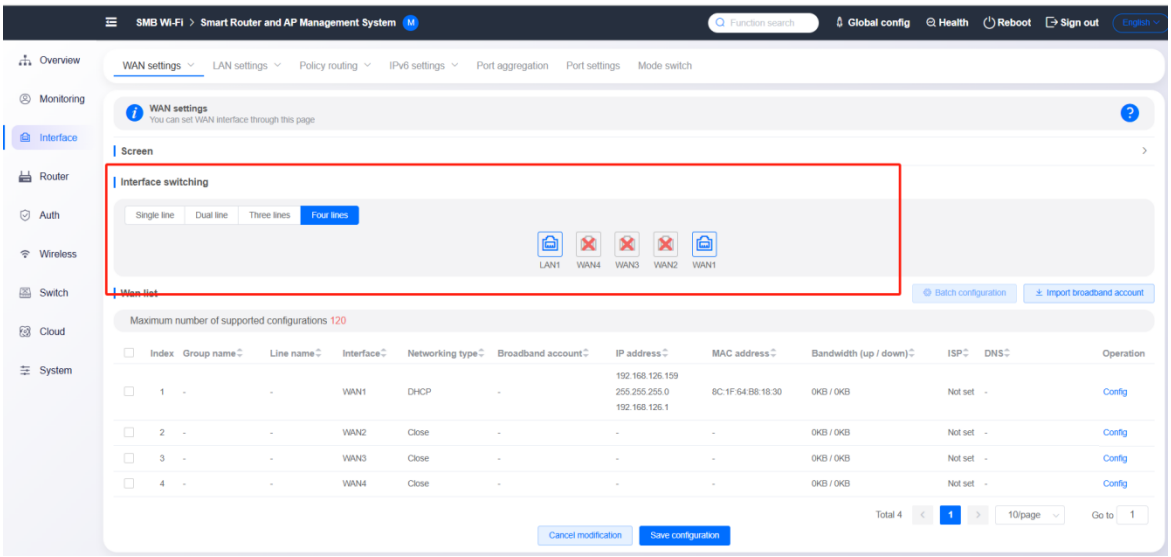
Screen

Filter the WAN port information that meets the conditions by group name or line name. The WAN port information that meets the filtering conditions will be displayed in the "WAN list";



Interface switching

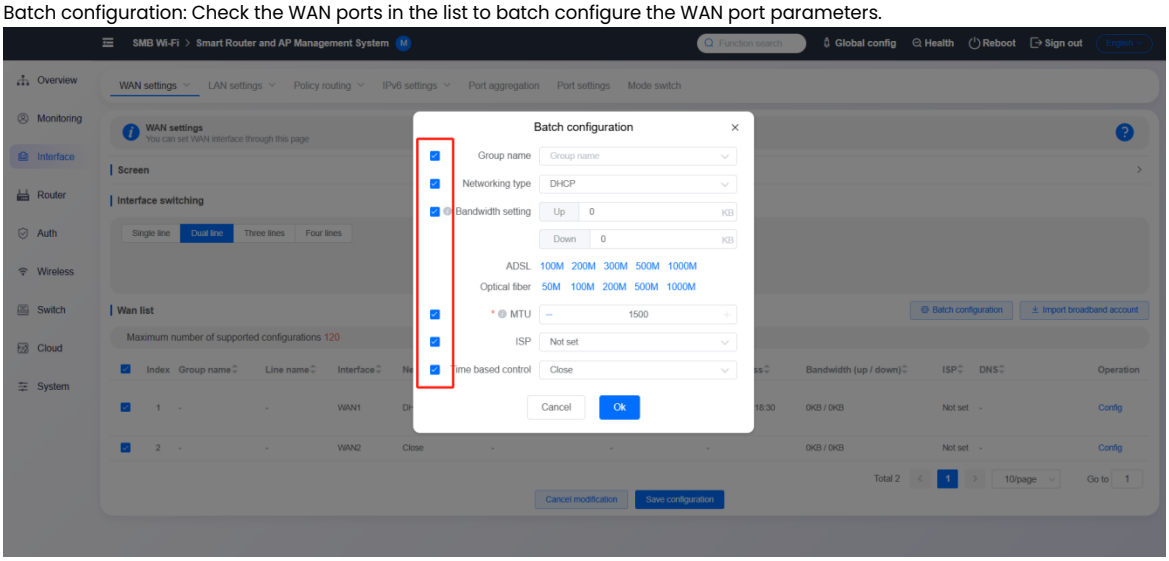
Set the interface as the WAN/LAN port type. You can convert unused WAN ports into LAN ports. The maximum number of WANs allowed to be set does not exceed the default number of WANs.



Example

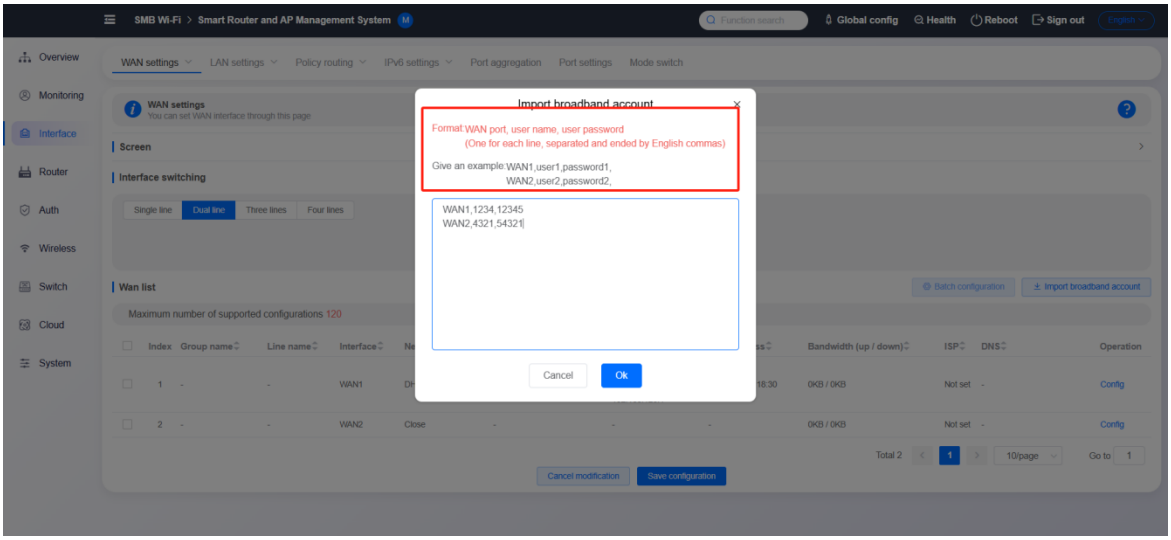
As shown in the figure above, the device used in this example is MR200, which has 5 RJ45 ports, WAN1 is a WAN port by default, and the remaining 4 are LAN ports. If 2 WAN ports are required, click here to select "Dual line" configuration and submit. The 2 rightmost RJ45 ports on the device hardware are WAN ports, and the remaining 3 ports are LAN ports.

Batch configuration: Check the WAN ports in the list to batch configure the WAN port parameters.

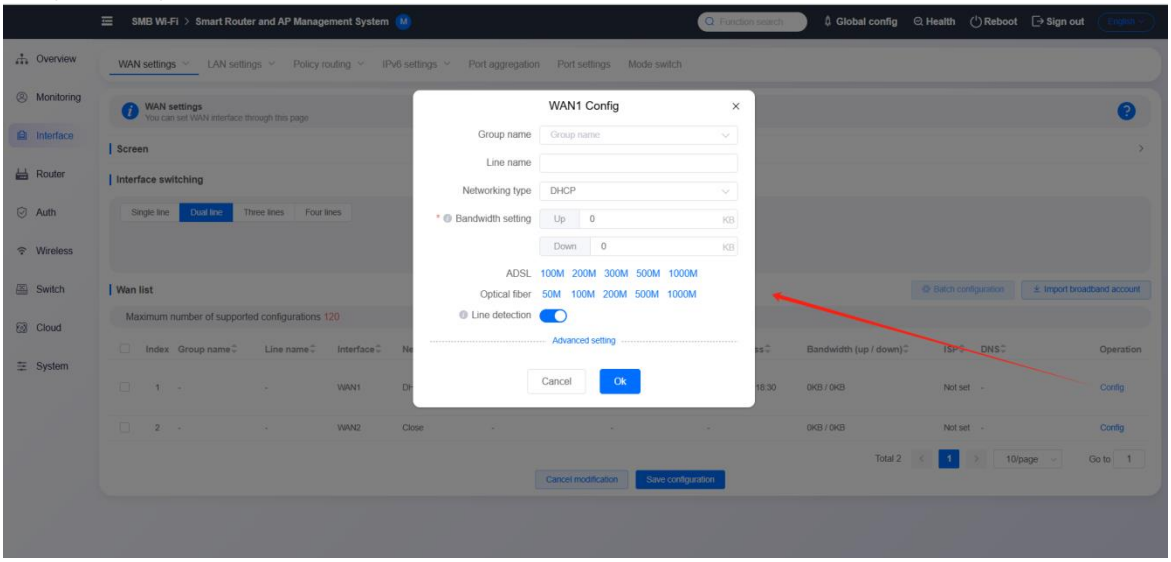


Import broadband account: When one or some WAN ports are connected to the Internet using PPPoE dial-up, you can use (batch) import bandwidth account to quickly add account and passwords. As shown in the following figure: (Commas are used in English

WAN1,1111,1111,
WAN2,2222,2222,
WAN3,3333,3333,
.....
After filling in, click "OK" and "Save Configuration".



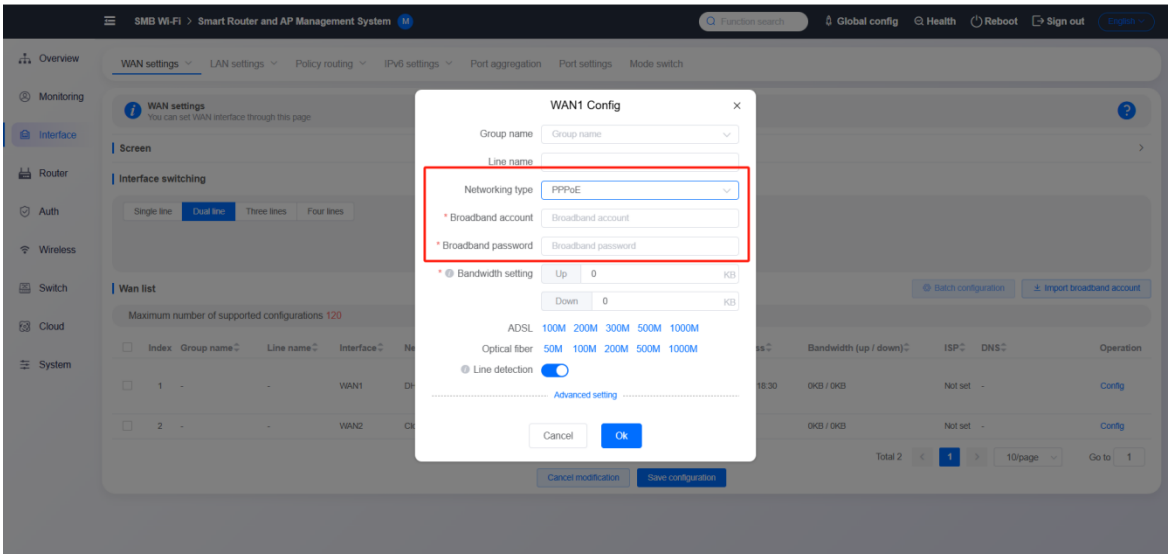
Config: can configure a WAN port separately.



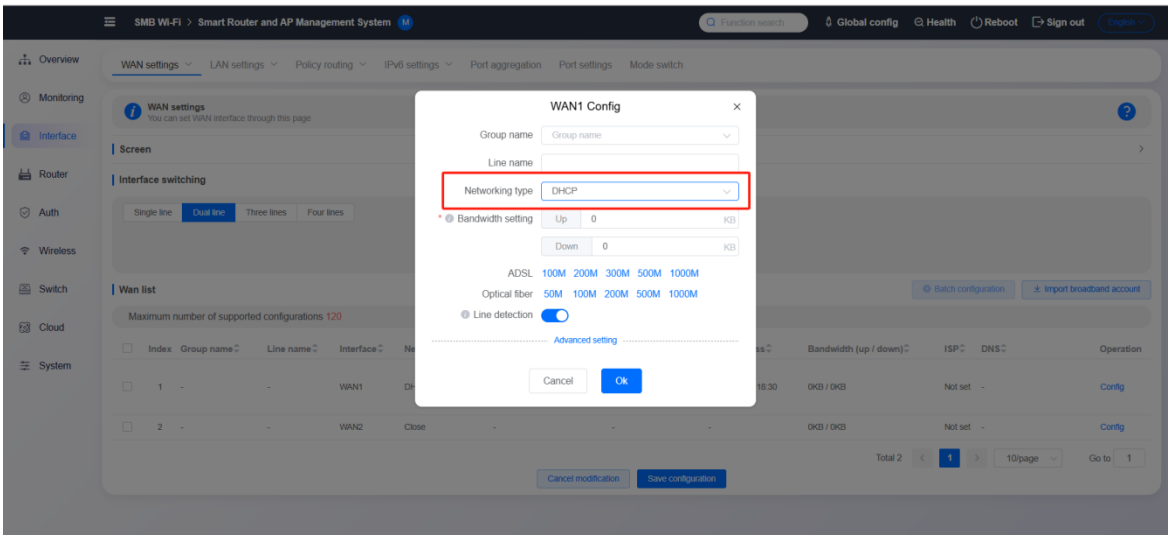
Network type: Determined by the upper-layer device. If the external network connection type is not clear, please connect the external network directly to the computer to see whether the computer can automatically obtain Internet access, or needs to dial up to the Internet, or needs to configure a static IP to access the Internet, to determine the external network type.

1. Disable: Indicates that the connection status of the port is disabled. The WAN portcannot connect to the Internet in the disable state

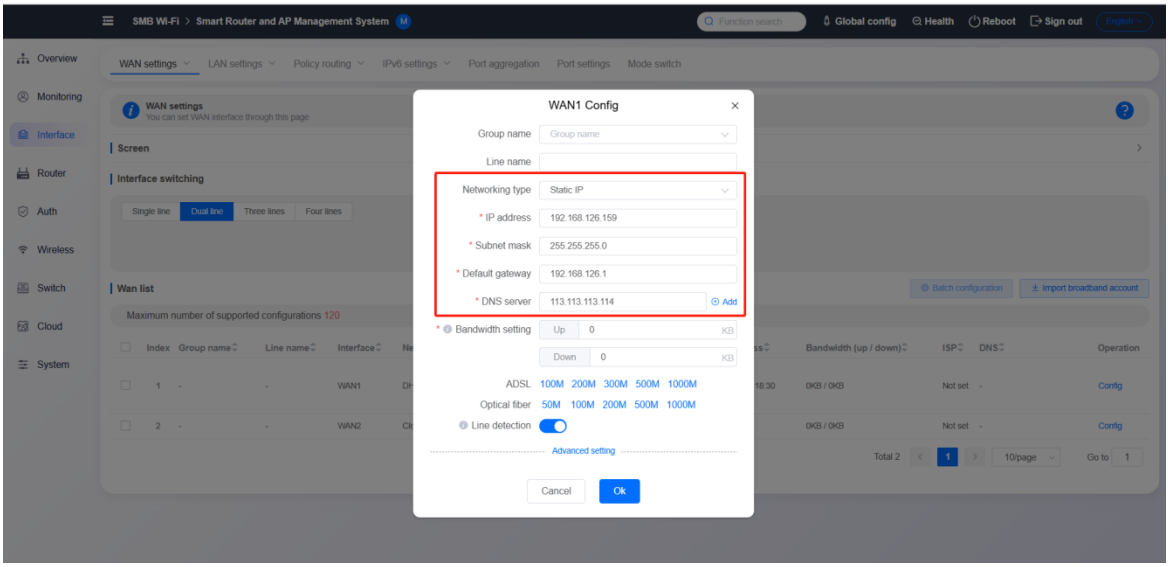
2. PPPoE: Indicates that the network type is using dial-up mode.Should fill in the operator or available bandwidth account and password, save and submit to connect. The broadband setting is generally set to 0 by default, indicating that the external network traffic is not restricted;



3．DHCP: The WAN port automatically obtains the external IP address to connect to the Internet. The IP address automatically assigned by the upper-layer device is used as the network IP of this device. When the upper-layer device is restarted or the IP segment is re-divided, this device will automatically obtain a new IP address.



4．Static IP: The WAN port uses a static IP address. Regardless of whether the network segment of the upper device changes or is restarted, the WAN port of this device uses the configured static IP and will not change automatically. Among them, IP address, subnet mask, gateway address, and DNS server are required items. If you don’ t know the DNS server address, you can fill in the gateway address. If there are multiple DNS server addresses, click "+" to add them. Regarding bandwidth setting, the upstream and downstream bandwidth values are 0 in default, mean no limitation; If you are not sure about the conversion of the bandwidth value, you can use the reference value below to automatically fill in. If the bandwidth is not within the reference value range, please manually set the export bandwidth value;



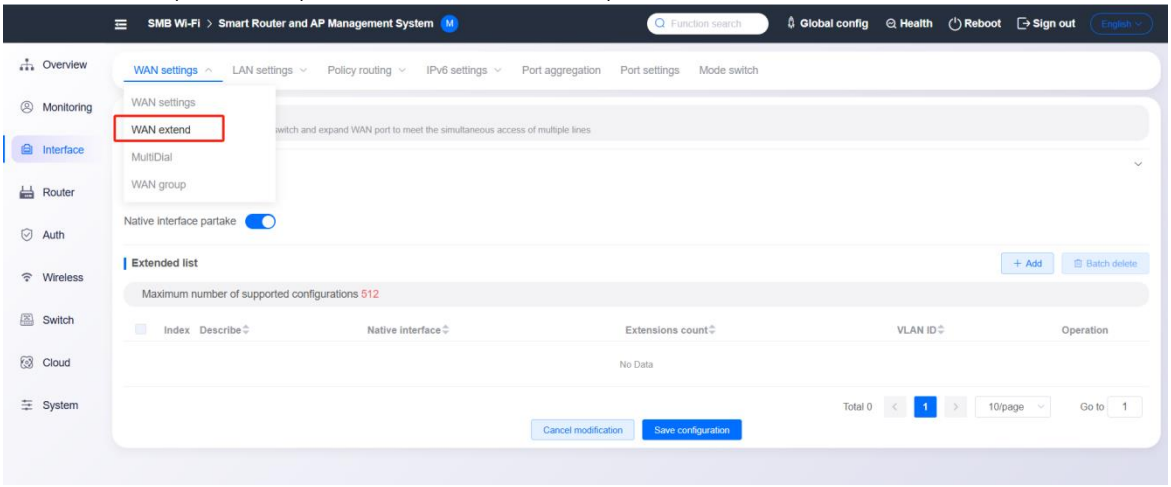
5．LAN: Port mirroring is only used. For detailed operations, please refer to the "Port Mirroring" function description;

6．Transparent bridging: Add a routing device to the network as a management device without changing the existing network environment.

Bandwidth setting: A reference value for setting the WAN export bandwidth. Can set it by referring to the values in the list. After selecting any reference value, the bandwidth setting value will be automatically filled in.
Line detection: used to enable the router to detect in real time whether the line network status is normal.
Advanced settings: Advanced parameter settings for external network configuration.
Working mode: Generally, the default gateway mode is used, and the interface performs NAT address translation; some special environments may use the routing mode (such as all intranet machines use public IP)
MTU: The maximum transmission unit of the data packet; The default parameters of DHCP and static IP range is 576-1500 ; PPPoE range is 576-1492;
DNS server: DHCP does not need to be set and will automatically obtain the upper layer. It must be filled in for static IP mode
MAC address: Random or cloned MAC address according to network conditions. Generally, the default MAC address does not need to be adjusted;
DNS resolution priority: For multiple WAN ports, the value of this value determines the export priority of DNS resolution.
ISP: The operator of the WAN line, such as Netcom or Telecom. If "Not set" is selected, the line needs to be used in conjunction with the policy routing function. In a single WAN port access environment, no need to set the operator;
Balanced: whether to participate in load balancing. If enabled, it will participate in the load according to the load balancing mode; if disabled, it will not participate in the default load.
Time base control: configure the corresponding WAN port to have interval redial, timed redial, timed disconnection and close options;
Abnormal IP detection: Check for abnormal IP headers, such as '10,172,192.168'. After detecting abnormal IP, the current line will be redialed.

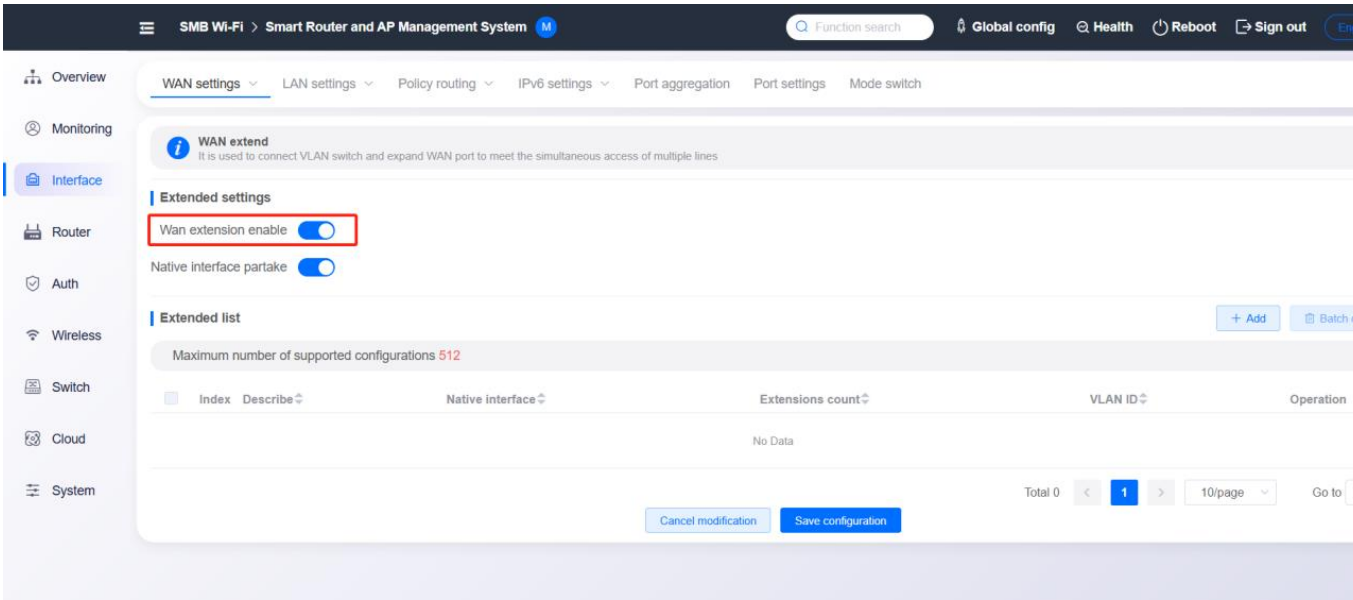
3.1.2 WAN extend

To use the WAN expansion function, you need to determine the number of WAN ports supported by the current authorization. The effect of the expanded WAN port here is the same as the WAN port on the hardware.



3.1.2.1 Extended settings

It is used to connect VLAN switches, expand WAN ports to meet the simultaneous access of multiple lines



Extended settings

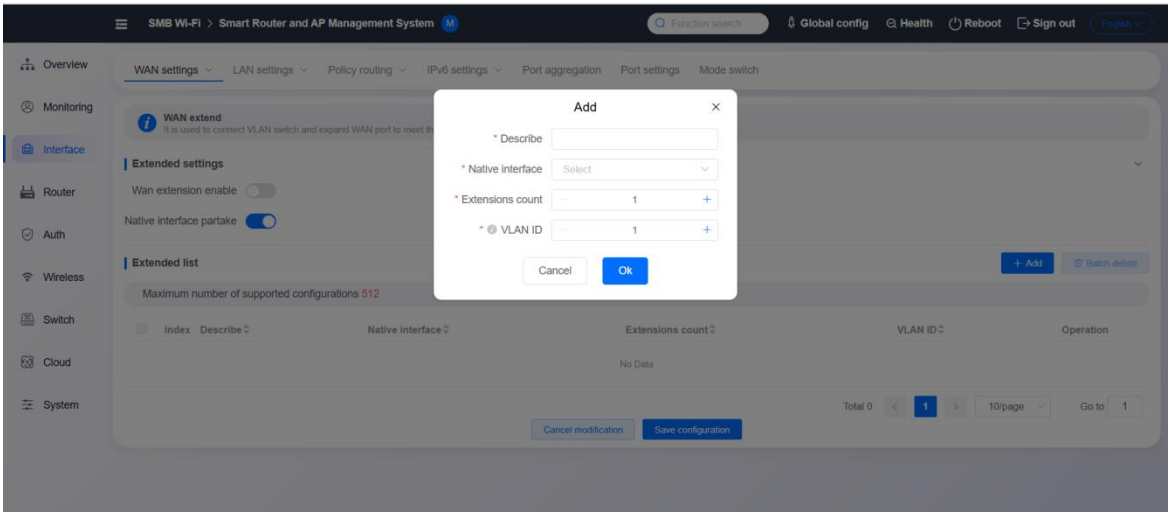
Please enable WAN extension firstly if you need to expand WAN; When the switch is turned off, the WAN extension function is disabled. If WAN extension rules have been configured, the rules will become invalid when the function is disabled;
Native interface partake: Whether to enable the native interface to participate in the extension. The native interface here refers to the physical native port on the hardware device. This function can be enabled when the upper-layer device has a VLAN or the network at this layer needs to be isolated. After enabling the native interface to participate in the extension, the WAN port will be labeled with a tag and cannot be used as a regular WAN port. The network cable of this WAN port can be connected to the trunk port (public port) of the switch.

WAN list

Display the corresponding interface information such as the native interface, extended interface, and VLAN ID after the WAN extension is successful

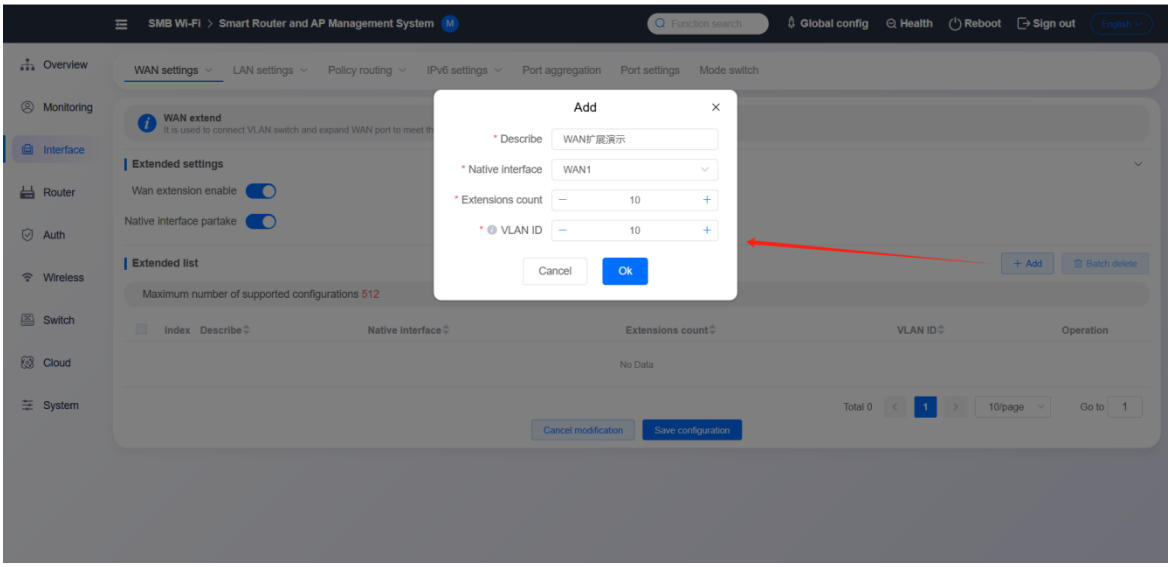
Add

Description: Customize the description content to distinguish it from other rules
Native interface: which WAN port is used for expansion. If it is connected to WAN 1, select WAN1 here; if it is connected to WAN 4, select WAN4 here (this port is used to connect to the uplink port on the switch)
Extension count: the number of WAN ports that need to be extended. The extended WAN ports are on the switch ports under this router. In other words, fill in the number of WAN ports that need to be extended on the switch (the sum of this extension number plus the actual WAN number of the device should be less than or equal to the number of interfaces allowed by the authorization). Generally, a 24-port switch can theoretically extend up to 22 WAN ports (one port is used as a uplink port, and the other port is used to make up for the extended WAN port). The correct way to fill in the extension quantity here should be: the maximum number allowed by the authorization minus the actual number of WANs (for example: a 24WAN authorization minus the number of authorizations occupied by 4 default physical ports, then fill in the maximum here 20, if the default interface has a 4/5G interface, the number of WANs that can be extended must be -1);
The VLan ID here comes from the VLan ID corresponding to the WAN set on the switch, ranging from 1-4080. Configure the VLAN ID of the switch before WAN expansion.
After making the above changes and submitting the configuration, the device will automatically restart, and the function will take effect after the restart.

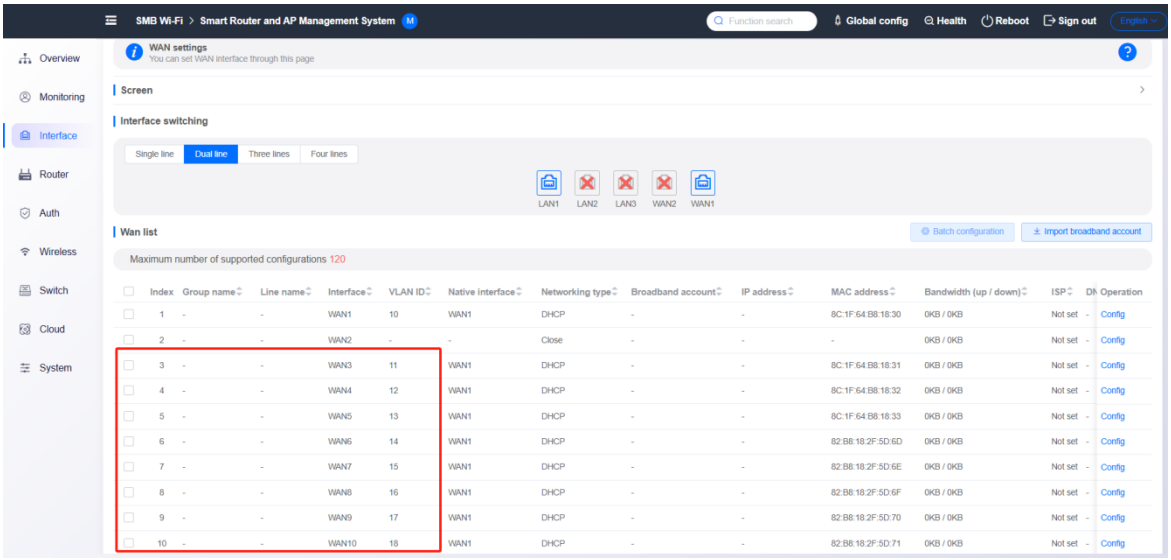


3.1.2.2 Extension Example

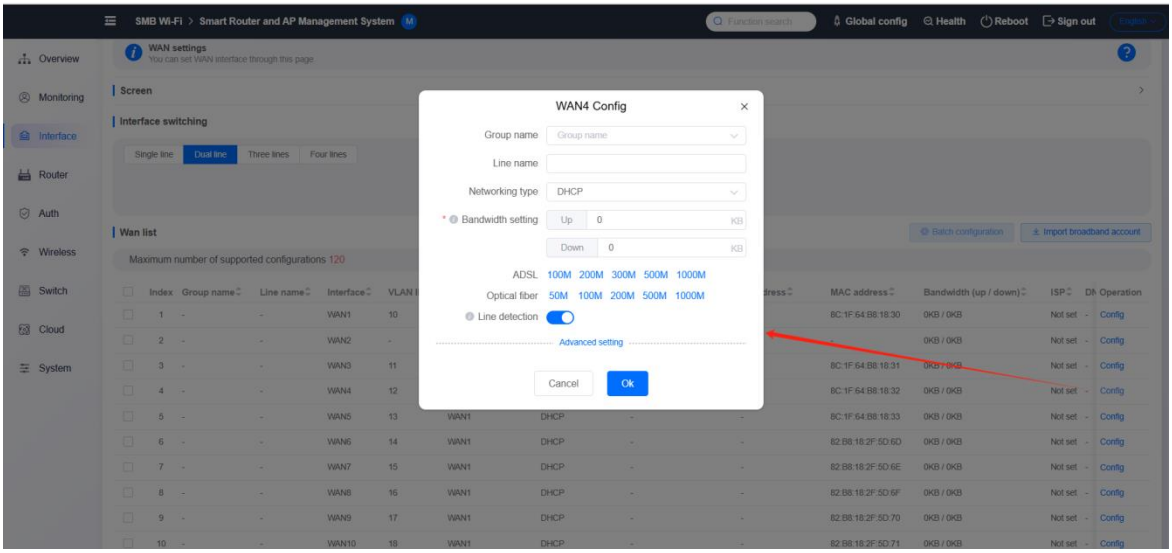
Assume that we have configured independent VLAN IDs for the switch ports,
Switch port 1 is VLAN ID 10 Access port;
Switch port 2 is VLAN ID 11 Access port;
Switch port 3 is VLAN ID 12 Access port;
...
Switch port 10 is VLAN ID 19 Access port
The following figure shows the configuration of the router using WAN2 port as the native interface and expanding 10 WAN ports:



And turn on WAN extension to enable, save the configuration and the network will automatically restart. After the normal restart, after the extension is successful, all WAN port information will be displayed in "Interface" - "WAN Settings". The effect is as follows:



Configure WAN parameters in Config.

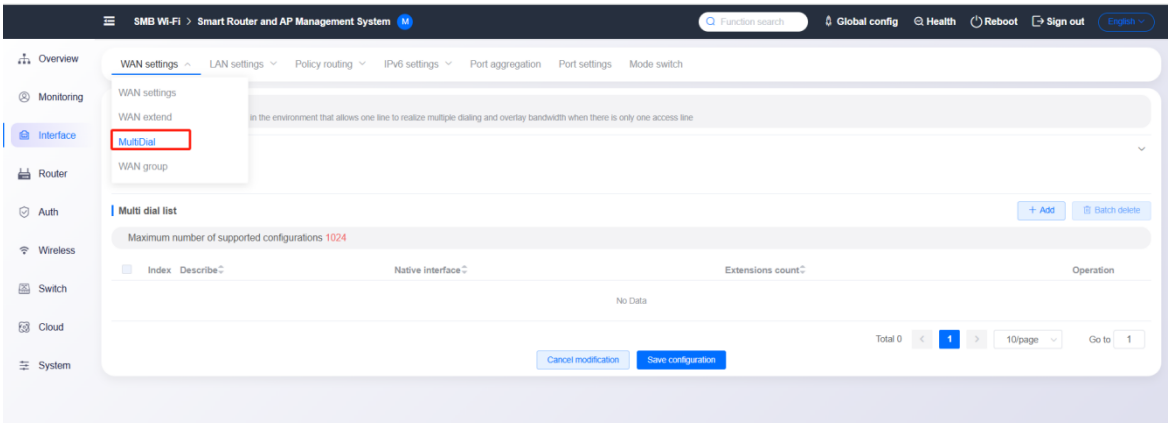


Note that the number of WAN extensions can only be less than or equal to the maximum number of WAN ports allowed by the license. The physical WAN port will occupy one WAN port authorization number.

3.1.3 MultDial

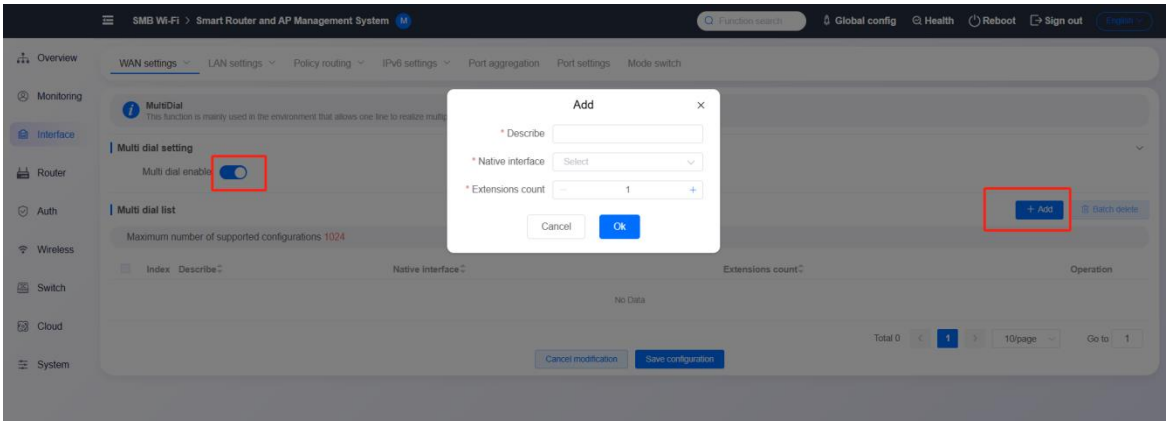
MultDial is mainly used in environments where there is only one ISP access line but multiple dial-up accounts are allocated, or where one line is allowed to perform multiple dial-ups and the bandwidth can be superimposed.

3.1.3.1 MultDial settings



MultiDial settings

Turn on or off the switch of the one-line multi-dial function. Whether it is turned on or off, the system will automatically restart after submission;



Add

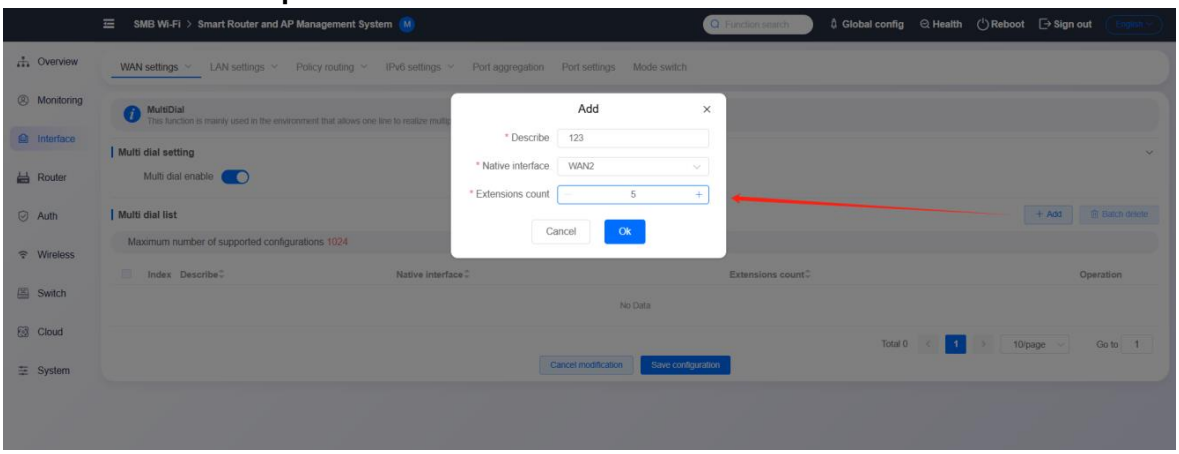
Describe：Customize description content to facilitate differentiation among many rules；

Native interface：Select the WAN port on which will be added for multidial;

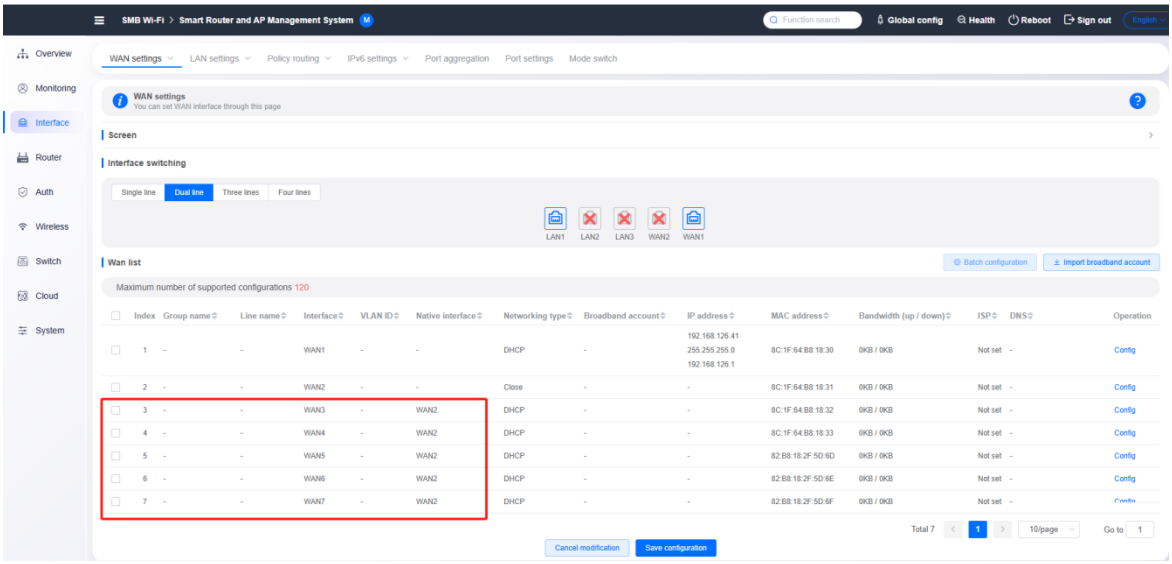
Extension count：How many lines will be used for multidial.

The virtual port created by multidial does not affect the use of the original interface, but if you want to dial successfully, you must ensure that the network of the selected original interface is unobstructed and the dial-up account and password provided by the upper-layer device are correct. After the rule configuration is completed, the multidial port is generally set to "dynamic IP" by default, and you need to manually enter the broadband account and password to achieve the effect of multidial.

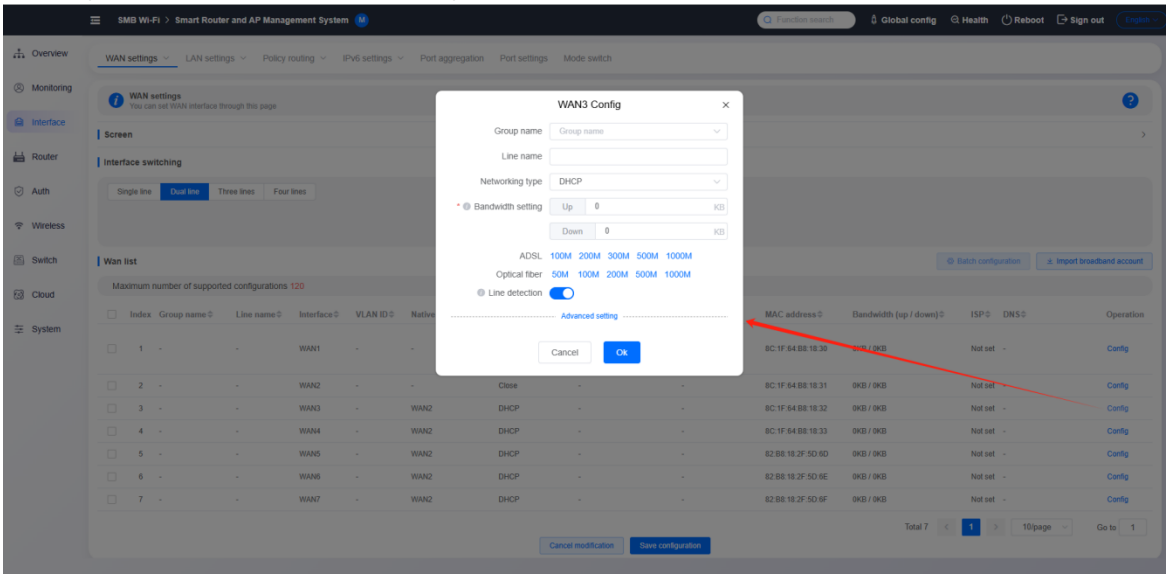
3.1.3.2 Multi-dial example



Turn on "Multi-Dial enable", save the configuration and the network will automatically restart. After the normal restart, all WAN port information will be displayed in "Interface " - "WAN Settings" after the expansion is successful. The effect is as follows:



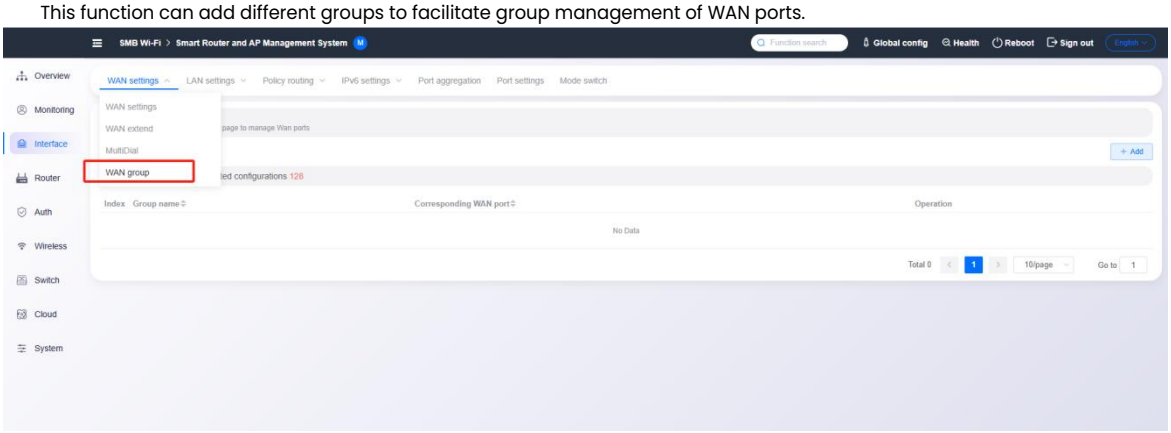
The configuration on the operation item can configure the parameters of a certain WAN port separately.



Note that the number of multi-dial lines can only be less than or equal to the maximum number of WAN ports allowed by the authorization. The physical WAN port will occupy one WAN port authorization number.

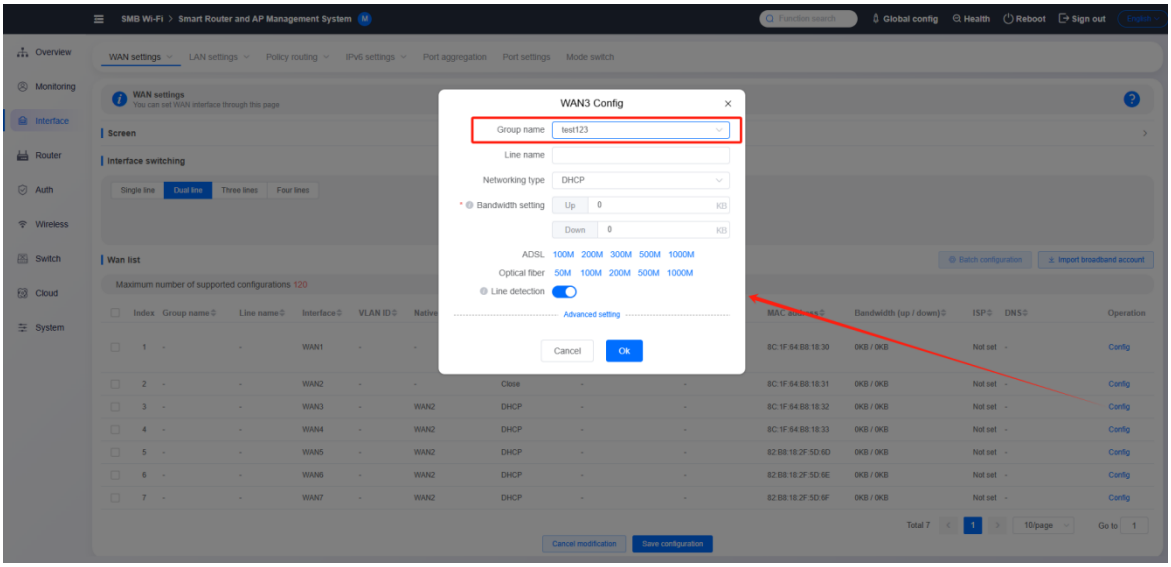
3.1.4 WAN group

This function can add different groups to facilitate group management of WAN ports.

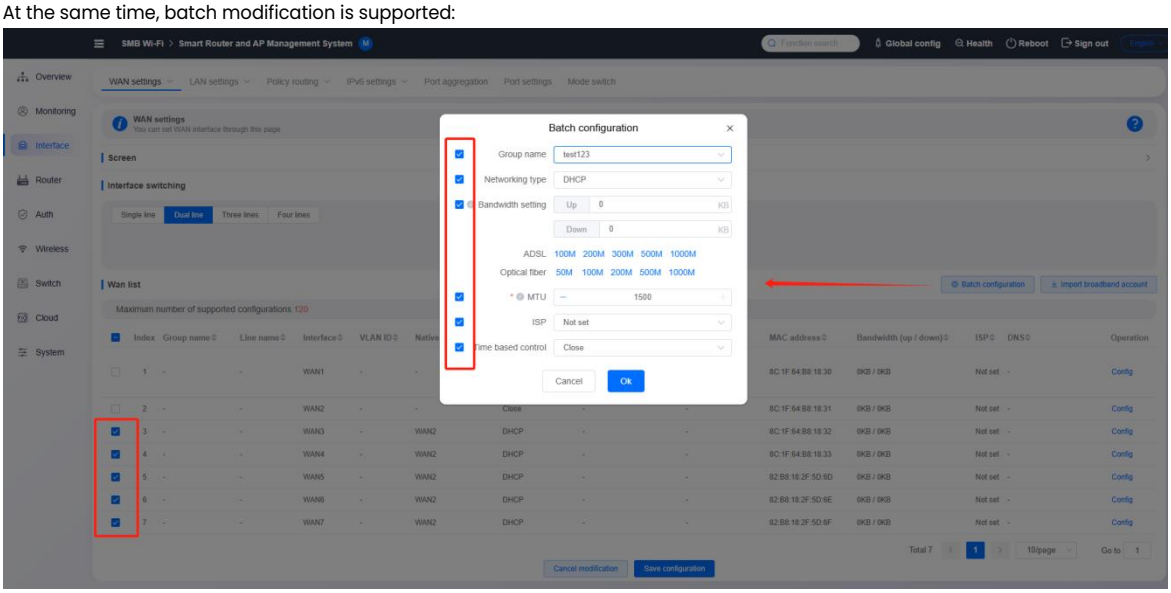


Add: input the group name

Go back to the WAN settings and select the desired grouping for different WAN ports:



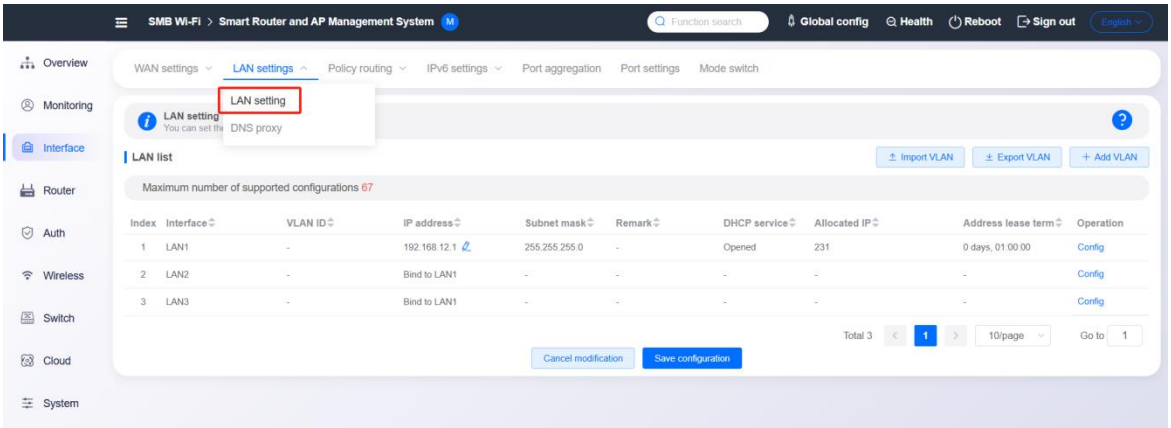
At the same time, batch modification is supported:



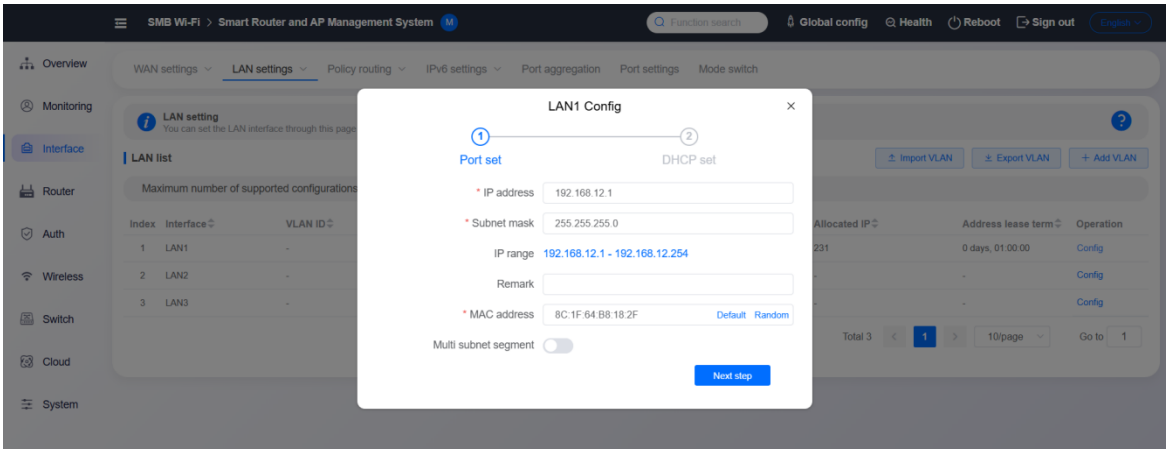
3.2 LAN setting

3.2.1 LAN setting

Click LAN setting, add/import/export VLAN ID, and the page will display the maximum number of VLAN ports supported by the main device



LAN list



Config: Configure the parameters of the LAN port, set the LAN port IP address, subnet mask, MAC address, multi subnet segment, DHCP and other parameters.

1. Port set

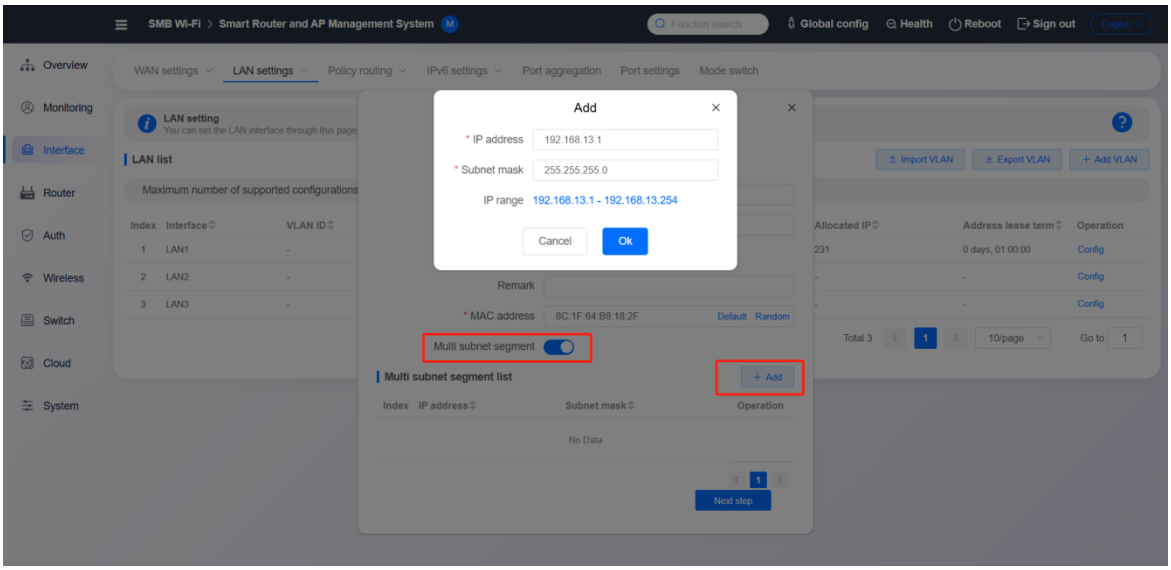
IP address: configure the IP address of the LAN port

Subnet mask: Set an appropriate mask value based on the access users. The default subnet mask used by the router is 255.255.255.0, which can be changed as needed;

Remark: Give a brief description of the LAN port for easy identification

MAC address: modify the MAC address according to the network conditions of the intranet. Generally, the default MAC address does not need to be adjusted;

Multi subnet segment: Enable or disable multiple subnets as needed, add or modify the parameters of multiple subnets as needed. Its function is basically the same as the router intranet address, and is usually used as the gateway address of the corresponding subnet. This address should not be set to the same subnet as other LAN port addresses, otherwise the submission will fail.



2. DHCP setting

DHCP service: Turn on the DHCP server, the terminal under the LAN port will obtain an IP address normally. Turned off the DHCP server, it will not be able to obtain an IP address.

Start address: The start address of the IP automatically assigned by the DHCP server. The range of the starting address is within the network segment calculated by the IP address and subnet mask;

End address: The end address of the IP automatically assigned by the DHCP server. The end address range is within the network segment calculated by the IP address and subnet mask.

Address lease time (seconds) : The validity period of the automatically assigned IP. After this period, the devices in the LAN will re-acquire the IP.

DHCP gateway: The default gateway address assigned by the DHCP server. This address is automatically changed according to the above "Starting Address". For example, if the starting address is filled in as 192.168.10.100, the DHCP gateway address here is automatically updated to 192.168.10.1

Subnet mask: The default is usually 255.255.255.0. Change the mask range as needed.;

Advanced setting:

Preferred DNS server: Fill in the DNS server. The preferred server will be used as the first DNS server

Alternate DNS server: Fill in the alternate DNS server. When the preferred server cannot be used normally, the alternate server will continue to work

Custom Option: Select and configure Option as needed. When any LAN port configuration or modification is submitted, the device will automatically restart to save and read the latest configuration data.

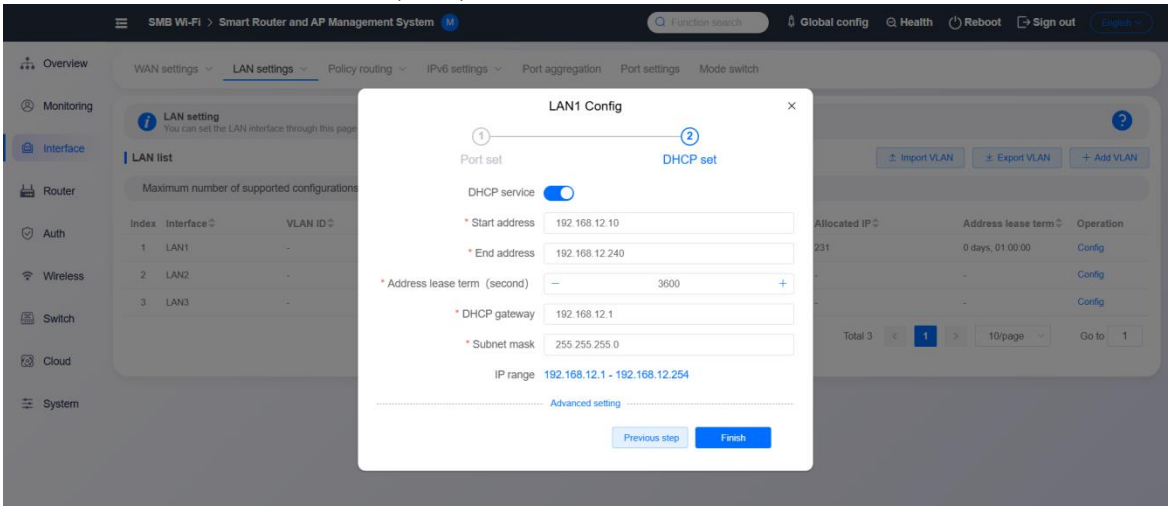
Format: ID+length+content; multiple options can be filled in

For example:

2B060104C0A801012C060104C0A801012D060104C0A80101 means there are 3 options: 2B, 2C, 2D

2B060104C0A801012C060104C0A80101 means there are 2 options, 2B and 2C

2B060104C0A80101 means there is only one option, 2B



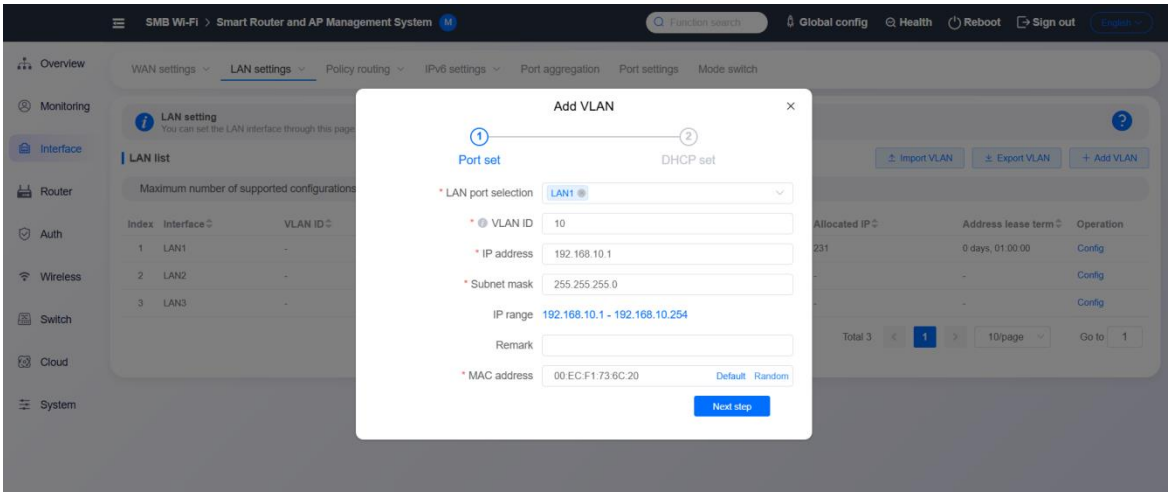
Add VLAN: The LAN supports multiple VLANs. VLAN is related to the uplink configuration. Please pay attention to the configuration.

1. Port set

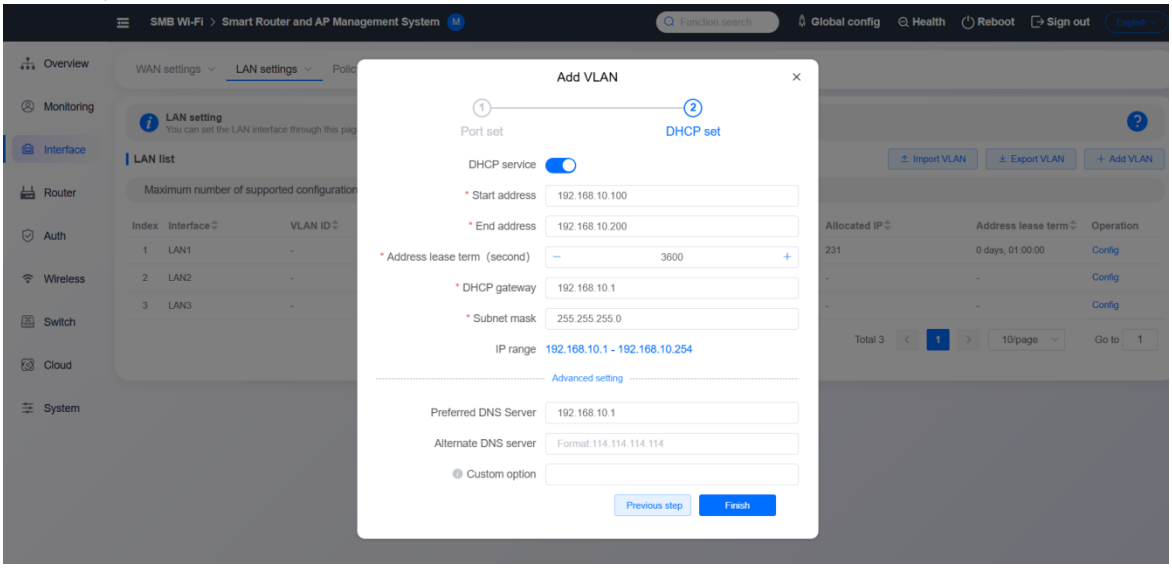
   VLAN needs to select the corresponding LAN port

   VLAN ID is unique and required

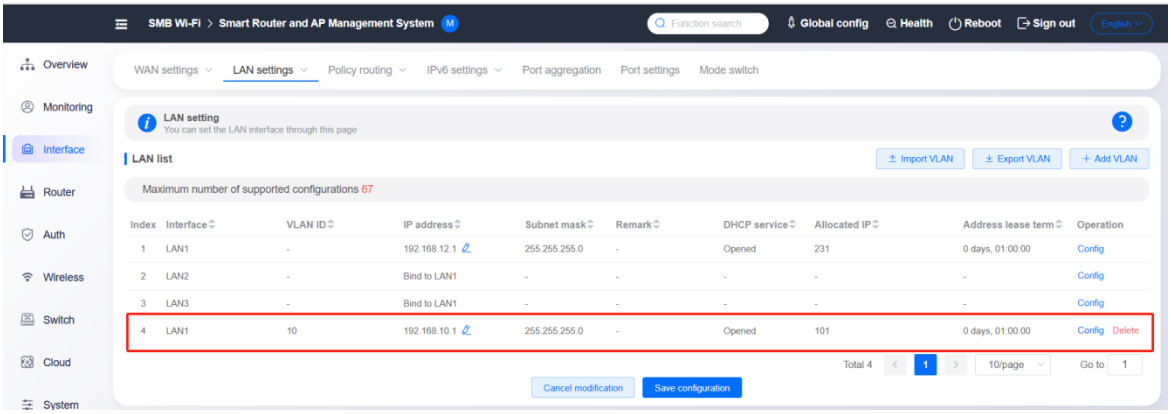
   The IP address cannot be the same as other addresses in the LAN and must be unique.



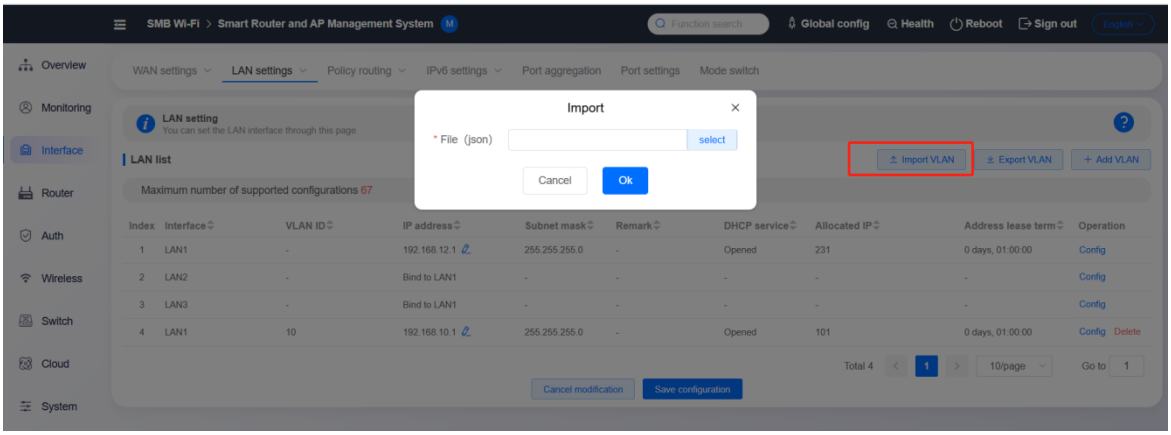
2. DHCP configuration: After enabling and setting, the VLAN will provide DHCP delivery service for the corresponding network segment.



Display effect after adding successfully

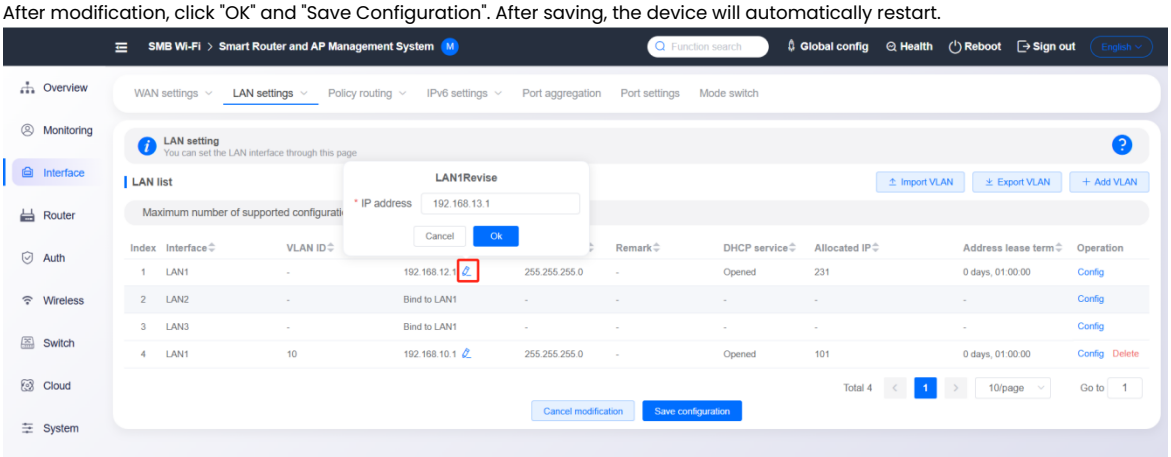


Export VLAN: Export the VLAN configuration that already exists in the rule separately. You can use it to import the VLAN parameters to the device that matches the parameters.



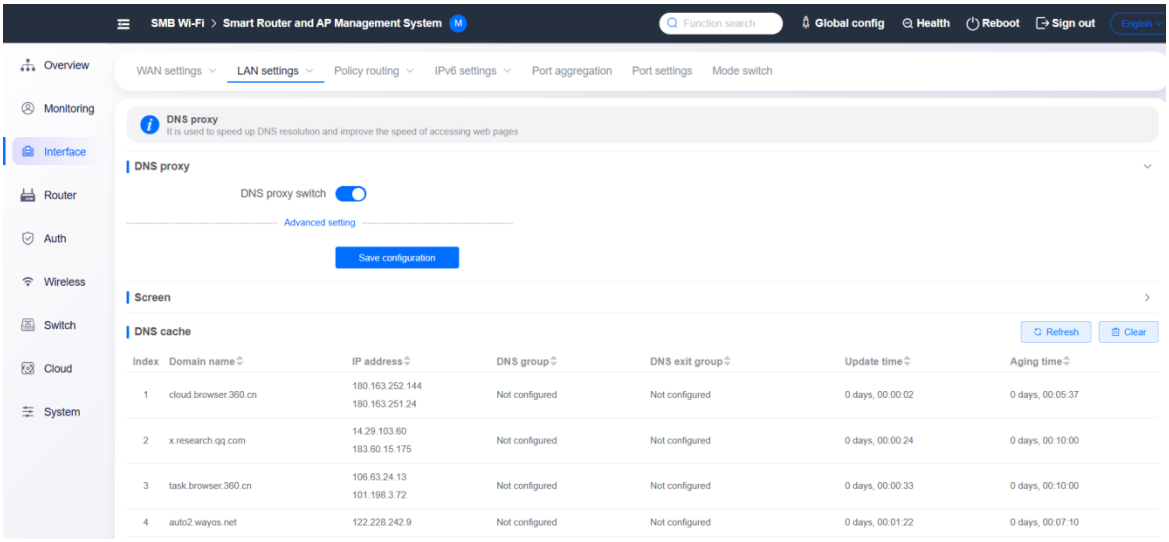
Import VLAN: The exported VLAN configuration parameters can be imported again for use.

LAN port (IP address) modification: You can directly modify the IP address of the LAN port in the "IP address" item of the LAN list. After modification, click "OK" and "Save Configuration". After saving, the device will automatically restart.



3.2.2 DNS proxy

Used to speed up DNS resolution and increase the speed of accessing web pages.



DNS Proxy

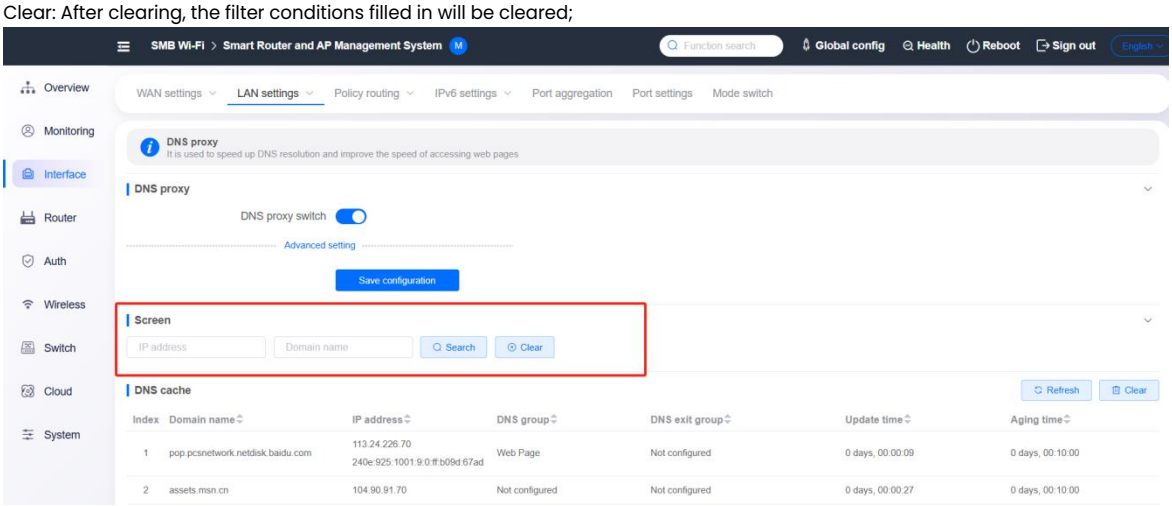
DNS proxy switch: When turned on, it can speed up DNS resolution and increase the speed of accessing web pages. After turning it on, the "Advanced Settings" rules will also be displayed.

Screen

By searching the DNS cache records for the remote IP address or domain name.

Search: Start filtering the current input conditions;

Clear: After clearing, the filter conditions filled in will be cleared;

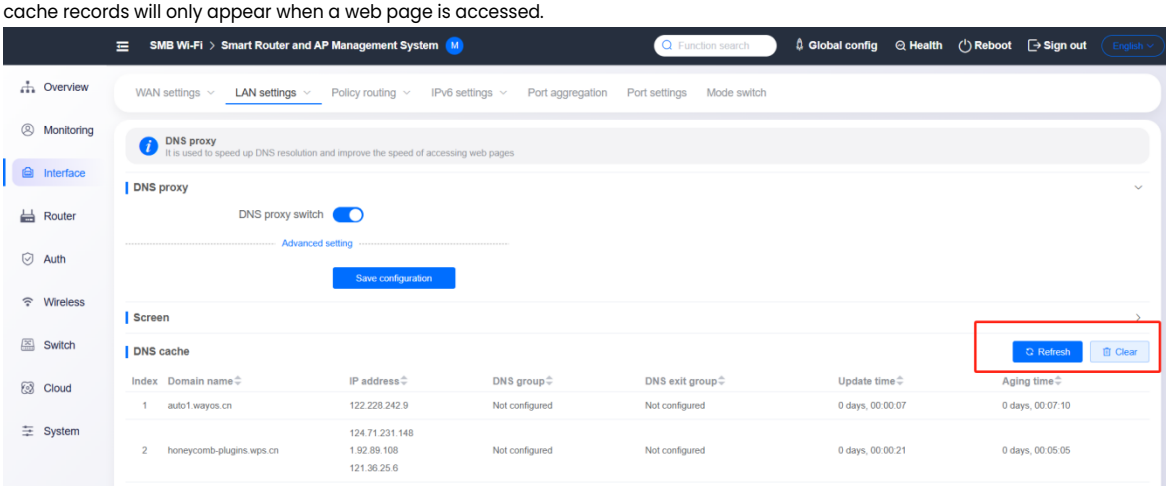


DNS cache list

Display the current DNS cache list

Refresh: Refresh the DNS cache list. When there is a new cache, the list will be automatically updated after refreshing;

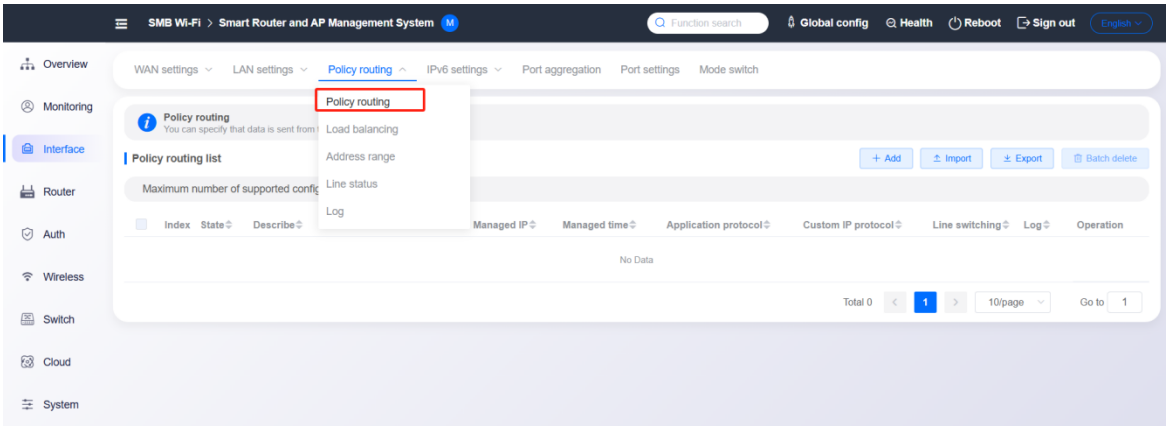
Clear (list): Clearing here means clearing the DNS cache list records. After clearing the records, they cannot be restored. New DNS cache records will only appear when a web page is accessed.



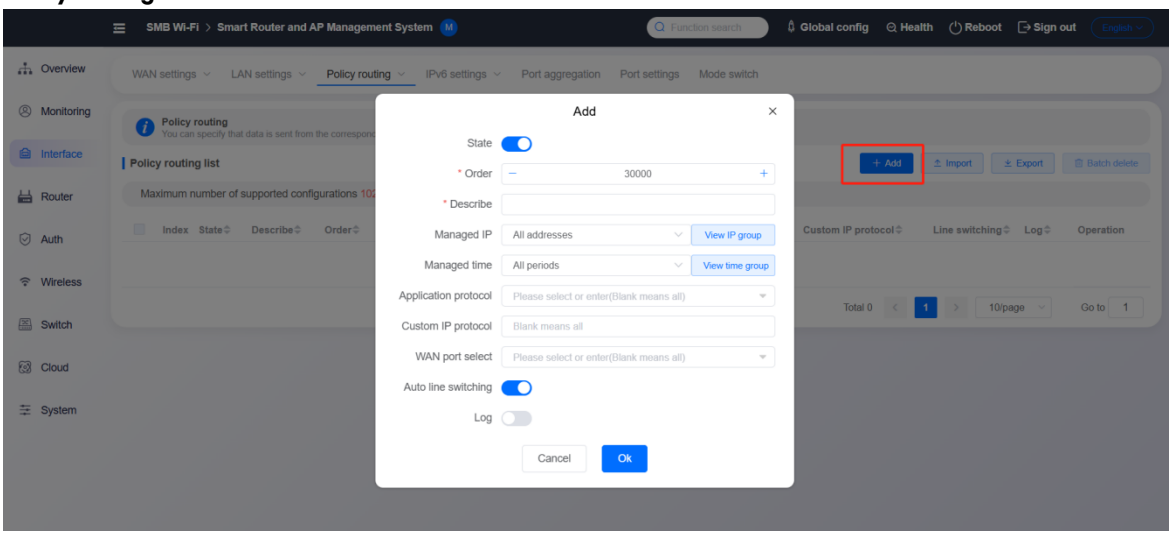
3.3 Policy routing

3.3.1 Policy routing

Can specify that data is sent from the corresponding WAN port. Generally, when a certain protocol is required in the network environment, or when users use a dedicated line or a specified WAN port, policy routing rules should be filled



Policy routing list



Add

State: The rule state is disabled or enabled. When the state is disabled, the created rule will not take effect;

Order: refers to the priority of rule execution. The higher the value entered, the higher the execution priority. If the order of different rules is the same, the rules will be triggered and take effect at the same time; if the same rules are created and the order is same, the device will randomly execute one of them; if the same rules are created and the order is different, the device will execute the rule with the higher order value;

Description: Write a note for this rule to clarify the role of this rule;

Managed IP: The rules are effective for those IP addresses or IP segment terminals. The policy rules will take effect on the IP address (segment) filled in, including:

" All addresses" refers to all terminals in this network.

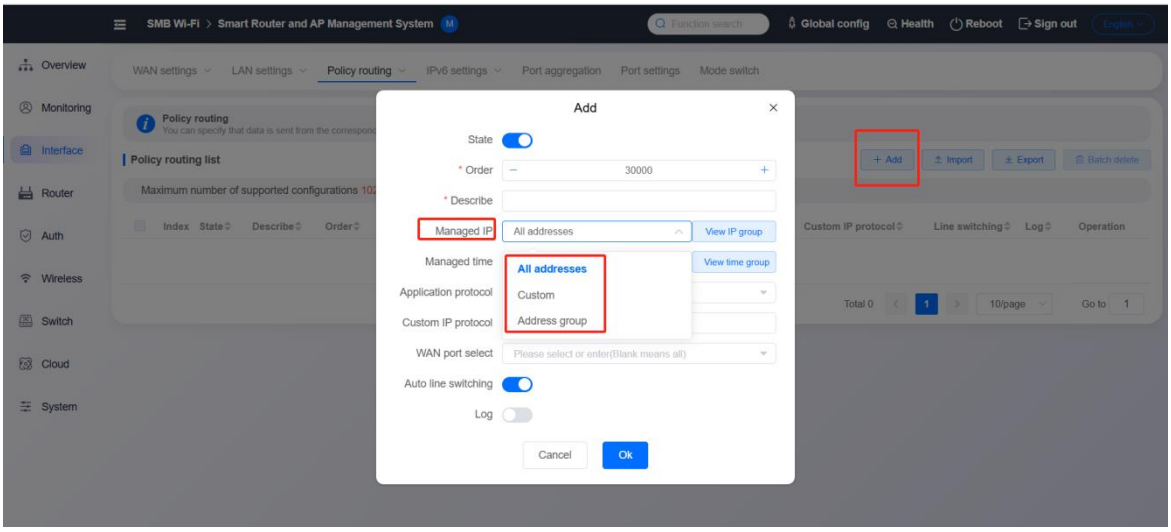
"Custom" can fill in a certain IP address or a certain range of IP addresses.

"Address Group" can quickly locate the "Managed IP" function through "View IP Group", and then add the intranet IP grouping and choose to use it.

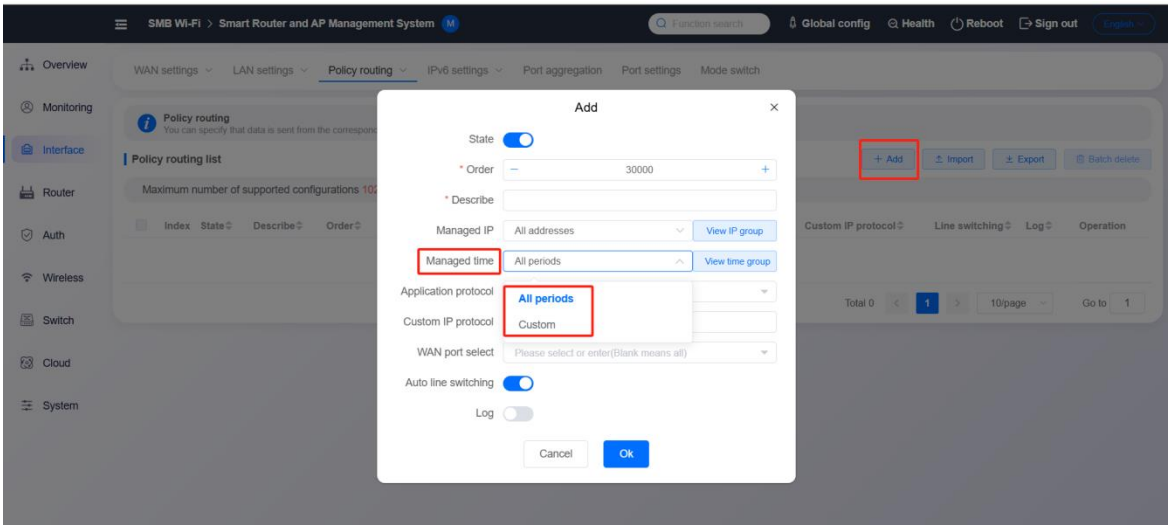
Managed time: The effective time of the policy routing rule. The rule is effective only within the set time. The rule is invalid outside the set time.

"All periods" refers to all periods.

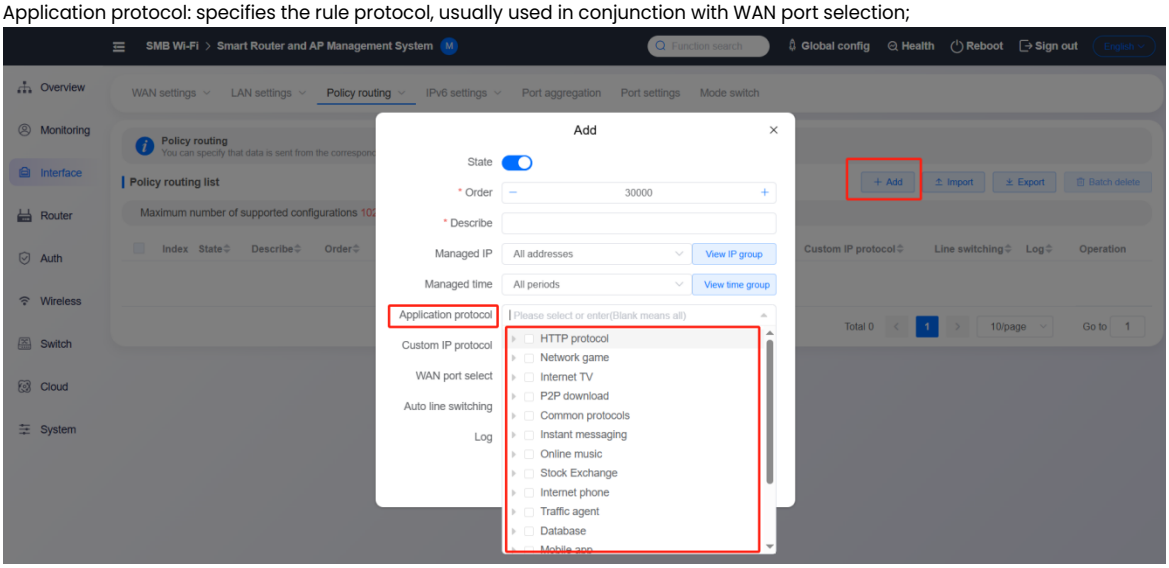
"Custom" allows you to customize the time period.



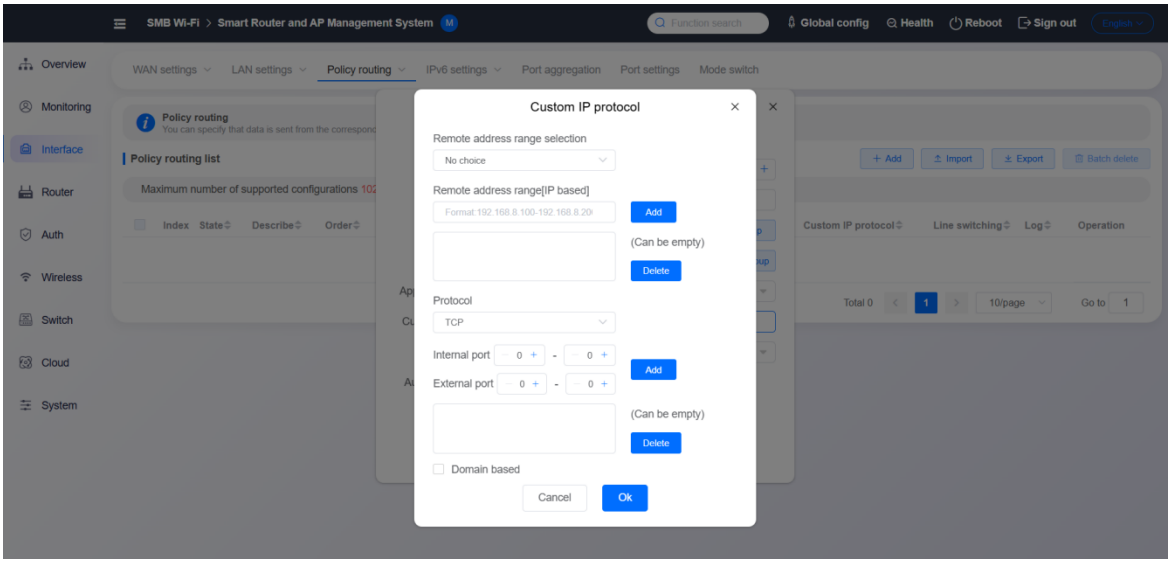
View time periods: Can quickly locate "view time group" and set time period templates;



Application protocol: specifies the rule protocol, usually used in conjunction with WAN port selection;



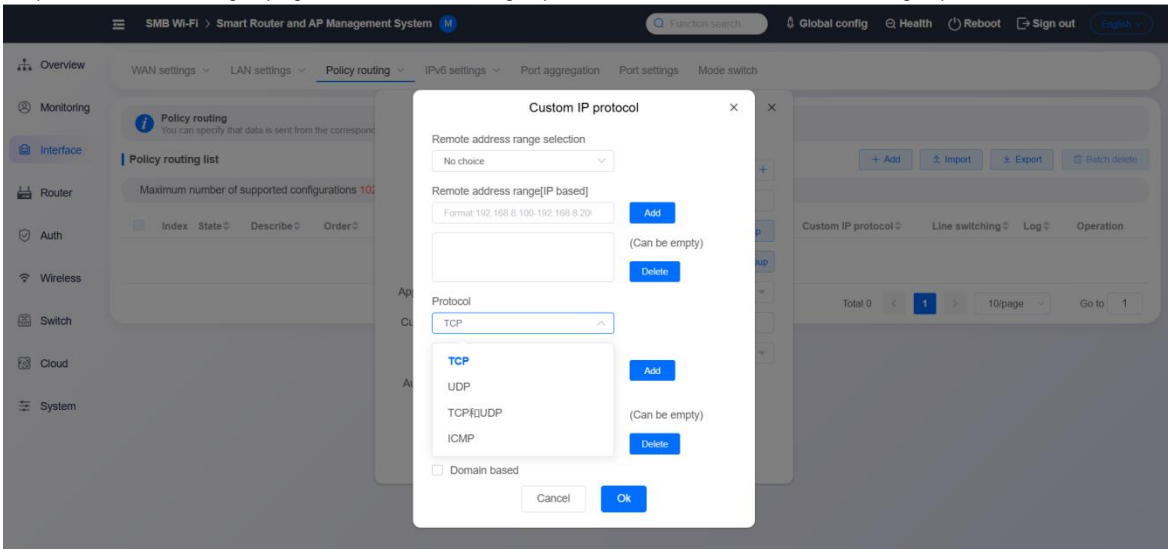
Custom IP protocol: When the application protocol option does not contain the protocol that needs to be set or there is a special remote address, fill in the corresponding address and port interface here. This function is used in the same way as "Application protocol"



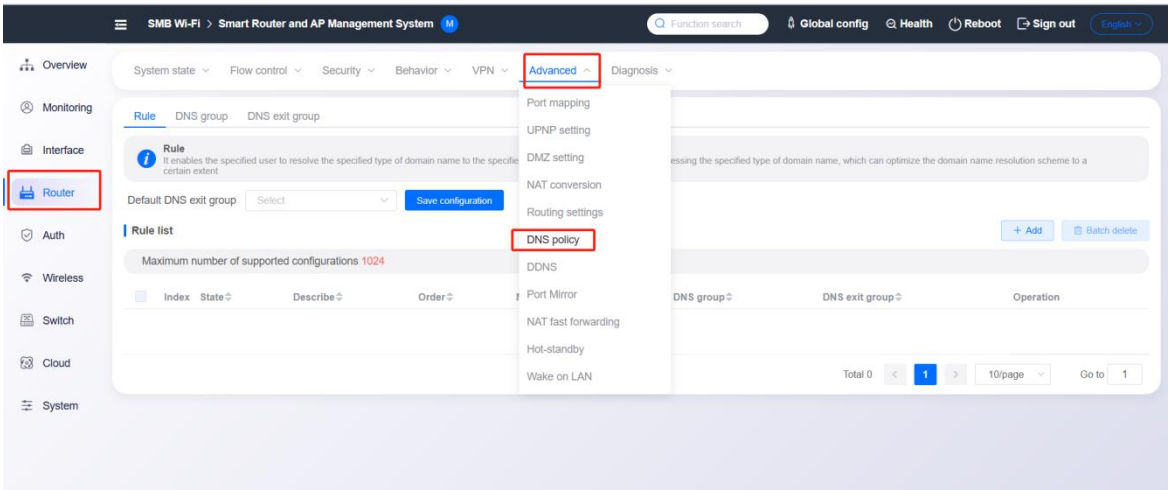
"Remote address range selection" selects the access object through the enabled address library. The commonly used China Telecom, China Mobile and China Unicom are already available by default, and their address ranges support custom addition;

"Remote address range [IP based on]" is used to enter the IP address that needs to be accessed.

"Protocol" selects the access object based on the type and port number, and "Domain Based " selects the access object based on the template of domain name grouping. You can customize the groups and domain name members in the DNS group.



DNS groups can be viewed in "Router" - "Advanced" - "DNS Policy" - "DNS Group":

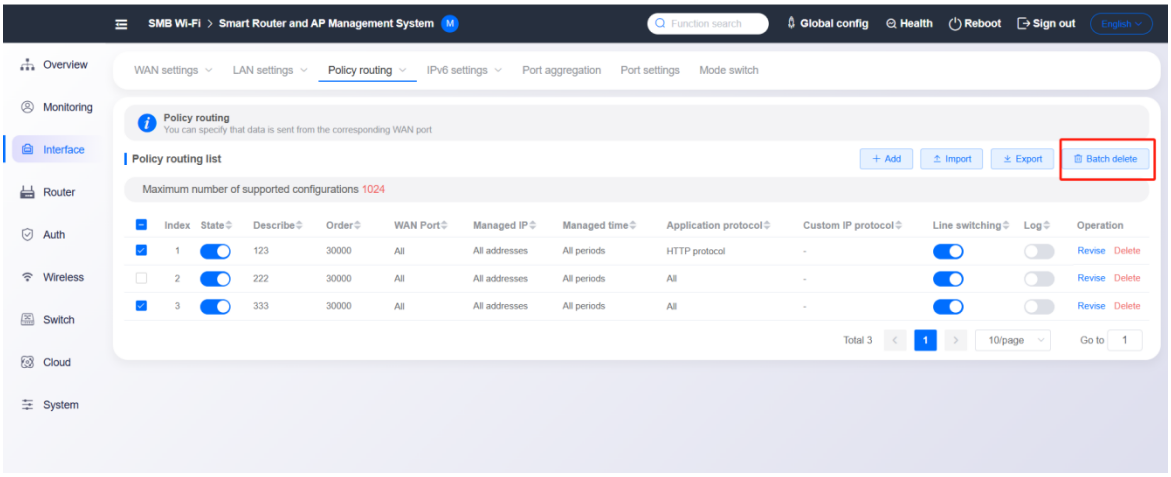


WAN port selection: Select the WAN port for the rule to take effect. You can select one or more at the same time. The number of WAN ports selected is related to the number of WAN ports currently set;

Automatically switch lines: When a certain WAN port in the above rules is unavailable or has other faults, whether to allow the rules to use other lines;

Log: Enable or disable the logging of routing rules. Generally, you can choose to enable it for easy troubleshooting.

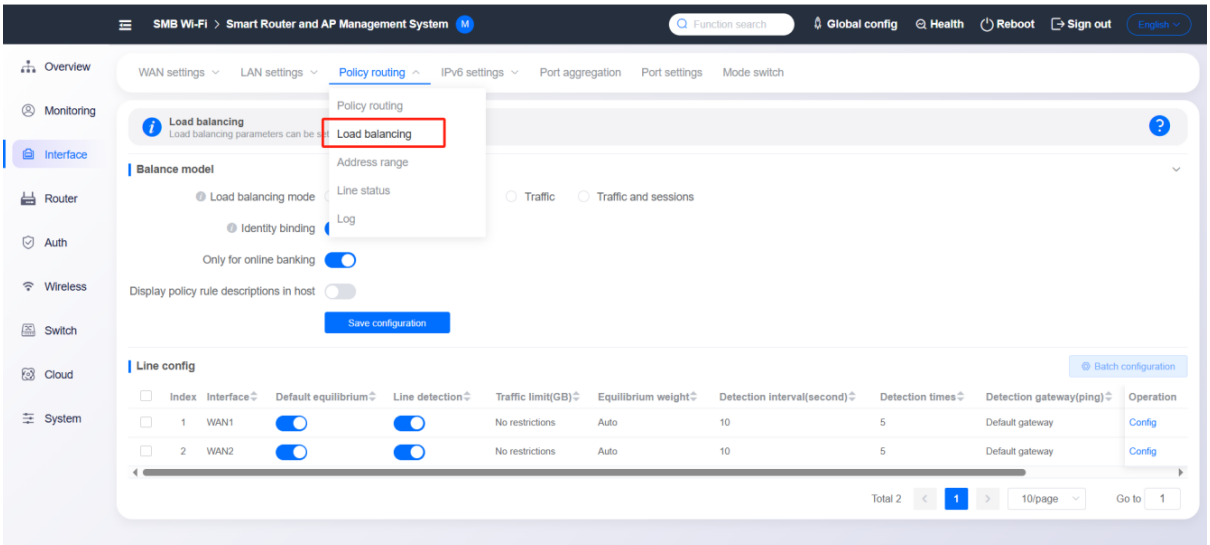
Import: Import policy routing rules. The import file has format requirements. It is recommended to export a policy routing file before using the import function, add or modify rules in the file according to the format, and then save and import.
Export: supports exporting policy routing rules, which can be used for rule backup;
Batch delete: When there are multiple rules that are not needed, you can select the rules and delete them in batches;
Modification: Re-edit this rule;
Delete: Delete the selected rules individually.



3.3.2 Load balancing

Load balancing is used to set the line's balancing mode, detection method, balancing weight , etc.

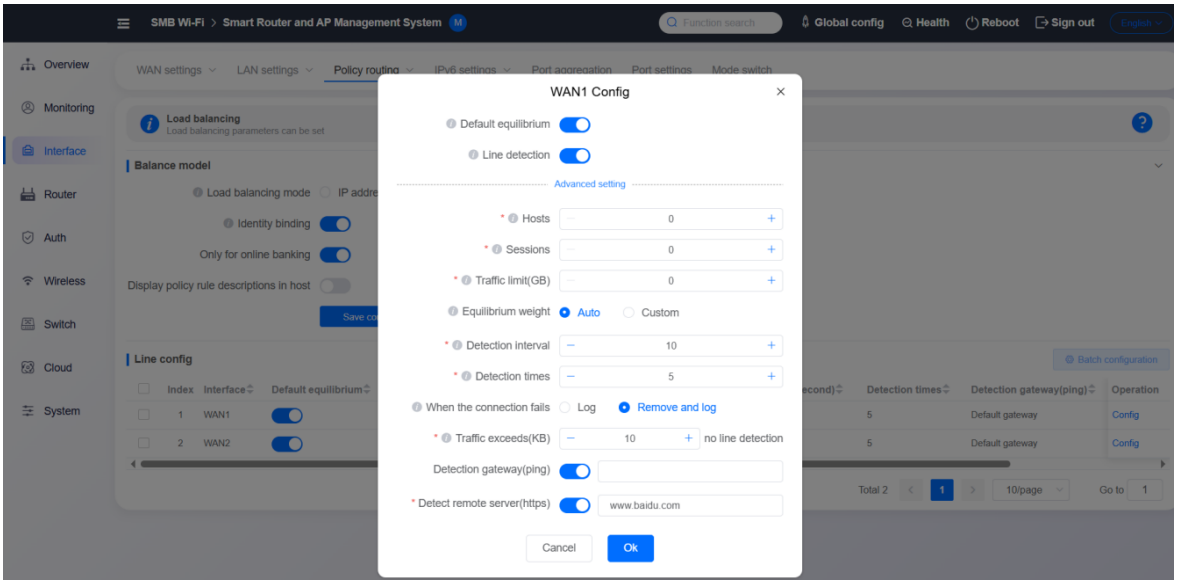
Balanced mode



Load balancing: Generally, load balancing is enabled by default on devices, and balancing is performed by the number of sessions by default, and balancing rules are created according to the number of WAN ports;
IP address: load balancing is performed based on the number of IP addresses. When you select load balancing based on IP address (number), the system will automatically balance the number of IP addresses on different WAN ports. The balancing result can be viewed in the "Line status - "Number of Hosts/Number of Sessions" column;
Number of sessions : that is the balance of the number of sessions of terminal users. The system will automatically balance the number of sessions on different WAN ports;
Traffic: This refers to the traffic balance generated by the end users. The system will automatically balance the traffic on different WAN ports.
Traffic and number of sessions: that is, the traffic and number of connections generated by the end users are balanced according to the mean ratio, and the system will automatically balance them on different WAN ports.
Identity binding: If multiple lines are configured, to enable the normal use of QQ, online banking, etc., please enable the identity binding function;
Only valid for online banking: only valid for online banking;
Display policy rule description in host : After turning it on, the policy name that takes effect on the connection will be displayed in the host monitoring connection

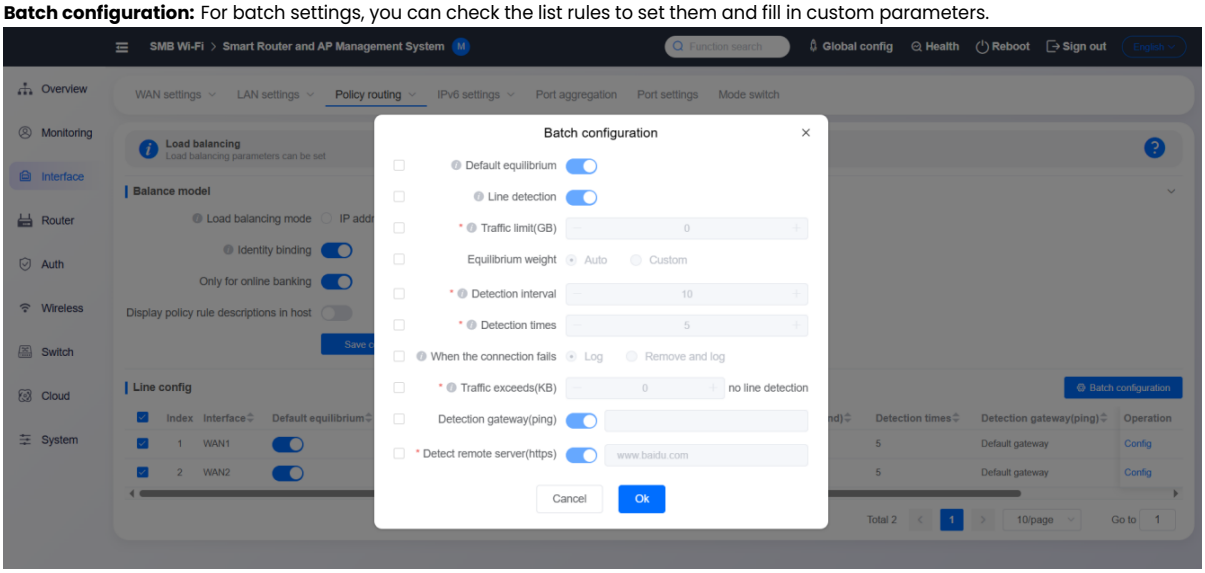
Operation Config

Configuration: After enabling load balancing, a balancing list rule will be automatically generated . Check the list rule to set it and you can fill in custom parameters.



Equilibrium weight: The larger the line capacity, the larger the value should be;
Line detection: Set whether to enable the line detection function for this line;
Detection interval: the time interval for detecting line status;
Detection times: after how many detection failures the line is judged as a connection failure;
Detect gateway (ping): If the value is empty, the default gateway address is used. If it is set, the set IP address is used. The detection method is ping;
Detect remote server (https): Remote server address: can be IP or domain name. This detection method uses port 443 of https.

Batch configuration: For batch settings, you can check the list rules to set them and fill in custom parameters.



Default equilibrium: Disable or enable. If you do not want this line to participate in balancing, just disable it. Lines that do not participate in balancing will only accept the data flow of the rules bound in the policy routing. If there is no data bound to the line in the policy routing, there will be no data flow on the line.
Line detection: Enable the line detection function. The advanced parameter options can only be enabled when activated, otherwise they are invalid. Line detection is mainly used to detect whether the line is smooth or not. For a multi-line environment, if one of the lines fails to be detected, the system will remove the line by default, and all conversations on the line will be automatically transferred to another line that has successfully detected and participated in the balancing;
Traffic limit (GB): limit the total traffic of a WAN port. When the traffic reaches the set value, the port will no longer export data.
Equilibrium weight: This value is mainly used to compare with the balance of other lines. The system will determine the load size of the line according to the value. The default value is automatically determined by the size of the bandwidth value. The export bandwidth value must be filled in to be effective. If it is changed to custom, please set this parameter according to the line weight ratio. The larger the parameter, the more data/users will pass through;
Detection interval: the interval time between automatic line detection;
Detection times: the number of line detections;
When the Connection failure: the way to handle the line when the line detection fails. Remove the line and record the log - delete the line and record it in the log. All connections on the line will be automatically transferred to other lines; Only record in the log - only record the disconnection log in the log, and do not delete the line;
No line detection when traffic exceed: When the traffic of the WAN port exceeds the set value, no line detection will be performed;

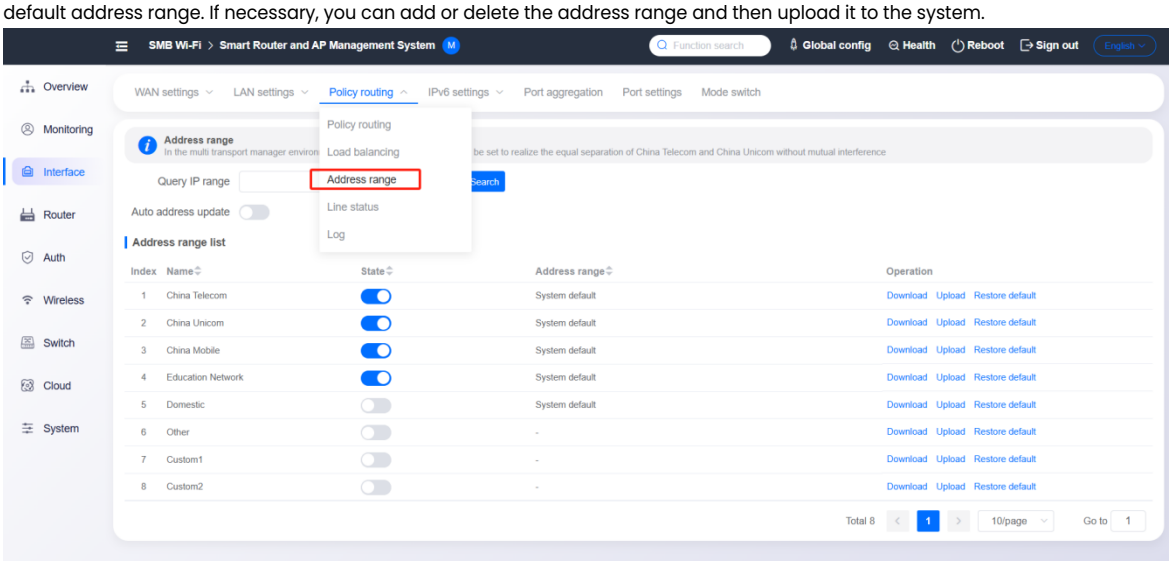
Detection gateway(ping): enable it means detecting the external gateway of this line. If the content is empty, it means detecting the default gateway. The default gateway of some ISPs may not allow ping, so you can manually configure other WAN addresses for testing;

Detect remote server(https): Enter a stable domain name or WAN IP address to detect whether the line is connected or not.

Note: By default, line detection uses ping to determine whether the line is connected or disconnected. Therefore, when filling in the detection IP or server address, please try to choose an address that is online for a long time and stably.

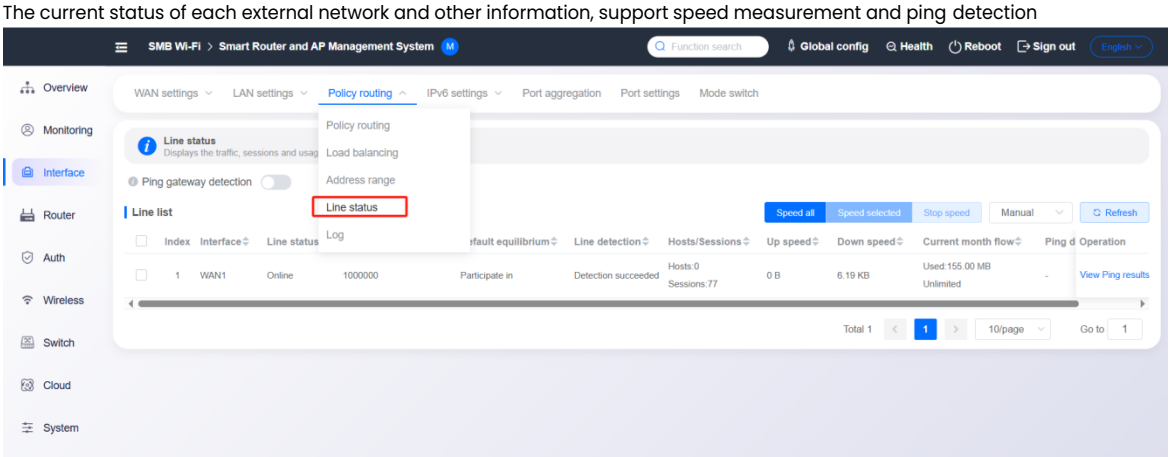
3.3.3 Address range

Used for policy routing in an environment with multiple operator lines. Just select the corresponding line and set the policy mode to separate the telecom and Netcom lines without interfering with each other. You can upload or download the current system default address range. If necessary, you can add or delete the address range and then upload it to the system.

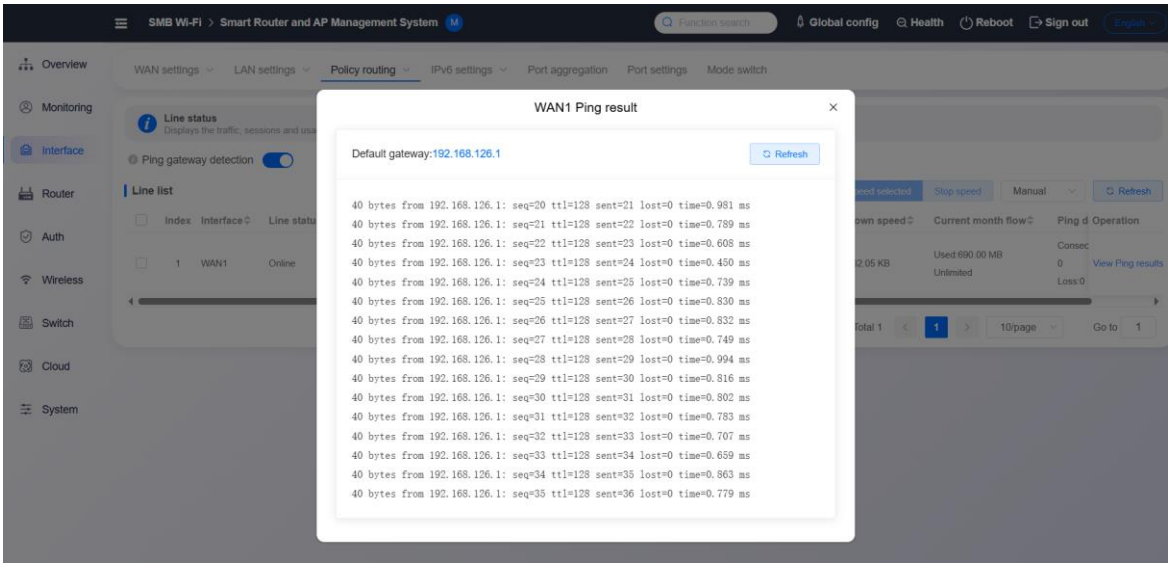


3.3.4 Line status

The current status of each external network and other information, support speed measurement and ping detection

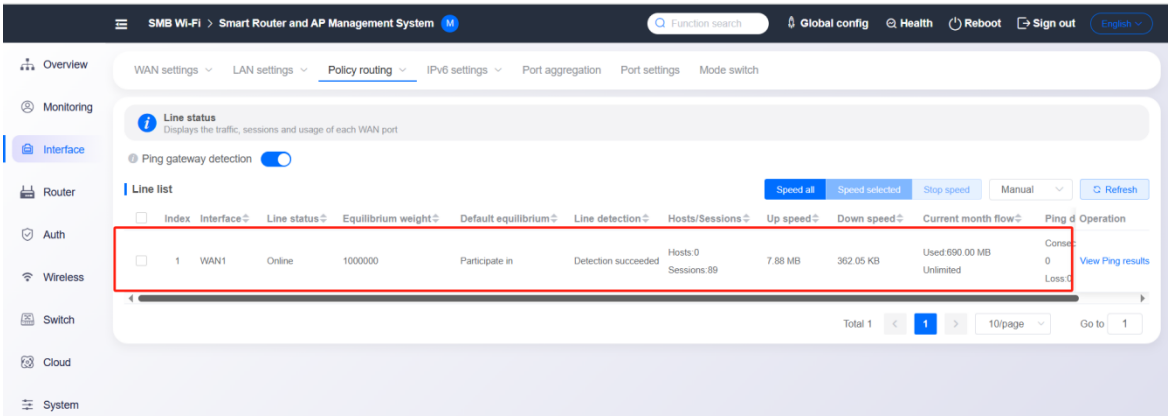


Ping gateway detection : After it is turned on, the gateway of the WAN port will be automatically pinged. You can view the corresponding situation by checking the ping results. To view the results of pinging the gateway, please click the "View Ping Results" button in the list .

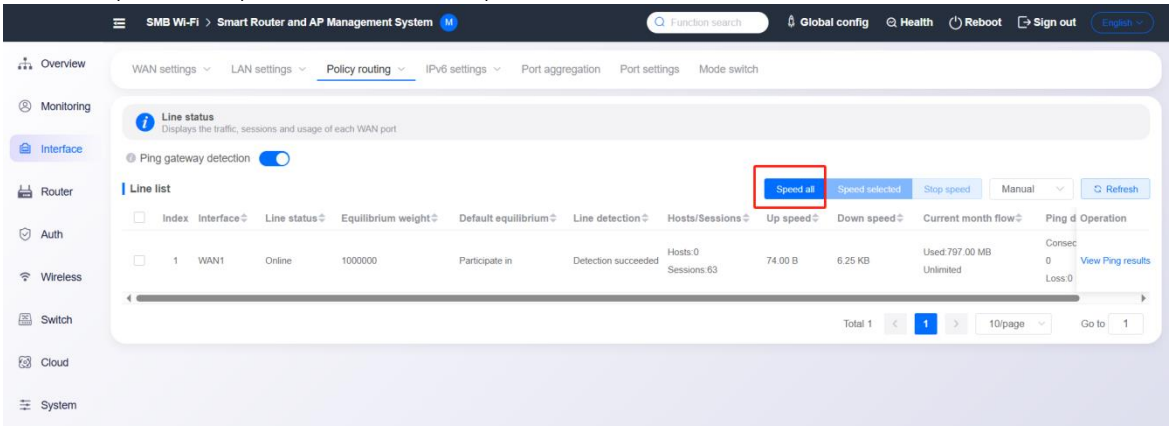


Line list

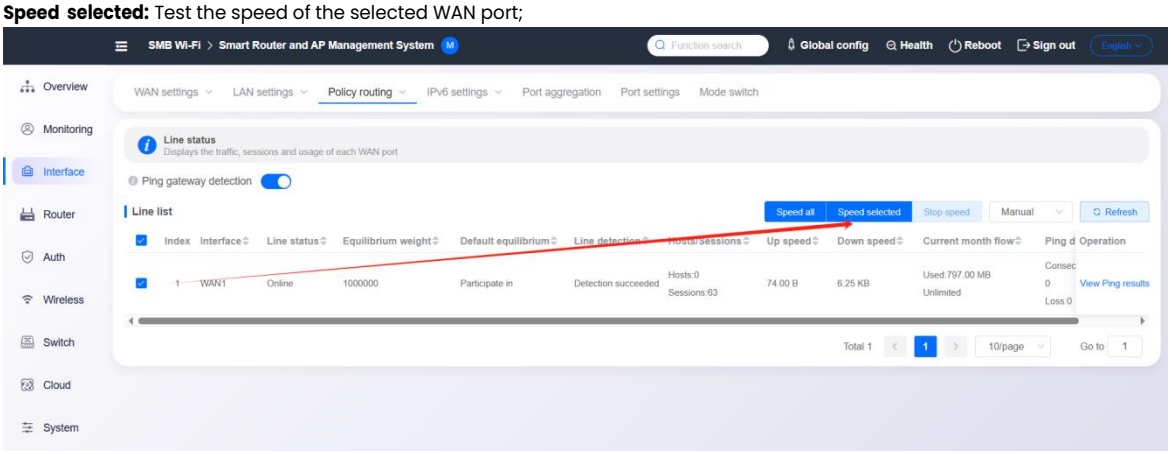
Displays the traffic and session usage of each WAN port .



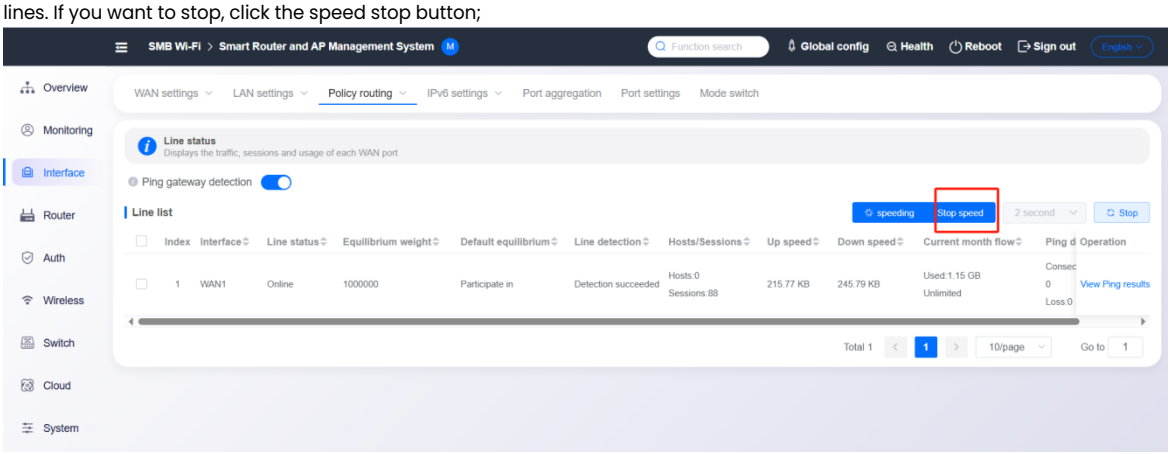
Speed All: This means to test the speed of all current WAN ports. After submitting the speed test all, the page list will automatically refresh the upstream and downstream speeds .



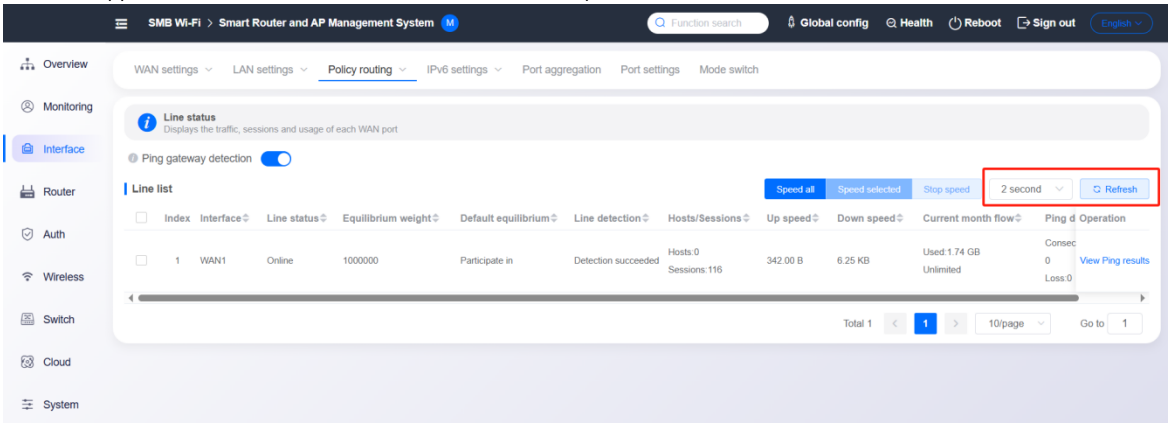
Speed selected: Test the speed of the selected WAN port;



Stop speed: After submitting the speed test for all and speed test selected , the page will automatically refresh the up and down lines. If you want to stop, click the speed stop button;

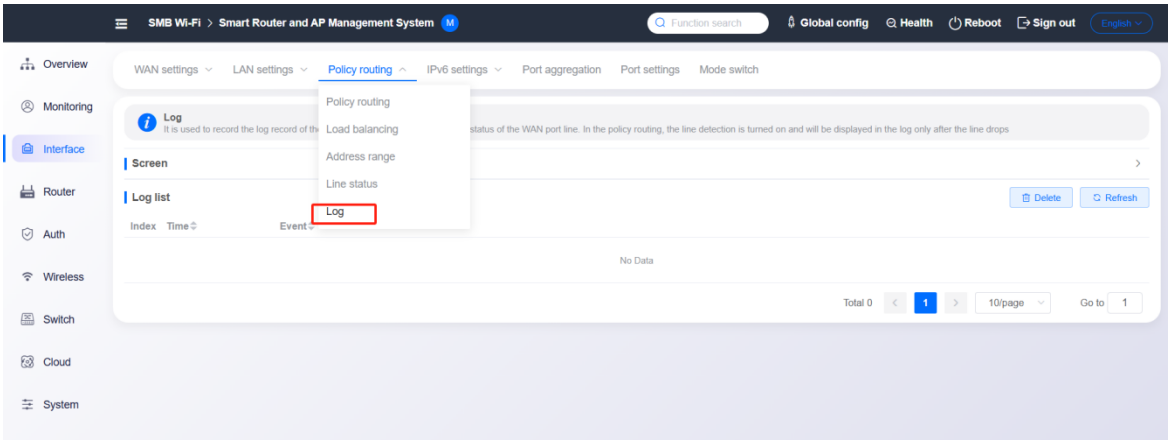


Refresh: Supports manual refresh and automatic refresh of WAN port status at different time intervals .



3.3.5 Log

It is used to record the log records of policy routing rules and the working status of the WAN port line. In policy routing, line detection is enabled for this line, and it will be displayed in the log only after the line is disconnected.



Screen:

Find relevant log information by message content.

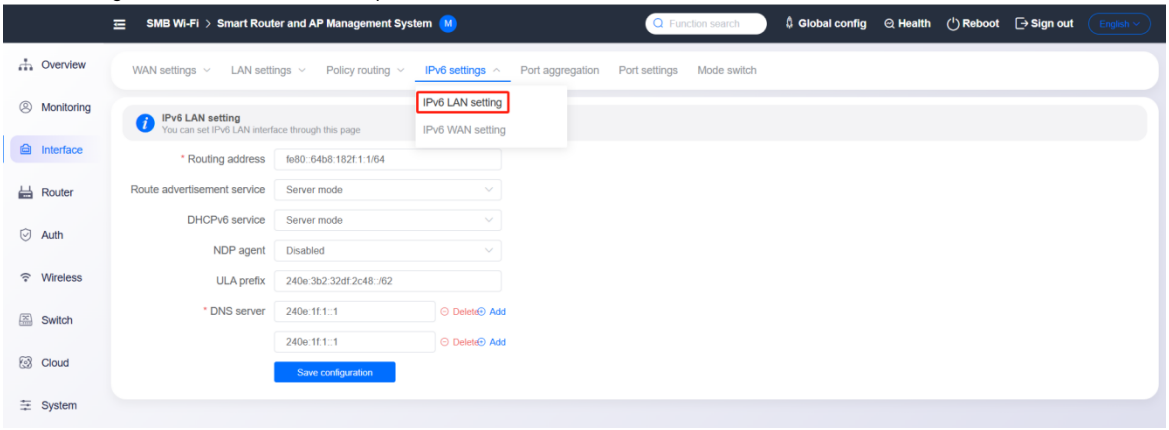
Log List

Display all log information or log information that meets the conditions and filters, and support export, delete and refresh operations.

3.4 IPv6 LAN setting

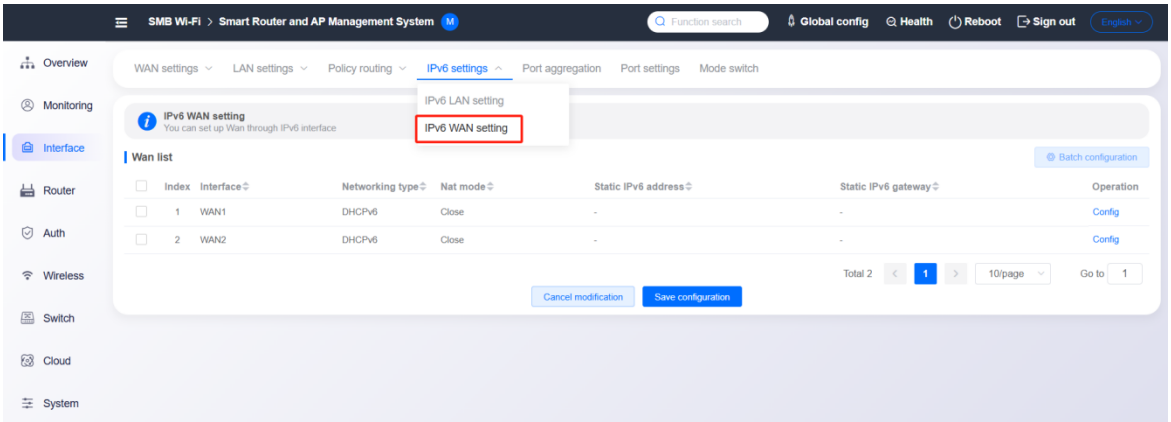
3.4.1 IPv6 LAN setting

Select Configure IPv6 LAN Interface as required.



3.4.2 IPv6 WAN setting

Set up an IPv6 WAN interface as needed.



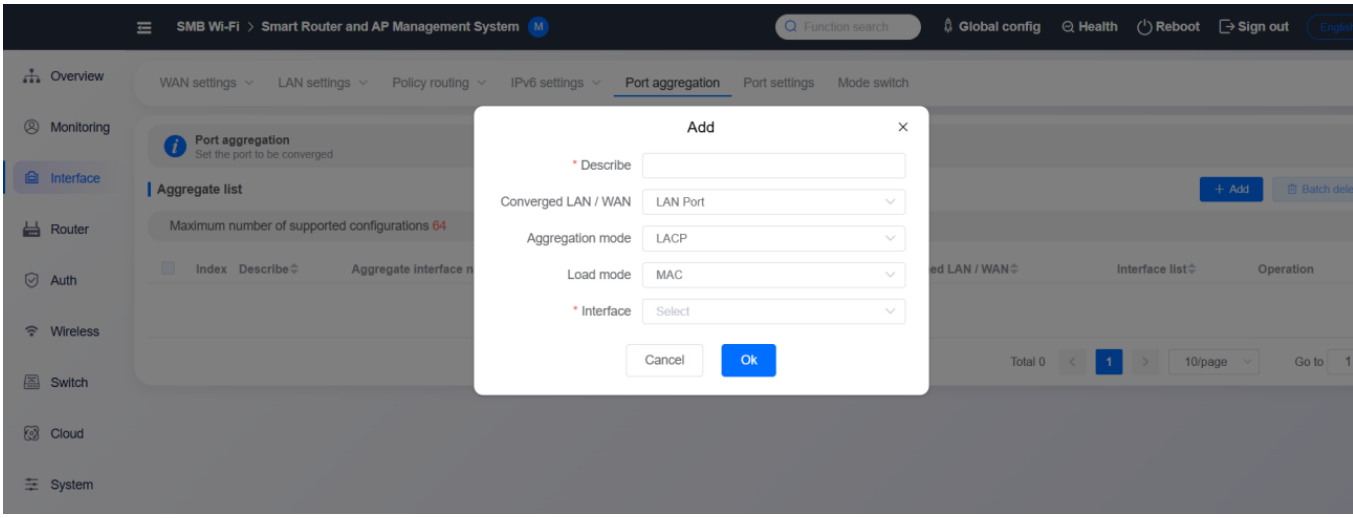
3.5 Port aggregation

Set the ports to be aggregated .

Aggregate list

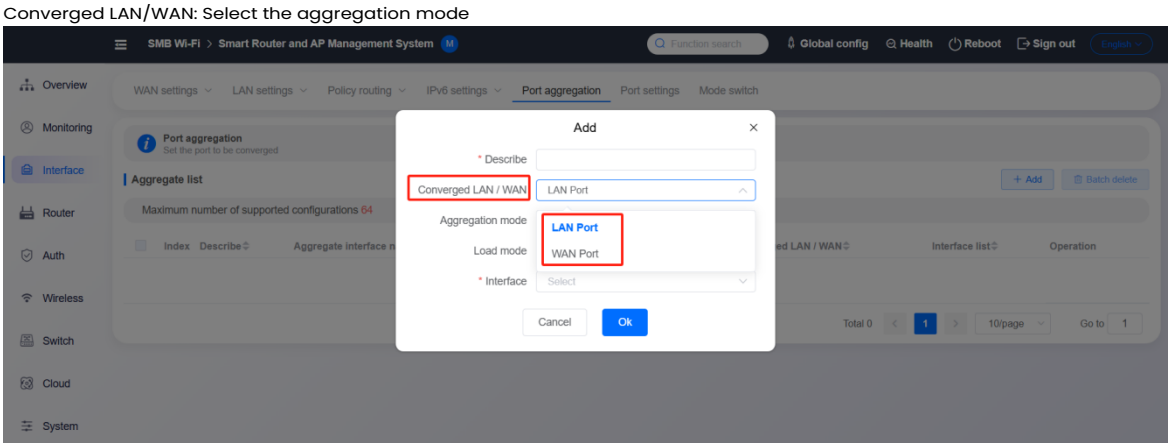
Display the added port aggregation list

Add

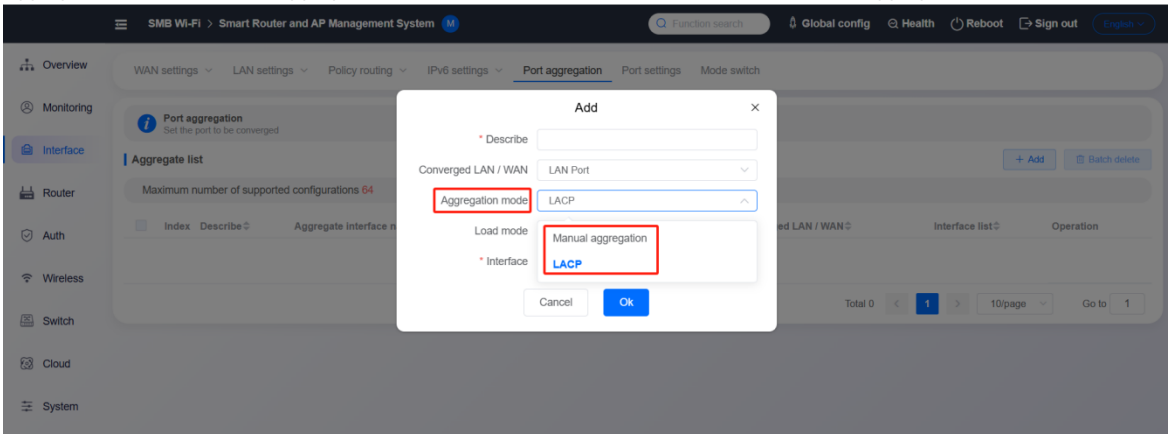


Describe: Make a note on this aggregation rule;

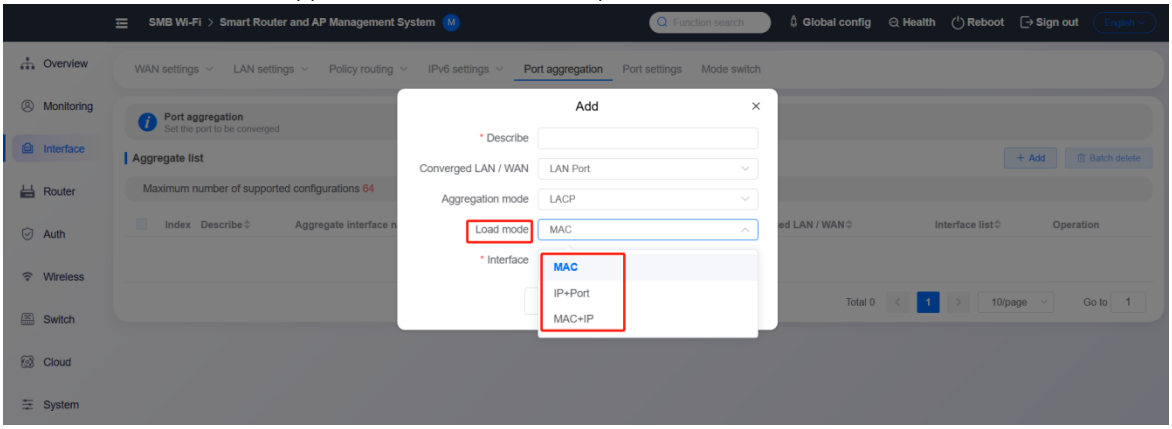
Converged LAN/WAN: Select the aggregation mode



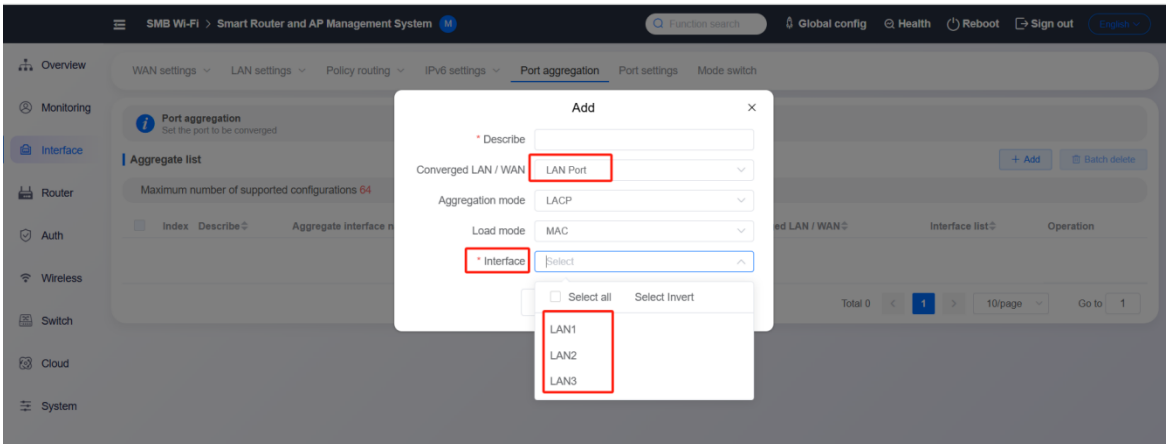
Aggregation mode: Select the aggregation mode, there are two modes to choose from: manual aggregation and LACP;



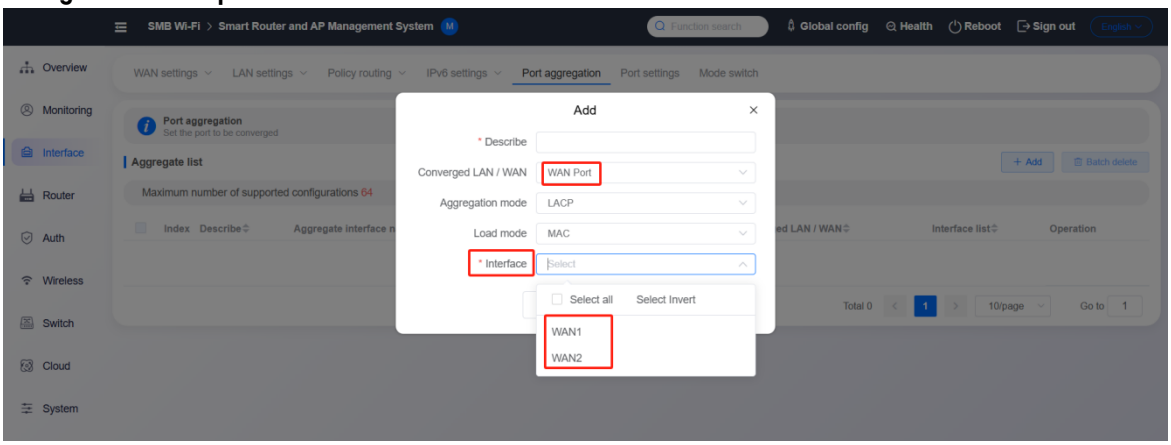
Load mode: Load mode currently provides three modes: MAC, IP+port and MAC+IP;



Interface: Select the corresponding aggregate interface. The interface selection will change with the change of aggregate LAN/WAN port.

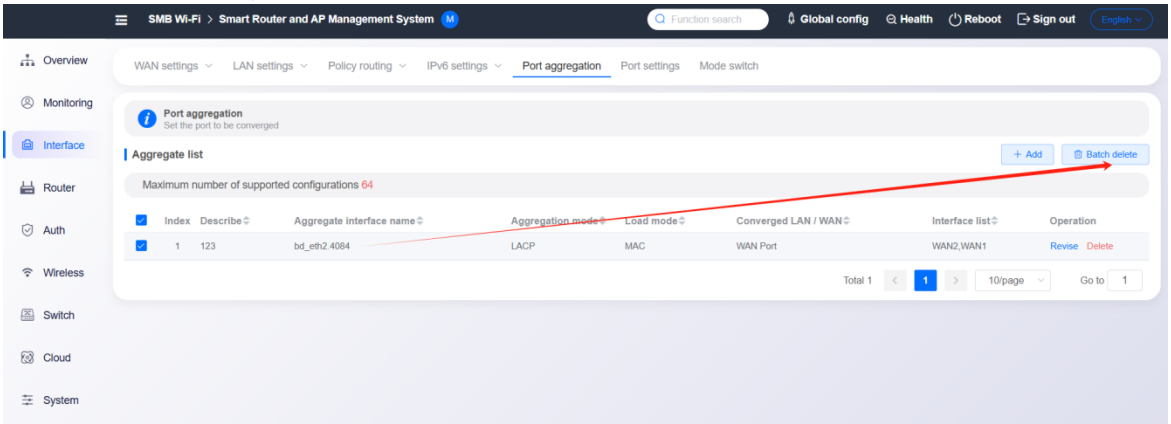


Configuration Examples



After the configuration is complete, the device interface will automatically restart.

Batch delete: After selecting the rules, you can delete the rules in batches;

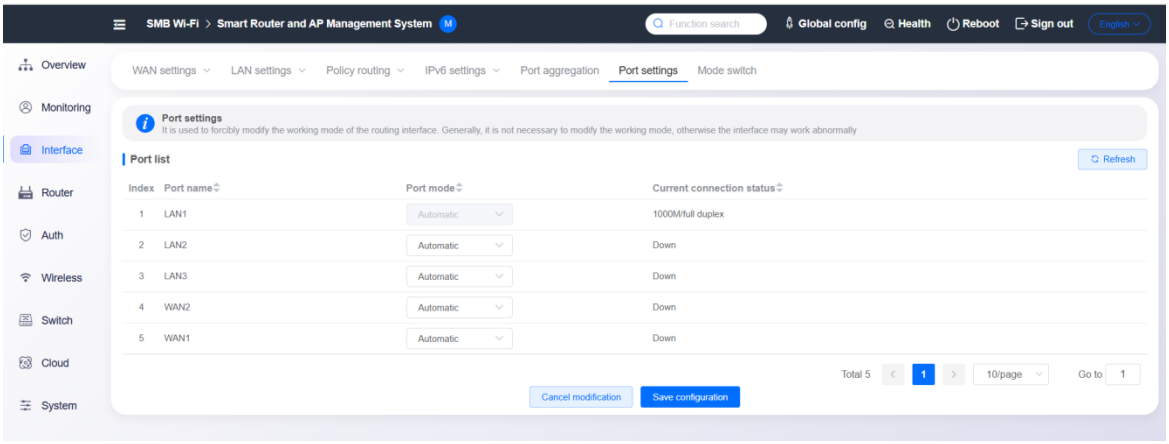


Delete: Delete this rule separately;

Modify: Modify this rule separately.

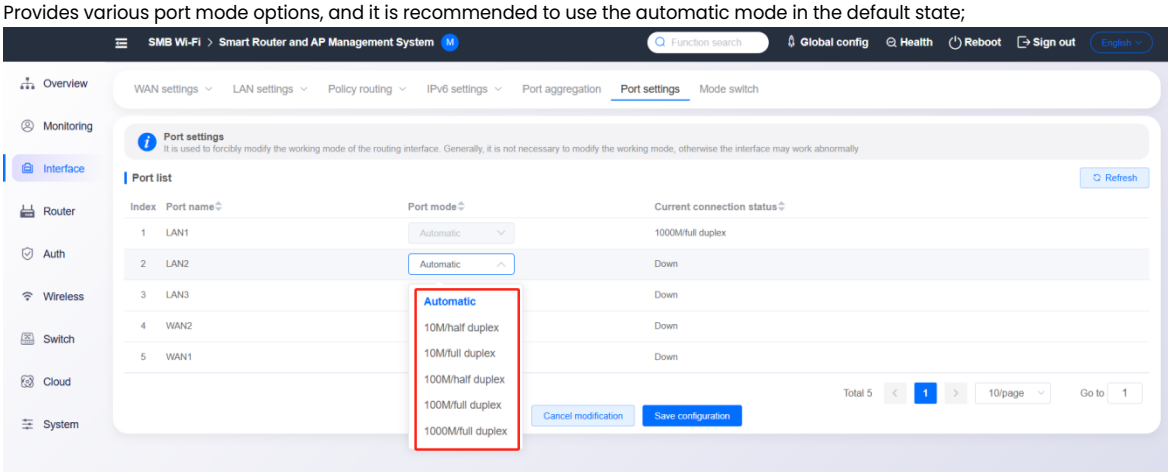
3.6 Port settings

This function is used to forcibly modify the working mode of the routing interface. Generally, the working mode does not need to be modified, otherwise it may cause the interface to work abnormally.



Port list

Provides various port mode options, and it is recommended to use the automatic mode in the default state;



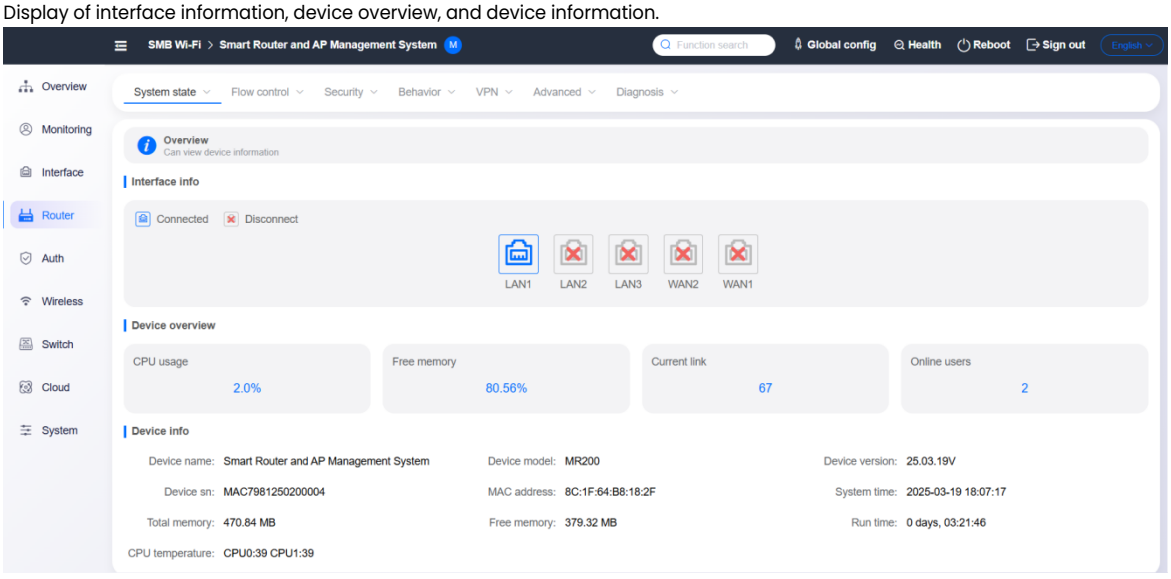
Refresh: You can refresh the negotiated rate and status of the port.

四、 Router

4.1 System state

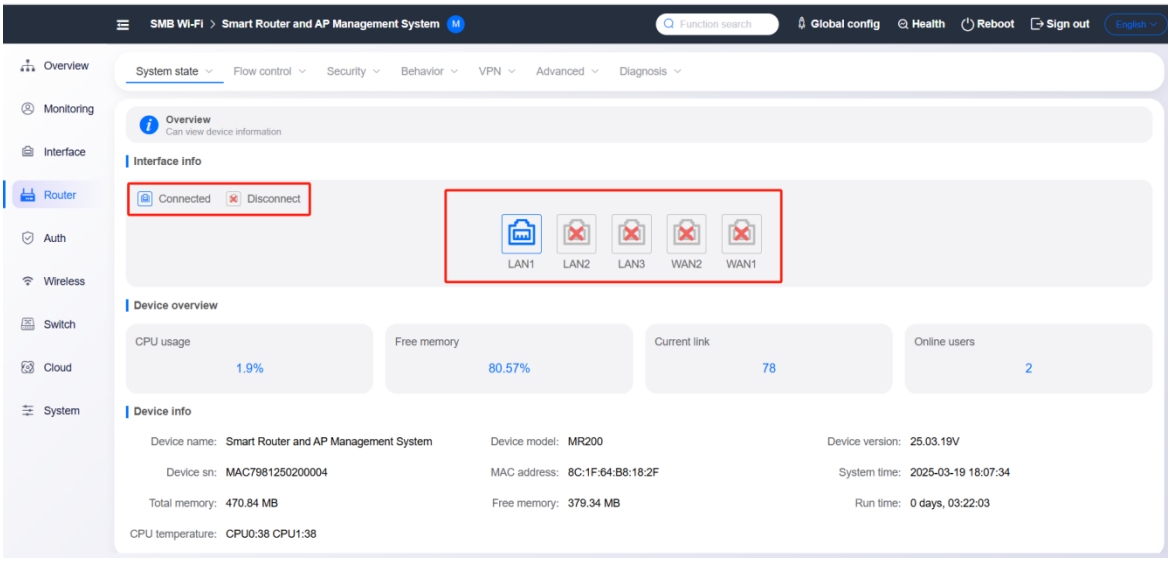
4.1.1 Overview

Display of interface information, device overview, and device information.

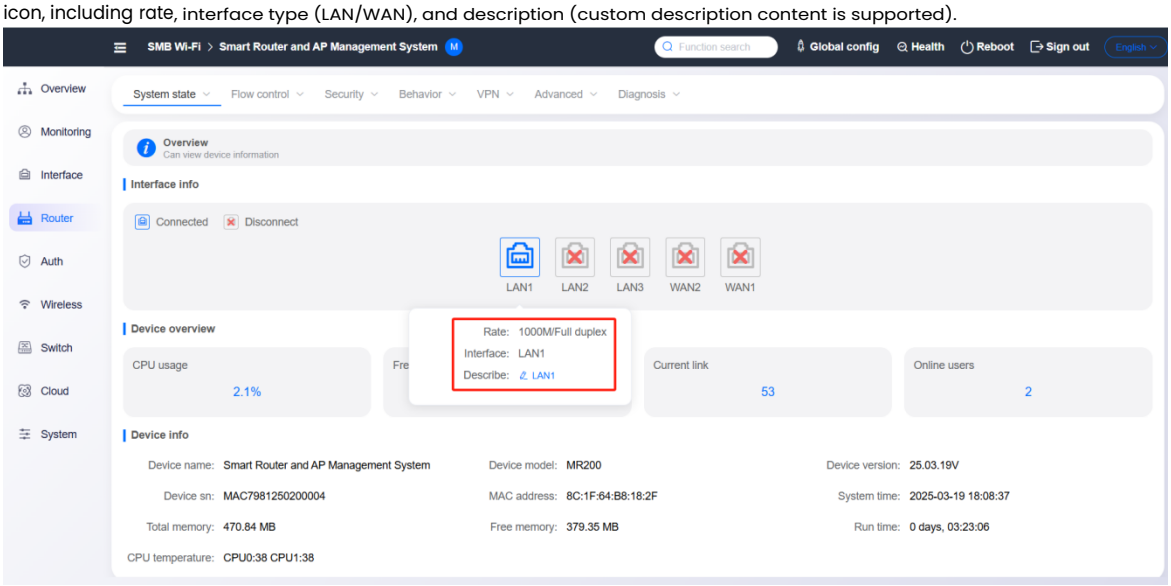


Interface Information

Displays the current connection status of all physical interfaces. A blue interface indicates that the corresponding interface on the device is connected to a network cable, and a gray interface indicates that it is not connected to a network cable.



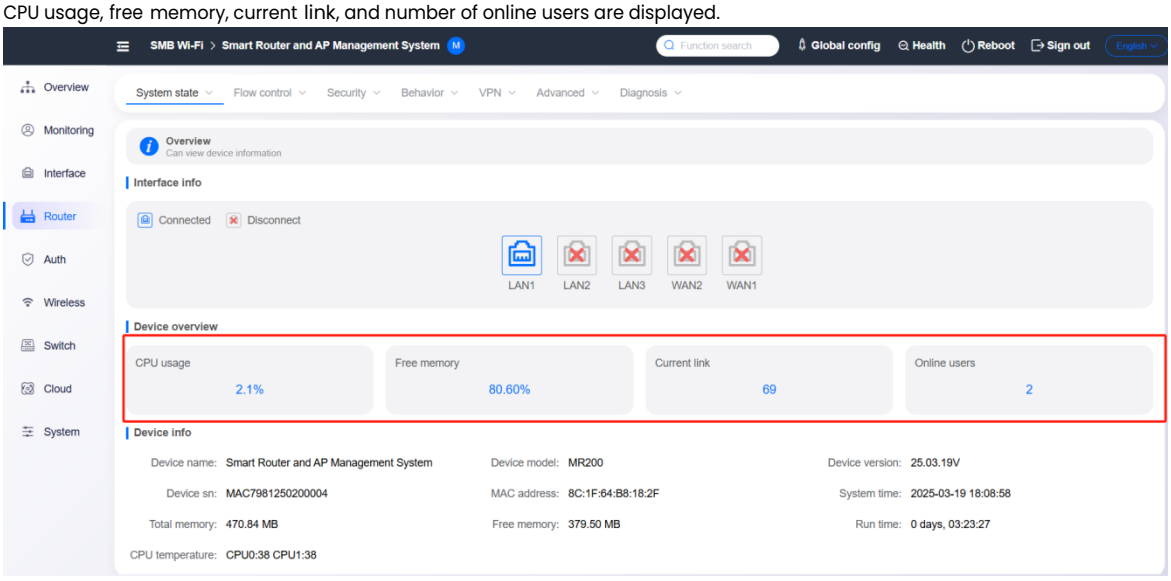
When the mouse points to any network port icon, the basic information of the current network port will be displayed above the icon, including rate, interface type (LAN/WAN), and description (custom description content is supported).



Note: The description of the interface must be 1-8 characters, letters, numbers, and only supports the following symbols in English: _-!@#$%^&*().

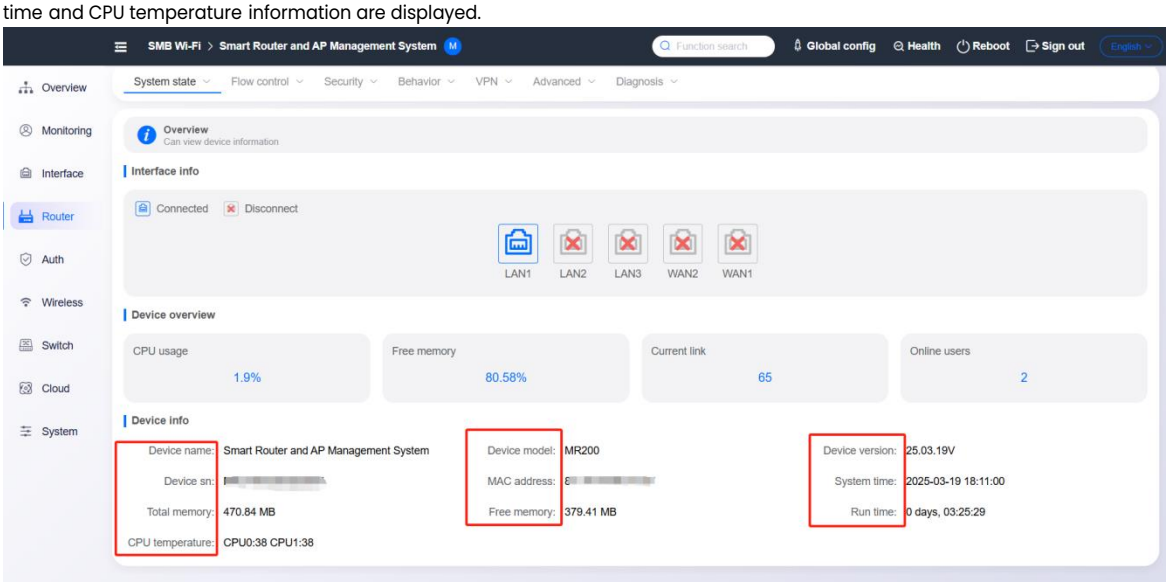
Device Overview

CPU usage, free memory, current link, and number of online users are displayed.



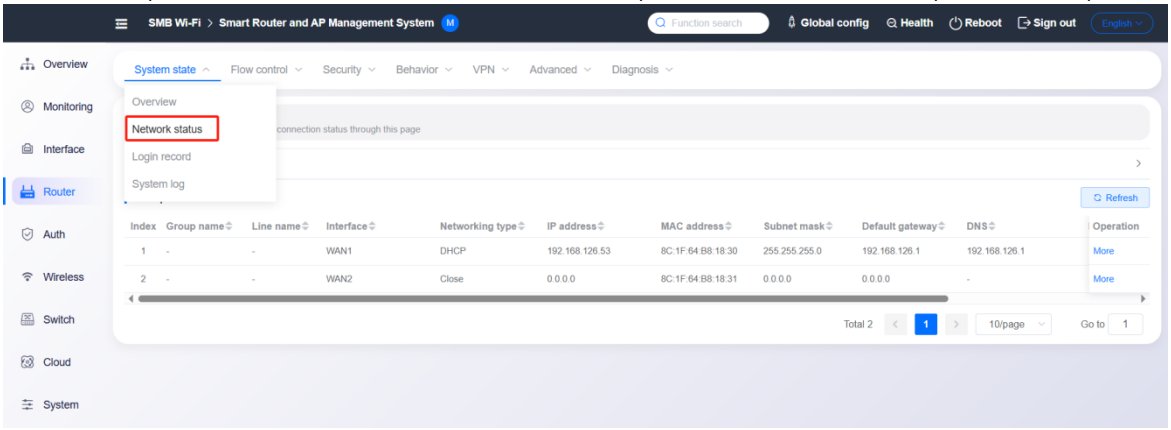
Device Info

Device name, device model, device version, device serial number, MAC address, system time, total memory, free memory, running time and CPU temperature information are displayed.



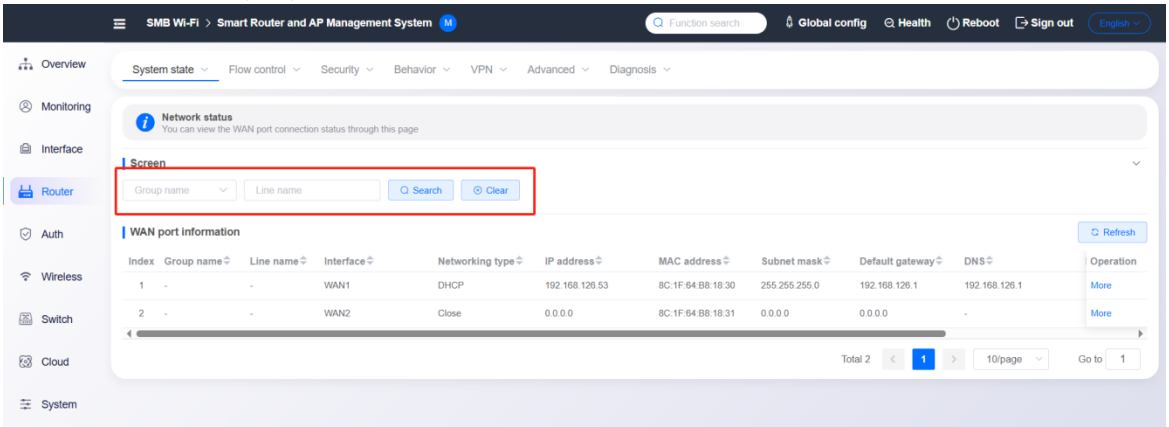
4.1.2 Network Status

Check the WAN port connection status. The network status here mainly refers to the status of the WAN port, 4G and SFP port.



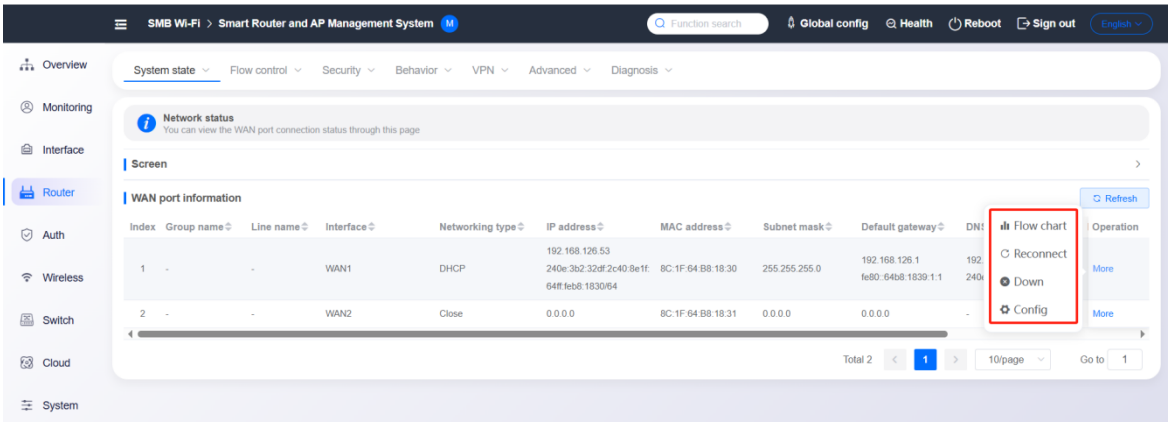
Screen

Perform conditional filtering by group name or line name.

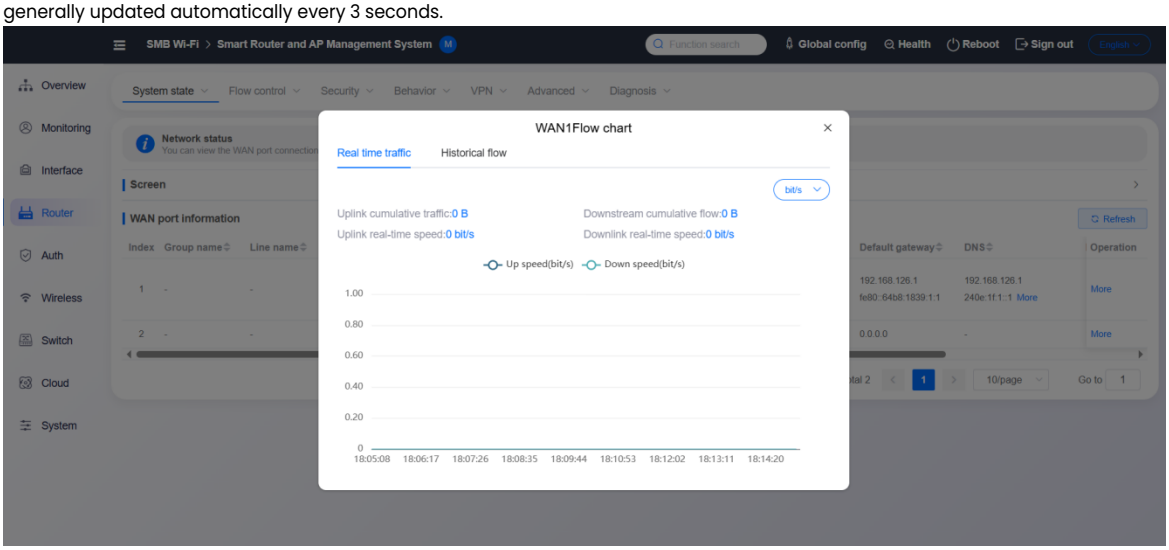


WAN port information

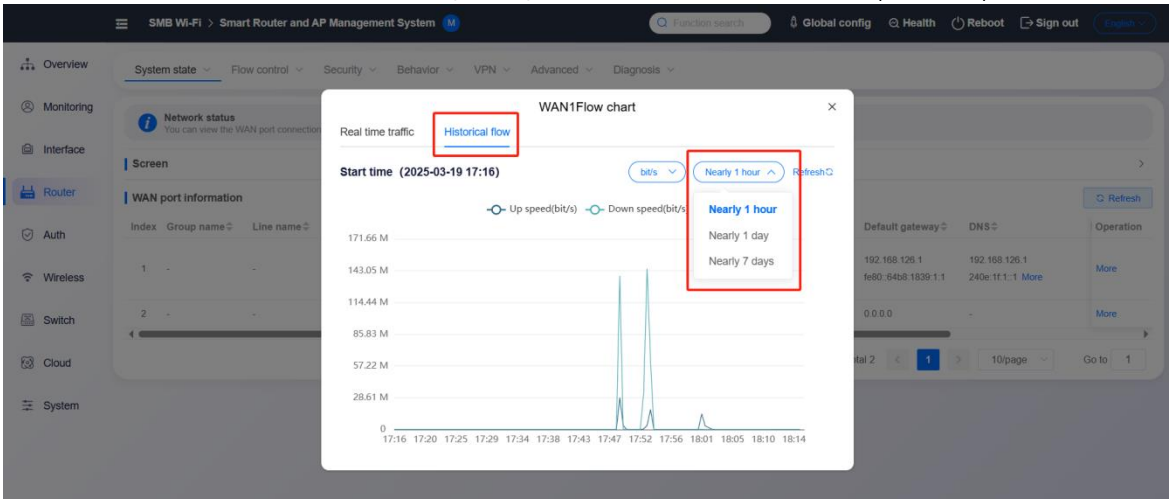
"More" in the list operation column supports viewing or operating the corresponding WAN port.



Traffic Graph: Click "Traffic Graph" to display the current WAN port real-time flow data and discount statistics. The statistics are generally updated automatically every 3 seconds.



Can also view historical traffic statistics, supporting viewing of traffic statistics for the last hour, day , and 7 days;



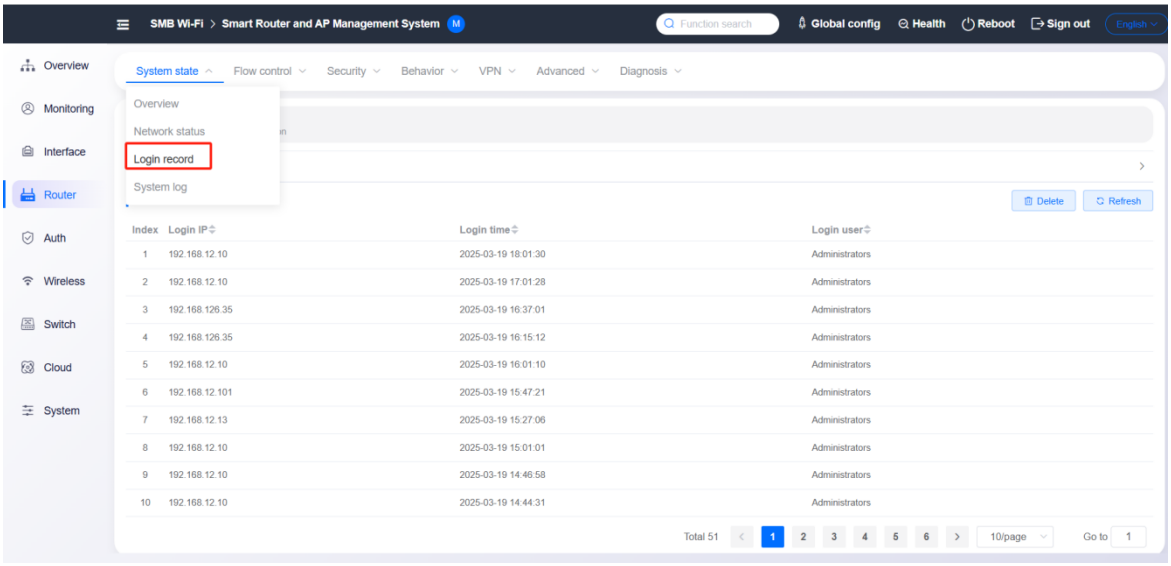
Reconnect: Automatically reconnect immediately after manual disconnection;

Disconnect: After clicking, the connection is disconnected and will not reconnect automatically;

Configuration: Jump immediately to the configuration page of the corresponding WAN port.

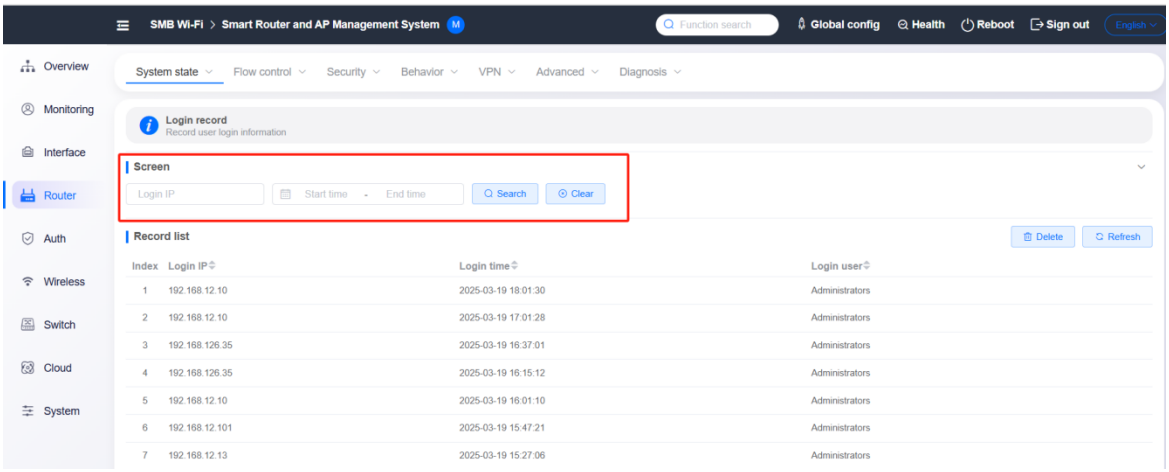
4.1.3 Login Record

Record information of users logging into this router.



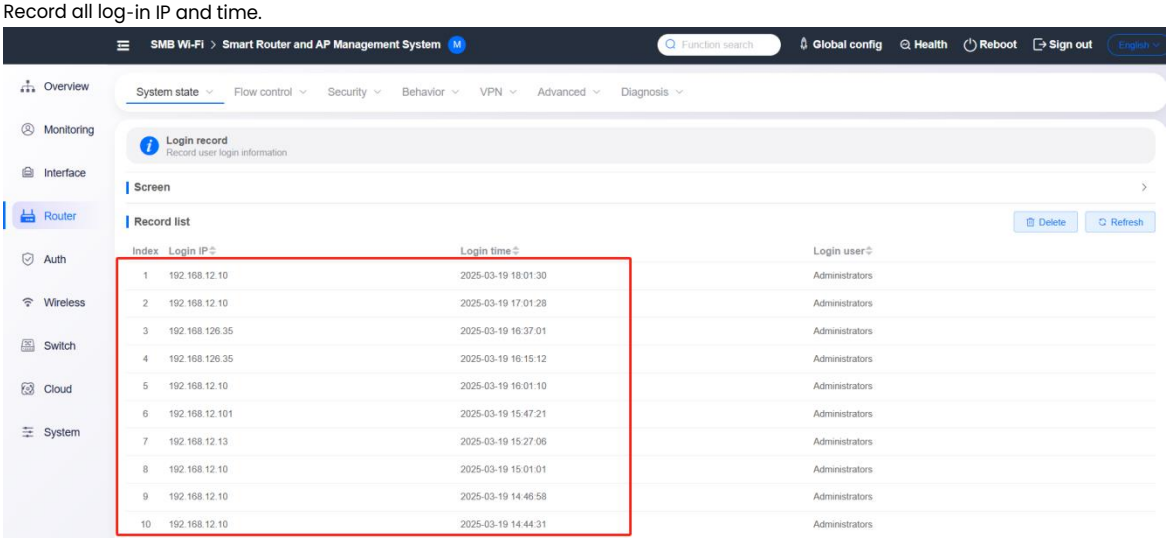
Screen

You can filter by "login IP" or "start time - end time".



Record List

Record all log-in IP and time.

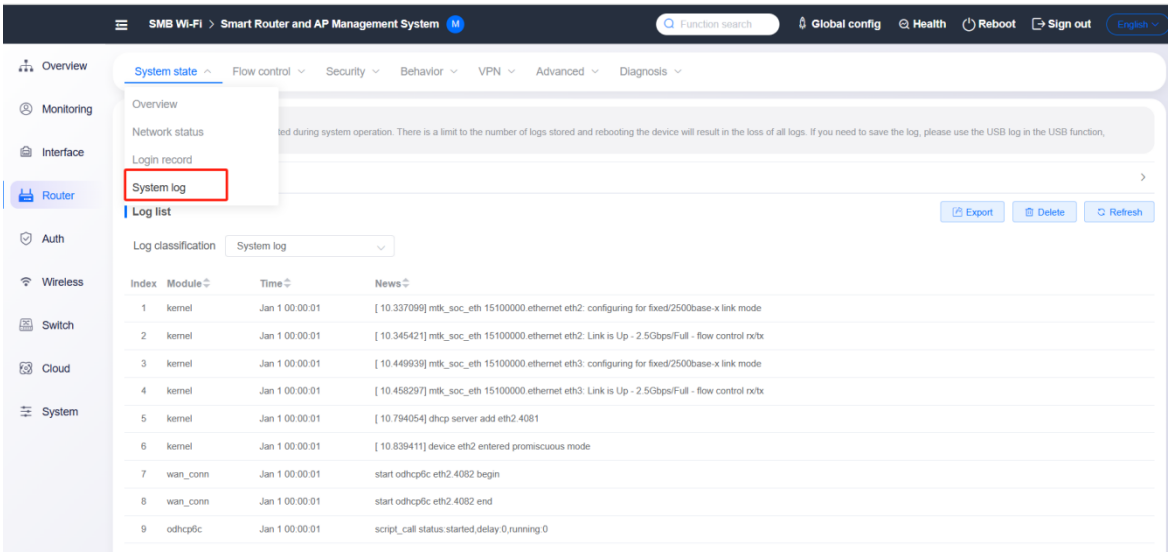


Delete: Clear the record information of other login records except this login;

Refresh: Refresh the list information of login records.

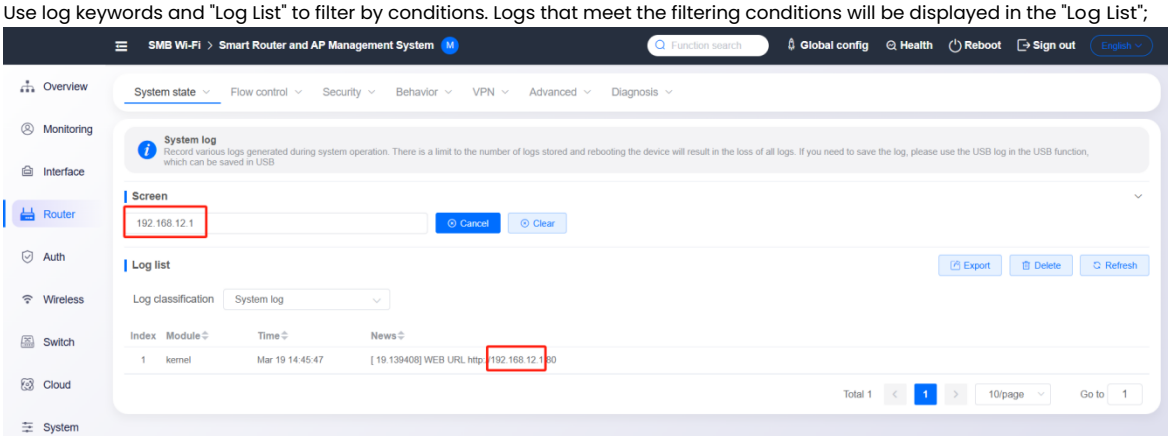
4.1.4 System Log

Records various logs generated during system operation. Log storage is limited in number and all logs will be lost if the device is restarted. If you need to save logs, use the USB log in the USB function to save the logs in the USB if there is USB port on the hardware



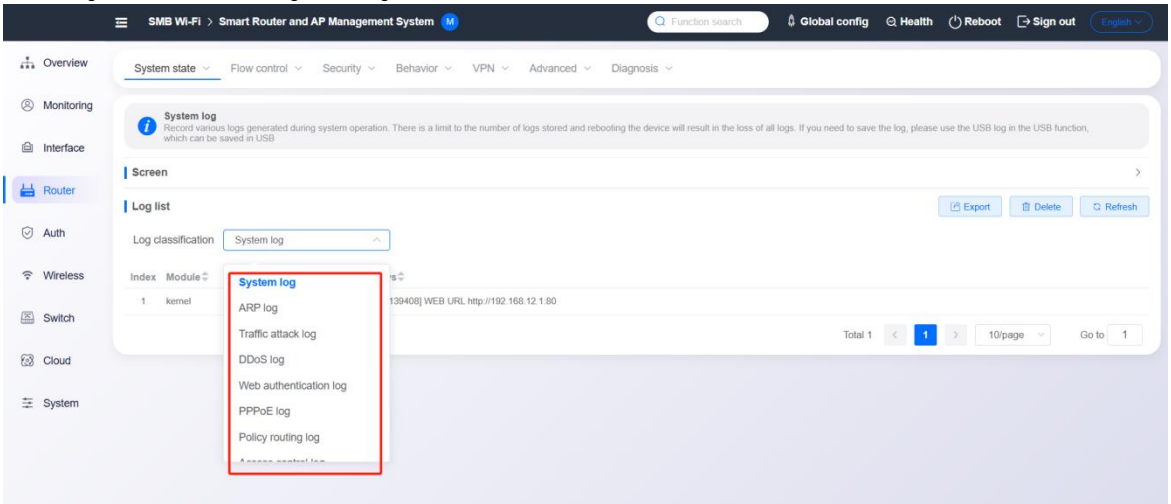
Screen

Use log keywords and "Log List" to filter by conditions. Logs that meet the filtering conditions will be displayed in the "Log List";



Log List

Includes system logs, ARP logs, traffic attack logs, DDoS logs, WEB authentication logs, PPPoE logs, policy routing logs, access control logs and behavior management logs.



Export: Select the log type to be exported and click Export to export the corresponding log;

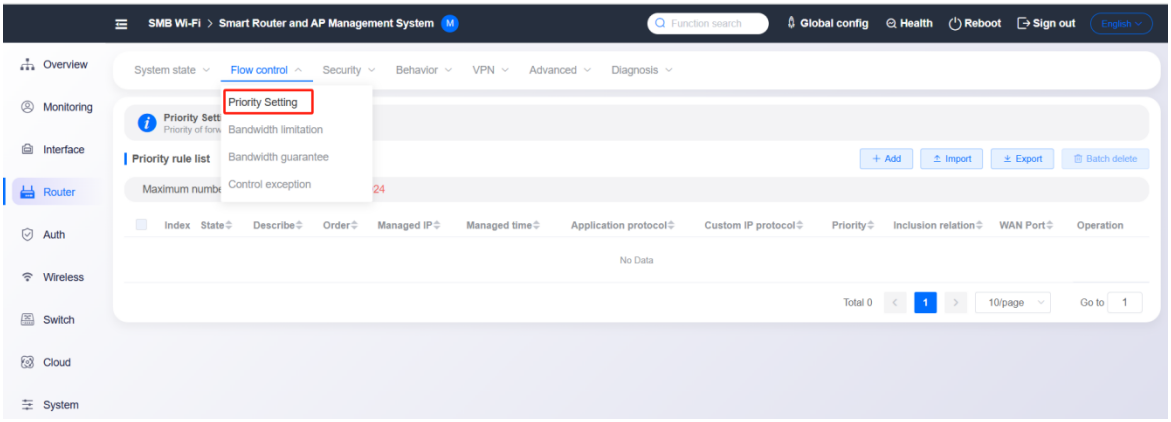
Delete: Select the log type to be deleted and click Delete. The log record will be deleted, but the deleted log cannot be restored.

Refresh: refresh line log record

4.2 Flow Control

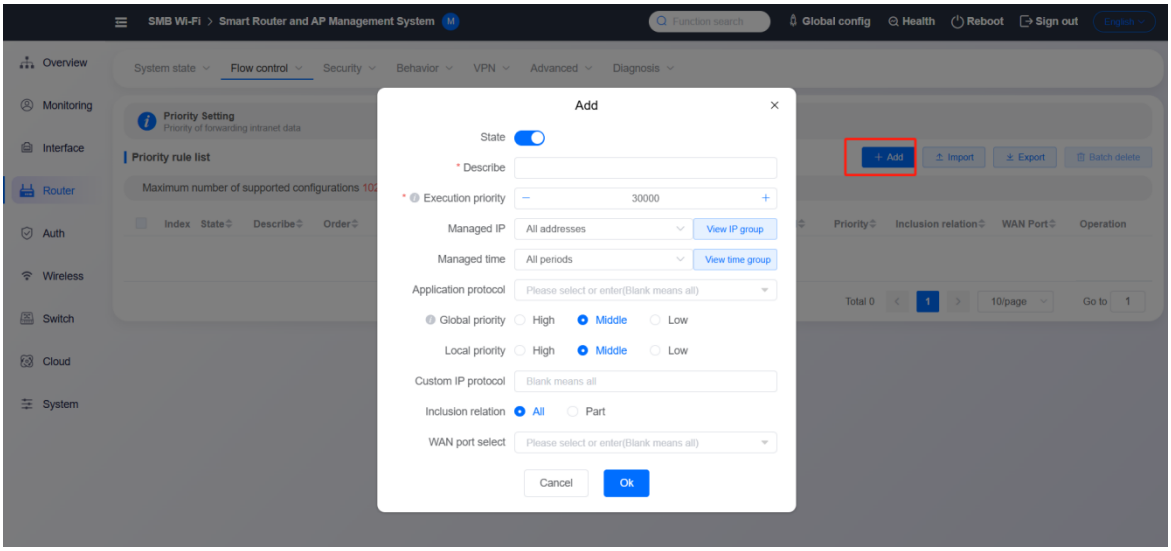
4.2.1 Priority Setting

To forwarding intranet data , mean the priority setting for the system to forward intranet data.



Priority Configuration List

Add: Add rules that require flow control priority as needed ;



State: The flow control priority rules set will take effect after it is turned on, and will become invalid if it is turned off;

Describe: Description of the rule, equivalent to the rule name;

Execution priority: the execution order between rules. The larger the value, the higher the priority.

Managed IP: refers to the IP address, IP segment, or IP group for which this rule needs to take effect.

"All addresses": means that the rule is effective for all global terminals;

"Custom": You need to fill in the IP address or IP segment;

"Address Group": Select the IP segment by selecting IP address group management, and click "View IP group" to add, modify, and delete.

Managed time: the time when the rule takes effect. The time needs to be specific to a certain time period of the week. The priority function will not take effect outside this time period.

"All time periods" : means all time periods;

"Custom": you need to manually fill in the specific time period;

If a time group is added, you can directly select to use it to make it effective. Click "View time group" to add, modify, and delete it.

Application Protocol: You can select different or all application protocols to take effect. The selected application protocols will take effect according to the rules.

Global priority: The priority of the data of this rule in all data in the LAN, high, medium, low. Please use this option with caution, the default is medium;

Local priority: The priority of data processing for this rule among all the data of this host, high, medium, or low;

Custom IP protocol: When priority processing is required for special remote IPs, but there is no corresponding application in the application protocol, the custom IP protocol function can be used;

Inclusion relationship: The inclusion relationship of the protocol.

All, indicating that both the application protocol and the custom protocol are matched successfully and the rule takes effect;

Part, indicating that any priority rule in the application protocol and the custom protocol that matches takes effect immediately;

WAN port selection: Select the WAN port on which the rule will take effect.

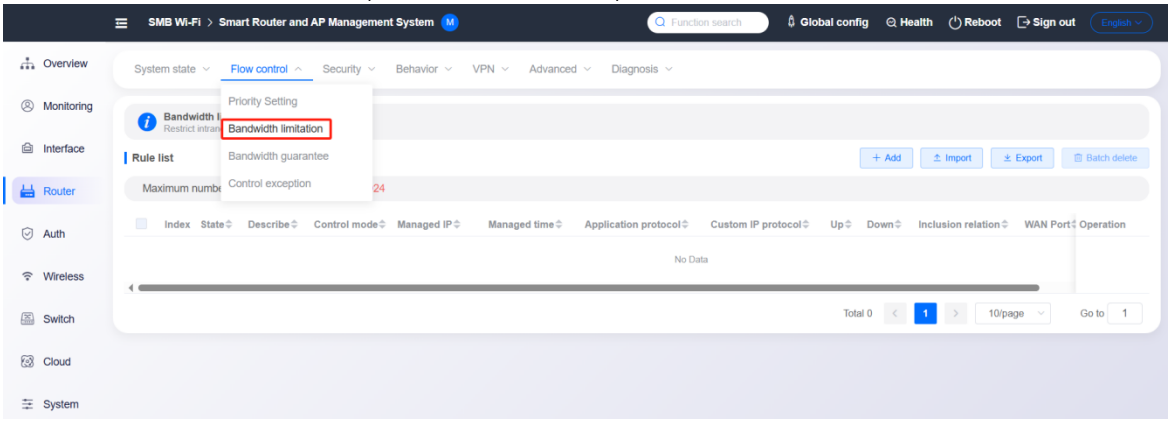
Export: Export all current rules in the priority rule list for use as a backup of the list rules. The exported rules will be directly downloaded to the specified path through the browser and saved;

Import: Import the exported priority rules into the device where they are needed, and use them as list rule recovery;

Batch Delete: Batch delete the rules in the selected rule list.

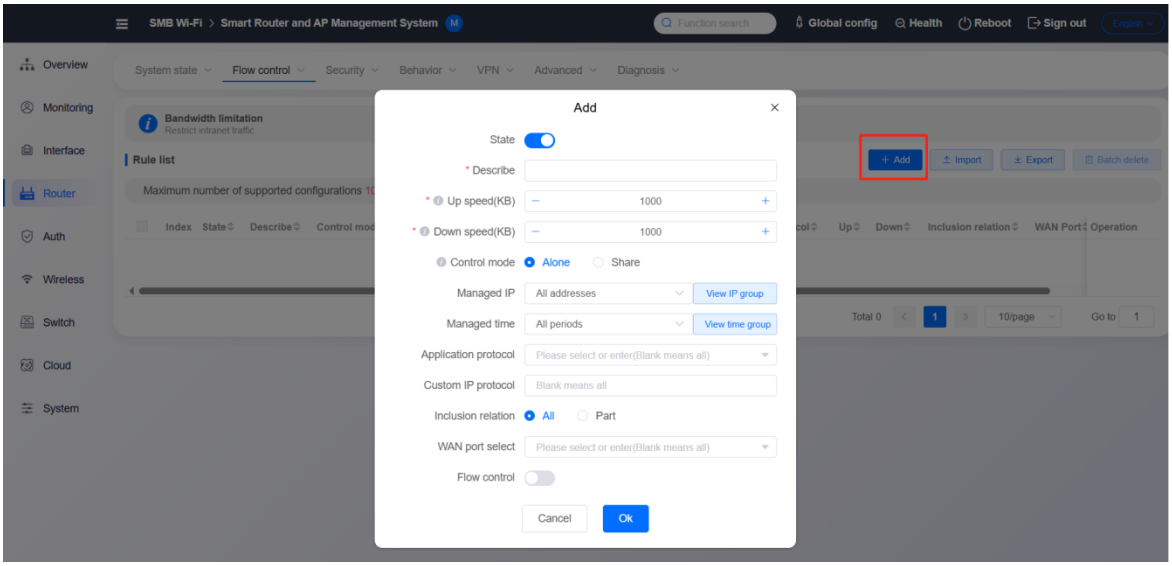
4.2.2 Bandwidth Limitation

Limit the intranet traffic, mean limit the upstream and downstream speeds of intranet terminals.



Route List

Add: Add bandwidth limitation rules;



State: whether the control rule is effective. If it is enabled, it means the rule is effective;

Describe: Description of the rule;

Up speed: The maximum upload speed limit. If it is set to 0, it means no limit;

Down speed: The maximum download speed limit. If it is set to 0, it means no limit.

Control mode:

Alone: The speed of each IP within this range will be limited to the set speed, that is, each IP within the set range will be individually limited;

Share: The total speed of all IPs within this range will be limited to the set speed.

Managed time: the time when the rule takes effect. The time needs to be specific to a certain time period of the week. The speed limit function will not take effect outside this time period.

"All time periods" : means all time periods;

"Custom": you need to manually fill in the specific time period;

If a time group is added, you can directly select to use it to make it effective. Click "View time group" to add, modify, and delete it.

Application Protocol: You can select different or all application protocols to take effect. The selected application protocols will take effect according to the rules.

Custom IP protocol: When priority processing is required for special remote IPs, but there is no corresponding application in the application protocol, the custom IP protocol function can be used;

Inclusion relationship: The inclusion relationship of the protocol.

All, indicating that both the application protocol and the custom protocol are matched successfully and the rule takes effect;

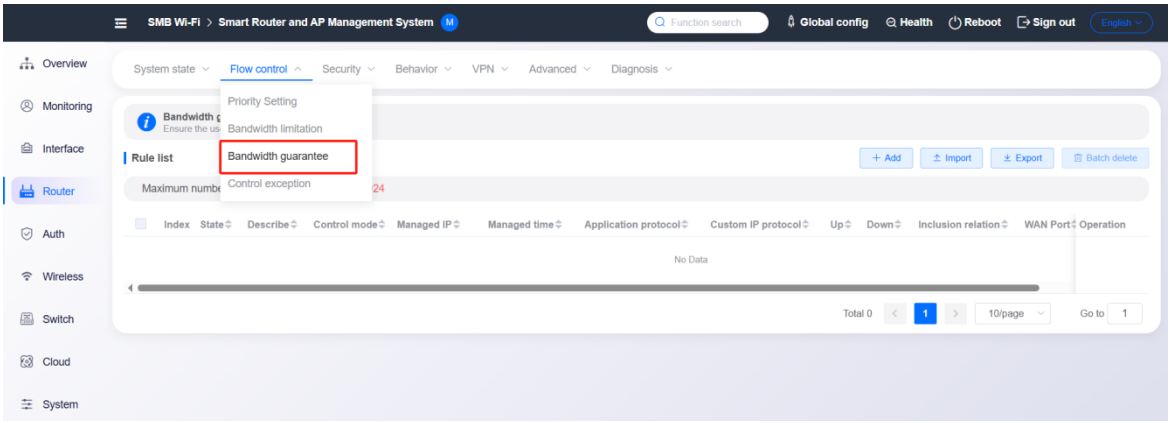
Part, indicating that any priority rule in the application protocol and the custom protocol that matches takes effect immediately;

WAN port select: Select the WAN port on which the rule will take effect.

Flow control: when the total download traffic of the WAN port (if the WAN port is selected in the above rule, it means the traffic of the WAN port; if the WAN port is not selected, it means all WAN ports of the current device) reaches the set percentage, the bandwidth limitation rule will be triggered, and the traffic will be allocated to the terminal according to the upstream and downstream in the rule.

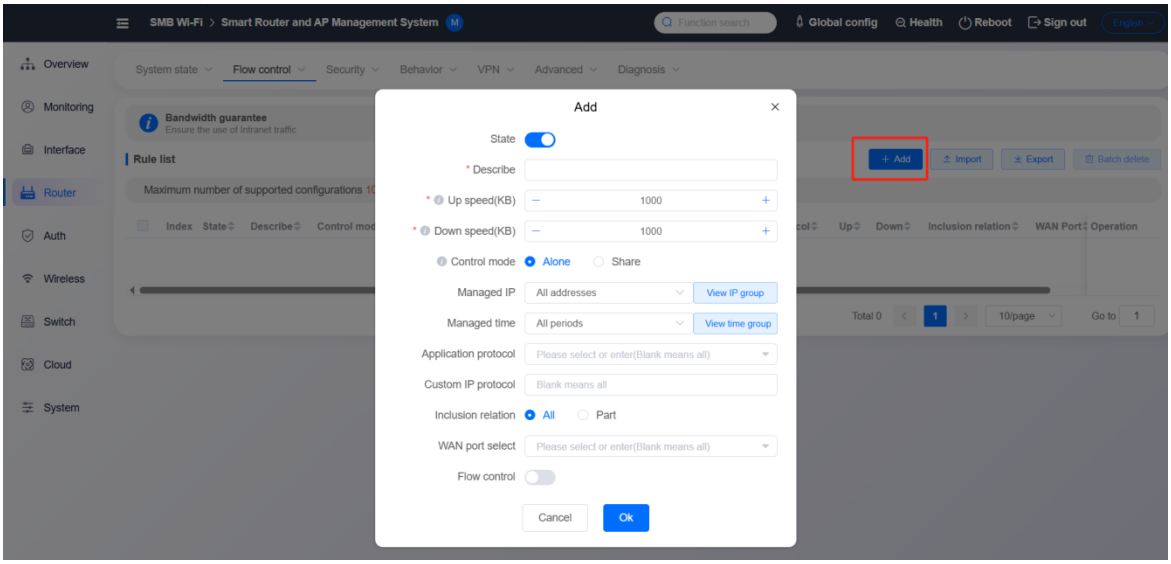
4.2.3 Bandwidth Guarantee

To ensure that the upstream and downstream bandwidths of intranet users are not evenly distributed, can set the bandwidth of a certain terminal or some terminals here.



Route List

Add: Add bandwidth guarantee rules;



State: whether the control rule is effective. If it is checked, it means the rule is effective;

Describe: Description of the rule;

Up speed: minimum guaranteed upload speed. If set to 0, it means no guarantee.

Down speed: The guaranteed value of the minimum download speed. If it is set to 0, it means no guarantee;

Control mode:

Alone: The speed of each IP within this range will be guaranteed to be within the set speed, that is, each IP within the set range is individually guaranteed;

Share: The total speed of all IPs in this range will be guaranteed to be at the set speed.

Managed time: the time when the rule takes effect. The time needs to be specific to a certain time period of the week. The function will not take effect outside this time period.

"All time periods" : means all time periods;

"Custom": you need to manually fill in the specific time period;

If a time group is added, you can directly select to use it to make it effective. Click "View time group" to add, modify, and delete it.

Application Protocol: You can select different or all application protocols to take effect. The selected application protocols will take effect according to the rules.

Custom IP protocol: When priority processing is required for special remote IPs, but there is no corresponding application in the application protocol, the custom IP protocol function can be used;

Inclusion relationship: The inclusion relationship of the protocol.

All, indicating that both the application protocol and the custom protocol are matched successfully and the rule takes effect;

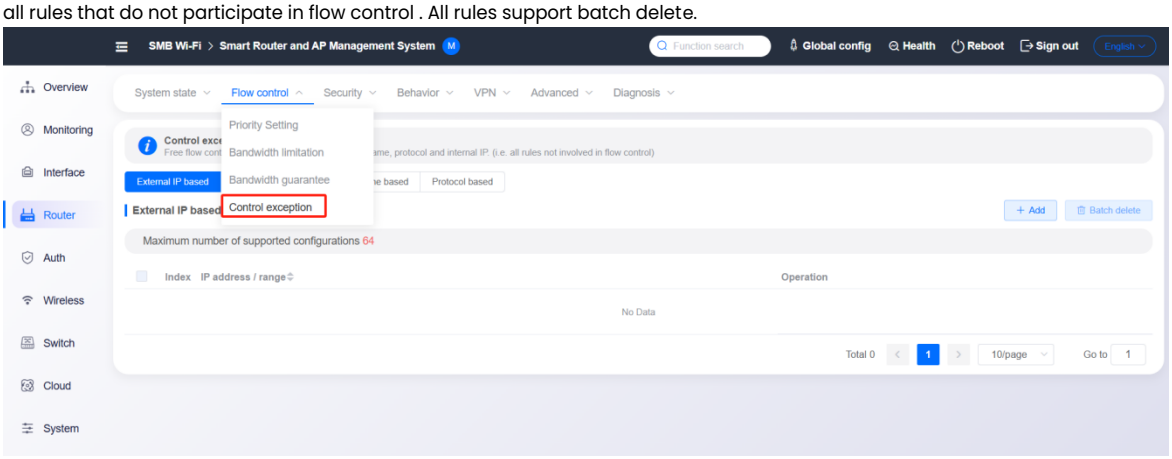
Part, indicating that any priority rule in the application protocol and the custom protocol that matches takes effect immediately;

WAN port selection: Select the WAN port on which the rule will take effect.

Flow control: that is, when the total download traffic of the WAN port (if the WAN port is selected in the above rule, it means the traffic of the WAN port; if the WAN port is not selected, it means all WAN ports of the current device) reaches the set percentage, the bandwidth guarantee rule will be triggered, and the terminal will be guaranteed bandwidth usage according to the upstream and downstream in the rule.

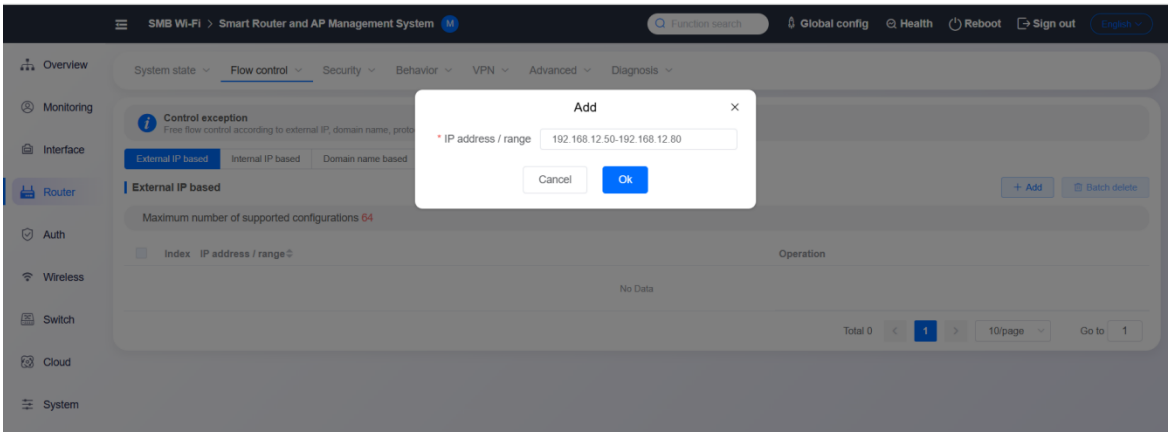
4.2.4 Control Exceptions

Based on bandwidth guarantee and restriction rules, set free flow control rules according to IP, domain name or protocol, that is, all rules that do not participate in flow control . All rules support batch delete.

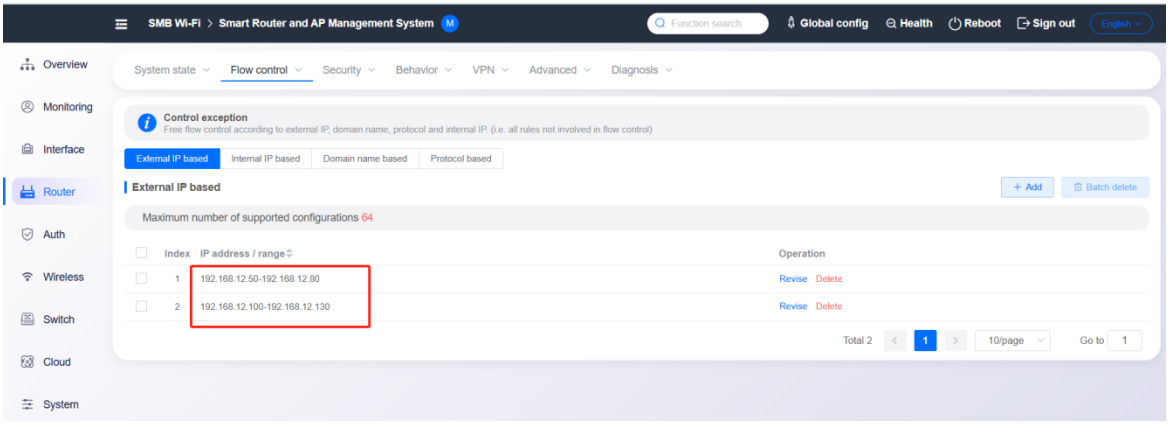


4.2.4.1 External IP based

When the terminal user accesses the set external IP address, the external IP address is not subject to flow control restrictions and guarantee rules. The external IP address setting supports single IP input and IP segment input. If the IP address segment is entered, the segment address needs to be entered from small to large range, otherwise the input fails and the error is as follows:

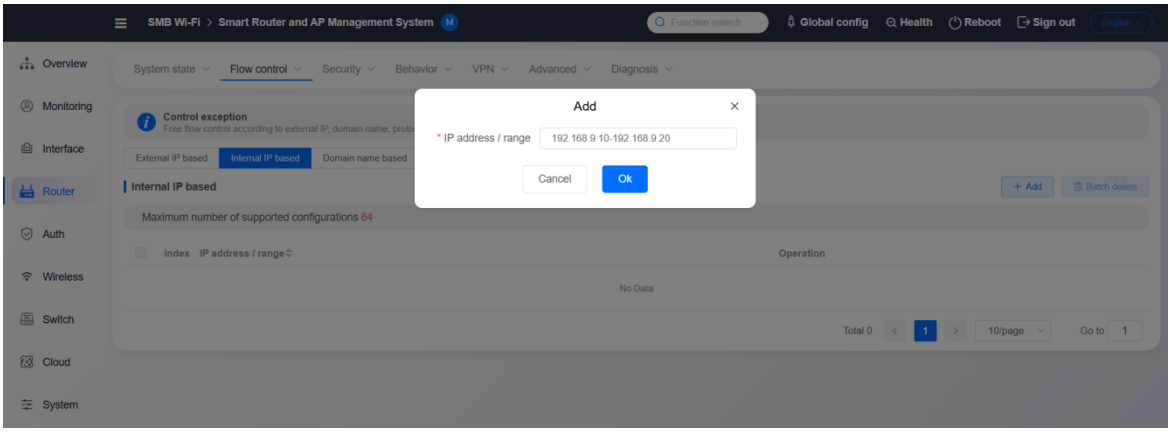


After filling in the address or address segment in the correct format, add it normally. If there are IPs in different segments that need exceptions, just add the rule again.

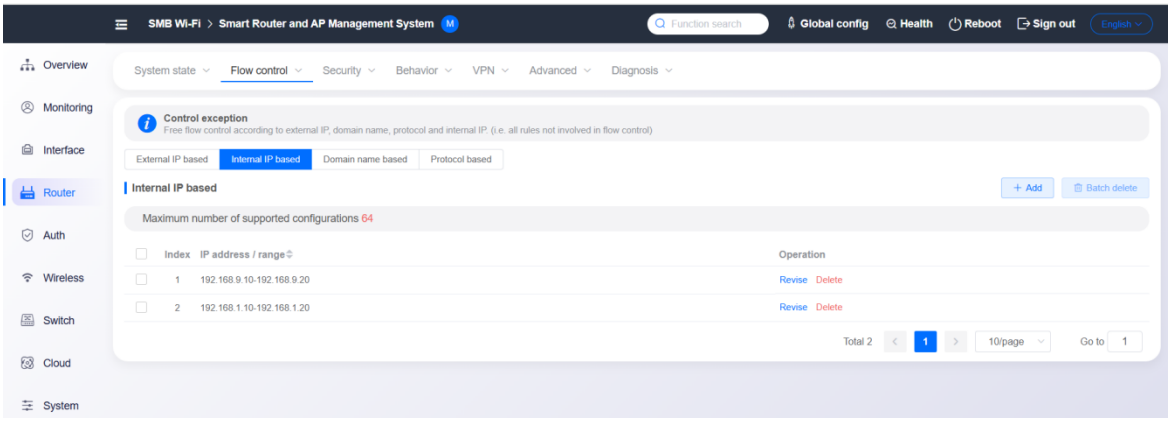


4.2.4.2 Internal IP based

When the terminal user obtains or configures the host IP address, it is not subject to flow control restrictions and guarantee rules, that is, it is not subject to bandwidth restrictions. The internal IP address setting supports single IP input and IP segment input. If the IP address segment is entered, the segment address needs to be entered from small to large range, otherwise the input fails and the error is as follows:

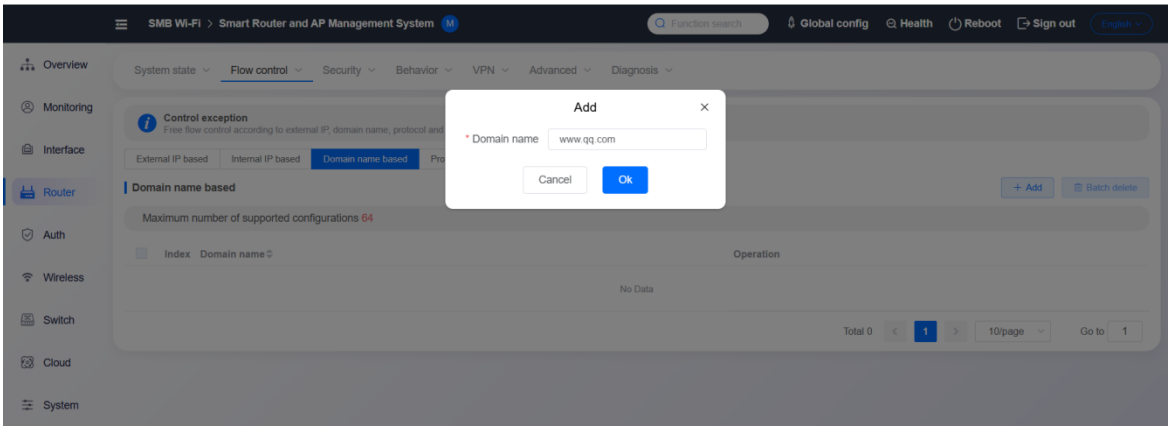


After filling in the address or address segment in the correct format, add it normally. If there are IPs in different segments that need exceptions, just add the rule again.



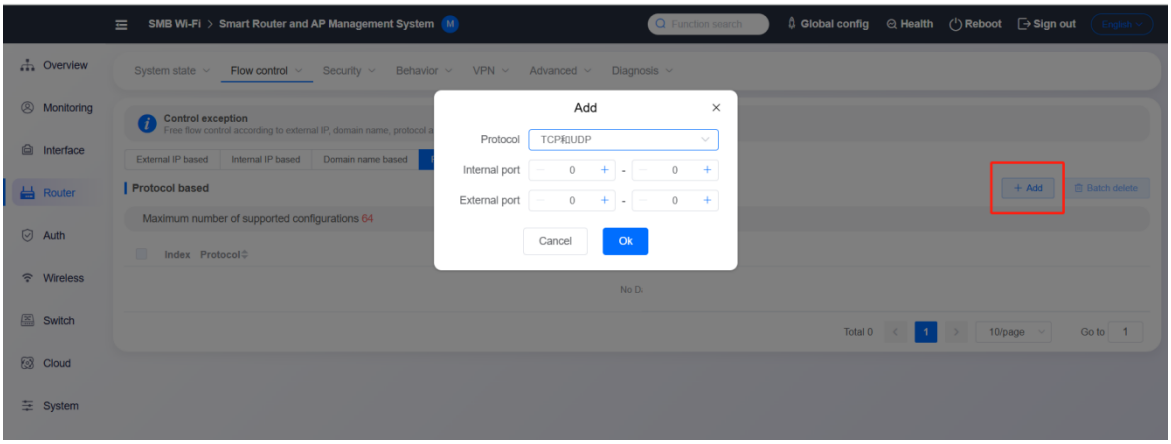
4.2.4.3 Domain name based

Make exceptions to the flow control rules for the remote domain name being accessed . Internal terminals will not be subject to bandwidth restrictions and bandwidth guarantees when accessing the domain name filled in here. The domain name format rules must be met when filling in the domain name. IP addresses or address formats that do not meet the domain name writing rules will not take effect.



4.2.4.4 Protocol-based

Flow control exceptions are made based on the protocol type + port method . Similarly, internal terminals are not subject to bandwidth restrictions and guarantee rule restrictions when accessing corresponding protocol content.

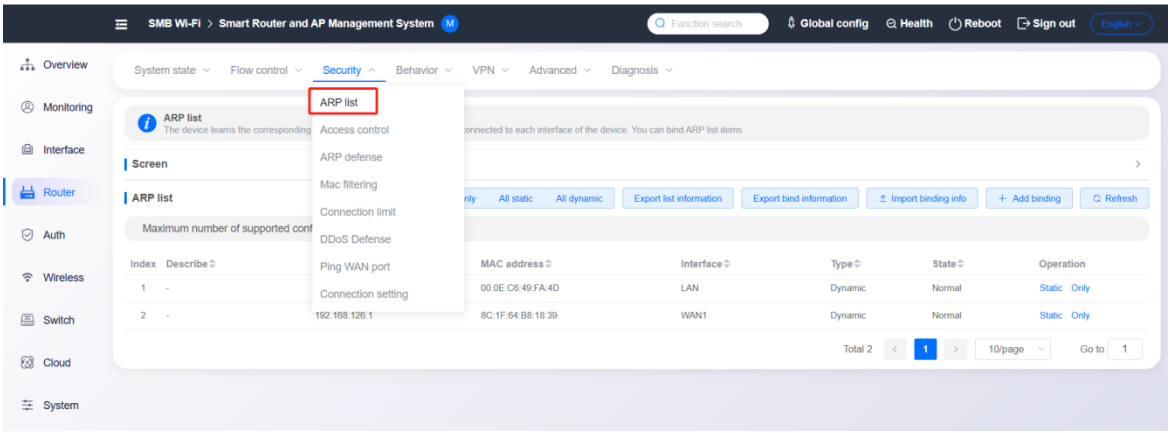


4.3 Security

Device security rules are set to prevent the device from automatically enabling defense mechanisms when encountering DDoS attacks during operation in a network environment.

4.3.1 ARP list

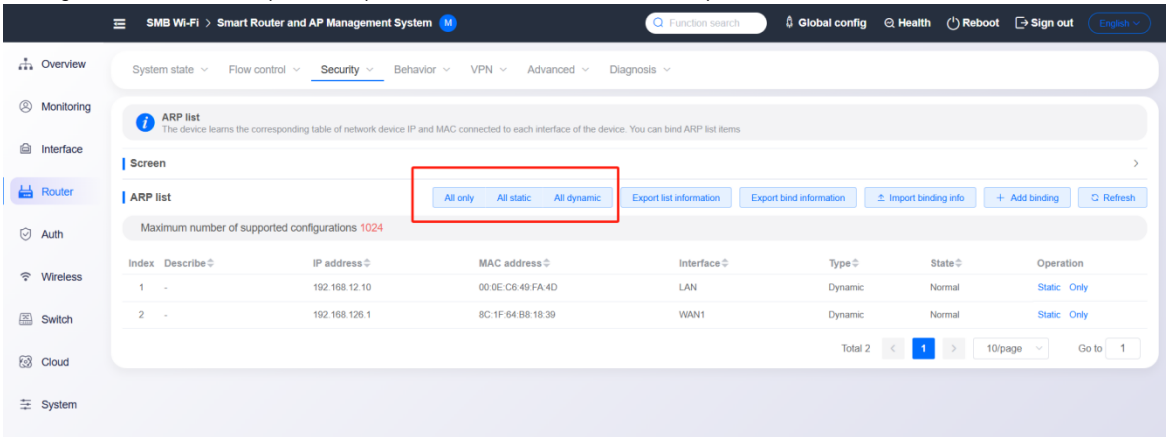
The device learns the IP and MAC correspondence table of the network devices connected to each interface of the device, and can bind the ARP list items .



Generally, all terminals in the intranet and the current WAN port will be displayed in the ARP list.

Screen

If you need to bind a certain IP statically, uniquely, or unbind it dynamically, you can set it here. If you need to confirm or view the binding status of a certain IP, you can expand the "screen" function and filter by the terminal's IP address or MAC address.

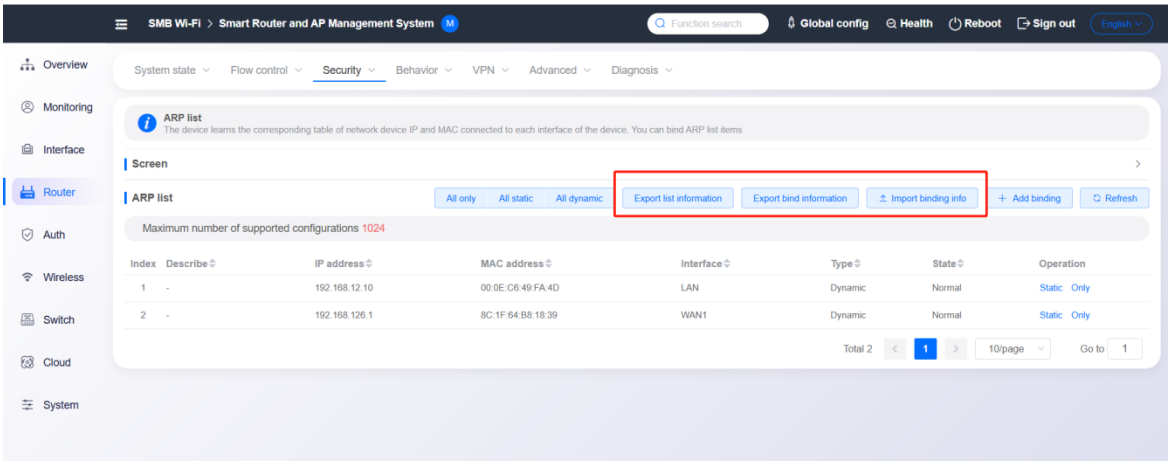


All only: One-click quick binding of all intranet terminal IP and MAC addresses to be unique. For a terminal bound as unique, the device will automatically learn the terminal's current physical MAC address and assigned IP address in the LAN. When the terminal connects to the network again, the device will automatically detect whether the IP obtained by the terminal and the bound MAC are the bound addresses. If any of the IP or MAC does not match the learned address, the terminal cannot use the network normally.

All static: One-click quick binding of all intranet terminal IP and MAC addresses to static. The difference from binding to unique is that when binding to unique, both the terminal's IP and MAC address must be matched successfully. The static mechanism is that

the IP learned by the device can only be used on the MAC terminal bound to it. Even if the terminal's MAC is not assigned to the specified original bound IP, it can still use the network normally, but the bound IP address will not be assigned to other terminals and can only be used on the specified terminal;

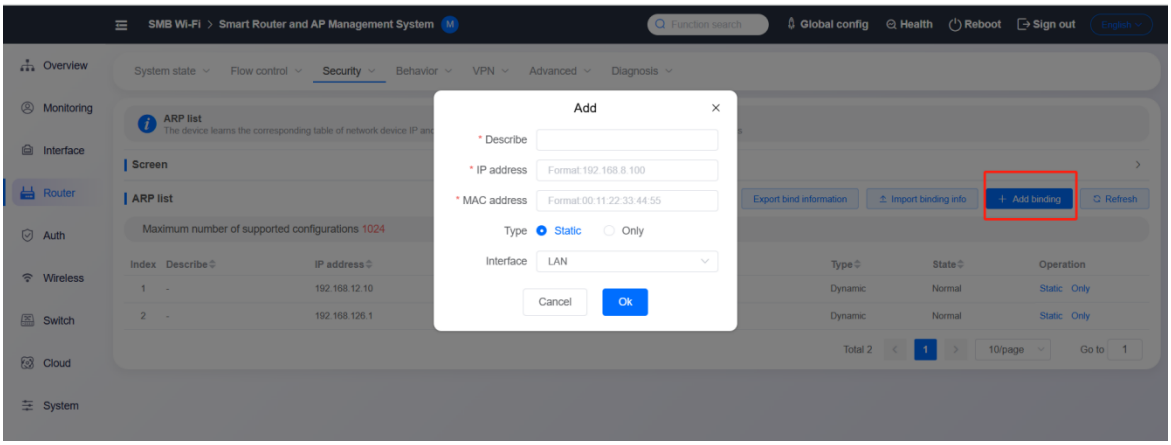
All dynamic: All intranet terminals are dynamic, not affected by MAC and IP addresses, and are based on the addresses assigned by the routing device;



Export list information: All ARP information in the list will be exported, including the ARP information of the WAN port;

Export bind information: Only the ARP binding information in the list is exported separately, generally used for backup;

Import binding information: re-import the backed-up ARP binding information, generally used for recovery;



Add Binding: Manually add an ARP binding address.

Describe: Customize the description content to facilitate differentiation among many rules;

IP address: Fill in the IP address of the terminal to be bound. The address format must follow the IP format, otherwise the input will fail. Please make sure to fill in the address correctly to avoid terminal network failure due to incorrect address filling;

MAC address: Fill in the MAC address of the terminal to be bound. The MAC address must be real and correct;

Type: Select the binding type as only or static. The difference between the two can be found above;

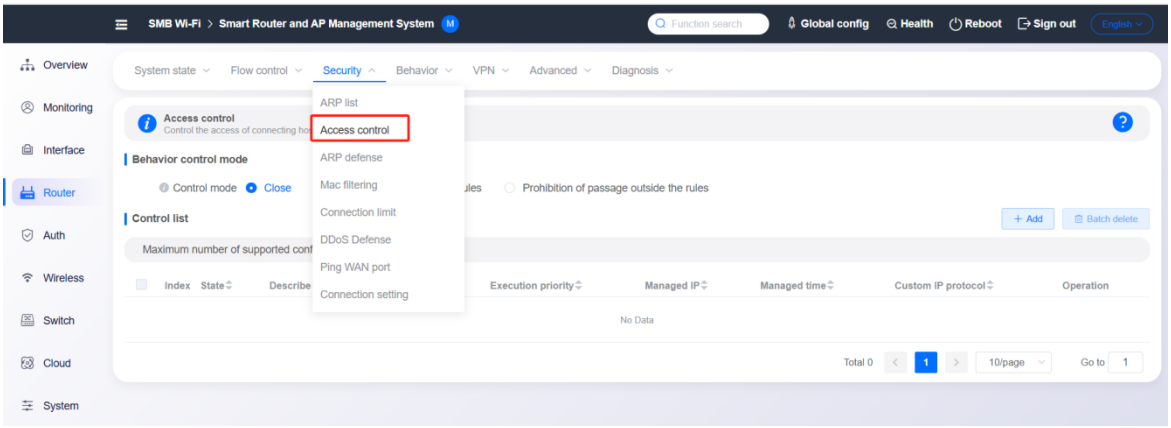
Interface: the bound address interface, LAN or external network, 4G.

ARP List

List of bound or unbound users. The list shows the current or detected terminal information, and you can perform "static", "only" or "dynamic" ARP binding on a terminal. Among them, the detection type terminal refers to a terminal that has been connected to the local area network wireless, disconnected and not connected to other wireless devices.

4.3.2 Access Control

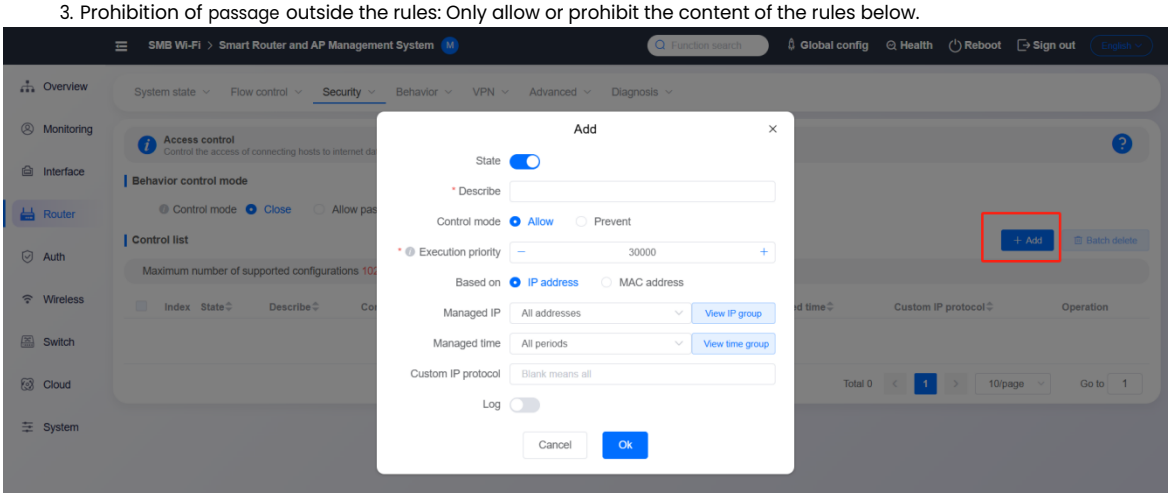
Control whether the terminal can access the external network or can only access certain application protocols.



Behavior control mode

There are three states: close, allowing passage outside the rules, and prohibition of passage outside the rules.

1. Close: If you choose Close, all the rules created below will not take effect;
2. Allow passage outside the rules: All restrictions or applications except those created in the rules below can pass;
3. Prohibition of passage outside the rules: Only allow or prohibit the content of the rules below.



Control List

Add: add specific access control rules, mainly create rules for terminals, applications and control methods;

State: Whether the rule is enabled. If it is enabled here and disabled above, the rule is still disabled.

Describe: Customize the rule name to distinguish it from other rules.

Control method: Allow means the rule content is allowed, and prevent means the rule content is blocked and not allowed to pass.

1. If the above setting is "Allow access outside the rules", selecting "Allow" here means that all access is allowed;
2. If you set "Allow content outside the rules" above, selecting "Prevent" here means that the content of this rule is blocked, and the rest can be used normally (passed);
3. If you set "Prohibition of access outside the rules" above, select "Allow" here to mean that only the content in the rules can be passed, and the rest (terminals or application protocols) cannot be passed;
4. If the above setting is "Prohibit access outside the rules", selecting "Prevent" here means prohibiting all global terminals and protocol access. This situation will also cause all terminals connected to this network to be unable to access the router WEB management page (regardless of wireless or wired), so you must pay attention to the configuration rules.

Execution priority: The execution priority order between rules. The higher the value, the higher the priority. If the priorities are the same, one of them will be executed randomly.

Based on IP address: If the global terminal IP needs to be effective for this rule, select "All addresses"; if you want to control access to some or a certain IP, select "Custom" and fill in a single or a range of IP addresses;

Based on MAC address: that is, create access rules based on the physical MAC address of the terminal. There are currently multiple virtual MACs on the mobile phone (different wireless networks connected to the same device may get different MACs of the terminal, which is a virtual MAC). If you want to achieve complete control access to a certain terminal , please fill in all virtual MACs of the terminal;

Managed time: the time period during which the rule is effective. The rule is not effective outside the set time period.

Application Protocol: Select the application protocol type for access control;

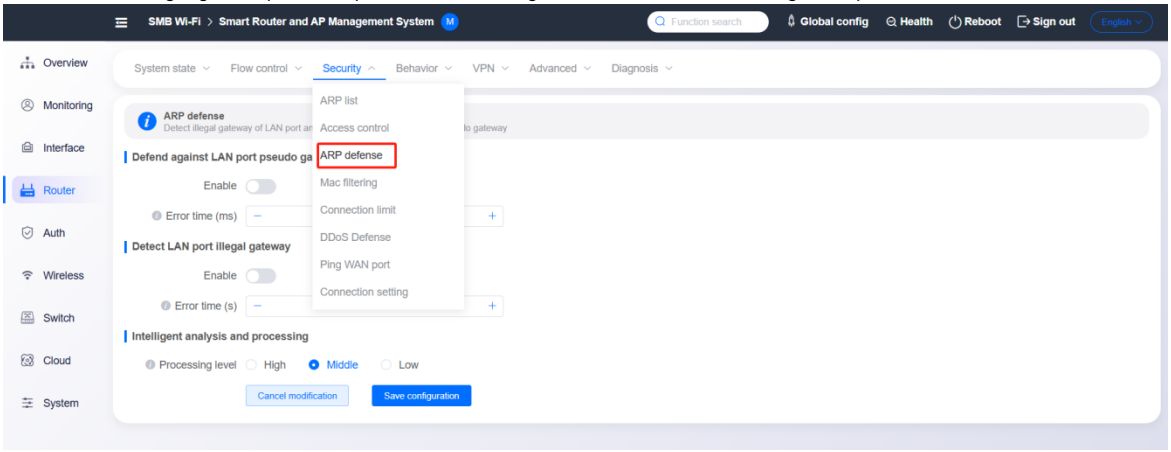
Custom IP address: You can define the remote IP, domain name and port protocol by yourself and use them as the control object;

Log: Enable access control rule logging. When a terminal (user) triggers the rule, the system will automatically record and save the log. If the log tool is turned off, no record will be saved.

Batch Delete: Batch delete the selected list rules.

4.3.3 ARP Defense

Can detect the illegal gateways on LAN ports and defend against ARP attacks from fake gateways.



Defend against LAN port pseudo-gateway ARP attacks

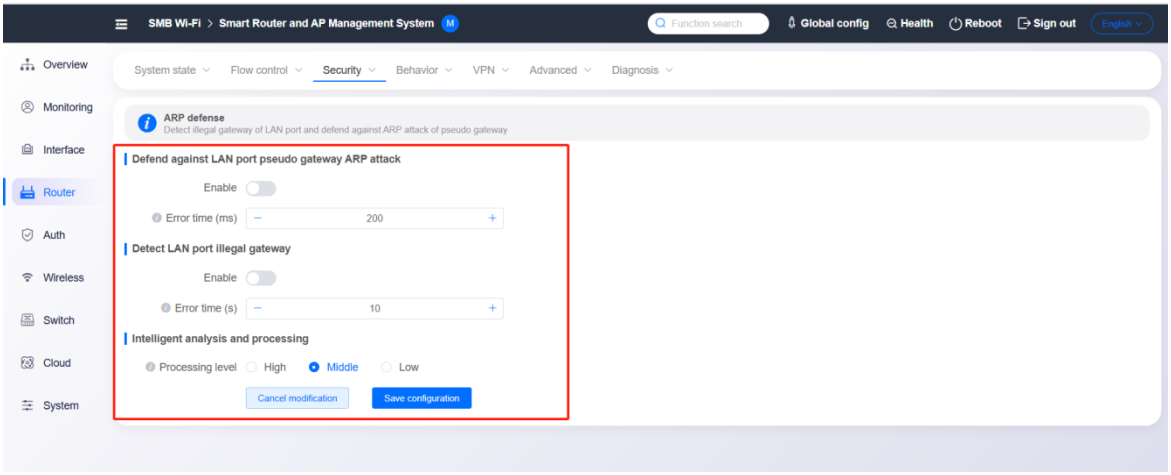
Defense against commonly used ARP attack software! If ARP attack software such as "Network Law Enforcement Officer" and "P2P Terminator" attacks the gateway of other computers, it will be recorded in the "ARP Log" to see whether there is an attack. The default time interval is 200ms.

Detect LAN port illegal gateway

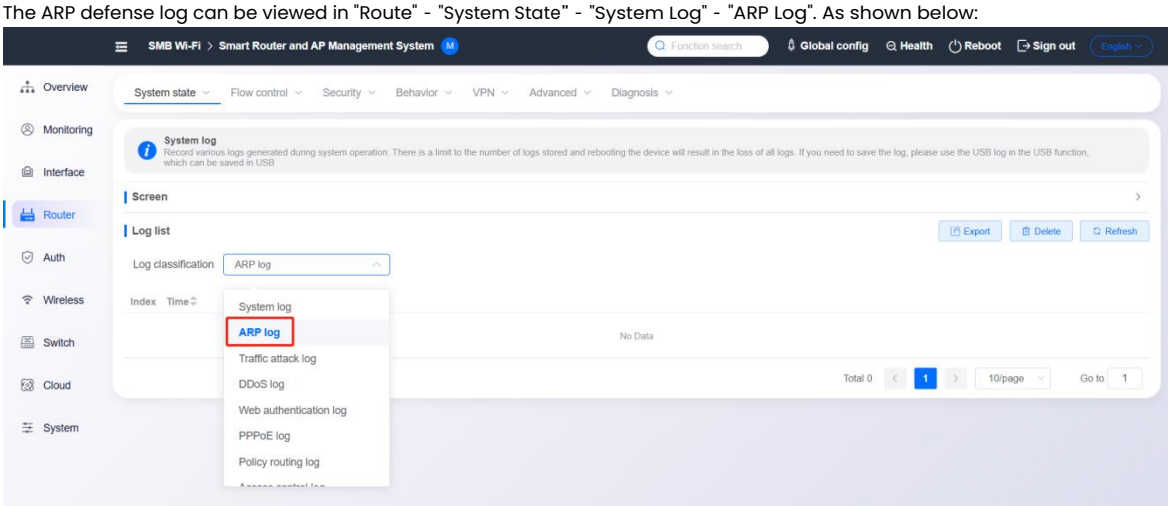
Check whether there is an IP in the intranet that is the same as the LAN IP of the router. If so, it will be recorded in the "ARP log". The default detection time is 10s.

Intelligent analysis and processing

The processing level of this ARP defense system. The higher the level, the safer it is. It can be adjusted according to the network environment.



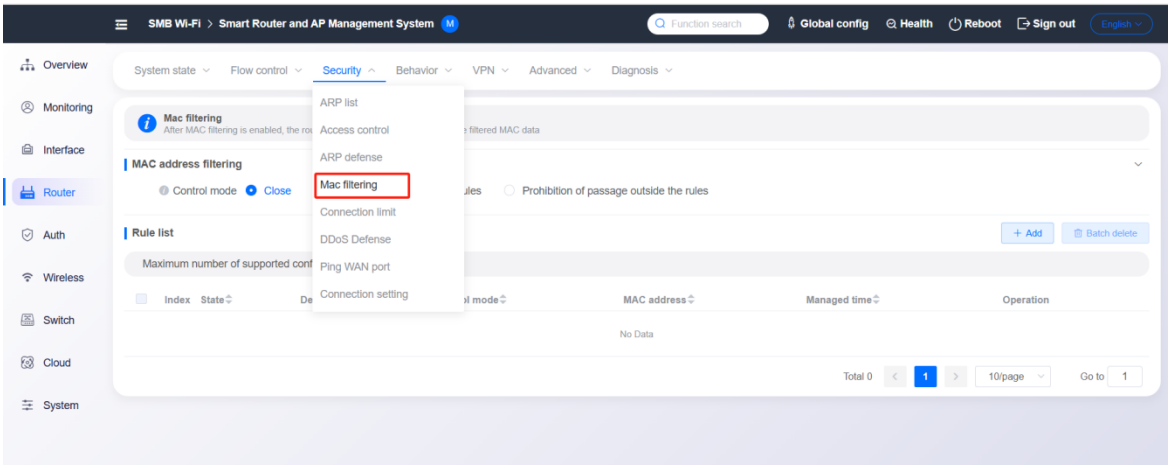
The ARP defense log can be viewed in "Route" - "System State" - "System Log" - "ARP Log". As shown below:



4.3.4 MAC Filtering

By enabling MAC address filtering and setting filtering rules to control the connected host's Internet access, after enabling MAC filtering, the router LAN port will no longer receive filtered MAC data. The most intuitive feeling is that the terminal filtered by

MAC will not be able to obtain an IP address from the router's DHCP, and manually configure a static IP and cannot access the Internet, and also cannot access the router's management interface.



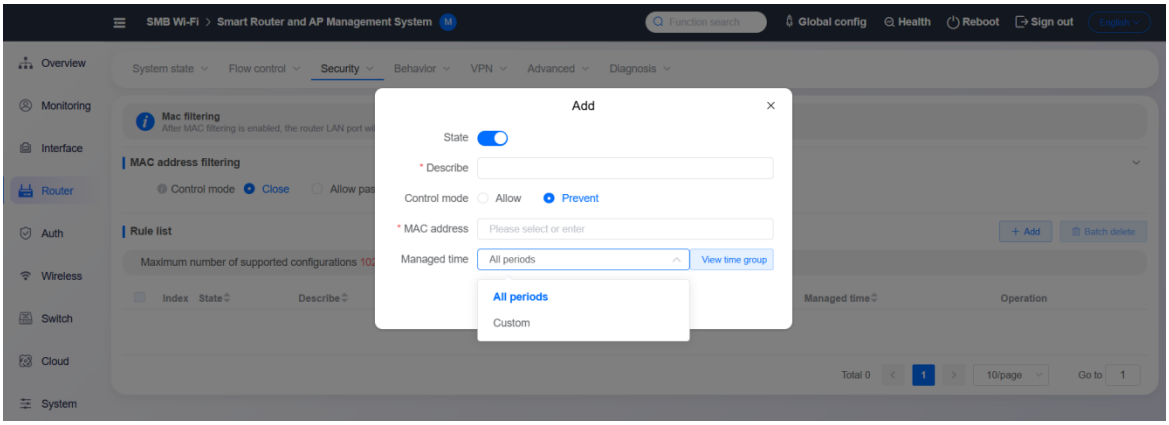
MAC address filtering

Provide 3 type MAC address filtering mode, please choose according to your needs;

1. Close: The filtering rule is off. Regardless of whether the rule is set below or whether the rule is allowed or blocked, MAC filtering will not take effect.

2. Allow the ones outside the rules: The added rules are executed according to the control mode, and the terminal MAC outside the rules is not restricted and passes directly. It is usually used in conjunction with the blocking rules;

3. Prohibition of passage outside the rules: The rules in the list are executed according to the control method. All MAC addresses outside the list will be prohibited from passing. It is generally used in conjunction with the allow rules.



Rule List

Displays the added MAC address filtering rules.

Add: Add MAC filter rule

State: Select whether to enable the rule;

Describe: A brief description of this rule. The default value is default , and it is recommended to change it to something that is easy to identify.

Control mode: divided into two categories: 'allow' and 'prevent'. Users can choose whether to allow this rule to pass;

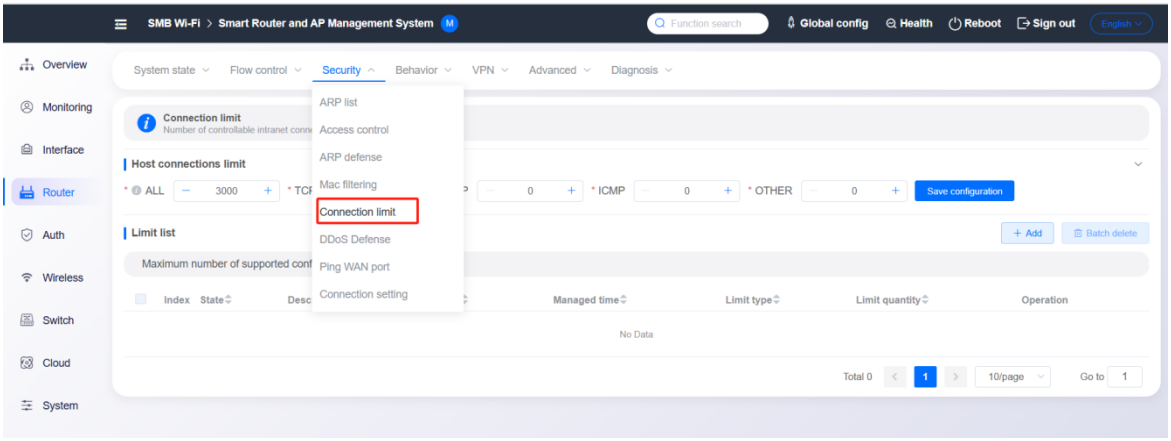
MAC address: Fill in the MAC address that needs to be controlled. The format is: 00:0A:0B:0C:0D:0E;

Managed time: Enable MAC filtering rules according to the set time. By default, all time periods are effective. If you need to use a specific time, you can select Custom time, where weekly and daily time periods are required.

4.3.5 Connection Limit

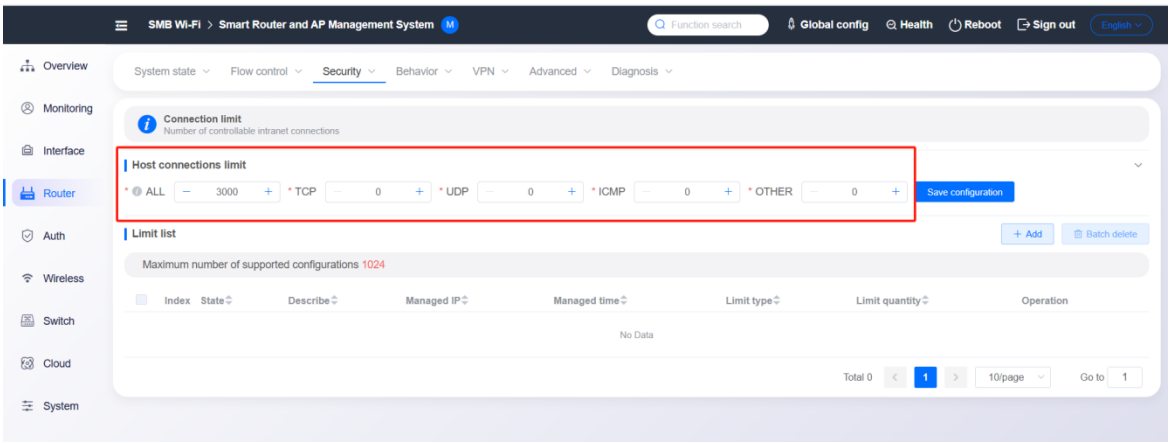
The connection limit can control the number of external connections through the device network. If the number of connections for a single IP is controlled , the maximum number of connections that can be established simultaneously by computers in the intranet can be controlled. This function provides very effective management for network administrators to control the use of P2P software such as BT, Thunder, emule , etc. in the intranet, which will cause a large number of connections.

Setting the appropriate number of allowed connections can effectively control the number of connections that can be generated when downloading P2P software, and relatively limit the bandwidth usage. In addition, if a computer in the intranet is infected with a virus similar to Shockwave and generates a large number of outgoing connection requests, it can also achieve a certain inhibitory effect.



Host connection limit

The number of connections of all hosts through this device . When the number of connections reaches the set value, it will no longer increase. The corresponding performance is that some terminals may be slow when requesting certain web page data. Therefore, the number of host connections can generally not be modified. The default value of ALL is 3000. The default value of TCP, UDP, ICMP, and OTHER is 0. The upper limit of these four cannot be greater than the set value of ALL.



Limit List

Displays the added rules for setting the number of connections for hosts (single or multiple IP addresses).

Add: Add rules as needed

State: Set the rule status to on or off;

Describe: Describe the rule to make it easier to distinguish among multiple rules;

Limit Type: Select the connection type to set the rule for, ALL, TCP, UDP;

Limit quantity: the specific value of the connection limit, 0 means no limit;

Managed IP address: The rule is effective for a certain IP or a certain range of IP (terminal or host);

"All addresses": means that the rule is effective for all global terminals;

"Custom": You need to fill in the IP address or IP segment;

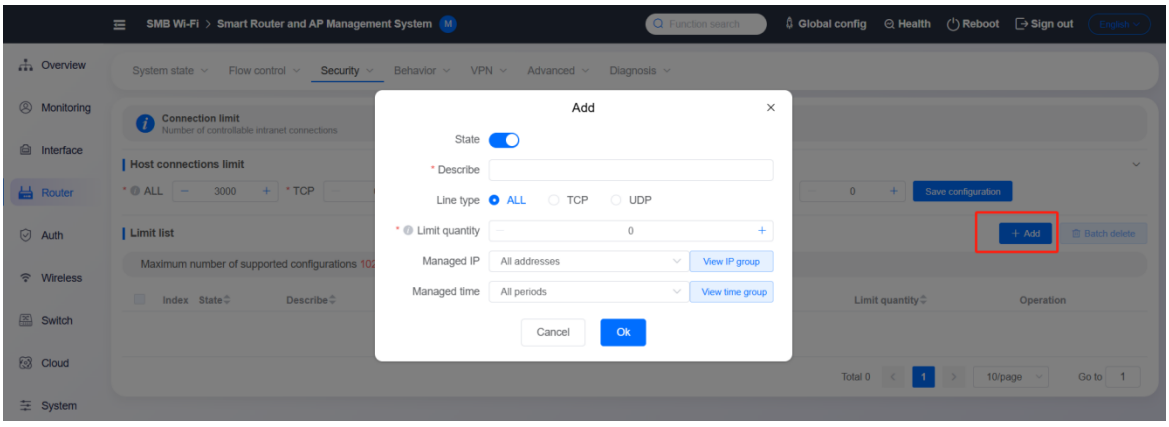
"Address Group": Select the IP segment by selecting IP address group management, and click "View IP address group" to add, modify, and delete.

Managed time: the time when the rule takes effect. The time needs to be specific to a certain time period of the week. The rule will not take effect outside this time period.

"All time periods" : means all time periods;

"Custom": you need to manually fill in the specific time period;

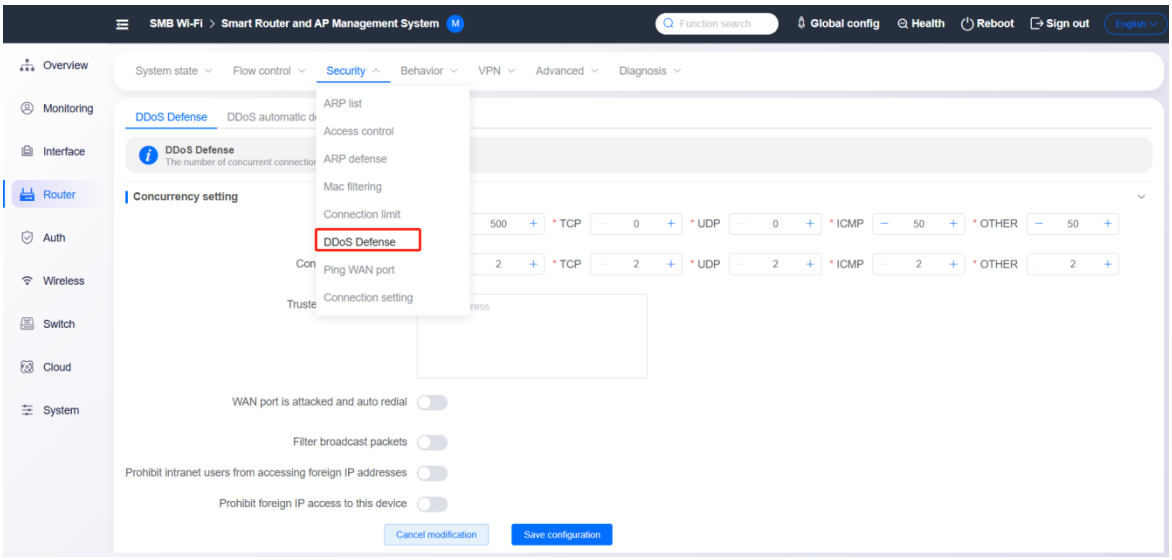
If a time group is added, can directly select to use it to make it effective. Click "View time group" to add, modify, and delete it.



Batch Delete: Select the rules to be deleted in batches.

4.3.6 DDoS Defense

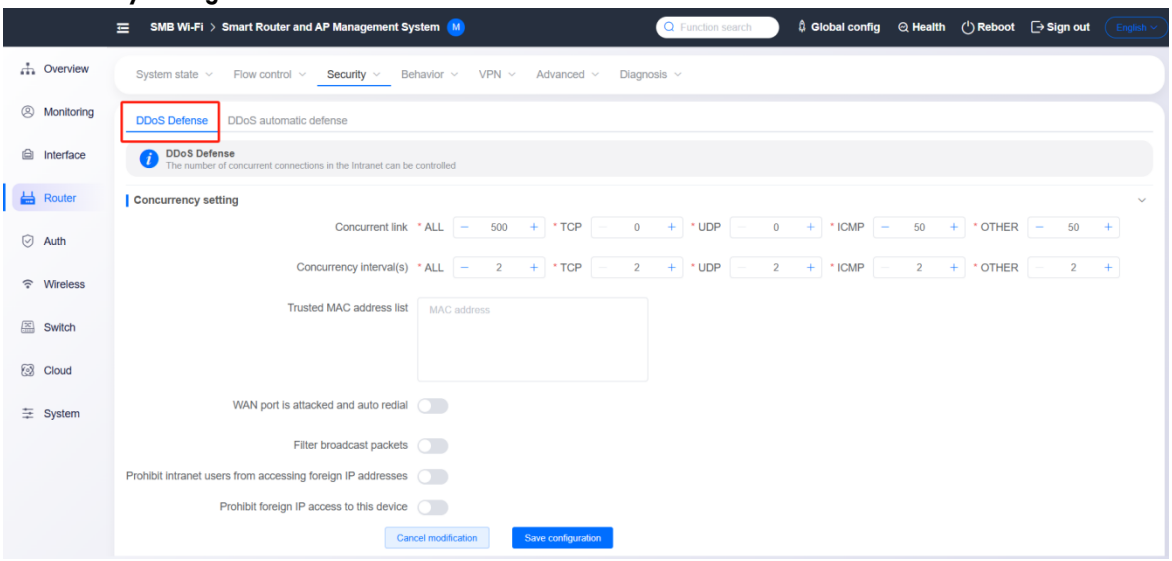
The number of concurrent connections in the intranet can be controlled.



4.3.6.1 DDoS Defense

The number of concurrent connections in the intranet can be controlled.

Concurrency settings



Concurrent link: The total number of links that a single terminal can initiate in a unit of time. If you create a rule below, the users in the rule will not be affected by the concurrent links set here;

Concurrency interval (seconds): Concurrent link unit interval time;

Trusted MAC address list: The MAC addresses filled in here will not be limited by the number of concurrent links;

WAN port is attacked and auto redial: When the device encounters a DDoS attack, the WAN port will be disconnected and will not automatically reconnect. When the automatic redial when WAN port is attacked is enabled, the WAN port disconnected by the DDOS attack will automatically dial;

Filter broadcast packets: After it is turned on, abnormal broadcast packets will be automatically filtered out;

Prohibit intranet users from accessing foreign IP addresses: Retrain intranet users to access foreign IP addresses;

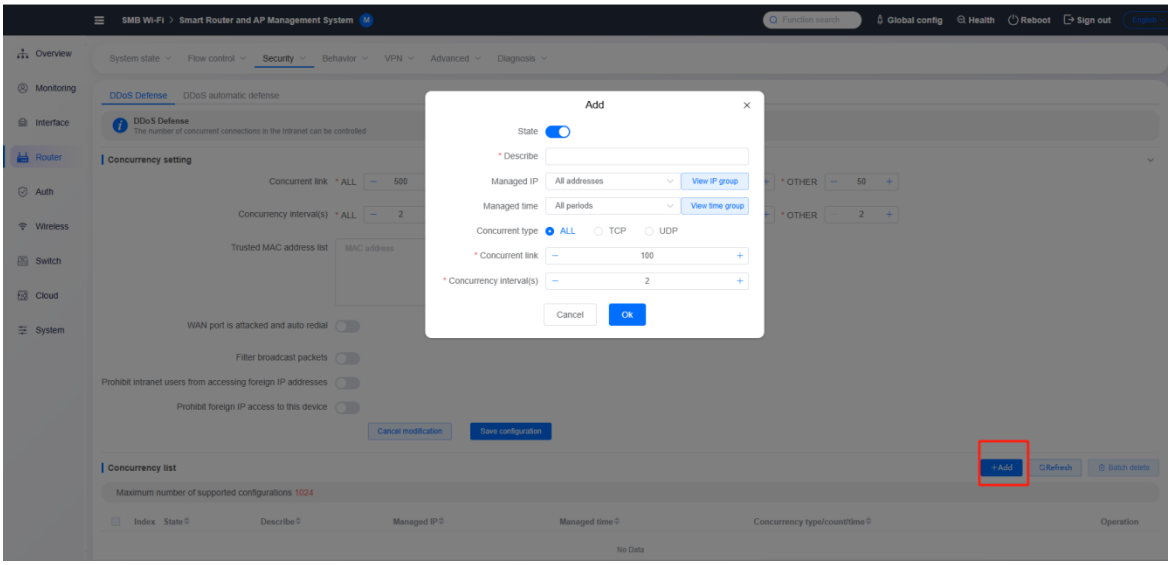
Prohibit foreign IP to access IP addresses: Do not allow foreign IP addresses to access this device;

The above configuration is for global DDoS connection configuration. When you need to set the number of DDoS connections for one or some terminals, you can set it through the Add button below.

Concurrency list

Displays a list of manually added rules.

Add: Set DDoS connection limit for a single host or certain hosts.



State: rule status is enabled or disabled

Describe: Set the rule name to distinguish it from other rules.

Managed IP: refers to the IP address, IP segment, or IP group for which this rule needs to take effect.

"All addresses": means that the rule is effective for all global terminals;

"Custom": You need to fill in the IP address or IP segment;

"Address Group": Select the IP segment by selecting IP address group management, and click "View IP group" to add, modify, and delete.

Managed time: the time when the rule takes effect. The time needs to be specific to a certain time period of the week. The rule will not take effect outside this time period.

"All time periods" : means all time periods;

"Custom" : You need to manually fill in the specific time period.

If a time group is added, you can directly select to use it to make it effective. Click "View time group" to add, modify, and delete it.

Concurrent Type: Select the concurrent connection type you want to set. Unselected types are not restricted by the rules.

Concurrent link: Set the number of links. The default value is 100, and the upper limit is 100000. Filling in 0 means no limit on the number of connections, and the default rules above will be followed;

Concurrency interval (seconds): The IP (terminal) connection concurrent time interval setting in the rule, the minimum value is 1 and the maximum value is 10000.

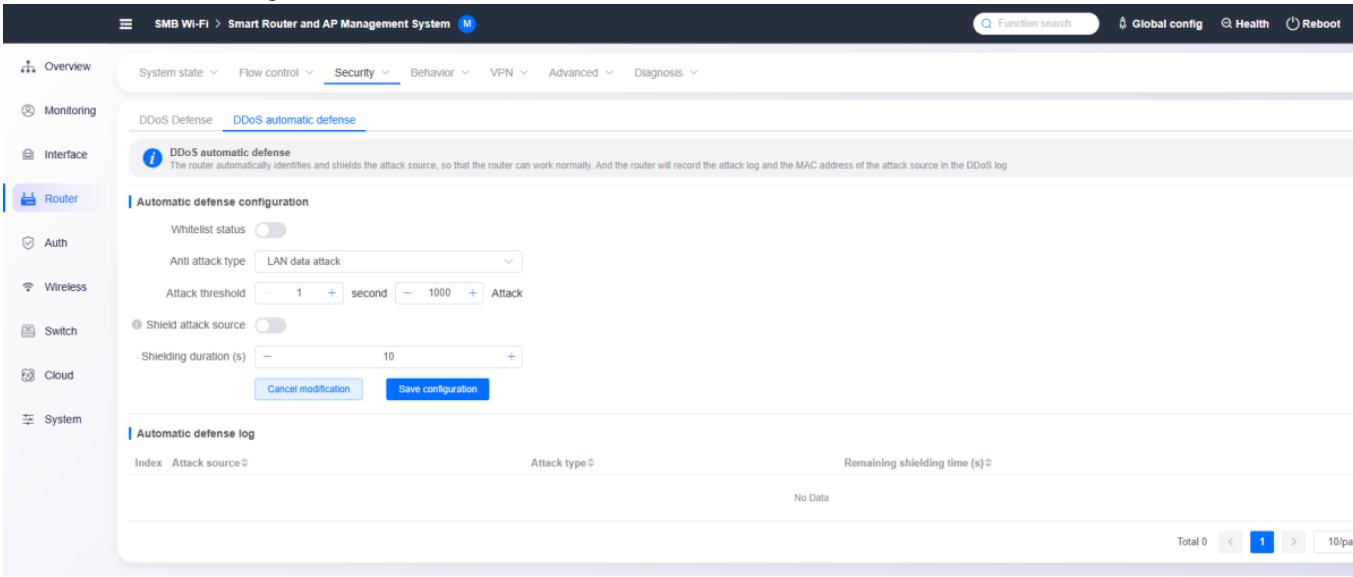
Refresh: refresh the currency list content;

Batch Delete: Batch delete one or more selected rules.

4.3.6.2 DDoS Automatic Defense

The router automatically identifies and shields the attack source, allowing the router to work normally. The router will also record the attack log and the MAC address of the attack source in the DDoS log

Automatic defense configuration



Whitelist status: Enable or disable the whitelist. The whitelist content in below will take effect only after it is enable.

MAC whitelist: The entered MAC address (terminal) will be treated as a trusted address and will not be subject to DDOS automatic defense detection.

Anti attack type: Select the attack type to be prevented according to your needs: connection attack, LAN data attack, LAN packet attack, IP fragment packet attack, DNS server receiving packet attack, DNS client receiving packet attack, DNS server sending packet attack;

Attack Threshold: Set the control limit of the number of attacks received by this attack type within a few seconds, that is, the number of attacks received within a certain period of time. Used in conjunction with the "Shield Attack Source" below;

Shield attack source: whether to enable shield attack source. If it is not enabled, the attack source will continue to attack. If it is enabled, the attack source will be shielded when the number of attacks exceeds 2 times.

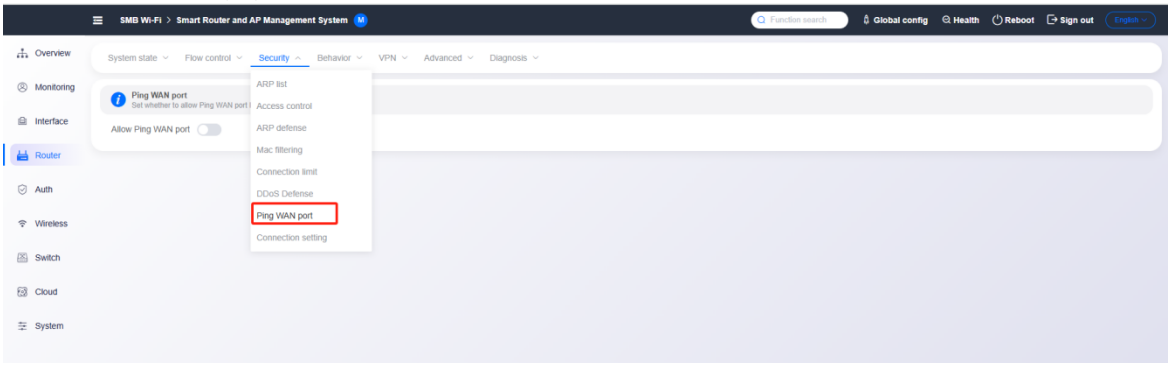
Shielding duration (seconds): The shielding time of the attack source. The shielded attack source cannot launch attacks again within the set time range. The default shielding time is 10 seconds, the minimum time is 1 second, and the maximum time is 10000 seconds.

Automatic defense log

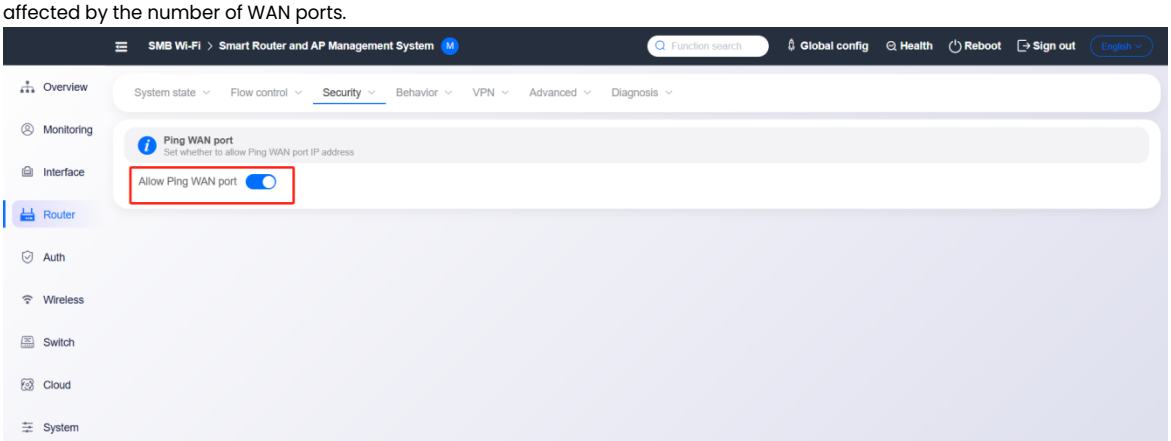
When an attack occurs, the automatic defense mechanism is automatically enabled and a defense log record is generated. The corresponding log will be displayed in the list below.

4.3.7 Ping WAN port

Set whether to allow Pinging the WAN port IP address.

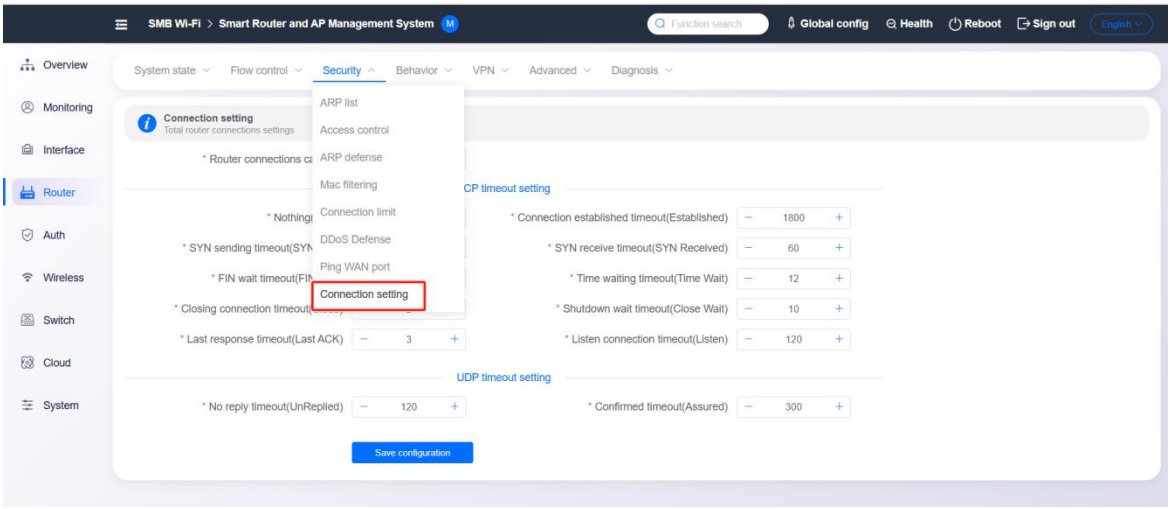


The default WAN port of the router is in Ping-disabled state. Please enable it if allow to ping WAN port. This function is not affected by the number of WAN ports.



4.3.8 Connection setting

It is mainly used to set the maximum number of external connections of the router. The default number of connections is automatically obtained according to the machine memory and is not modified by default.

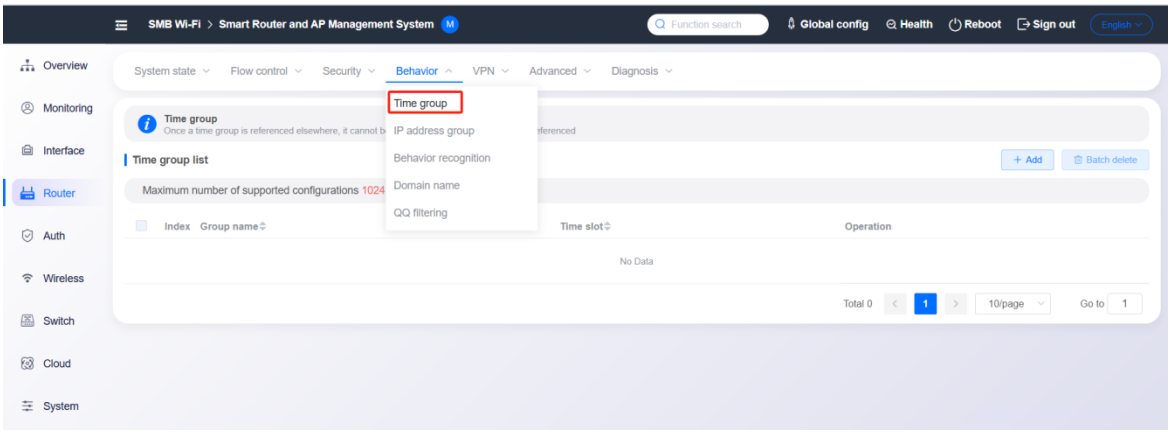


4.4 Behavior

4.4.1 Time Group

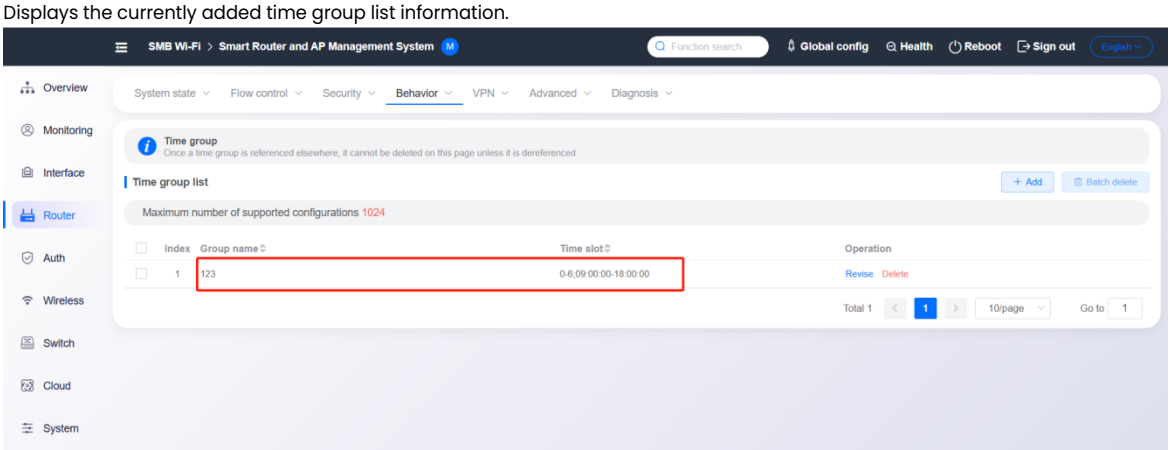
Can create time groups as needed. Directly select the time group, add a time group manually, then select a time to creating behavior or flow control rules .

Once a time group is referenced elsewhere, it cannot be deleted from this page unless it is unreferenced.

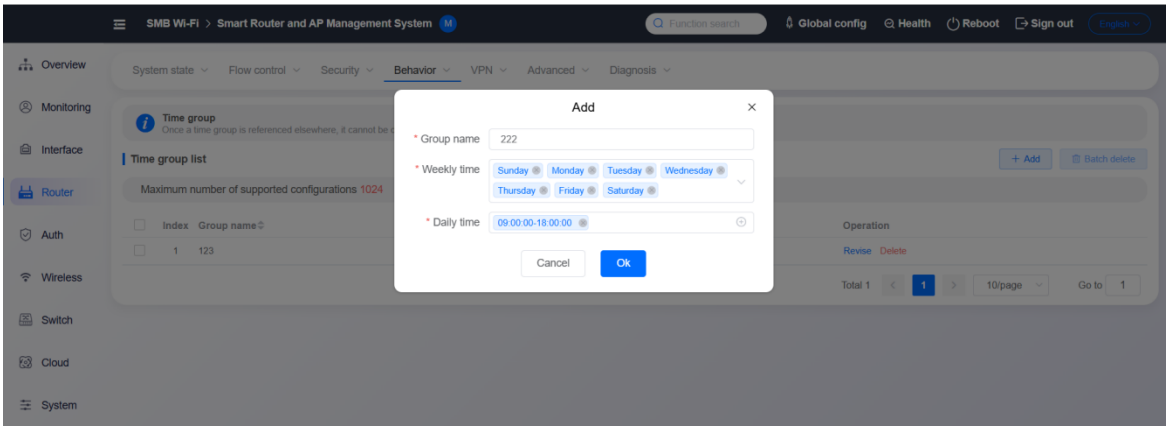


Time Group List

Displays the currently added time group list information.



Add: Add a time group as needed.

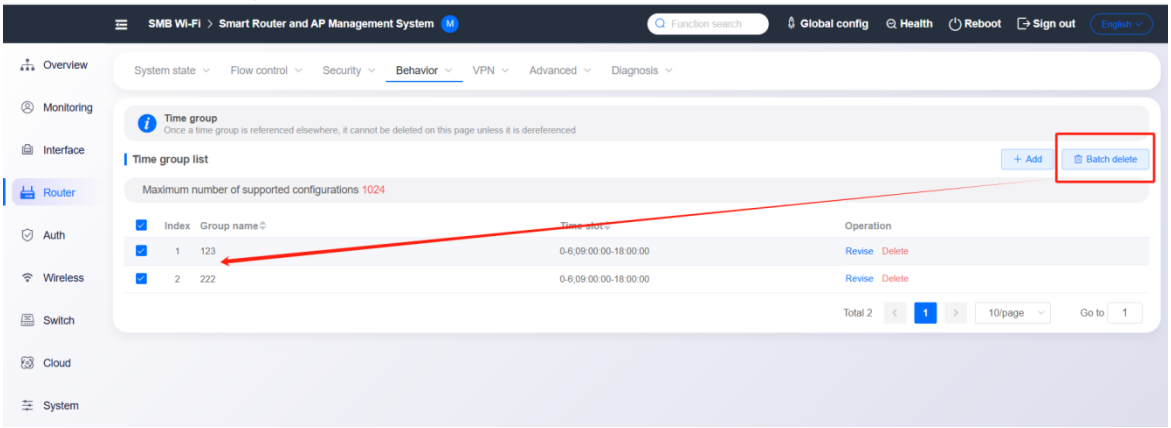


Group name: Customize the time group name to facilitate differentiation among multiple groups;

Weekly time: Select the weekly time, which is a required option. Select all to select all weekly times, and unselect to select the unchecked weekly times in addition to the checked ones ;

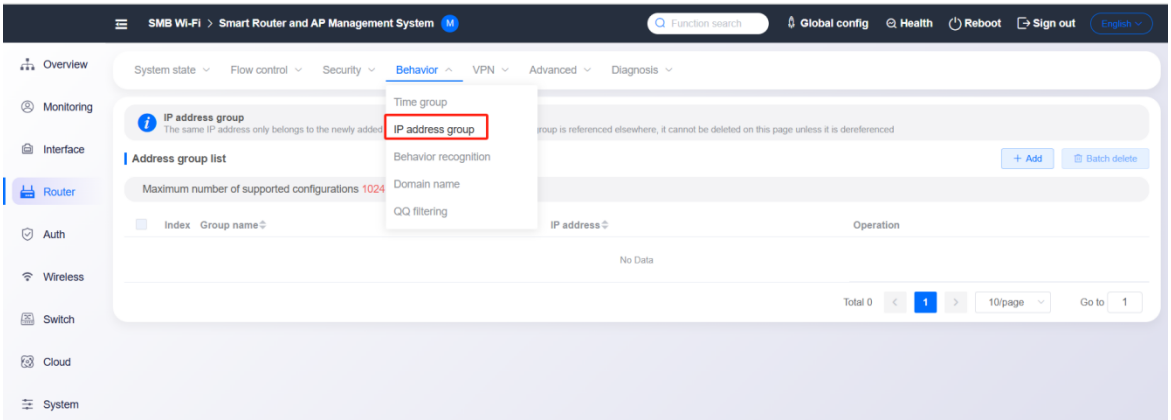
Daily time: To set the time period for each day, you need to select the start time and end time, and the start time cannot be less than the end time. If there are multiple time periods, click the plus sign at the end to add them.

Batch Delete: When there are multiple time groups that need to be deleted, you can check them and click "Batch Delete" to confirm. However, the time groups referenced above do not support deletion.



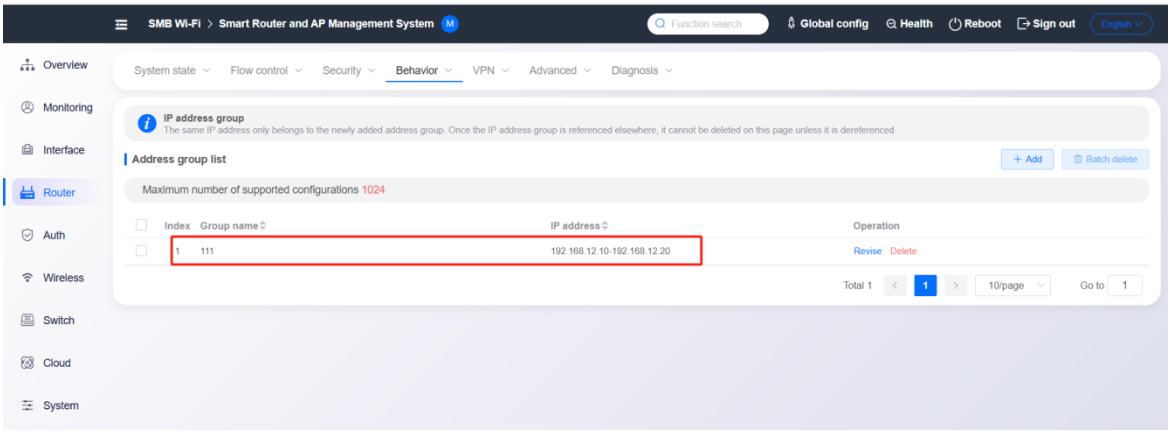
4.4.2 IP Address Group

Can create IP address groups as needed, Select IP address group when creating behavior or flow control rules, It should be noted that once an IP address group is referenced elsewhere, it cannot be deleted on this page unless it is unreferenced.

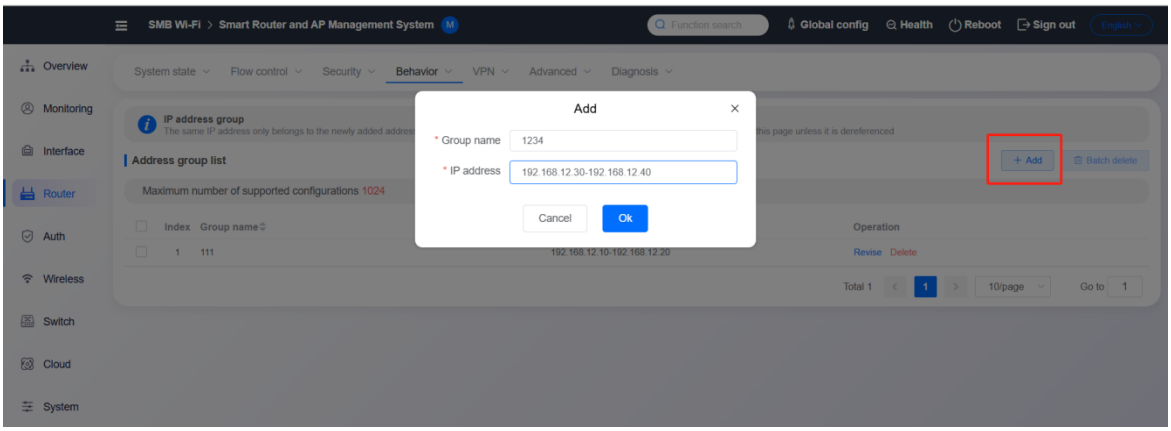


Address Group List

Displays the address group list information that has been added currently.

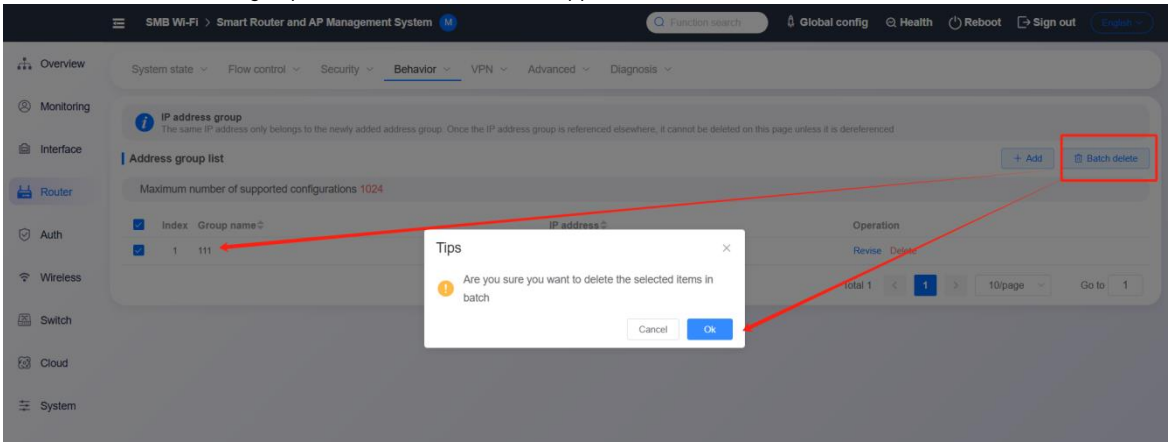


Add: Add an address group as needed



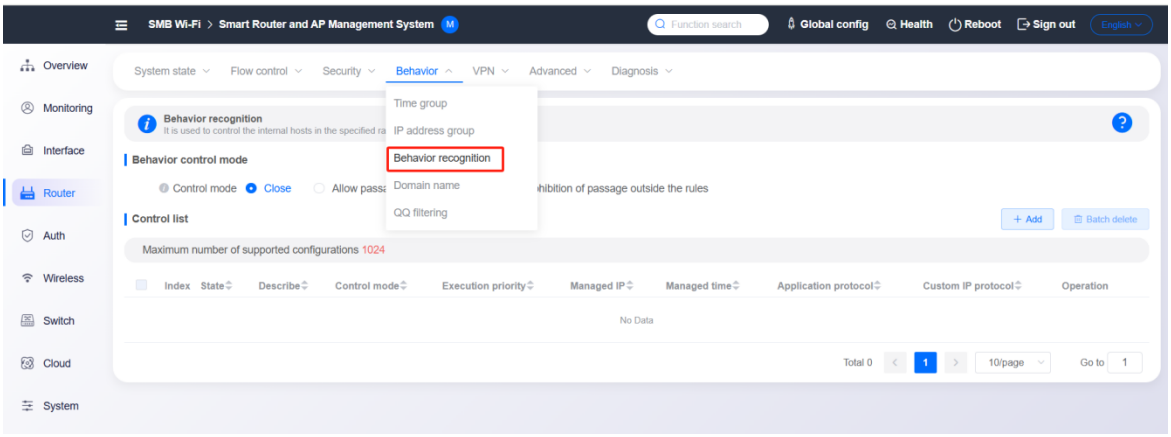
Group name: Customize the IP address group name to facilitate differentiation among multiple groups;
IP address: this is the IP address segment Set a start address and an end address. The rules that reference the address group containing this address object will take effect within this address segment. Click the plus sign to add multiple address segments.

Batch Delete: When there are multiple time groups that need to be deleted, you can check them and click "Batch Delete" to confirm. However, the time groups referenced above do not support deletion.



4.4.3 Behavior recognition

Used to control application protocols of internal hosts within a specified range



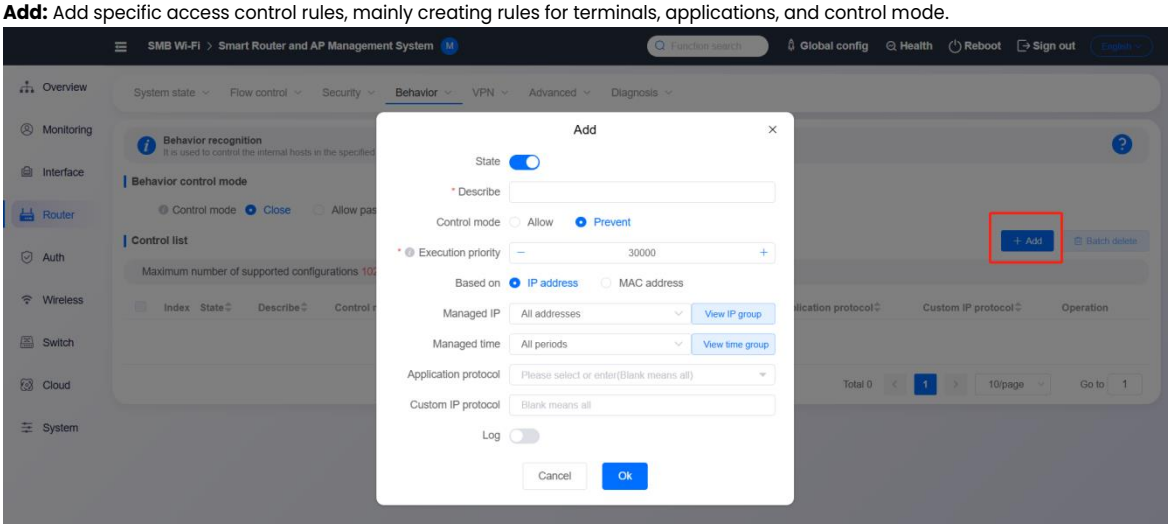
Behavior Control Mode

Control mode: There are three states: closed, allowing passage outside the rules, and prohibition of passage outside the rules,

1. Close: If you choose Close, all the rules created below will not take effect;
2. Allow passage outside the rules: All restrictions or applications except those created in the rules below can pass;
3. Prohibition of passing outside the rules: Only allow or prohibit the content of the following rules;

Control List

Add: Add specific access control rules, mainly creating rules for terminals, applications, and control mode.



State: Whether the rule is enabled. If it is enabled here and disabled above, the rule is still disabled.

Describe, it is rule name, customize the rule name to distinguish it from other rules;

Control mode: Allow means the rule content is allowed, and prevent means the rule content is blocked and not allowed to pass.

1. If the above setting is "Allow passage outside the rules", selecting "Allow" here means that all access is allowed;
2. If you set "Allow passage outside the rules" above, selecting "prevent" here means that the content of this rule is blocked, and the rest can be used normally (passed);
3. If "Prohibition of passage outside the rules" is set above, selecting "Allow" here means that only the content in the rules can be passed, and the rest (terminals or application protocols) cannot be passed;
4. If the setting above is "Prohibition of passage outside the rules", selecting "prevent" here means prohibiting all global terminals and protocol access. This situation will also cause all terminals connected to this network to be unable to access the router WEB management page (regardless of wireless or wired), please pay attention to the configuration rules.

Execution priority: The execution priority order between rules. The higher the value, the higher the priority. If the priorities are the same, one of them will be executed randomly.

Control based on terminal address type: control is effective by using the type of IP address or MAC address;

Based on IP: If the global terminal IP needs to be effective for this rule, select "All Addresses"; if control the access of some or a certain IP, select "Custom" and fill in a single or a range of IP addresses;

Based on MAC address: create access rules based on the physical MAC address of the terminal. There are multiple virtual MACs on the mobile phone (different wireless networks connected to the same device may get different MACs of the terminal, which is a virtual MAC). If achieve complete control access to a terminal , please fill in all the virtual MACs of the terminal;

Managed time: the time period during which the rule is effective. Access control rules are not effective outside the set time period.

Application Protocol: Select the application protocol type for access control;

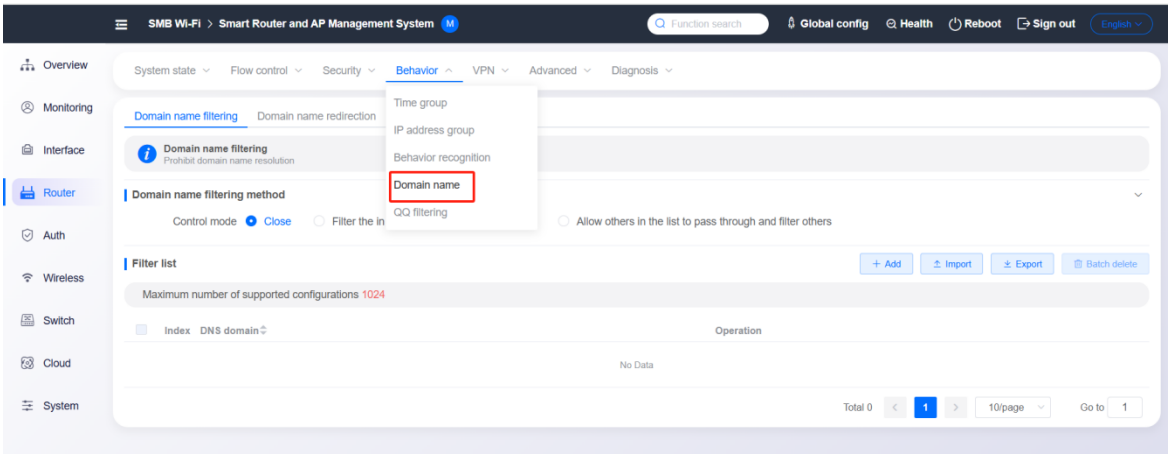
Custom IP address: Can define the remote IP, domain name and port protocol, and use them as the control object;

Log: Enable access control rule logging. When a terminal (user) triggers the rule, the system will automatically record and save the log. If the log tool is turned off, no record will be saved .

4.4.4 Domain Name

4.4.4.1 Domain Name Filtering

Set whether to filter the added domain name. The blocked domain name will not be successfully resolved (that is, the address cannot be accessed).



Domain name filtering method

Contains close,Filter the domains in the list and allow others to pass, and allow others in the list to pass through and filter others.

Close: If you choose to close, the filtering domain names added below will not take effect;

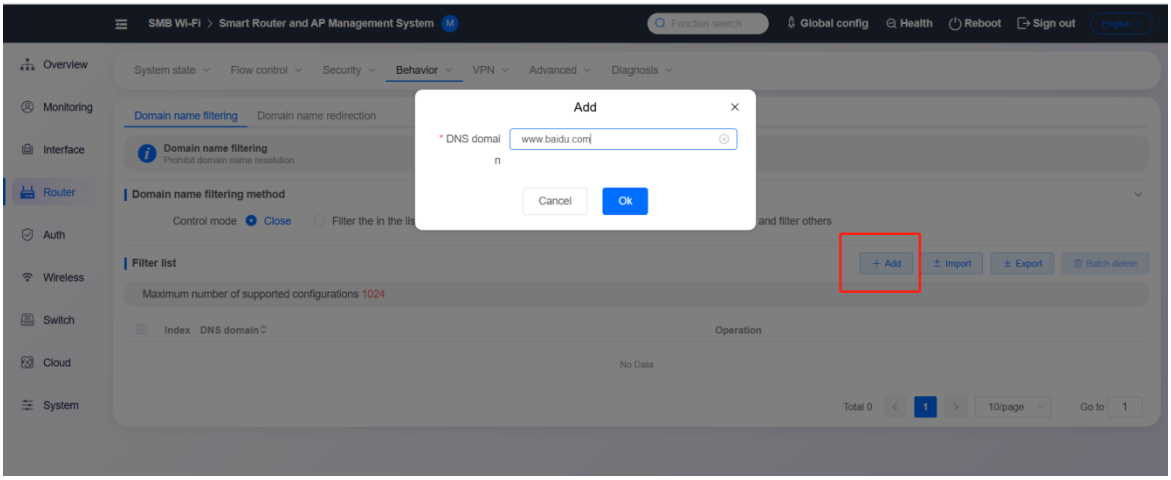
Filter the domains in the list and allow others to pass: except for the domains added below, all other domains can pass the resolution;

Allow others in the list to pass through and filter others: Only allow the domain names added below to be resolved, and other domain names cannot be resolved. Please pay attention to this setting rule to avoid global network failure;

Filter List

Displays all added filtering rules.

Add: Add the domain name that needs to be managed and resolved.

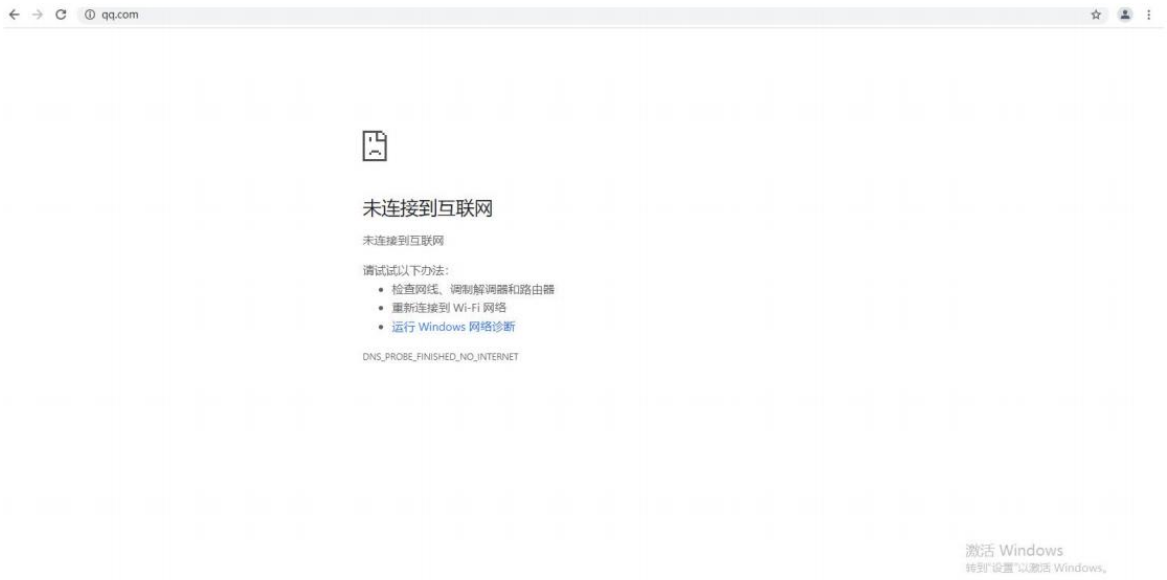


If select "Close", any domain name added below will not be blocked from resolution and can be accessed normally ;

If select "Filter the domains in the list and allow others to pass", it means that the domain name added below will not be resolved (cannot be accessed), but the domain name outside the rule can be resolved and used normally; for example, the domain name configured in the figure above is baidu.com, and the terminal fails to access the domain name;



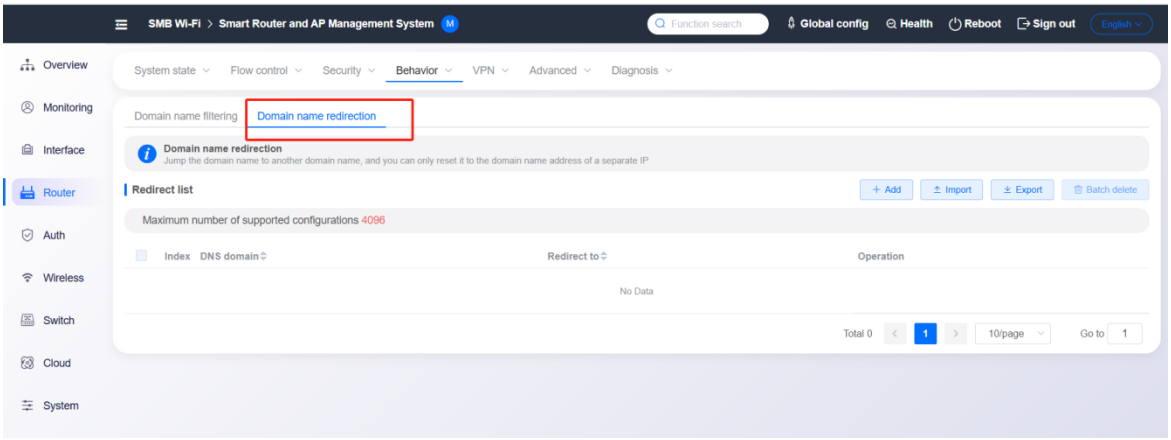
If select "Allow others in the list to pass through and filter others", it means that only the domain names in the list can be resolved and accessed, and the domain names not in the list cannot be accessed. For example, if baidu.com is filled in above, the terminal can access it normally, but the other domain names will fail to access, such as accessing qq.com will fail.



Import: Import the backed up domain name filtering file into the device to restore the rules.
Export: Export the current domain name filtering rules to achieve backup.
Batch Delete: Delete selected rule entries in batches.

4.4.4.2 Domain name redirection

Redirect a domain name to another domain name, mean redirect it to a separate IP domain name address. Domain name redirection can redirect a website with http protocol to another website with http protocol. It should be noted that domain name redirection does not support https websites.



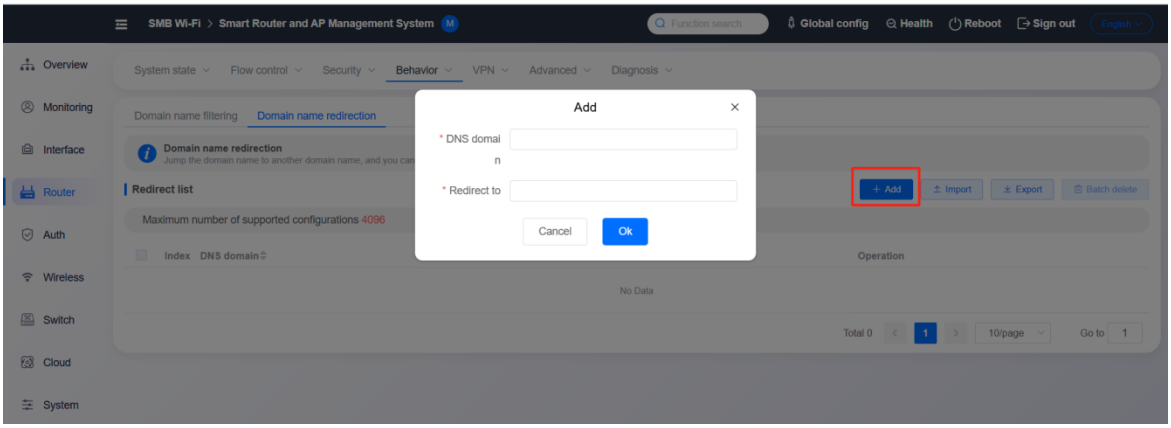
Redirect List

Displays all added redirection rules.

Add: Add redirection rules as needed.

Import: supports redirection rules in rule format. If we don't know the rule format, we can add a redirection rule first and then export it, then add or modify the content in the original file (please be sure to follow the original file format, otherwise the rule import will fail).

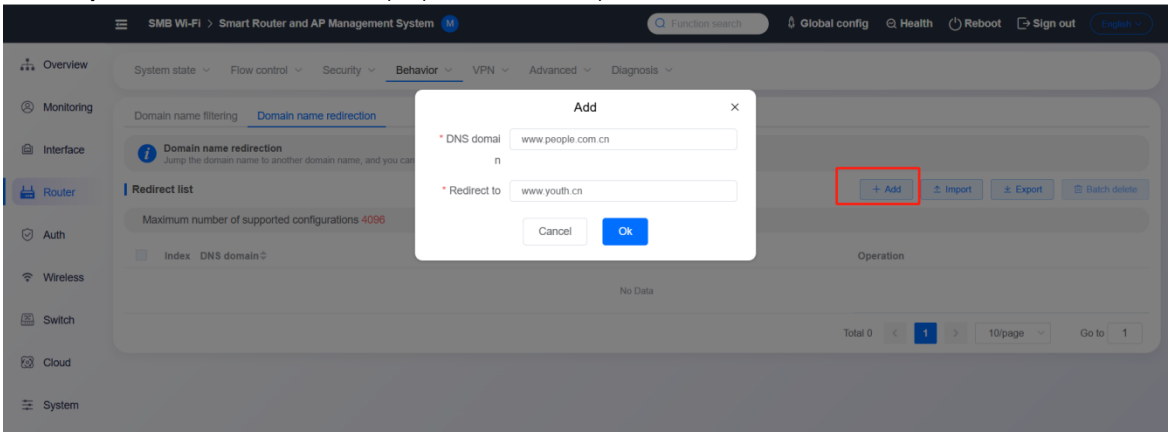
Export: Supports exporting the created redirection rules. If no rules are added, the exported file content will be empty



DNS domain: fill in the domain name that needs to be redirected. Be sure to fill in the domain name according to the standard domain name and the domain name must be a real http website domain name;

Redirect to: which new http website should be redirected to.

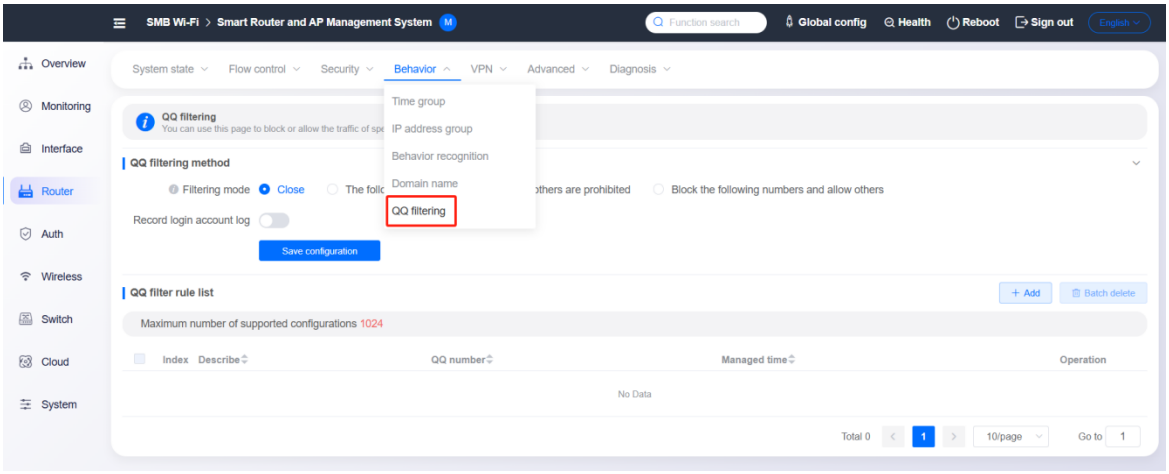
For example: To redirect the website www.people.com.cn to www.youth.cn, add the rules as shown below:



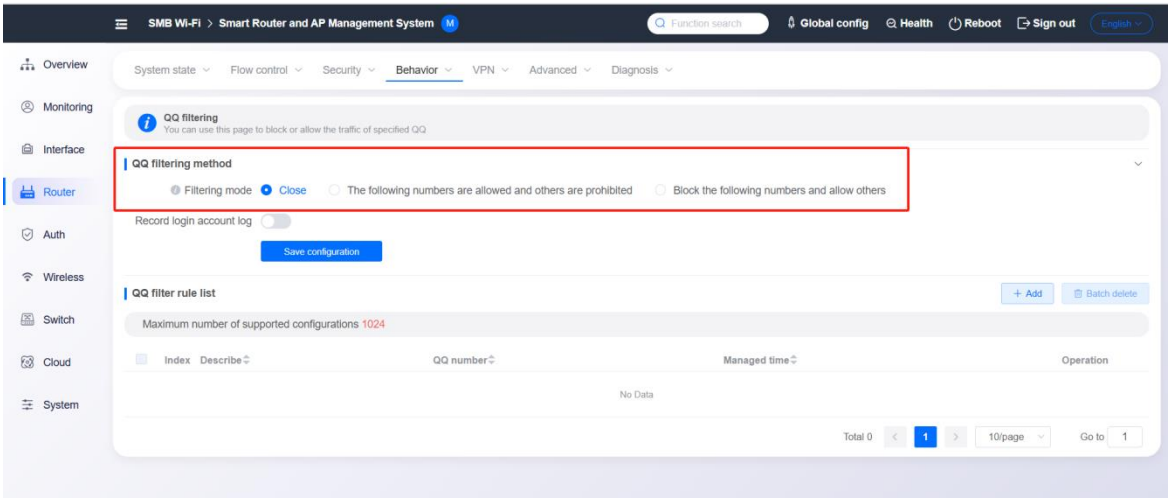
The access address is www.people.com.cn, and the web page actually jumps to www.youth.cn

4.4.5 QQ Filtering

What is filtered here is the QQ login that is not logged in by mobile terminals, that is, the QQ number logged in by mobile terminals such as mobile phones cannot be filtered.



QQ filtering method



Filtering mode: Close, The following numbers are allowed and others are prohibited, Block the following numbers and allow others.

1. Close: If you choose Close, all the rules created below will not take effect;

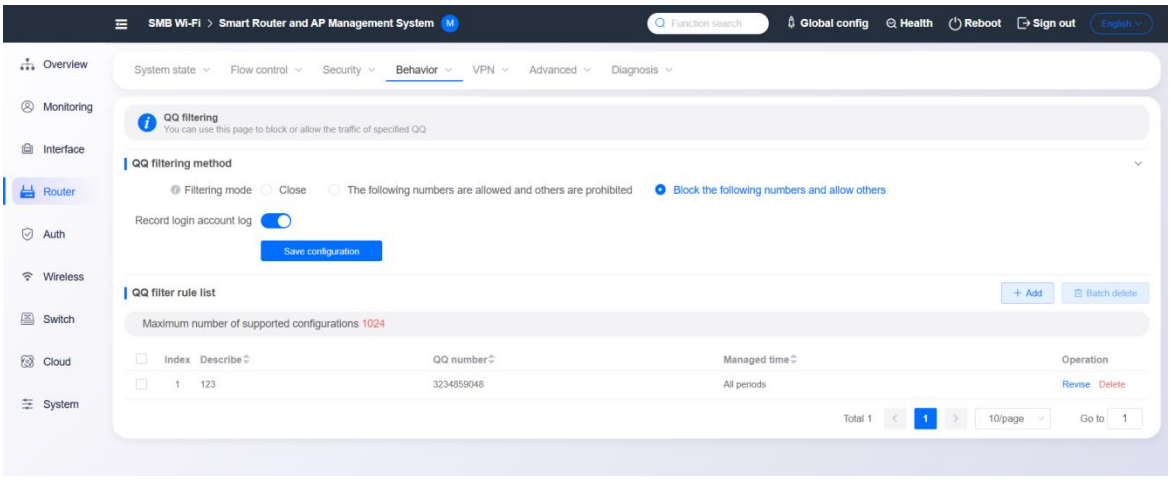
2. The following numbers are allowed and others are prohibited: After enable it, the QQ numbers added below can be used normally, and other numbers cannot be logged in. If this rule is created after logging in, the logged-in QQ numbers not in the rule will automatically go offline in one minute;

3. Block the following numbers and allow others: After enable it, the QQ numbers added below cannot log in successfully. If they have logged in successfully online, the QQ numbers set in the rules will automatically go offline in one minute. QQ numbers not included in the rules can go online normally.

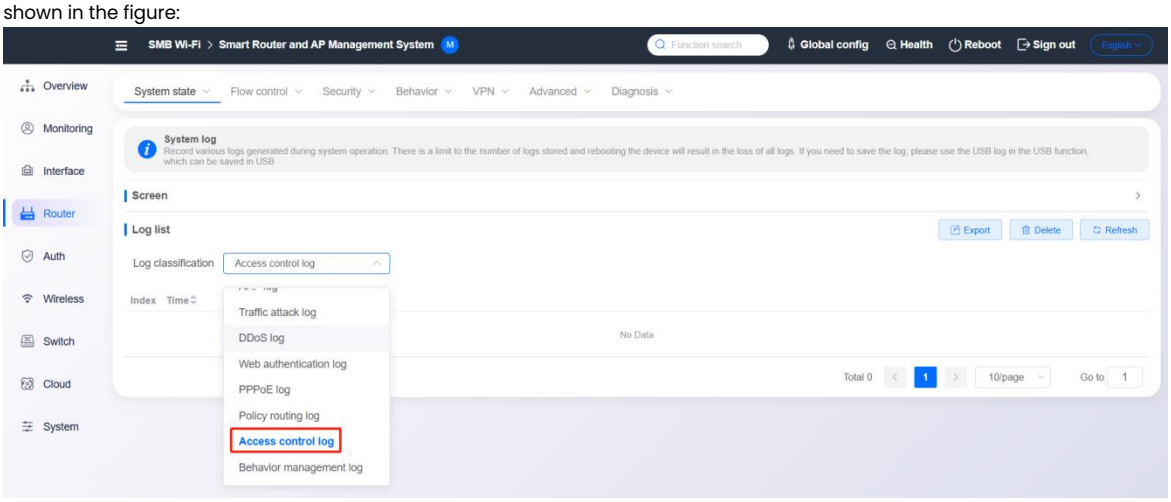
A blocked QQ number can only log in normally when the rule is turned off, otherwise it cannot log in online.

Record login account log: After turning it on, the system will record the QQ number login log.

For example: If you add the QQ number "3234859048" and select the filtering method as "Block the following numbers and allow others", then the QQ number will change from being online to being offline and will not be able to log in again.

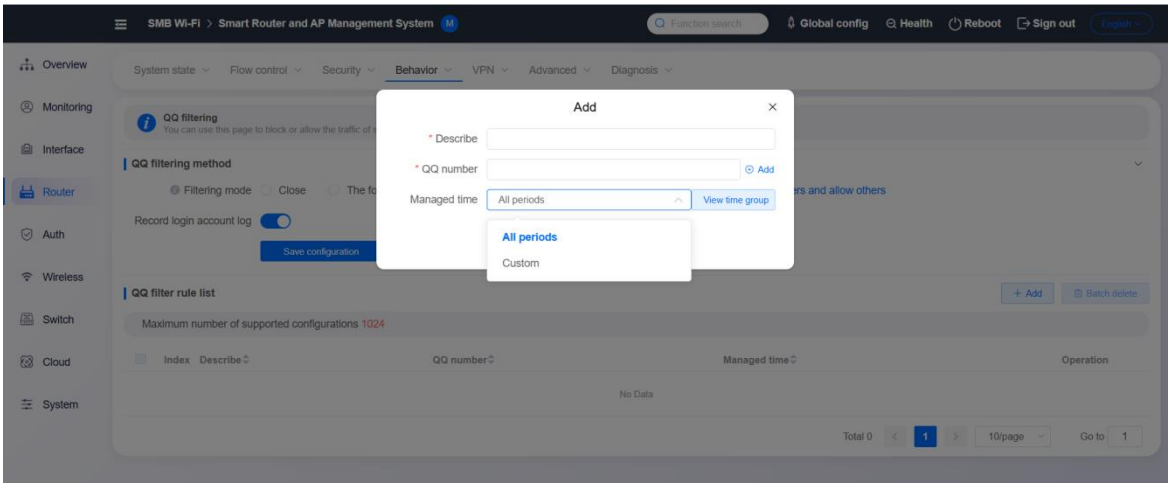


After enabling the access control log, logging into the account will trigger the rules and generate log records. In the log category of " **Router** " - " **System State** " - " **System Log** " - "Log List", select Access Control Log from the drop-down menu to view it, as shown in the figure:



QQ filter rules list

Add: to add the QQ number that needs to be controlled and filtered;



Rule describe: Customize the rule name to distinguish it from other rules;

QQ number: Fill in the real and correct QQ number, otherwise the filtering function will be affected;

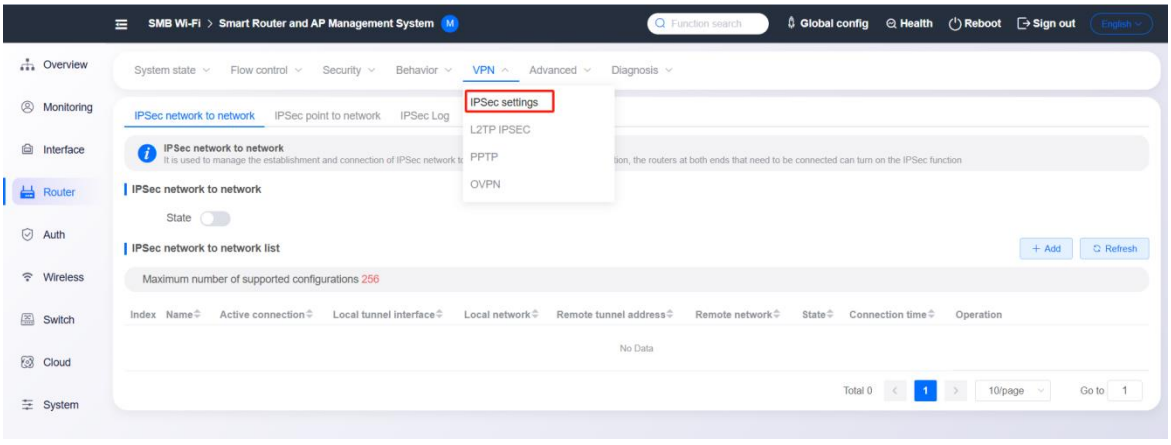
Managed time: that is, the time period during which the rule is effective. QQ filtering rules are not effective outside the set time period.

4.5 VPN

Support IPsec, L2TP, PPTP and OpenVPN;

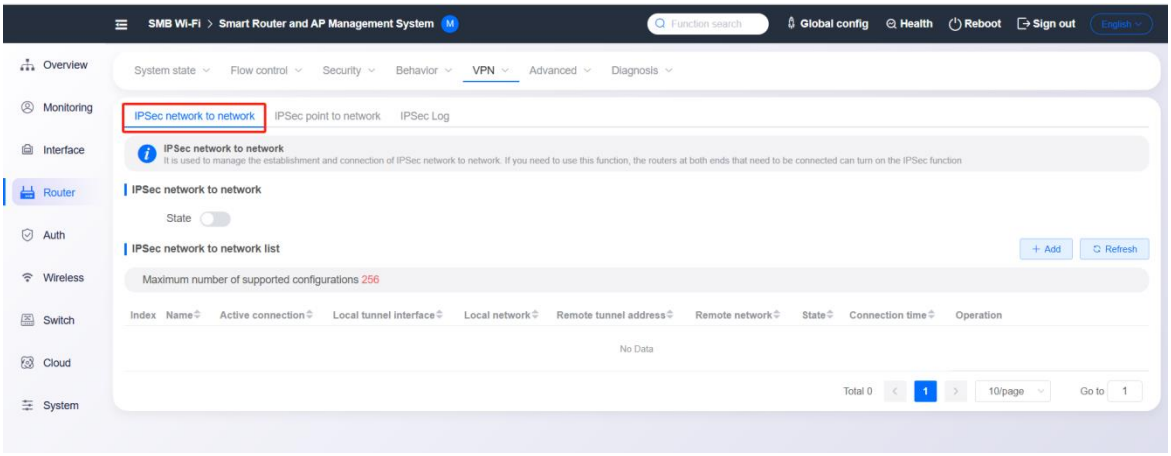
4.5.1 IPSec

Used to manage the establishment and connection of IPSec network-to-network. The IPSec function needs to be enabled on both ends of the connected routers.



4.5.1.1 IPSec network to network

Generally, network-to -network is used in scenarios where the trust between the two parties is extremely high, can achieve the effect of mutual access to intranet resource services.



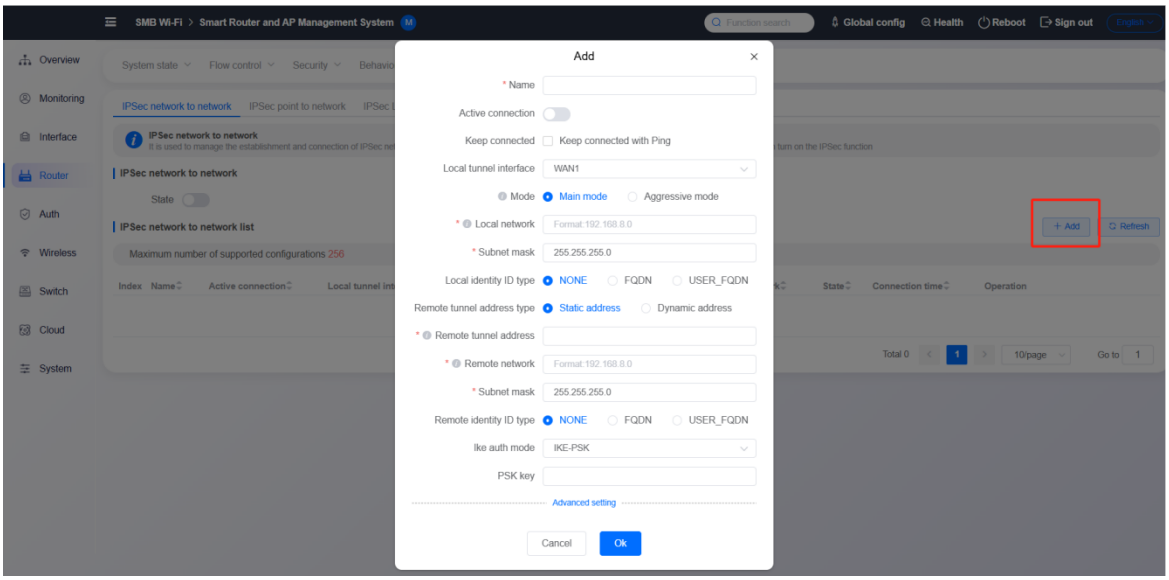
IPSec network to network

After the state is enabled, the network- to-network is take effective;

IPSec network to netwrok list

Add network- to-network rules as required

Add:



Name: Customized network-to-network name, the rule is 1-31 characters, Chinese characters, letters, numbers and _-!@#$%^&*().;

IPSec network-to -network active connection: Enable IPSec network-to-network active connection, the device will actively initiate a connection request to connect with the other end; if the local end turns off IPSec network-to-network active connection, the device will not actively connect to the other end device, but wait for the other end device to initiate a connection request (provided that the other end has enabled active connection); If both parties do not check the active connection, then neither party will actively initiate a connection request, can only manually click "Connect";

Keep connected: After checking, keep pinging the other party's intranet;

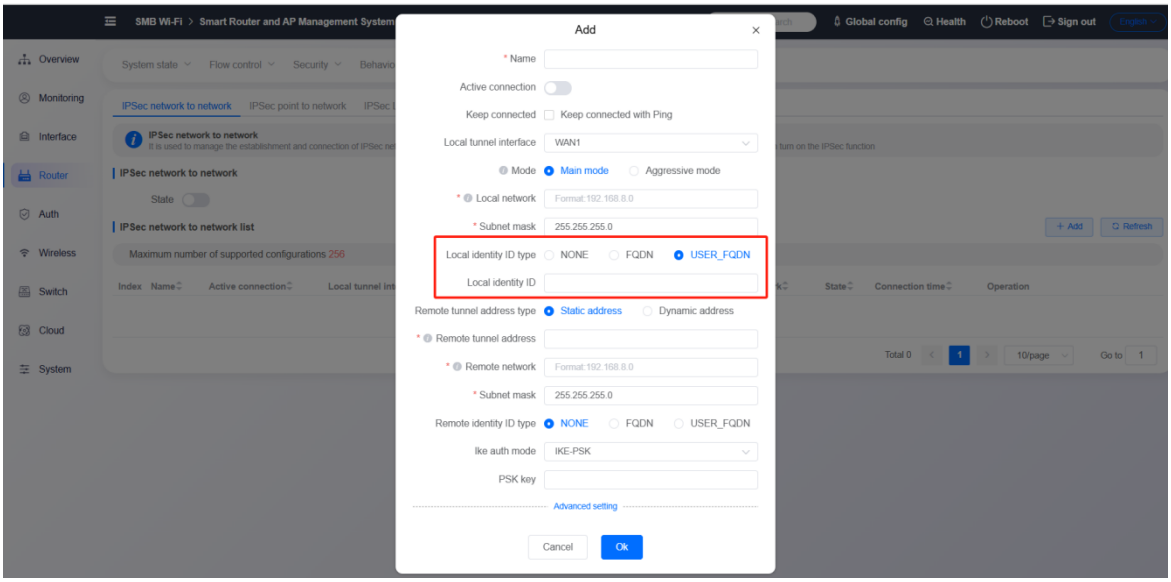
Local Tunnel Interface: Which WAN port is used to establish network- to-network. If WAN1 is selected here, the IP address of WAN1 on the other end must be filled in when filling in the "Remote Tunnel Address" (dial-up mode is not supported);

Mode: Select main mode or aggressive mode according to your needs. The difference between the two is that the main mode encrypts the identity ID, while the aggressive mode does not. Other configuration methods (the process) is basically the same;

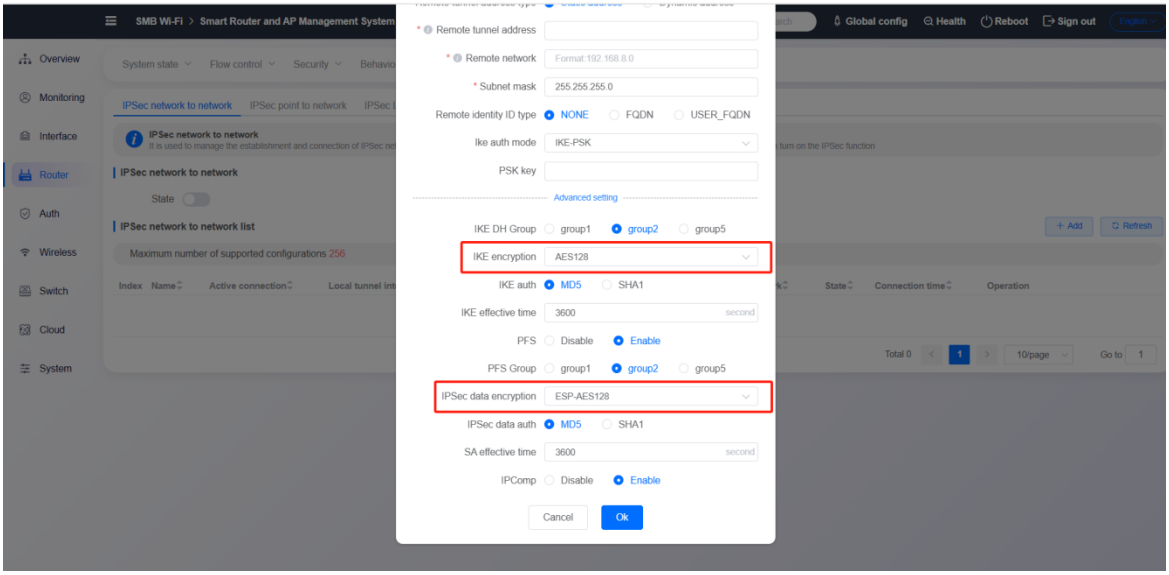
Local network: that is, the local intranet segment address. For example, if the local intranet address is 192.168.1.1, its format is 192.168.1.0 ;

Subnet mask: The system default is 255.255.255.0, and the size of the mask can be modified as needed;

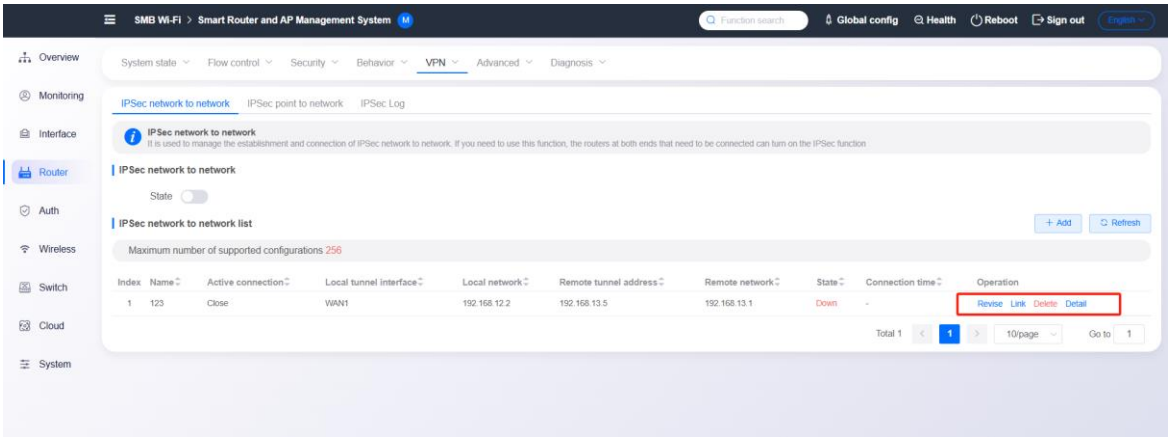
Local identify ID type: The system defaults to NONE, and NONE does not require an ID. If you confirm that the local ID has other types, please select "FQDN" or "USER_FQDN" according to the actual situation, and enter the local ID in the input box below



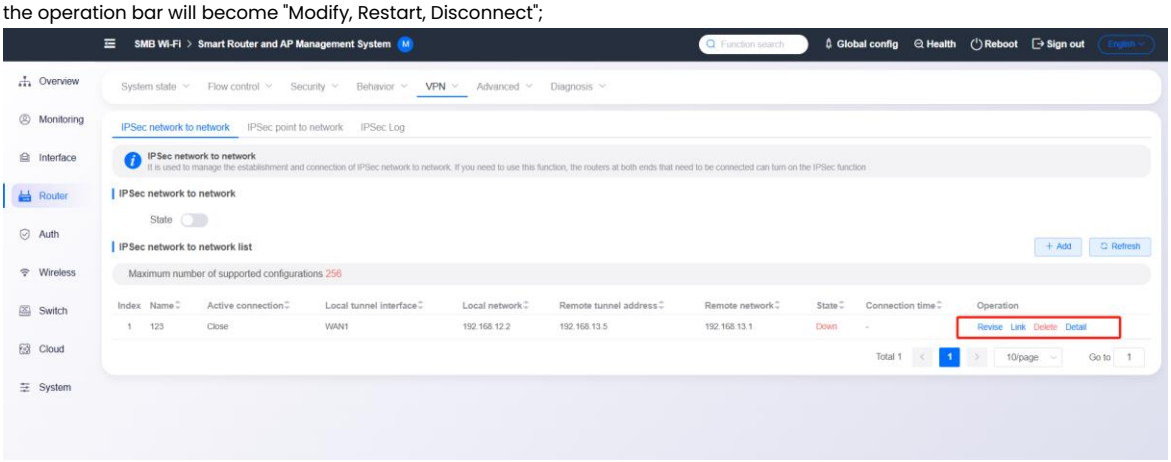
Remote tunnel address type: the type of external network connection of the peer device, which can be either static or dynamic (the dial-up type is not supported, or you can apply for a public IP address from the operator). It is generally recommended to use a static address. If a dynamic address is used, the network-to-network connection will fail if the external network address changes.
Remote tunnel address: the external IP address of the peer device. This address is preferably a static public IP address. If a network- to-network connection is created between intranets, the public IP addresses of both devices need to be filled in.
Remote network: This is the intranet IP address of the peer device. If the peer device is 192.168.8.1, then 192.168.8.0 should be filled in here .
Subnet mask: The system default is 255.255.255.0, modify as needed;
Remote identify ID type: The system defaults to NONE, and NONE does not require an ID. If you confirm that the remote ID has other types, please select "FQDN" or "USER_FQDN" according to the actual situation, and enter the remote ID in the input box below;
IKE Auth Mode: By default, only IKE-PSK authentication type is used;
PSK key: Set the verification key. The keys on both ends must be consistent for verification to succeed. Otherwise, verification failure will result in failure of network-to-network creation .
In advanced settings, the default configuration is generally used. If the peer device is not a product of the same company, please be sure to note that the encryption type is AES128.



Each network-to-network rule created is displayed in a list format, and the rules can be modified, connected, and deleted in the displayed list.

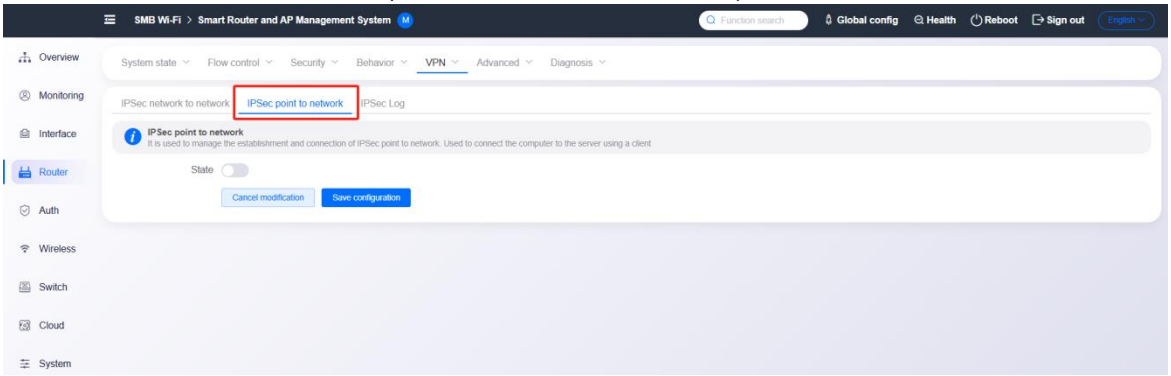


If the network-to-network connection is in connected state, it will also be displayed as "Connected" in the list, and the buttons in the operation bar will become "Modify, Restart, Disconnect";



4.5.1.2 IPSec Point-to-Network

Used to manage the establishment and connection of IPSec point to network. Used for computers to connect to the server using the client. That is, after it is turned on, this system will become the server of IPSec point to network



IPSec point to network

State: Enable or disable the point to network service status. Only when it is enabled, the rule parameters be configured.

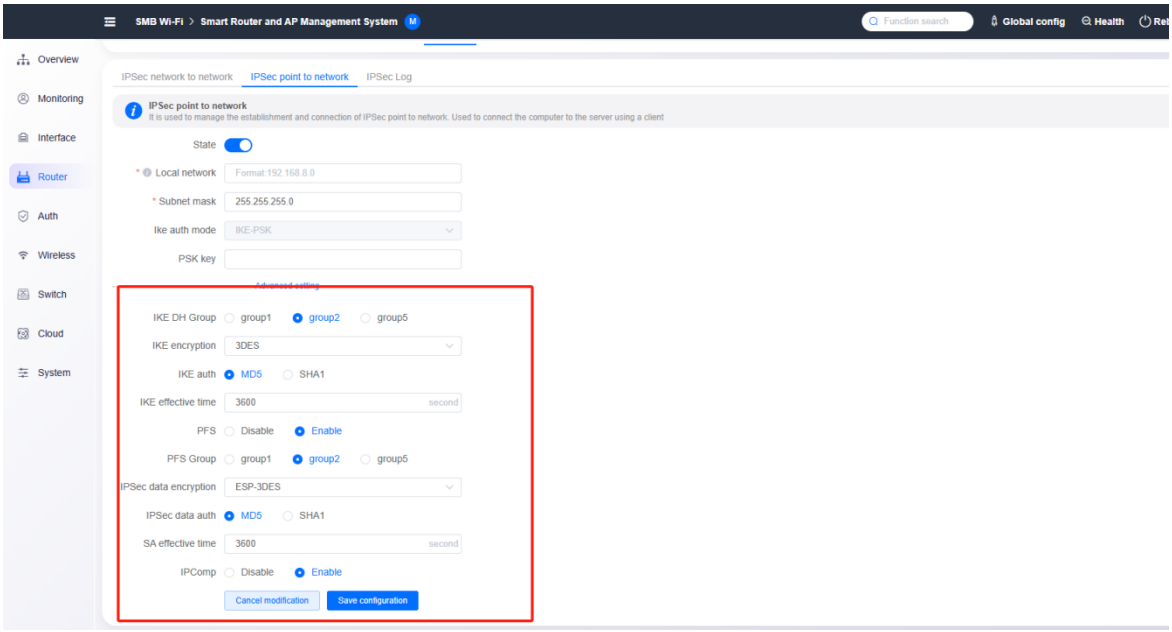
Local network: that is, the local (server) intranet address. If the intranet address is 192.168.1.1, this should be filled in as 192.168.1.0 ;

Subnet mask: The default is 255.255.25.0, and the mask segment can be modified as needed;

IKE Auth Mode: This item cannot be selected. There is only one authentication mode, IKE-PSK. To enable this function, please fill in the PSK key.

PSK key: Input the key . When the client connects to the server, the key must be filled in correctly, otherwise the connection will fail.

Advanced settings: The parameters in this item are generally not modified, but the client must be configured according to the requirements here when connecting to avoid connection failure.



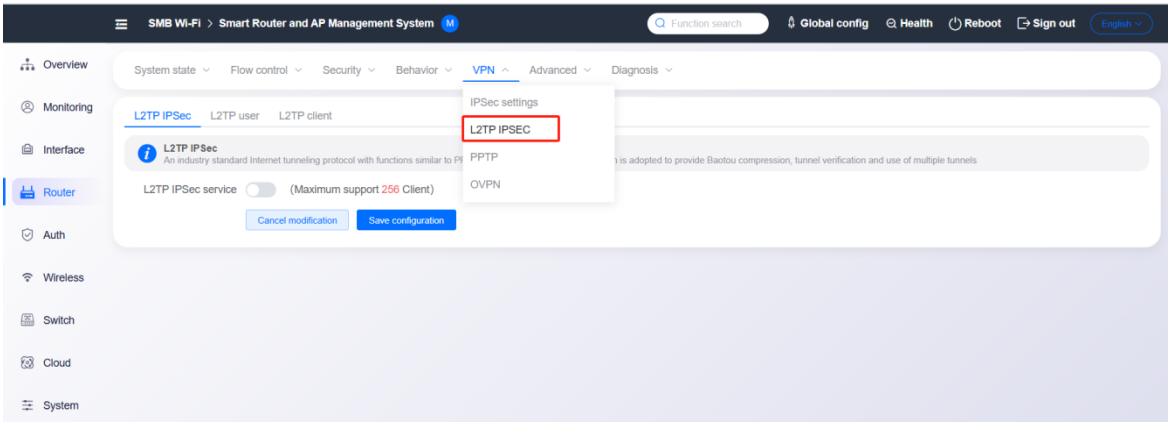
Note: IPSec point-to-network client connection requires the use of dedicated VPN connection software, and vpn-client-2.1.7-release.exe is recommended.

4.5.2 L2TP IPSEC

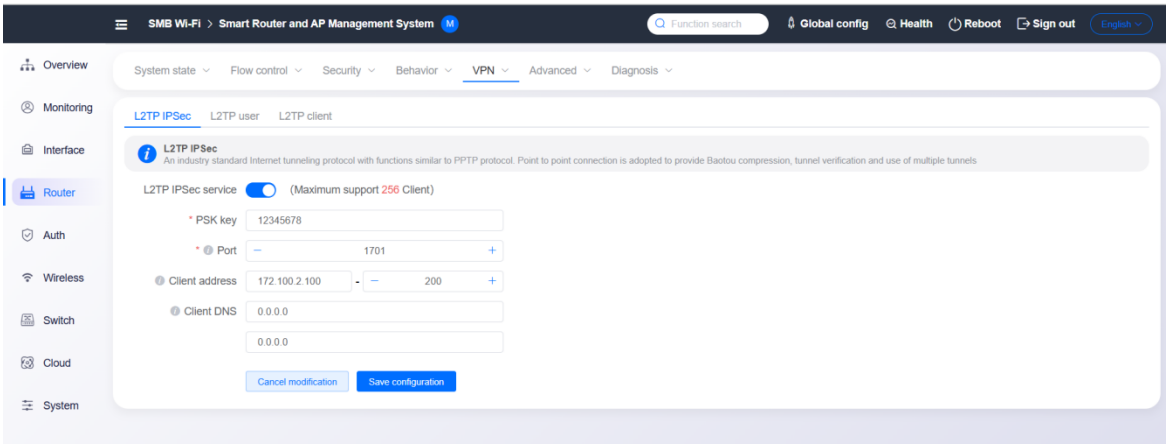
L2TP IPSec is an industry-standard Internet tunneling protocol that is similar in function to the PPTP protocol. It uses point-to-point connections, provides header compression, tunnel authentication, and uses multiple tunnels

4.5.2.1 L2TP IPSec

Configure the L2TP IPSec server



L2TP IPSec Service: Enable or disable the L2TP IPSec server. Only when it is enabled, the server parameters be configured.



PSK Key：Input the PSK key；

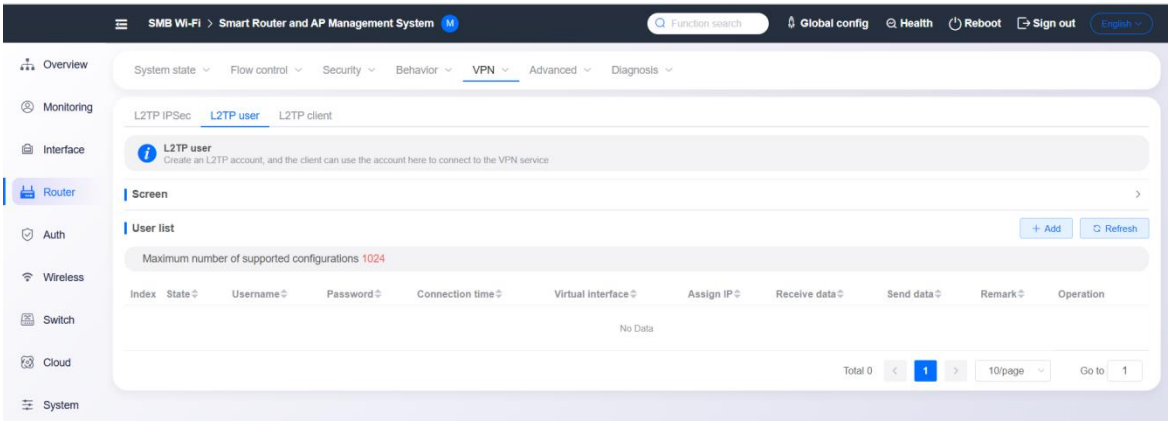
Port: The default port of L2TP IPSec is 1701, which is usually not modified;

Client address: the DHCP address pool range assigned by the server to the client. This IP is the virtual IP when connecting to L2TP. Please do not set this IP in the same network segment as other IPs on the router, otherwise it will cause IP conflicts and network failures.

Client DNS: The DNS address assigned to the client. It is recommended to fill in the local DNS address.

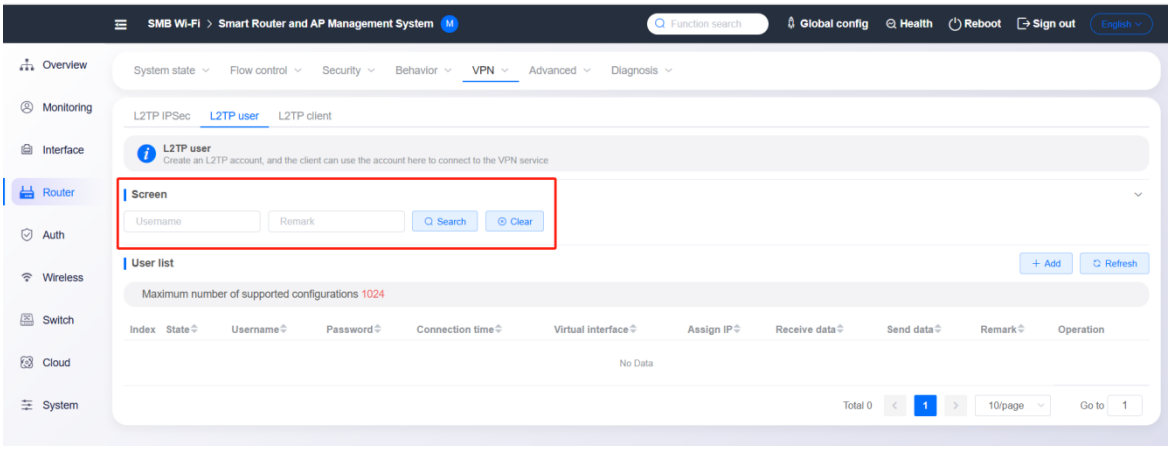
4.5.2.2 L2TP user

The client should have an account and password to connect to the server. In this menu, can create a user account and an L2TP account. The client can use this account to connect the VPN service.



Screen

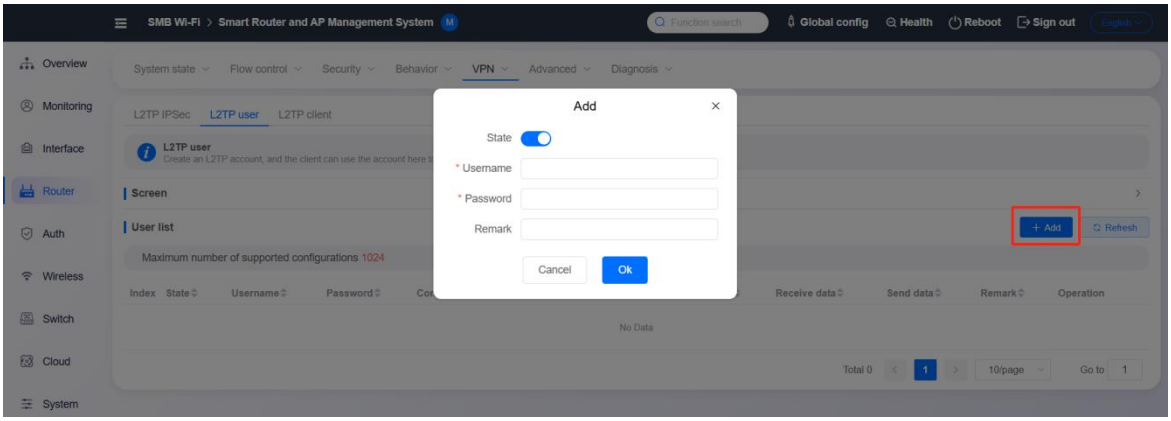
Supports conditional filtering and searching for users by user name and remarks, and user information that meets the filtering criteria is displayed in the " **User List** ".



User List

Display the added L2TP user account information.

Add: Add L2TP account.

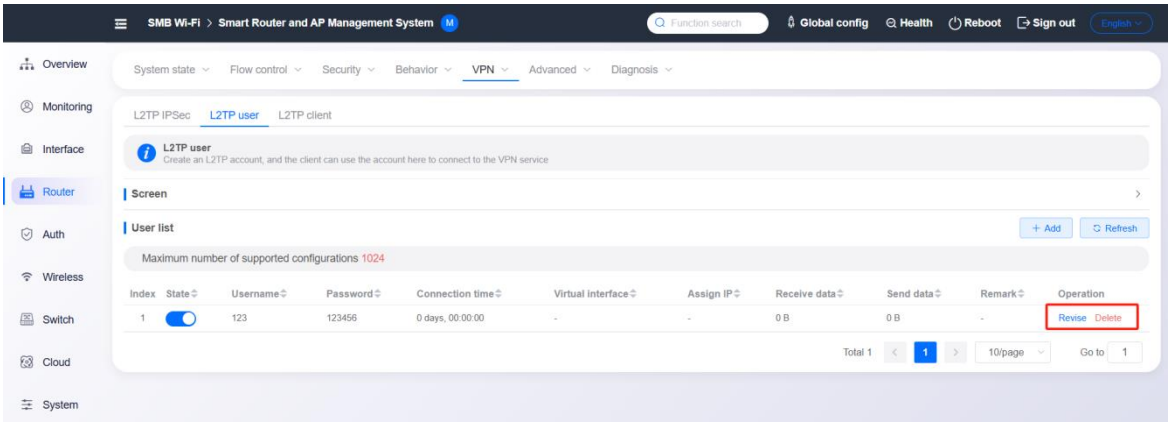


State: Set the user account status to enable or disable. A disabled account cannot be used normally.

Username: Set the user account;

Password: Set the user connection password;

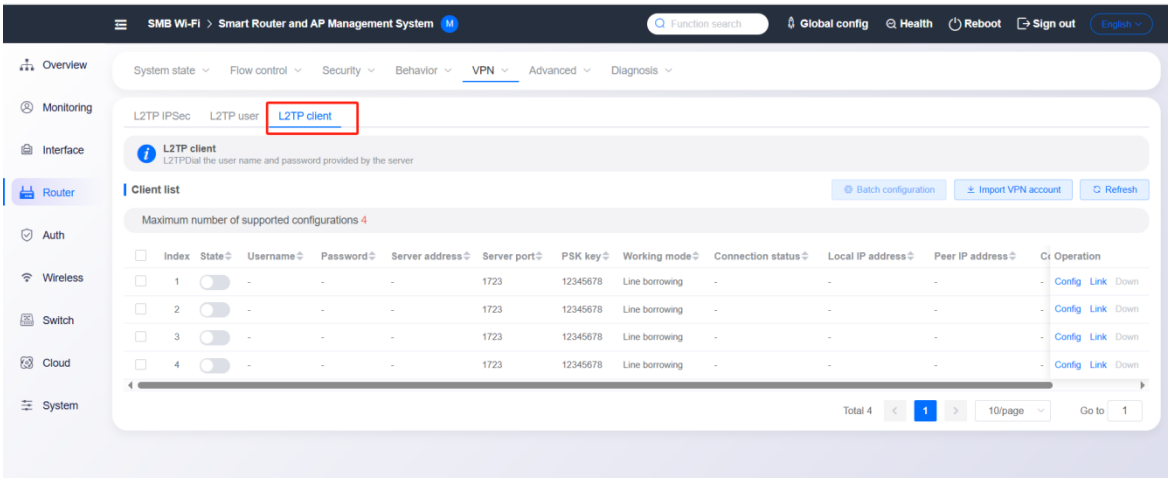
Remarks: Optional item, define the remarks content.



After the account is added, it is displayed in a list format. The account can be revised or deleted. The list also displays the connection status and data reception of the current account.

4.5.2.3 L2TP Client

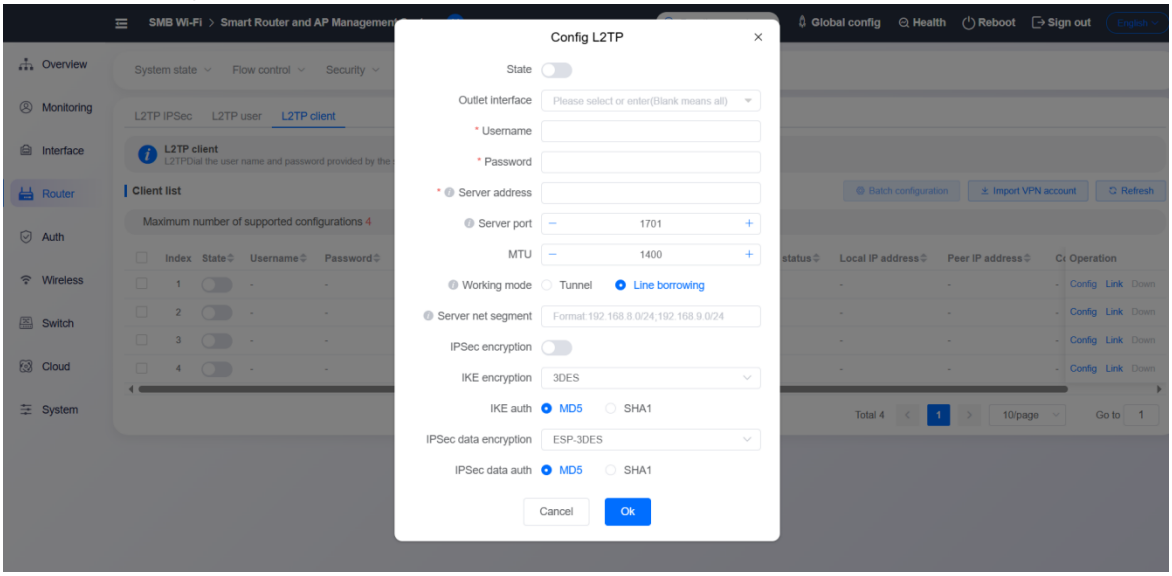
Build the connection by the account from L2TP server. It should be noted that the client of this system cannot use the account set by the server of this system. The maximum number of supported clients depends on the device model. The maximum number of supported clients varies for different models.



Client list

Display the connection status of L2TP client; It should be noted that L2TP client account and PPTP client account are shared. The list operation bar supports account config, link up and link down.

Configuration: configure and modify accounts, rule parameters, etc.



State: This refers to the usage status of the account. When it is disabled, the account cannot be used.

Outlet interface: which WAN port does the L2TP client is outlet; The selected WAN port must be unobstructed and available.

Username: user account;

Password: L2TP user login password;

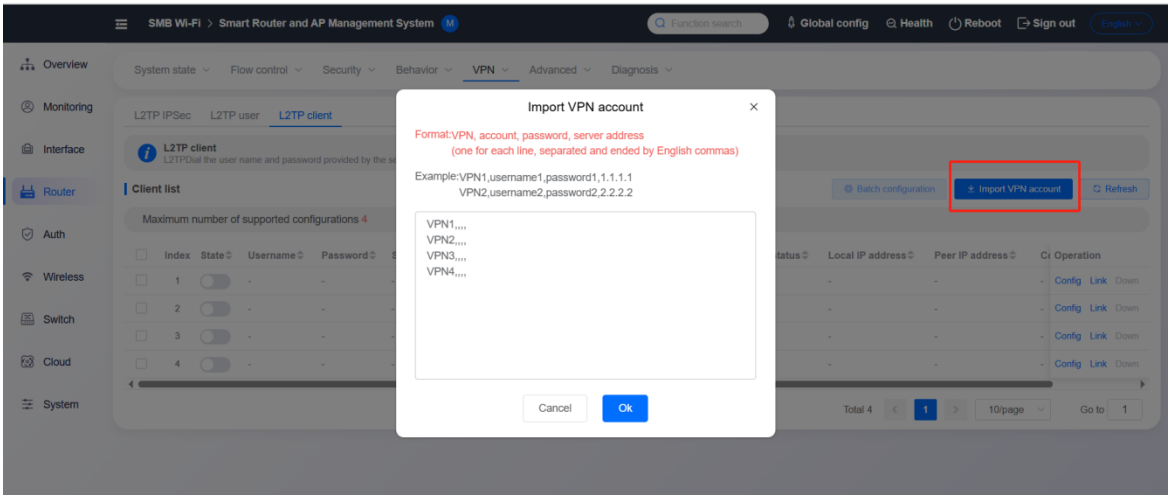
Server address: Enter the public IP address of the L2TP server;

Server port: L2TP server port. The default port is 1701. Please check the port number of the actual server before making any changes.

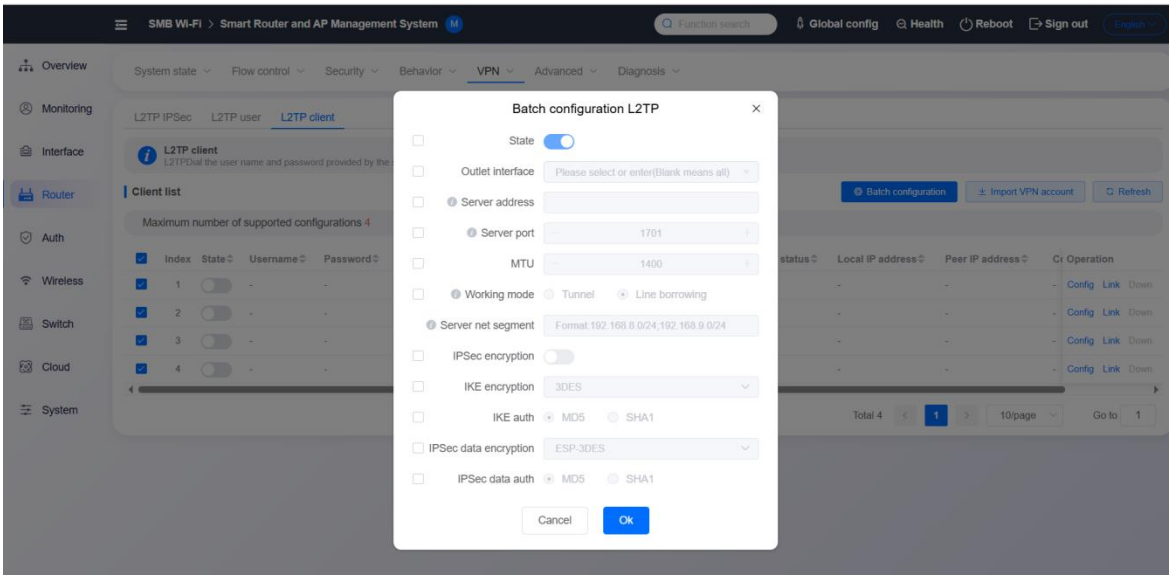
MTU setting: The default value is 1400 , generally it is not modified;

Working mode: Select tunnel mode and line borrowing mode;
Tunnel mode: The router is used only as a VPN connection. It can share the internal resources of the virtual network segment, but cannot access the external resources of the server (that is, the borrowing line function cannot be used).
Line borrowing mode: The router client can borrow the server's network to access external resources through the server's network, but cannot access the server's internal resources.
Server net segment : This item is effective only when the tunnel mode is selected. Enter the server's intranet segment here (for example, if the server's intranet address is 192.168.2.1, then enter 192.168.2.0/24 here). Note that the server's intranet segment cannot be the same as the local segment. If they are the same, please modify the local segment or the server segment .
IPSEC encryption: whether to enable IPSEC encryption. If the server has enabled encryption and set a key, you must also enable it here and enter the password set by the server;
PSK key: Enter the key set on the server;
IKE encryption: encryption method, 3DES by default in this device;
IKE auth: MD5 by default for this router. If the server is SHA1, please select SHA1;
IPSEC data encryption: ESP-3DE5 encryption by default for this router. please check the server' s encryption before making any changes.
IPSEC data auth: MD5 in default for this router. Please check the server' s data before making any changes.

Import VPN account: When the device supports multiple L2TP clients and multiple L2TP clients, can batch import the VPN accounts. The batch imported accounts are all in borrowed line mode.



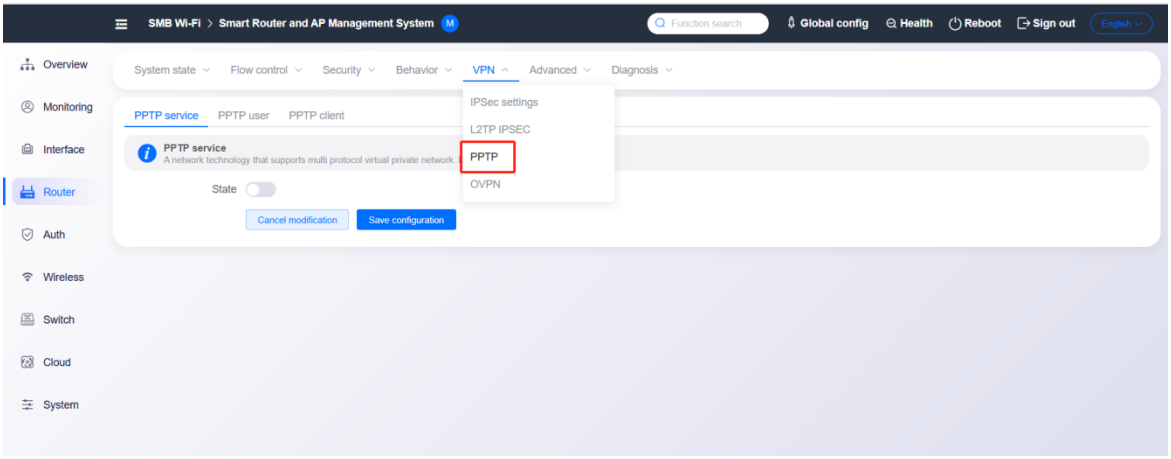
Batch configuration: Batch modify and edit parameters of established connection rules



Refresh: Refresh all information in the list

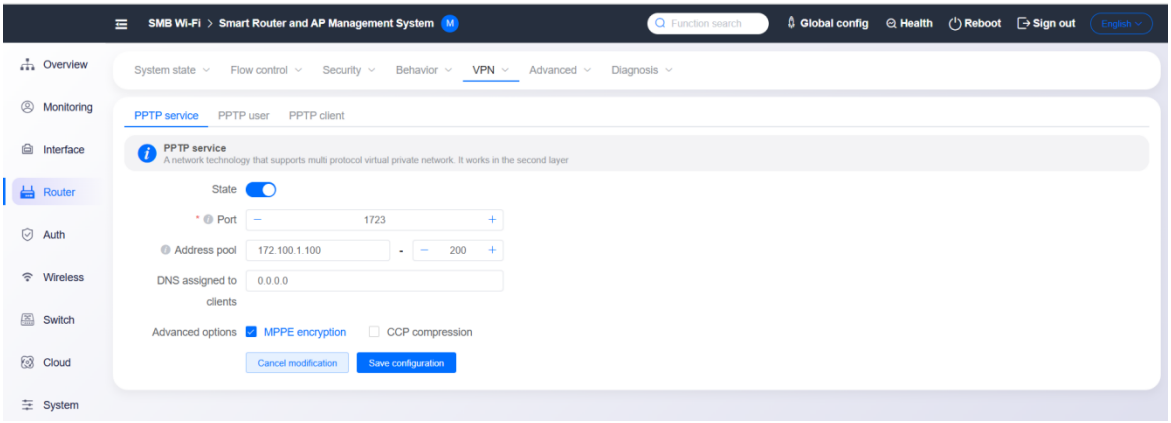
4.5.3 PPTP

PPTP VPN is a network technology that works at Layer 2 and supports multi-protocol virtual private networks.

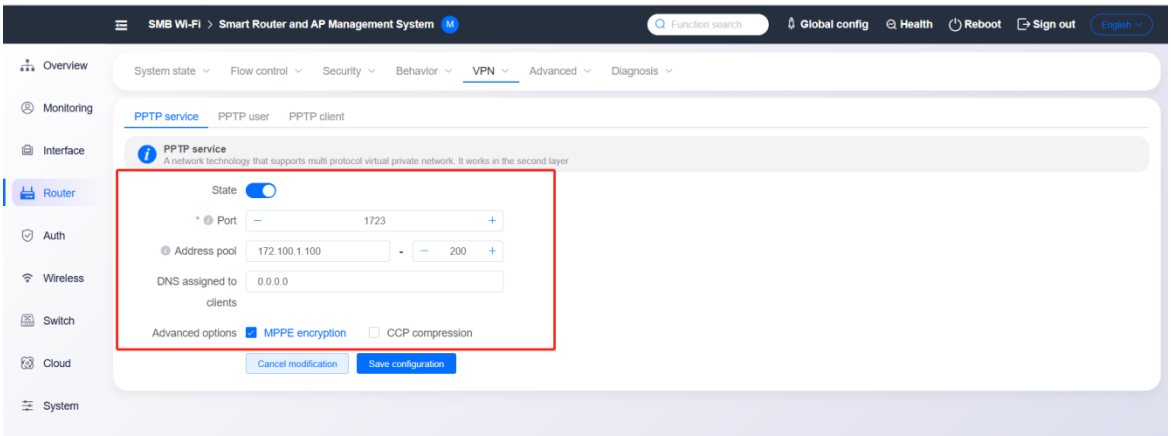


4.5.3.1 PPTP Service

Used to configure PPTP server status and parameters.



PPTP service is working under PPTP service state is enabled.



State: Disable or enable the PPTP service.

Port: The default port of the PPTP server is 1723. The system generally has fixed settings for each VPN port and generally does not make changes. Before modify it, please confirm whether the modified port has any conflicts;

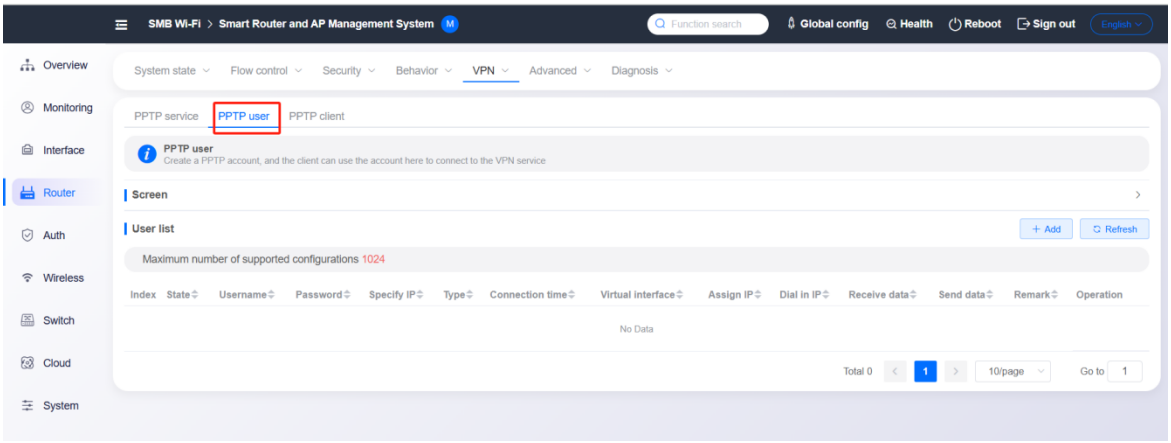
Address pool: The available range of IP addresses allocated to clients. Enter the starting address in the first input box and the ending address in the second input box. For example, the format is: 10.10.10.100-200; allocated to clients;

DNS assigned to clients: The DNS address assigned to the client. It is recommended to fill in the local DNS address;

Advanced options: Support MPPE encryption and CCP compression. If check this option, should check the corresponding encryption method when configuring the client .

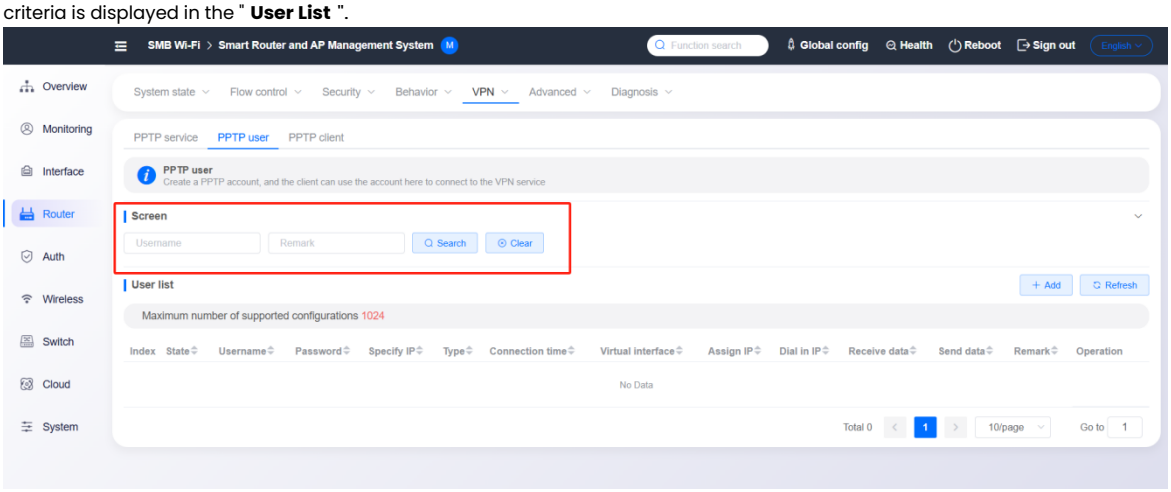
4.5.3.2 PPTP users

After creates a PPTP user account and the PPTP user connection is successfully, the account connection status, time, data sending and receiving, and mark information are displayed in the list.



Screen

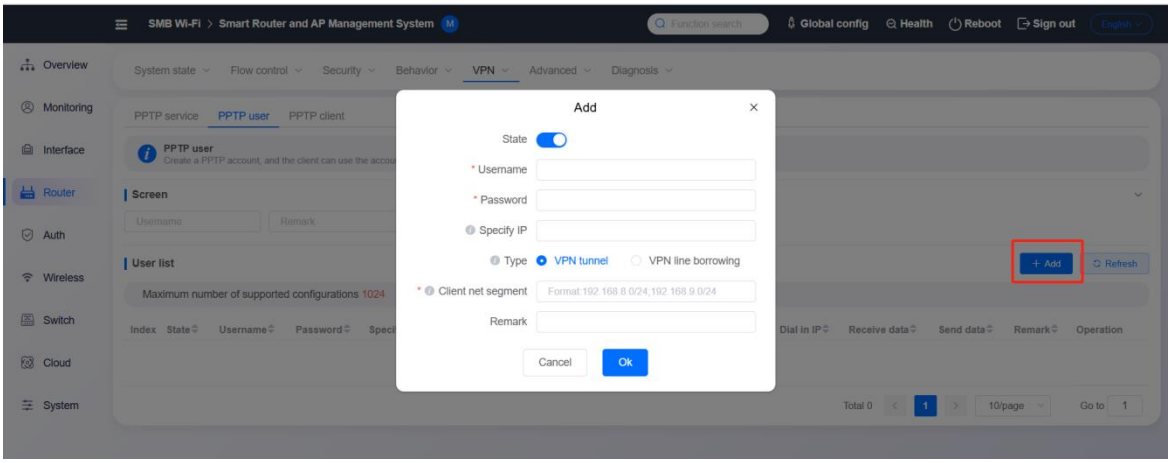
Supports conditional filtering and searching for users by user name and remarks, and user information that meets the filtering criteria is displayed in the " **User List** ".



User list

Display the added PPTP user account information.

Add: Add a PPTP user account. Different router can create different number of PPTP users, different router can support different number of PPTP users. Please pay attention to this.



State: After it is enabled, the account can be used normally. After it is disabled, the account cannot be used (dial-up fails);

Username: Set the user account. The rule is 1-31 characters, including Chinese characters, letters, numbers and _-!@#$%^&*().;

Password: Set the PPTP dial-up password, the rule limits 4-31 characters ;

Specify IP: Set a dedicated IP address for the account. This address cannot conflict with the client or server intranet address. After specifying the IP address, only the account can use this IP address, and this IP address will not be allocated to other accounts. If the specified IP is empty, the client will default to using 172.100.1.101;

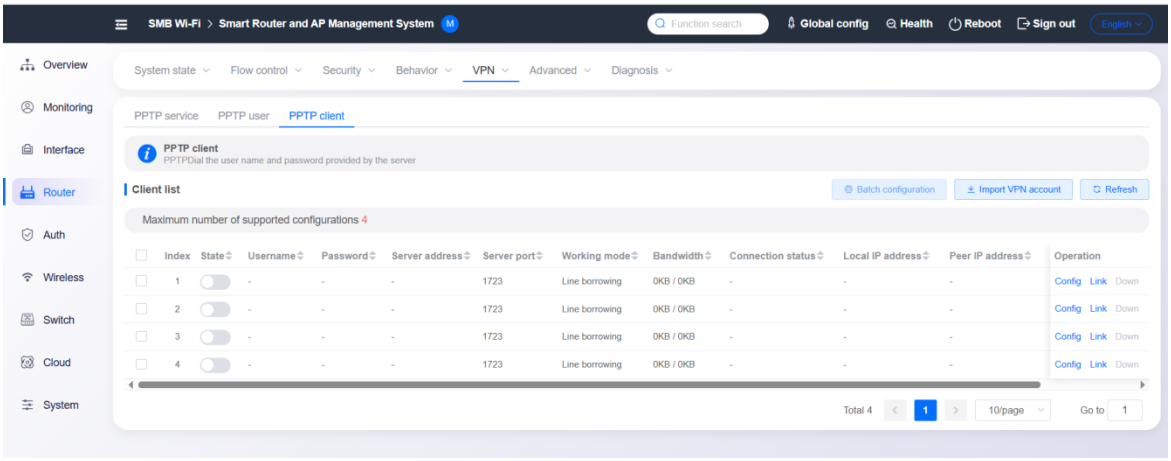
Type: Select the type of PPTP account: VPN tunnel, connects two LANs to form a virtual LAN, mainly used for LAN shared access; VPN line borrowing , the client accesses the Internet through the server's external network line, which can be understood as an IP proxy. The client can use the borrowing line as a policy routing rule to allow the required data to go through the VPN borrowing line path;

Client net segment: In VPN tunnel mode, fill in the client intranet segment address. For example, if the client intranet address is 192.168.2.1 , should fill in 192.168.2.0 /24 here. No need to fill in the borrowed line mode ;

Remark: Customize the note content.

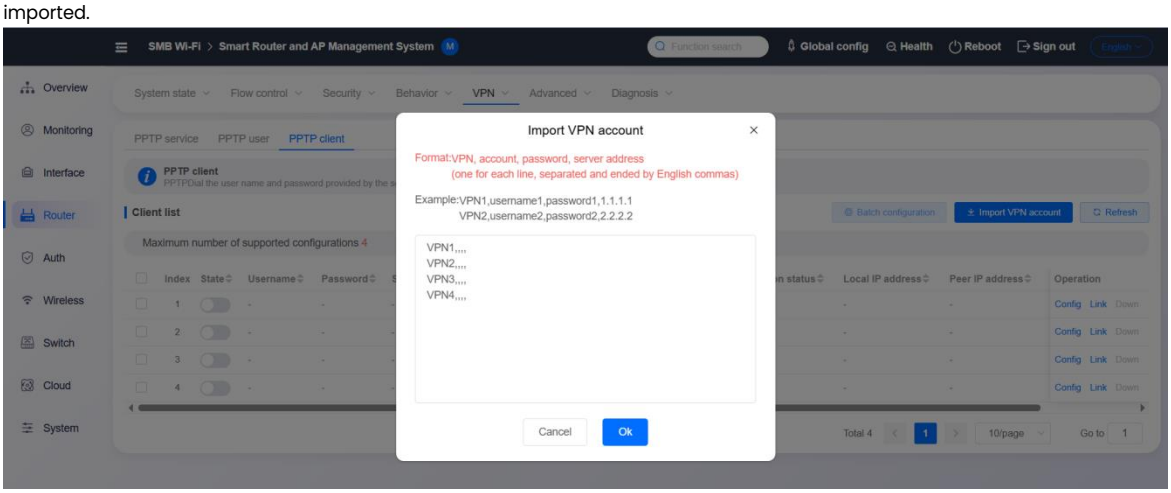
4.5.3.3 PPTP Client

This router is work as PPTP client, should dial to the PPTP server by the account and password provided by the server . The account at the PPTP client and the L2TP client account are shared, so if an account is added and edited in the L2TP client, the same account will be showed in the PPTP client list.

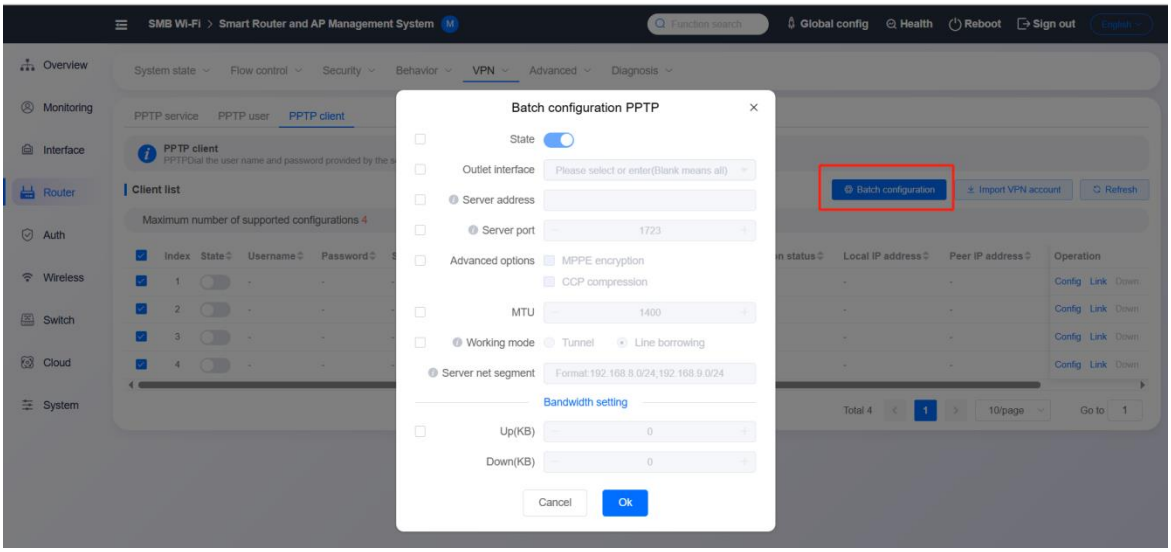


Client list

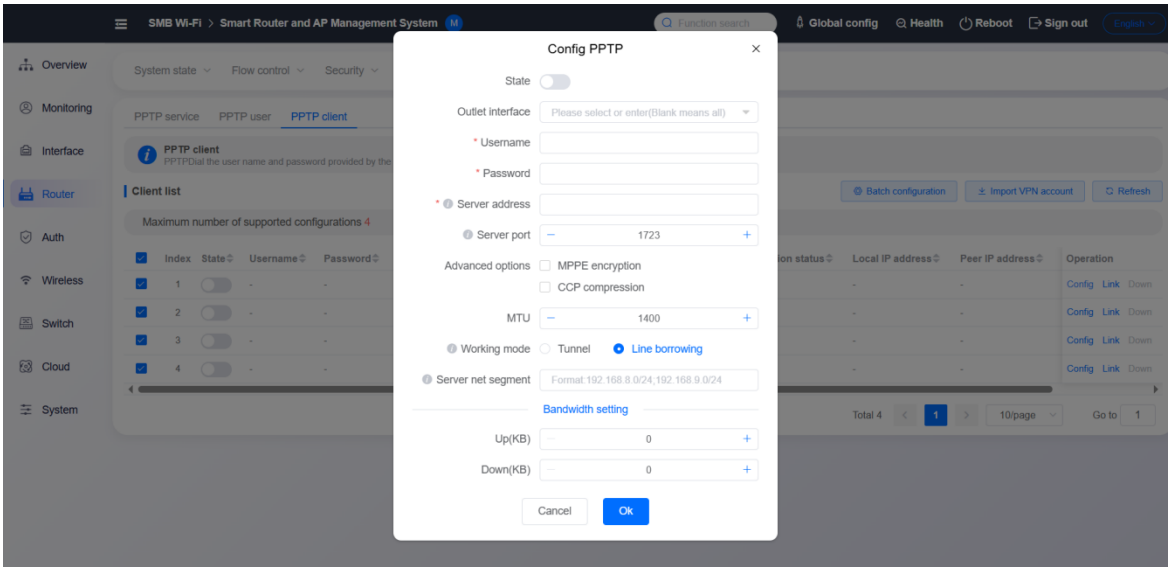
Import VPN account: When the system supports multiple PPTP client dial-up and multiple VPNs need to be dialed at the same time, can import the VPN account from import VPN account; The default imported VPN account is the borrowed line mode; if the system only supports 1 client dial-up, even if multiple accounts are imported, only the first VPN account can be successfully imported.



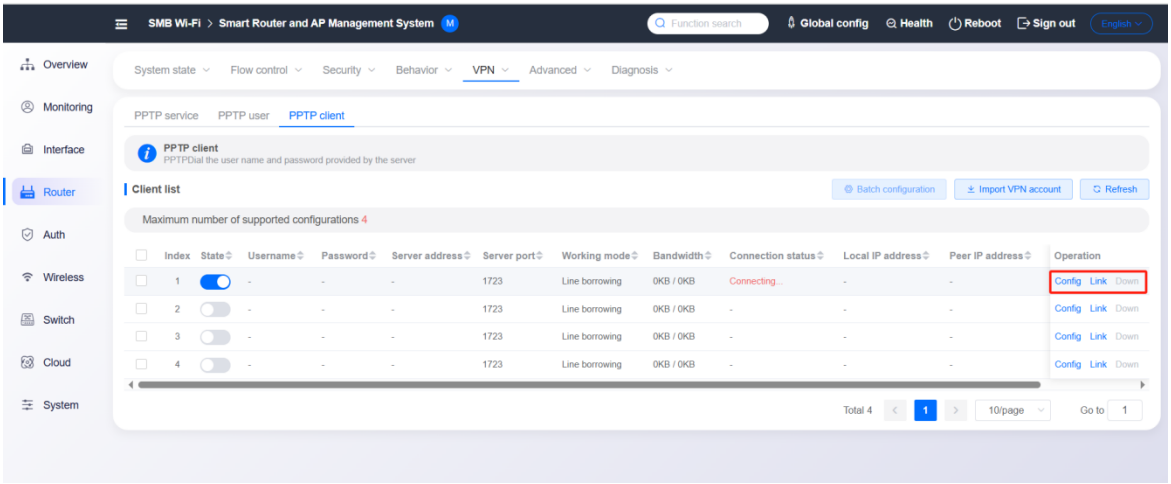
Batch configuration: If we want to configure multiple or a certain VPN account,can click Batch configuration.



Config: Modify the PPTP client account configuration content.

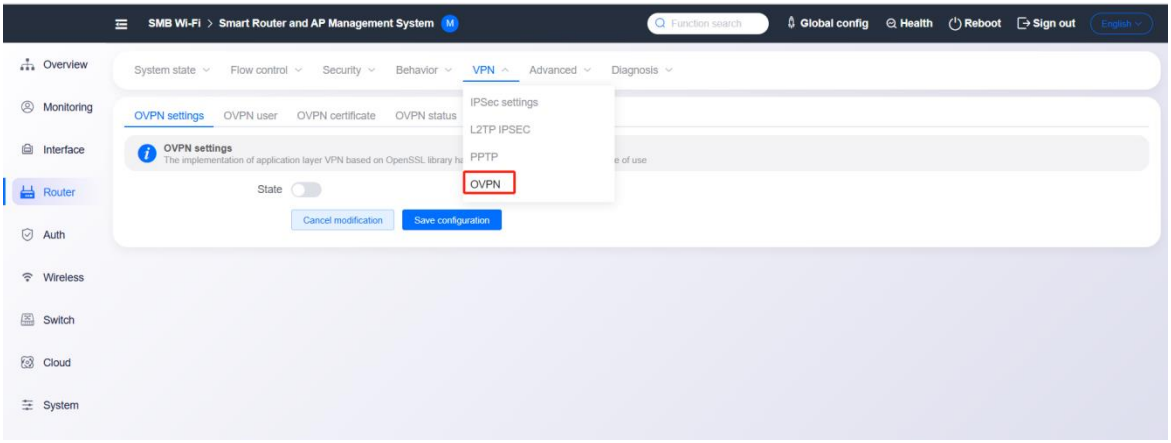


State: After it is enabled, the account can be used normally. After it is disabled, the account cannot be used (dial-up fails);
Outlet interface: Select the client data export (WAN port) port. After being specified, the client data will only be exported from this WAN port. The specified export must be unobstructed and usable. The system generally defaults to ALL, which means all the WAN port used by the current system can be used. This client account can be used randomly as an export;
Username: user dial-up account;
Password: user dial-up password;
Server address: Fill in the server's public IP address;
Server port: the server port. The default port is 1723. Before modify it, please confirm the server port appropriately.
Advanced options: support MPPE encryption and CCP compression. Before selecting these two options, please confirm with the server whether they are supported;
MTU: The default value is 1400, and it is generally not recommended to modify it;
Working mode: Select the mode of the account client, either tunnel mode or line borrowing mode ;
Server net segment : Fill in the network segment of the server's intranet. Note that the server's intranet segment cannot be the same as the local network segment. If same, please modify the local network segment or the server's network segment . For example, if the server's intranet address is 192.168.8.1 , then 192.168.8.0/24 should be filled in here;
Bandwidth settings: Set the uplink and downlink speed limits for this account. The default value is 0, which means no limit.
When the client is connected successfully, the user list column on the server will show that the account is connected and related data, the connected client account operation column will be displayed in the client connection list, supporting modification and disconnection operations on the current account.



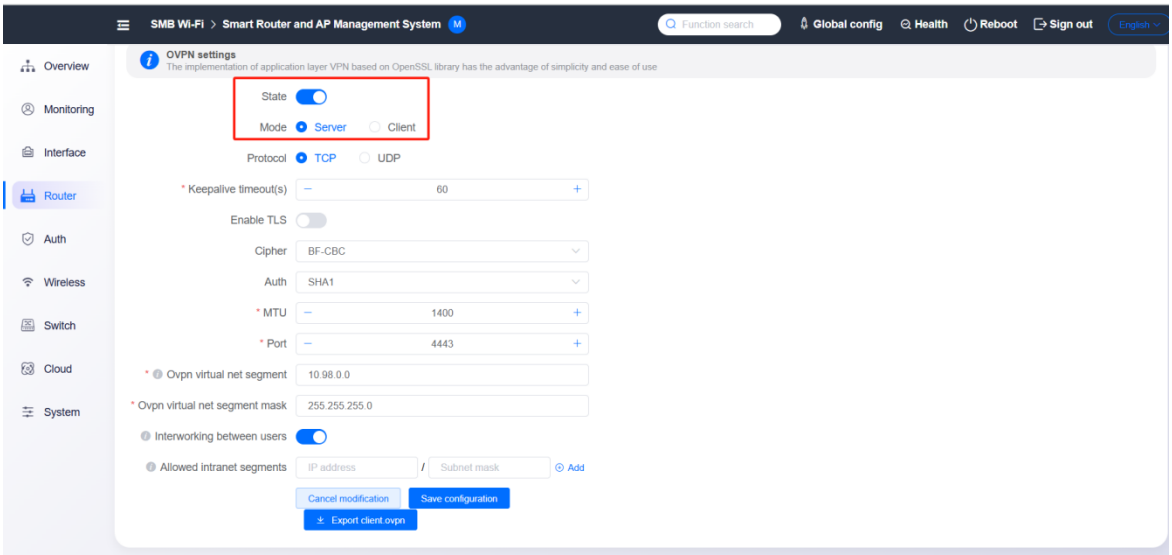
4.5.4 OVPN

The application layer VPN is implemented based on the OpenSSL library, which has the advantage of being simple and easy to use.



4.5.4.1 OVPN settings

After the OVPN status is enabled, pls select the OVPN mode as OVPN server or the OVPN client.



State: Only when the OVPN status is enabled, the next step parameters be configured;

OVPN Mode: Select whether this router is the OVPN client or server;

---Server---

Protocol: Customize the protocol used by the OVPN service. The default is TCP protocol;

Keepalive timeout (seconds): If no data is received from the client within the set time, it is considered a connection timeout;

MTU: define the MTU value of VPN data transmission, which is used in special environments and generally kept at the default value;

Port: customize a port used by the OVPN service. The default is 4443, which can be changed to other unoccupied ports. Please check to avoid conflicts with other ports before changing.

OVPN virtual network segment address: customize a virtual network segment address used to connect to VPN. This network segment is used to assign the client's OVPN address (please avoid the network segment in use. If you are using 192.168.XX, please use the IP segment of 10.X or 172.X);

OVPN virtual net segment mask: customize a virtual network mask used to connect to VPN;

Interworking between users: After it is enabled, OVPN clients can communicate with each other;

Allowed intranet segments: Allow the VPN client to access the internal network segment after connecting in. Fill in the network segment in the local area network.

---Client---

Protocol: Select the protocol type used for the VPN connection. It must be consistent with the protocol type on the server, otherwise the VPN connection will fail.

Keepalive timeout (seconds): If no data is received from the client within the set time, it is considered a connection timeout;

MTU setting: The MTU value of the VPN connection can be customized by the user, and the default value is generally used;

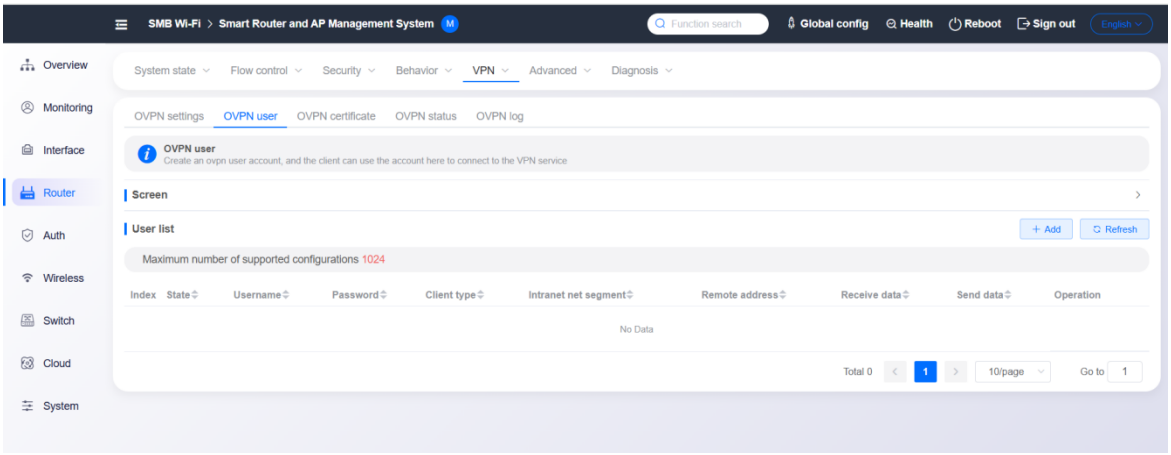
Username: Enter the OVPN account provided by the server ;

Password: Enter the OVPN password provided by the server;

Server address: Fill in the OVPN server public IP address plus the server port. If there are multiple public networks on the server, click the Add button to add it.

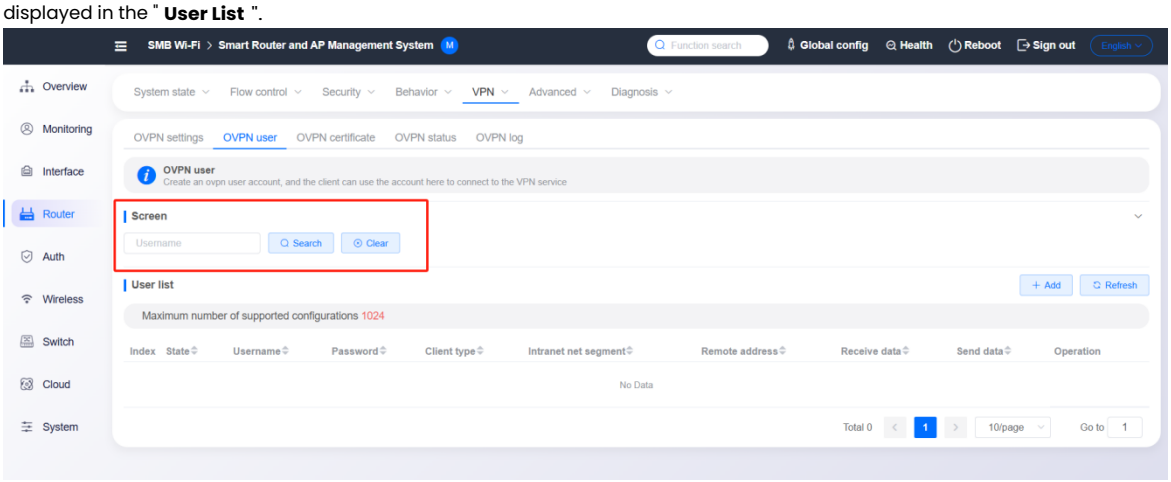
4.5.4.2 OVPN user

Create an OVPN user account. The client can use this account to connect to the VPN service.



Screen

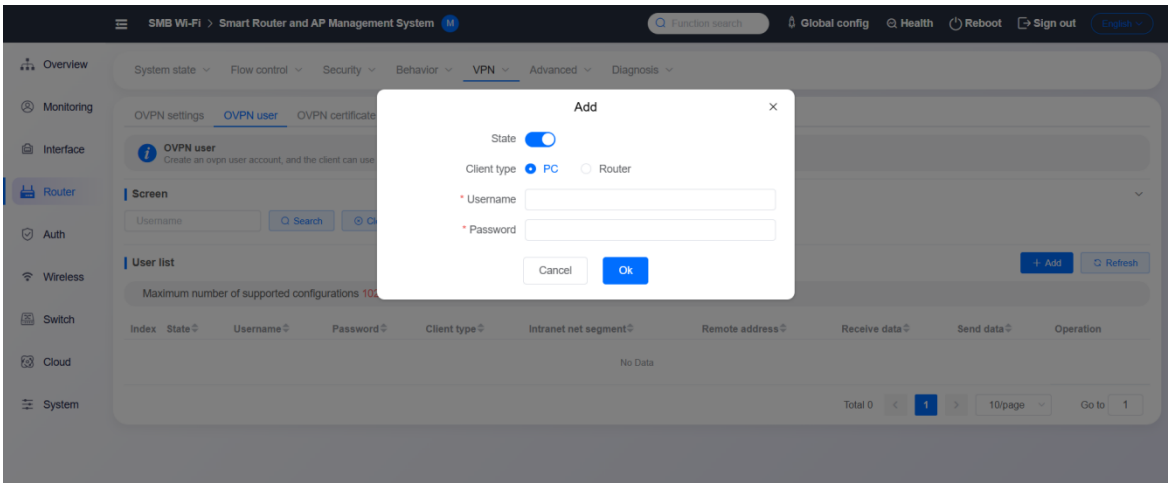
Supports conditional filtering and searching for users by user name, and user information that meets the filtering conditions is displayed in the " **User List** ".



User List

Display the added PPTP user account information.

Add: Add an OVPN user account.

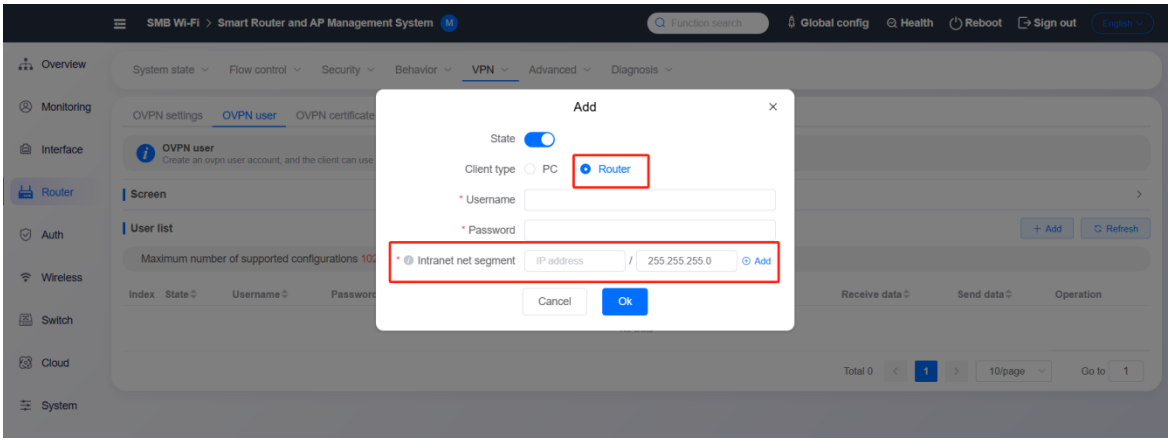


User status: The user account can be used normally when it is enabled, and the account cannot be used normally when the status is disabled;

Client Type: Select the type of client;

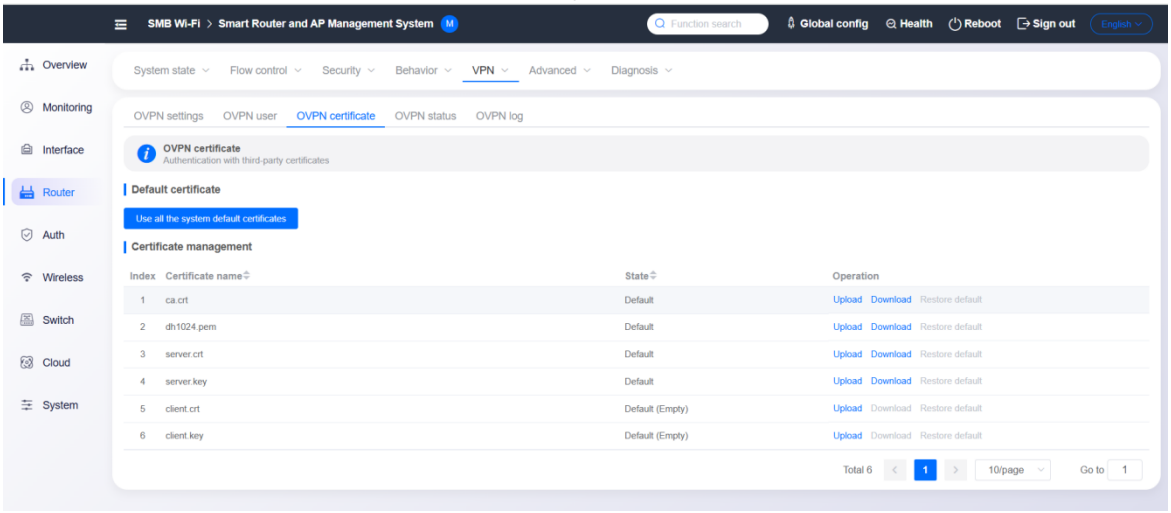
Password: The password corresponding to this account set by the server;

Intranet net segment: This item is only available if the client is a router type. Please fill in the intranet segment of the client router . It should be noted that the client's intranet segment cannot be the same as the server's intranet segment .



4.5.4.3 OVPN Certificate

It require OVPN certificate for OPVN function; The OVPN certificate will be used for the 3rd certification identify, support it in default for this router; Can update the certificate after uploading the new one.



Default Certificate

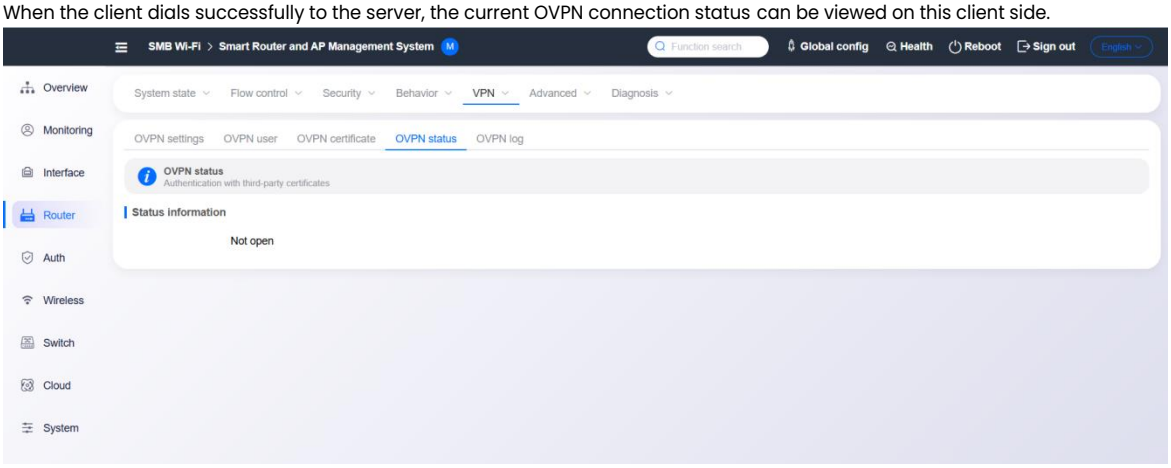
The system comes with its own certificate.

Certificate Management

The operation item can upload a new certificate or download the currently used certificate. After updated the new certificate, it supports **"Restore Default"** certificate.

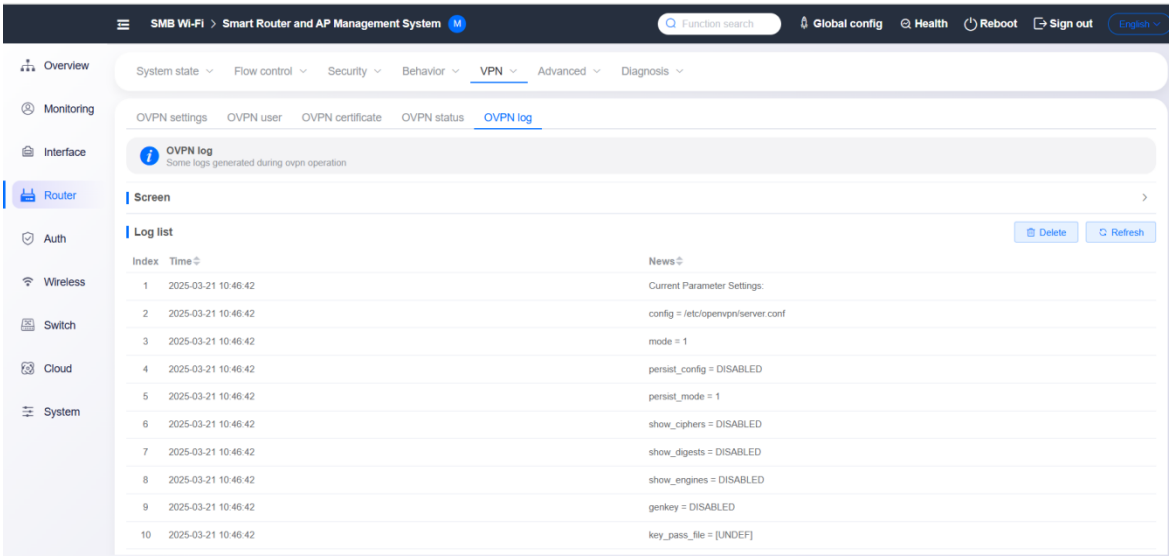
4.5.4.4 OVPN status

When the client dials successfully to the server, the current OVPN connection status can be viewed on this client side.



4.5.4.5 OVPN log

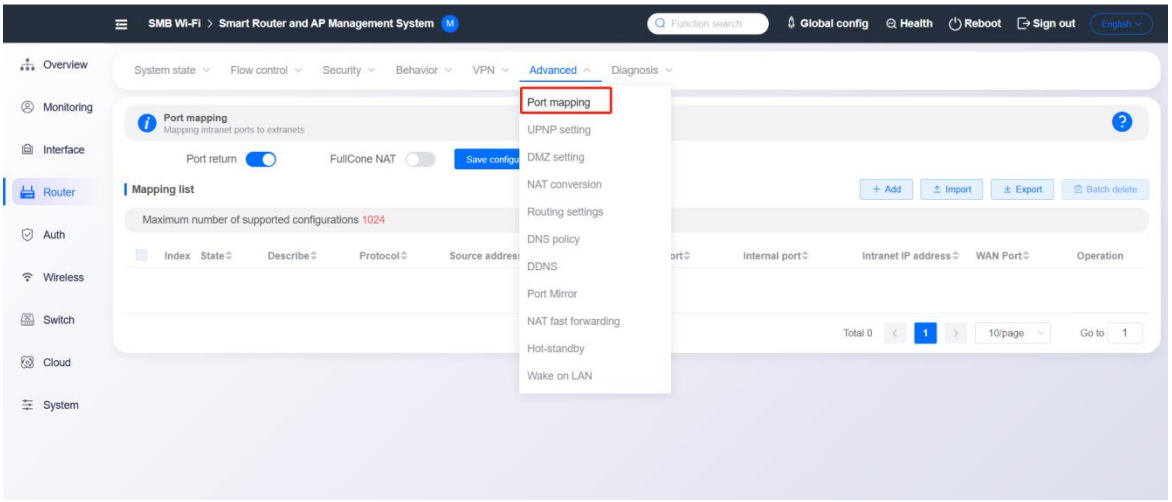
Record OVPN related logs. The operation items support refresh and delete operations. Deleted logs cannot be restored.



4.6 Advanced

4.6.1 Port Mapping

Configure mapping rules to map the intranet port to the external network so that other hosts on the external network can access the port content.

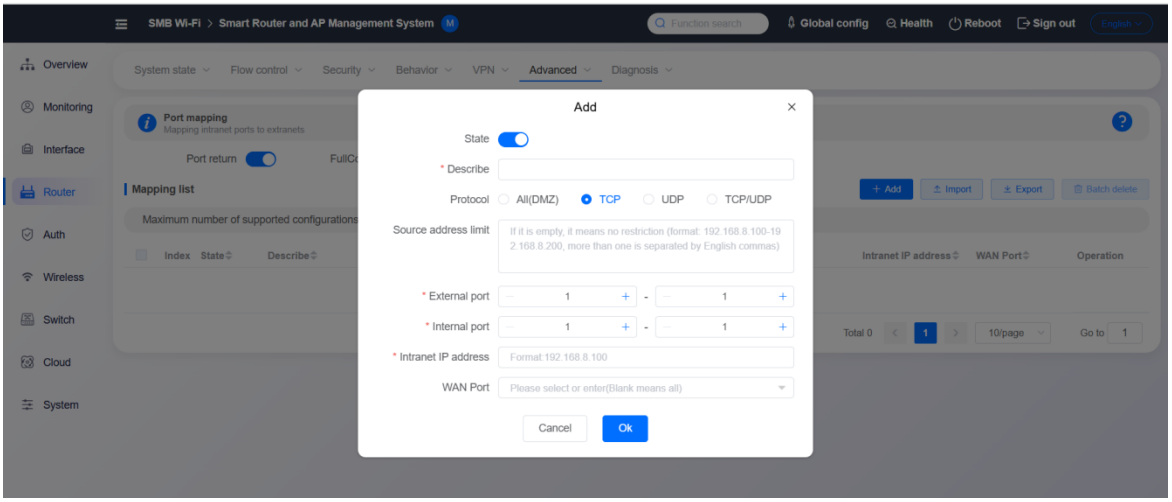


Port return: The system generally enables port return by default;

FullCone NAT: The system is disabled by default. It is generally recommended to enable this function in a CDN environment.

Mapping List

Add : Add a mapping rule.

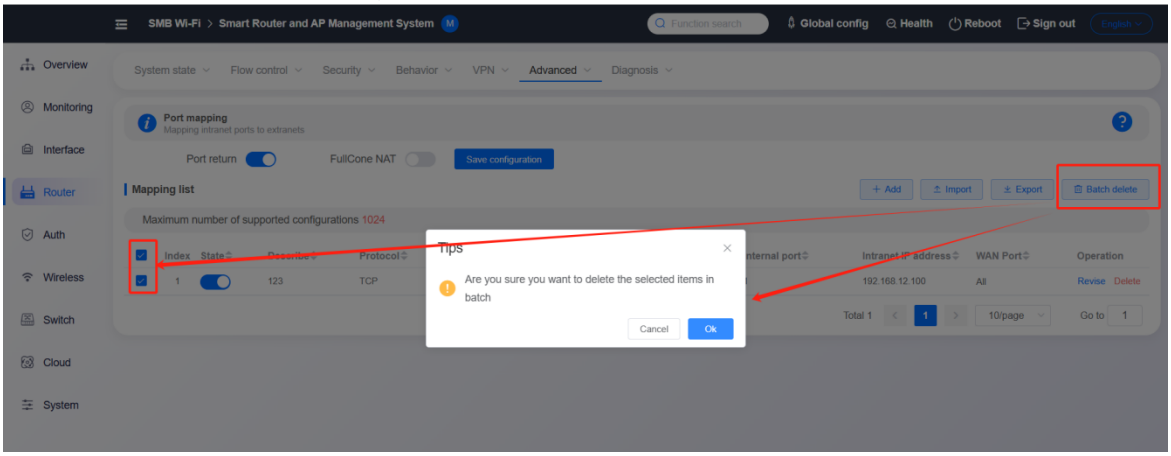


Status: Whether the rule status is enabled. If it is disabled, the mapping rule will not take effect.

Describe: Add a description of the rule to make it easier to distinguish among many rules;

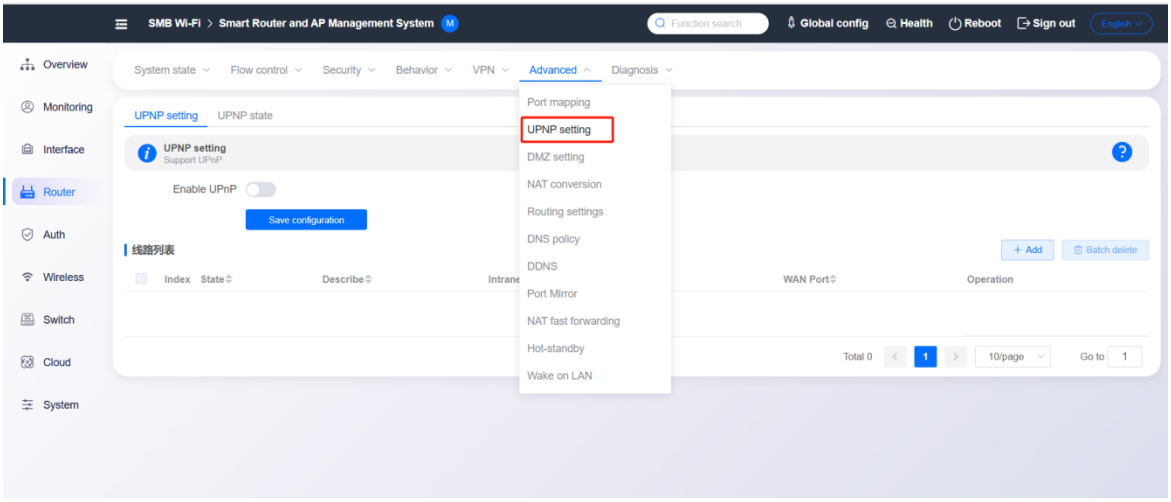
Protocol: Select the mapping protocol type. Unchecked protocols will not be mapped successfully.
Source address limit: Only the filled-in address (or address segment) can access the mapped content. If it is empty, it means no restriction;
External port: The terminal accesses the mapped content through this port plus the WAN port IP address where the mapped host is located. This port cannot conflict with other local ports;
Internal port: The port used when the internal LAN accesses the mapped machine, which is generally determined by the software itself. If the internal port to be mapped is the same as the external port, please do not fill in the internal port;
Internal IP address: The internal IP address that needs to be mapped, which is a required field;
WAN port: Select the port mapping rule export. The terminal accesses the mapped host or address through the set WAN port IP plus port.

Import: Can import port mapping rules in batches. If import file format and rules are not insured,can add a mapping rule and then export it. Can add, delete, and modify the content in the exported file, then import it again.
Export: Export the mapping rules created in the system.
Batch Delete: Check the created mapping rules and click the Batch Delete button. The deleted rules cannot be restored.



4.6.2 UPNP setting

UPnP is a communication protocol standard. If the computer supports UPnP mechanism and the computer UPnP function is turned on, the UPnP function of the router can be enabled. After enabling UPNP, P2P download software will have a certain acceleration effect, but at the same time it will also generate a greater load on the network. Excessive P2P downloads will affect the normal use of the network. Please use this function based on the request.

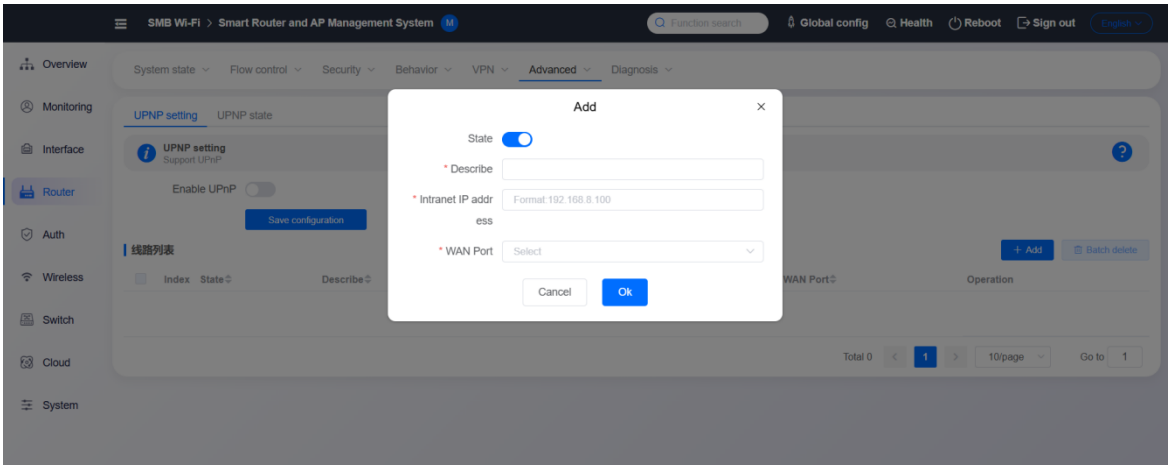


4.6.2.1 UPNP setting

Enable UPnP: The default state is disabled, can configure the corresponding rules after enabling it;
Default WAN port: Select the WAN port where the UPnP port is mapped;
Show in Network: After selecting Enable, the application software that needs to automatically map ports will be displayed in the list, making it easier for administrators to view the software types in use;

Route List

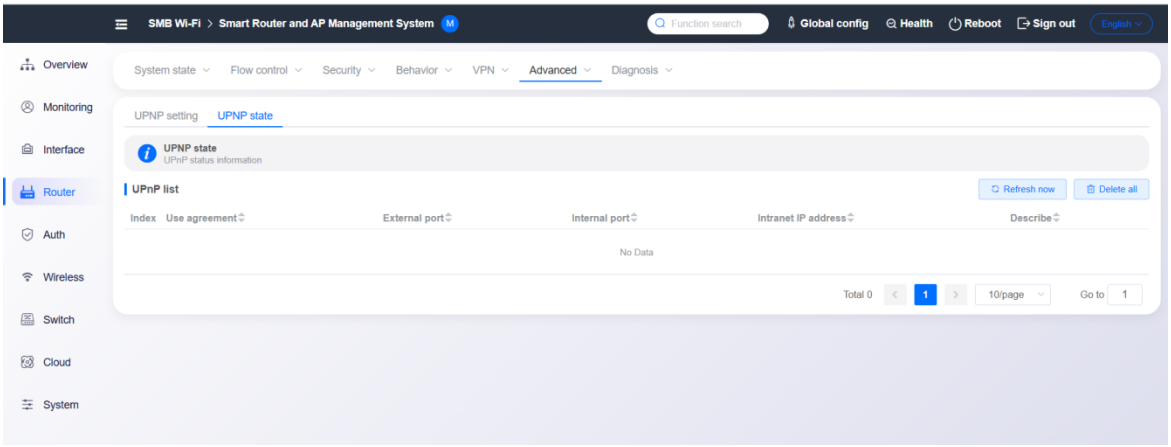
Displays the currently generated UPnP information.
Add: Manually add UPnP enable rules;



State: Control switch for a single rule, enable or disable;
Describe: A brief note and description of the rule;
Internal IP address: The internal IP address that the rule is effective for;
WAN port: The external network outlet where the rules take effect.
Batch Delete: Batch delete the selected currently generated UPNP information.

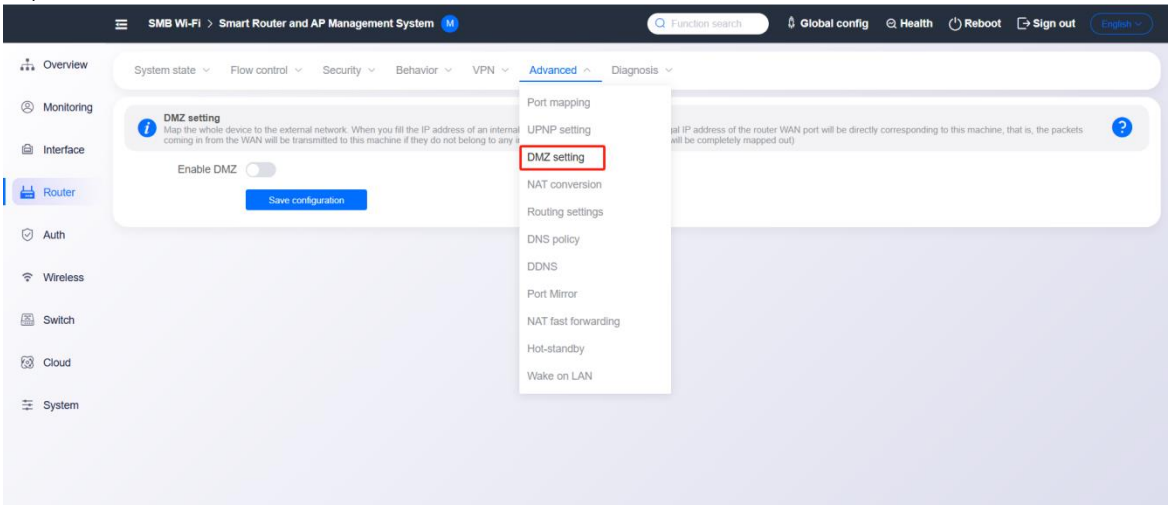
4.6.2.2 UPNP state

Displays the status information after UPNP is enabled. The operation items support "Refresh Now" and "Delete All".



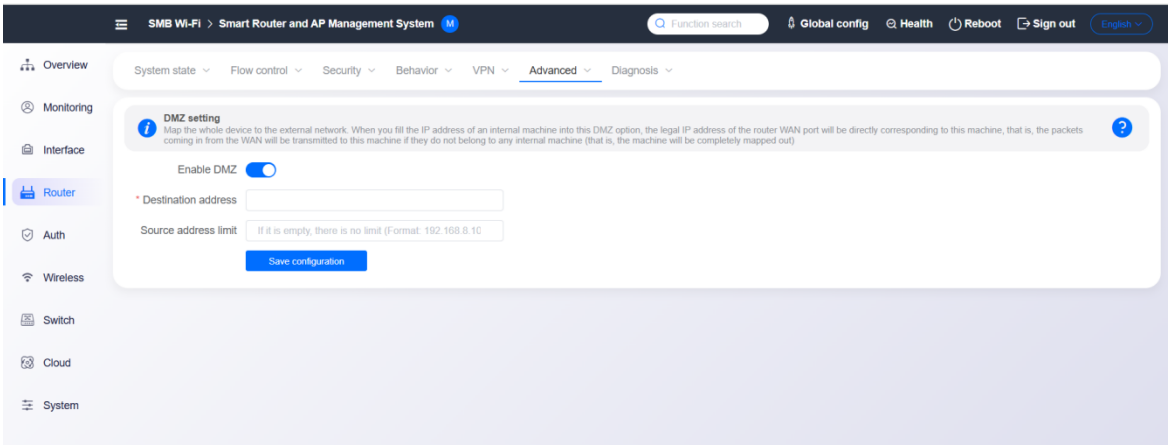
4.6.3 DMZ settings

Map the entire device to the external network.



DMZ setting

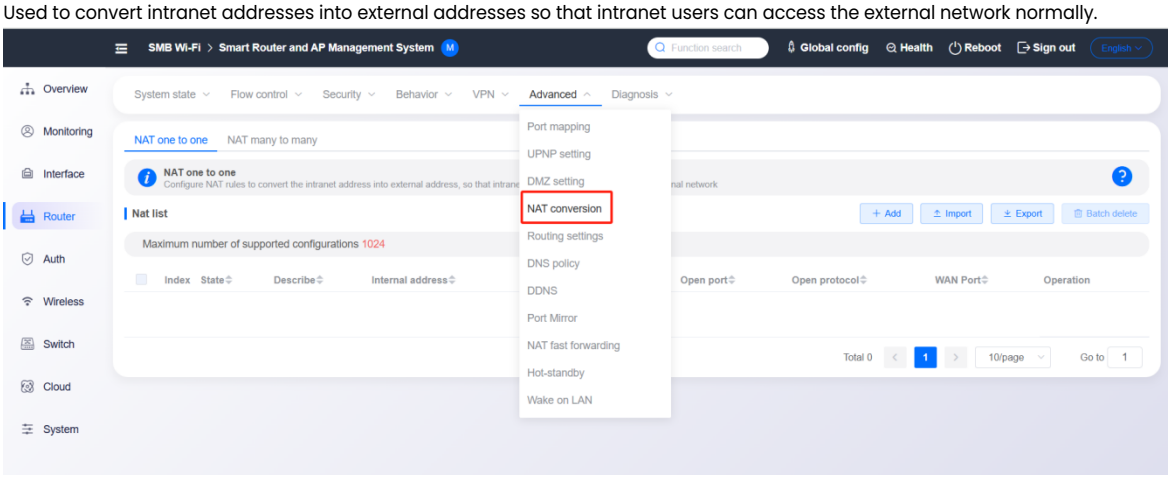
When the IP of an internal machine is filled into this DMZ option, the legal IP address of the router WAN port will be directly mapped to this machine. That is to say, packets coming from the WAN end, if they do not belong to any internal machine, will be sent to this machine (that is, this machine will be completely mapped out).



Enable DMZ: DMZ is disabled by default, and rules can only be configured when it is enabled.
Destination address: needs to be set to the internal machine IP address of the DMZ;
Source address limit: Optional, the address or address segment allowed to be accessed by the external WAN port . The three formats allowed are " 202.103.24.68 ", "202.103.24.68-202.103.44.150", and " 202.103.24.0/24 ".

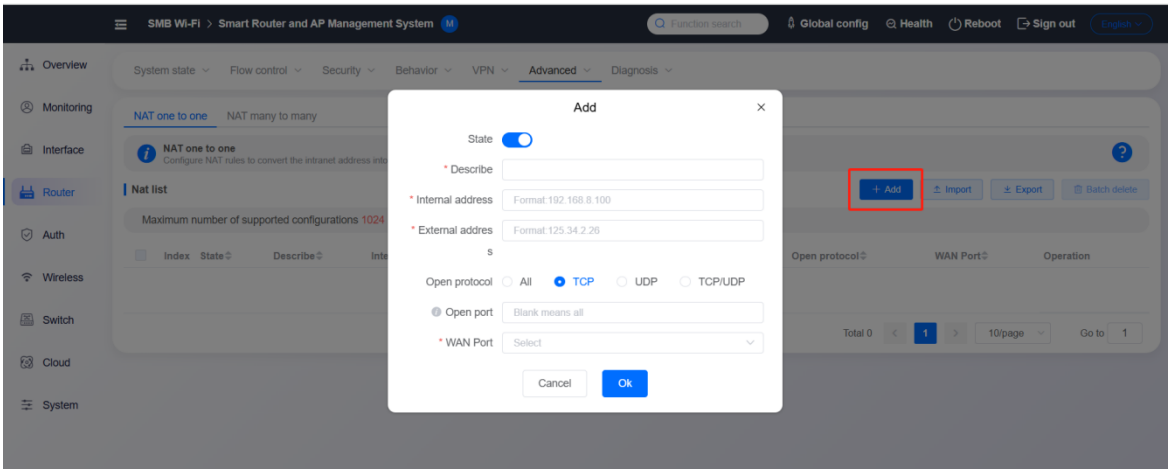
4.6.4 NAT conversion

Used to convert intranet addresses into external addresses so that intranet users can access the external network normally.



4.6.4.1 NAT one to one

By configuring NAT rules, the source address of data sent by a host is converted into a corresponding external network address, so that internal network users can access the external network normally.



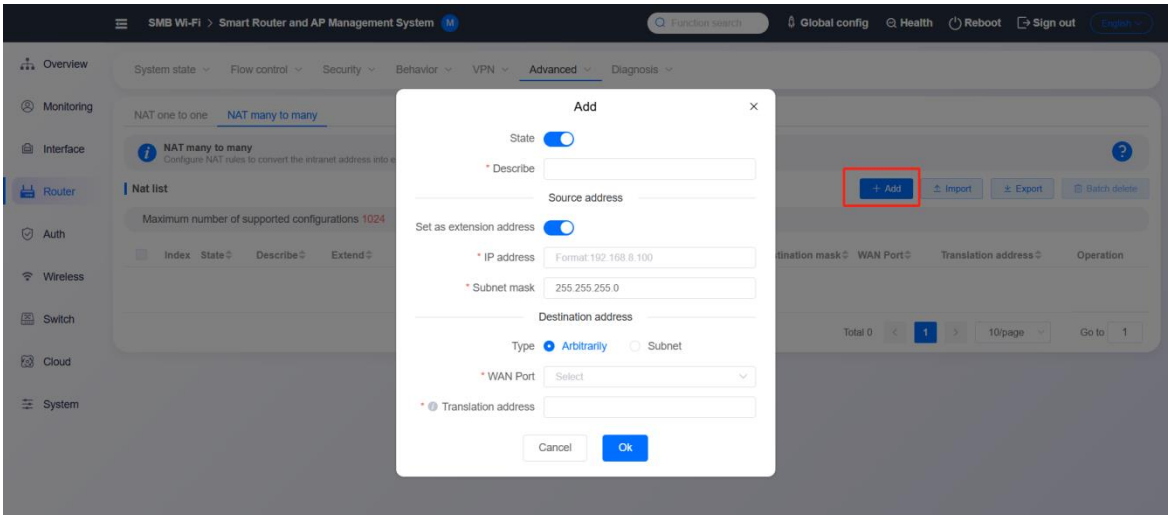
NAT List

Add: Add a one-to-one rule.
State: Whether the rule status is enabled. If it is disabled, the created one-to-one rule will not take effect.
Describe: Add a description of the rule to make it easier to distinguish among many rules;
Internal address: Fill in the local area network address for one-to-one network address translation. For example: 192.168.1.100;
External address: Fill in the external address for one-to-one network address translation. For example: 218.35.97.7 ;
Open protocol: Select the protocol that needs to be open for conversion;
Open port: Fill in the open port of the external address. If it is empty, it means all ports are open. The format is: 100,200,300:305;
WAN port: Select which WAN port is the one-to-one internal host data export.
Export: Export all current rules of the NAT list for use as a backup of the list rules. The exported rules will be directly downloaded to the specified path through the browser and saved;

Import: Import the exported NAT rules into the device where they are needed, and use them as list rule recovery;
Batch Delete: Batch delete the rules in the selected rule list.

4.6.4.2 NAT many to many

By configuring NAT rules, the specified intranet continuous addresses are converted into specified external addresses, so that intranet users can access the external network normally.

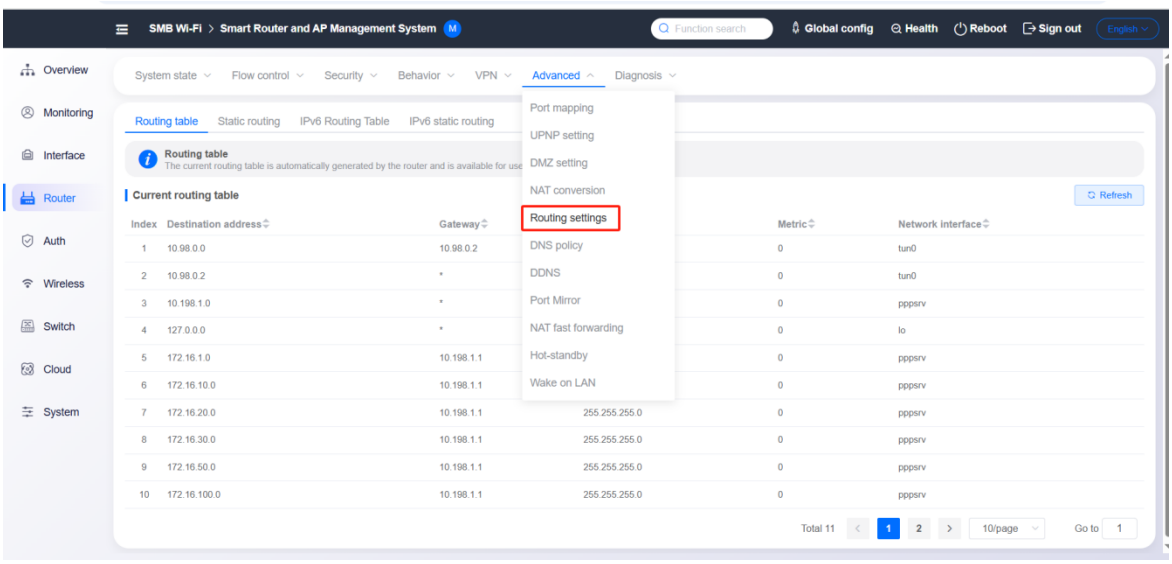


NAT List

Add: Add many-to-many rule.
State: Whether the rule status is enabled. If it is disabled, the created many-to-many rule will not take effect.
Describe: Add a description of the rule to make it easier to distinguish among many rules;
Source address is set as extension address: whether to block the intranet extension address, generally the default is on;
Source IP address: an IP address in the intranet that needs to be converted, which is a required field;
Source address subnet mask: Enter the subnet mask, generally the default value is sufficient;
Destination Type: Select the type of conversion.
WAN port: specifies the export of converted data;
Translation address: Fill in the IP address segment to be converted. This address segment supports a maximum range of 16 addresses, such as: 221.18.10.6-221.18.10.21.
Export: Export all current rules of the NAT list for use as a backup of the list rules. The exported rules will be directly downloaded to the specified path through the browser and saved;
Import: Import the exported NAT rules into the device where they are needed, and use them as list rule recovery;
Batch Delete: Batch delete the rules in the selected rule list.

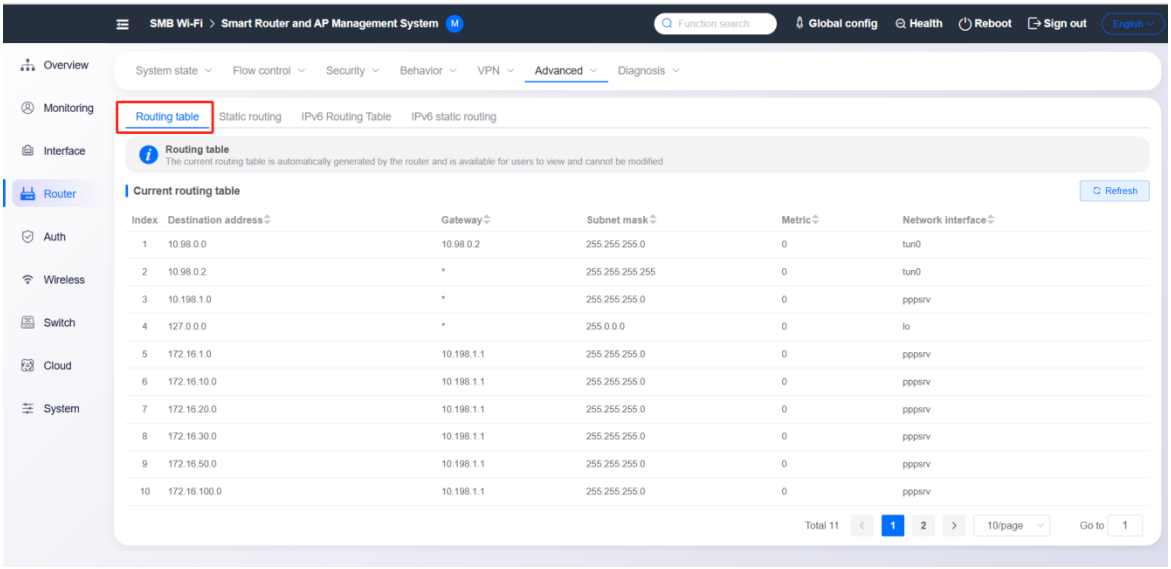
4.6.5 Routing Settings

This unit is mainly used to configure the routing table. The routing table refers to a table stored on a router or other Internet network device, which stores the paths to specific network terminals and, in some cases, some metrics related to these paths. The main job of a router is to find the best transmission path for each datagram passing through the router and effectively transmit the data to the destination.



4.6.5.1 Routing Table

The current routing table is automatically generated by the router and is provided to users for viewing but cannot be modified.

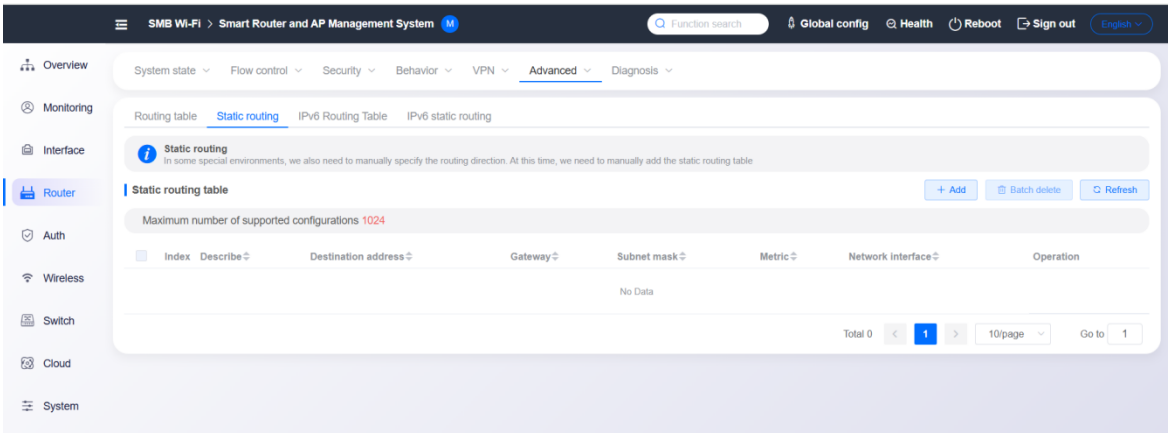


Current routing table

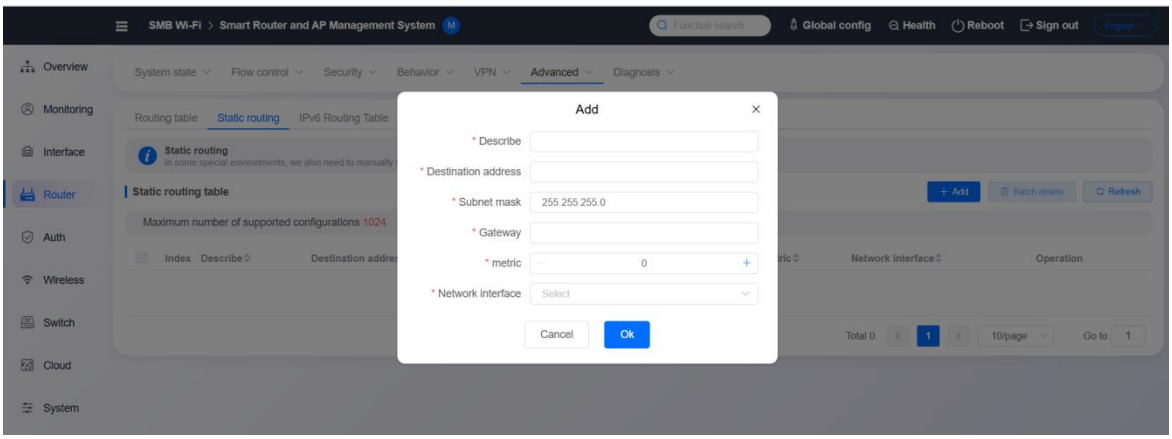
Display all current routing table information, and only refresh operations can be performed.

4.6.5.2 Static Routing

In some special environments, please manually specify the path of the static routing table, as shown in the figure:



Add



Describe: Customize the specification description content to facilitate differentiation in rules;

Destination address: the destination IP address of the static routing table;

Subnet mask: Configure the subnet mask as required;

Gateway: Fill in the gateway address according to the actual situation;

Metric: Generally, the system defaults to 0 and does not need to be modified;

Network Interface: Select the WAN port of the static routing table.

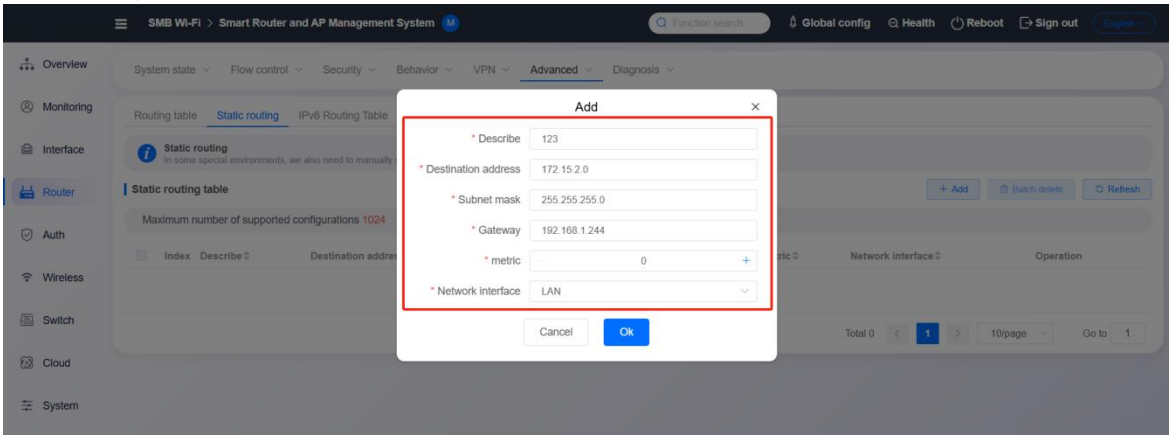
Static routing table

Displays all static routing table information and supports modification and deletion of single information.

Batch Delete: Batch delete selected routing table rules.

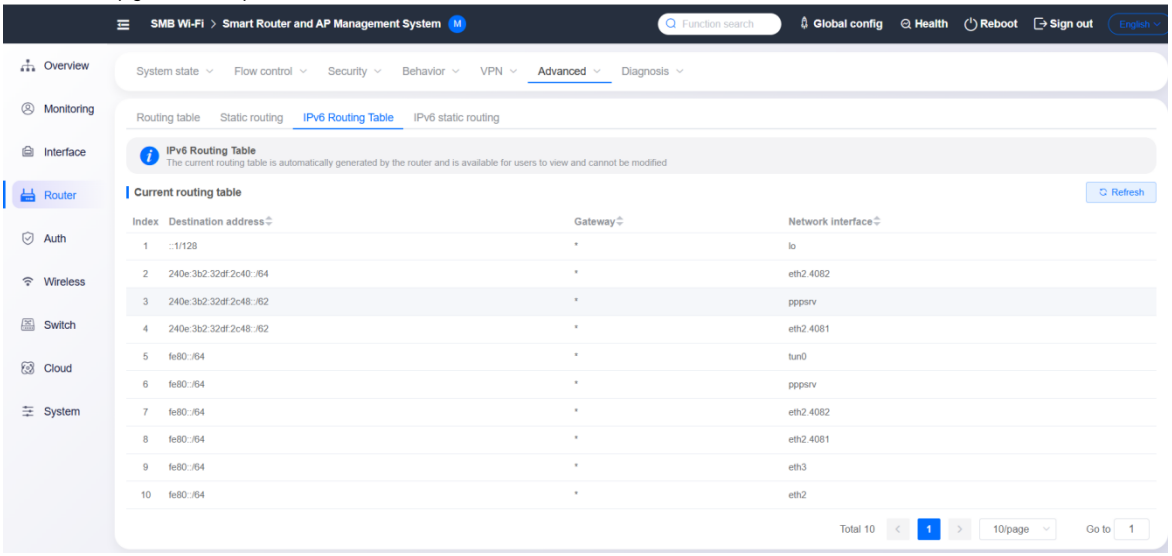
Refresh: Refresh the displayed information of the current list.

For example: If there is a layer 3 switch connected to the lower layer of the router LAN1 port, the IP of the switch is 192.168.1.244 , and the layer 3 switch has a network segment of 172.15.2.1/24. The host under the layer 3 switch uses the IP of the 172.15.2.X network segment to access the Internet, and uses 172.15.2.1 as the gateway address. Then, we need to add the static route as shown in the figure to enable the host under the layer 3 switch to access the Internet normally.



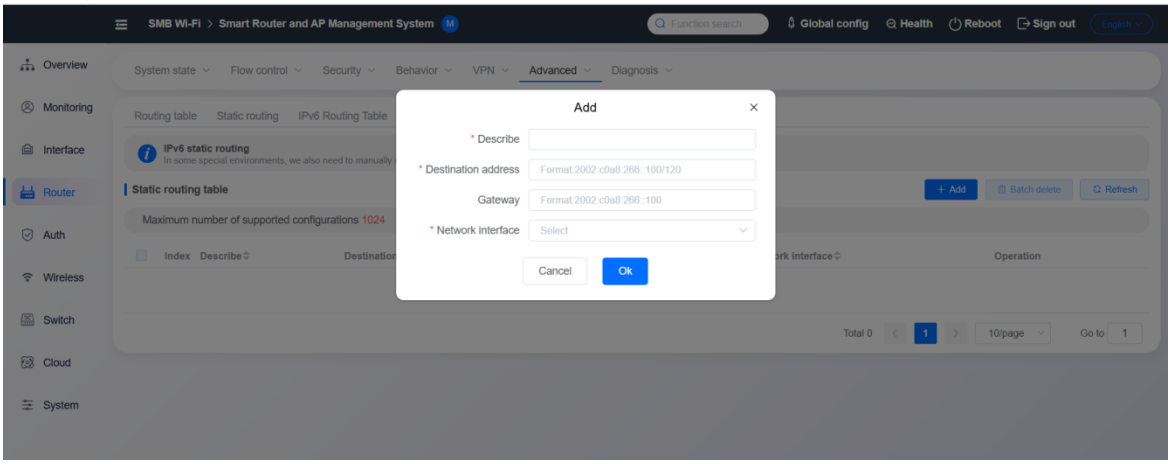
4.6.5.3 IPv6 Routing Table

The principle and function are the same as the above (IPv4) routing table, the difference is that this is an IPv6 routing table automatically generated by the router.



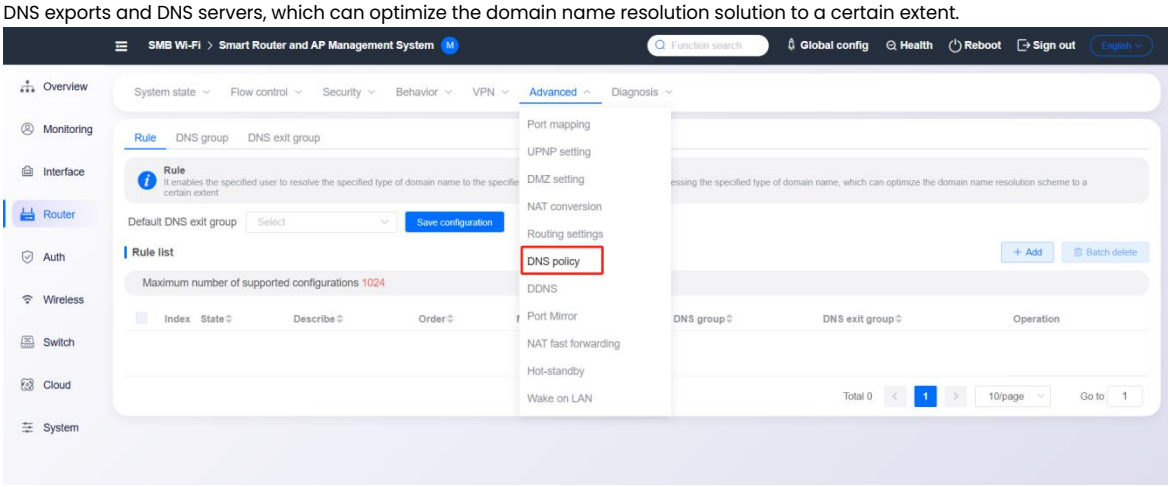
4.6.5.4 IPv6 Static Routing

The principle and function are the same as the static routing (IPv4) mentioned above. Please refer to "Static Routing" and fill it in according to your needs and system requirements



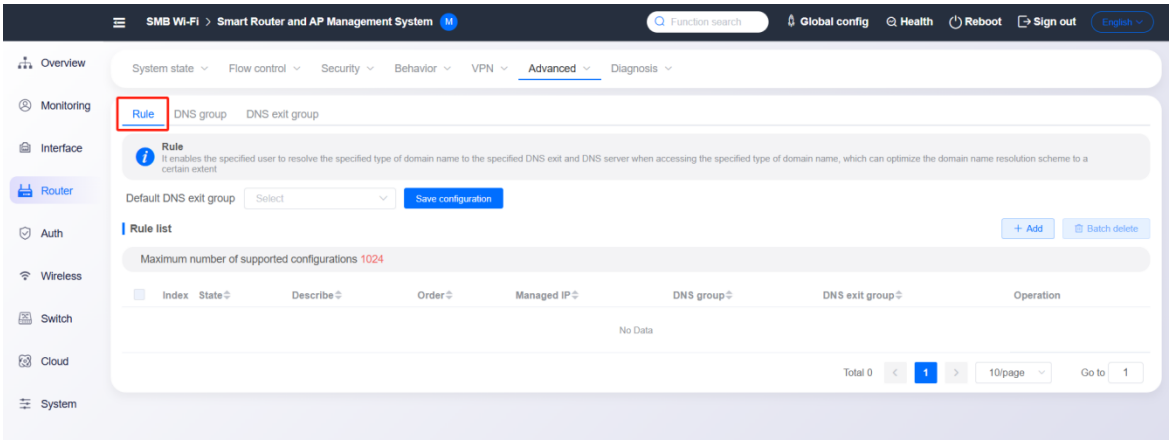
4.6.6 DNS policy

By allowing designated users to access designated types of domain names, the domain names will be resolved on designated DNS exports and DNS servers, which can optimize the domain name resolution solution to a certain extent.



4.6.6.1 DNS rule

By allowing designated users to access designated types of domain names, the domain names will be resolved on designated DNS exports and DNS servers, which can optimize the domain name resolution solution to a certain extent.

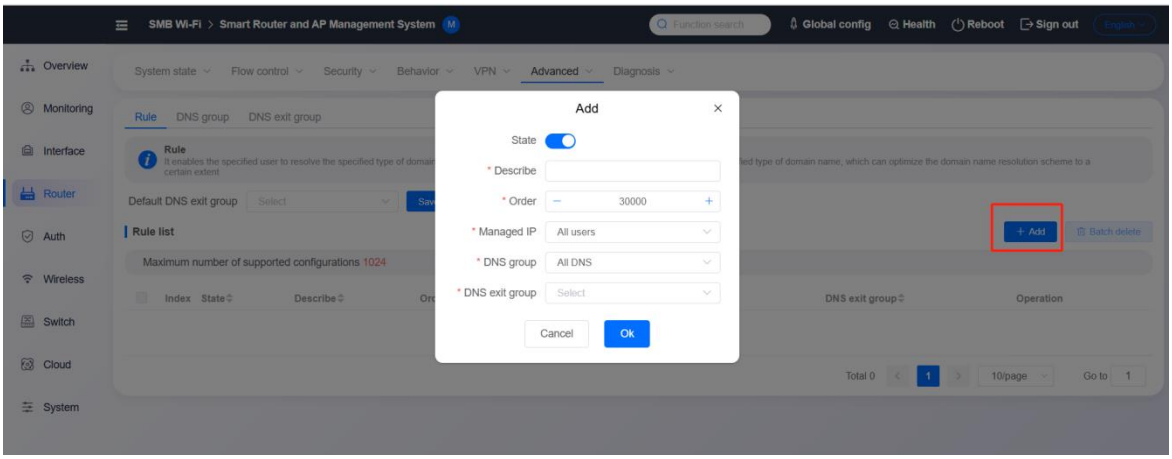


Default DNS exit group: Select a DNS export group as the default, create at least one DNS exit group before set it.

Rule List

Displays detailed information of all rules.

Add:



State: Control switch for a single rule, enable or disable;

Describe: A brief note and description of the rule;

Execution order: refers to the priority of rule execution. The higher the value entered, the higher the execution priority. If the execution order of different rules is the same, the rules will be triggered and take effect at the same time; if the same rules are created and the execution order is the same, the device will randomly execute one of them; if the same rules are created and the execution order is different, the device will execute the rule with the higher order value;

Managed IP: The rules are effective for those IP addresses or IP segment terminals. The policy rules will take effect on the filled IP address (segment), where: "All users" refers to all terminals in this network. The added "address group" can be directly selected for use.

DNS Group: Select a group as the control object;

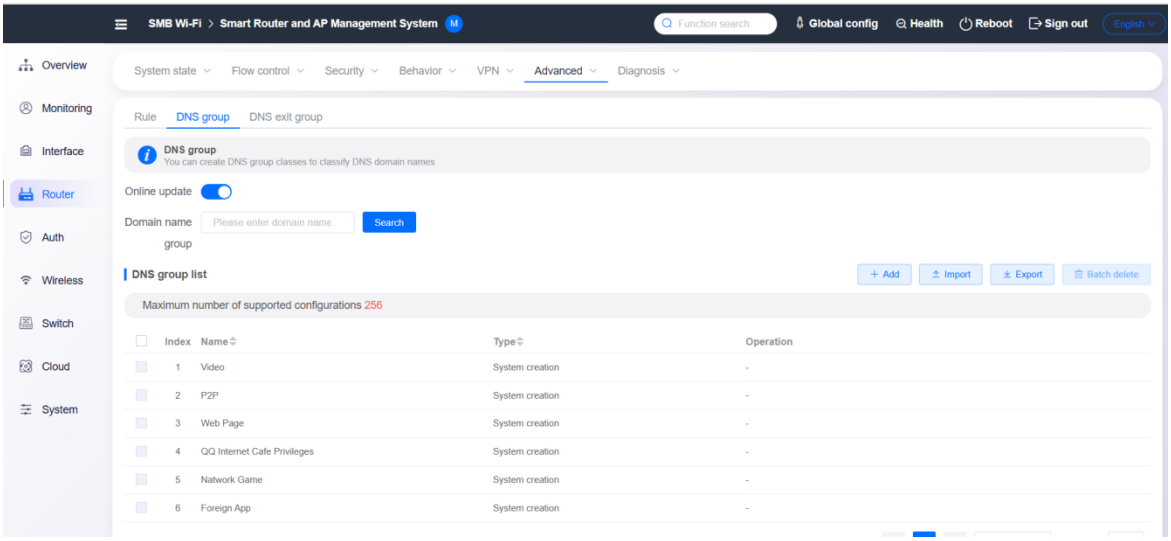
DNS exit group: Assign the selected DNS group to an exit group .

Batch Delete: Delete selected rule entries in batches.

Note : If the DNS server or exit group is abnormal, resulting in inability to resolve or resolution failure, access to the domain name will fail. The rules currently in use cannot be deleted.

4.6.6.1 DNS group

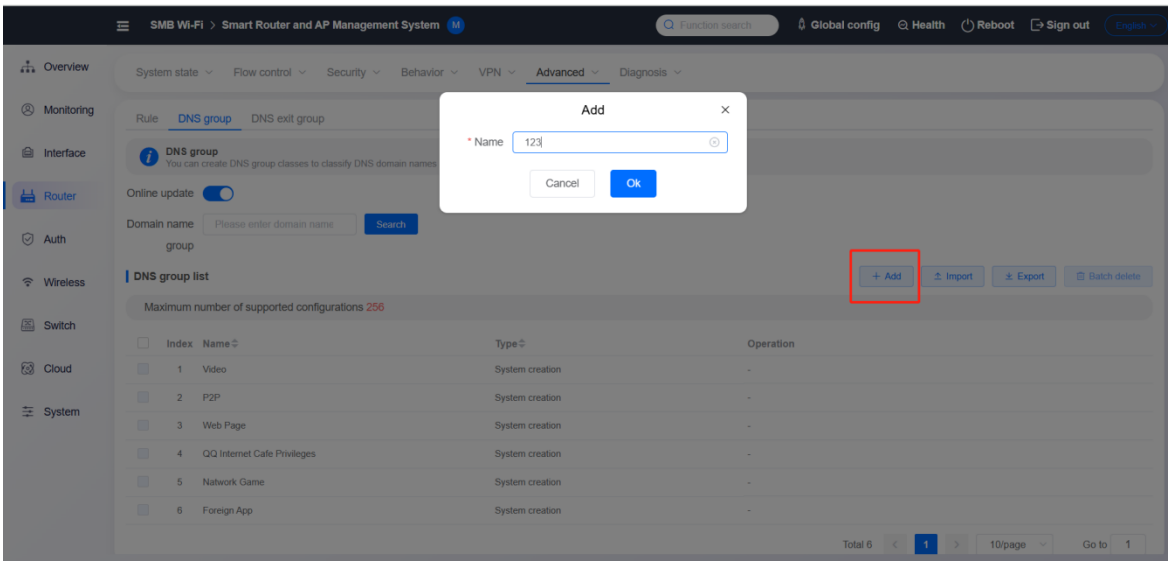
Create or view the DNS group that can classify DNS domain names . DNS group is available in default



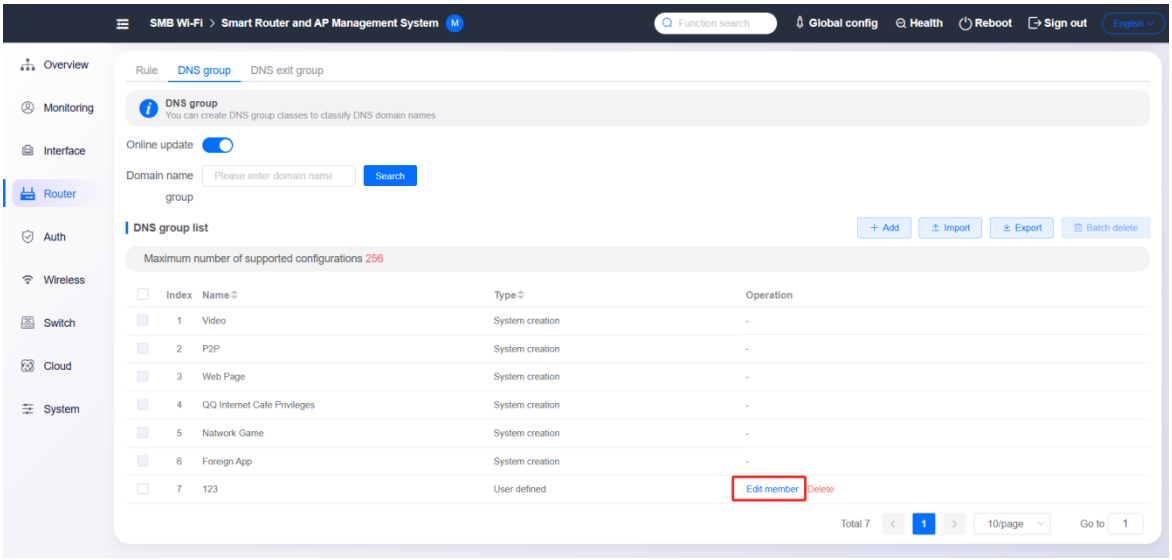
Online Update: Automatically update the DNS group list.

Add:

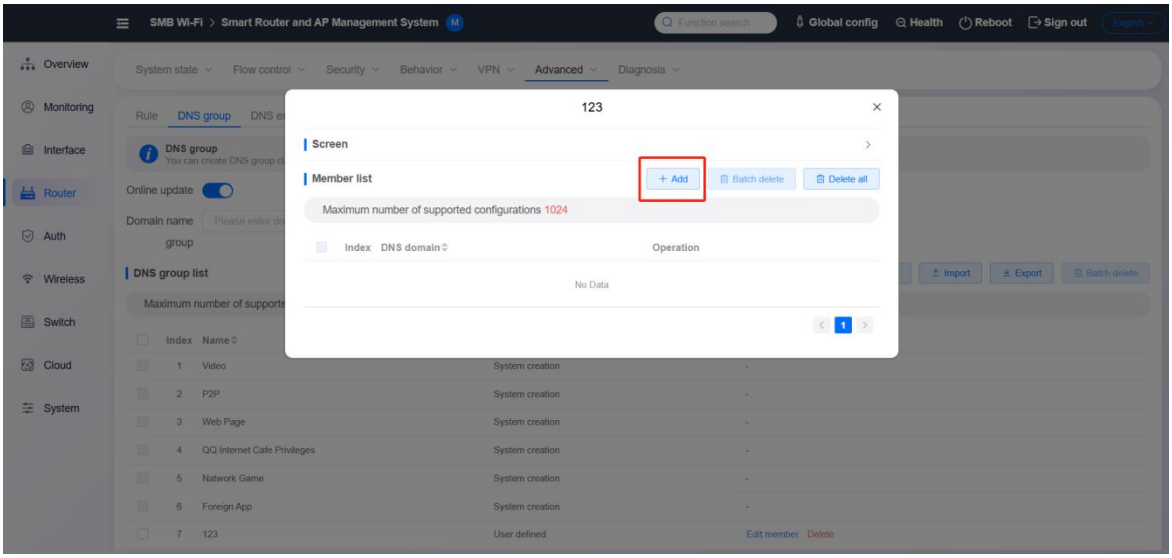
1. Add DNS group names and custom groups as needed;



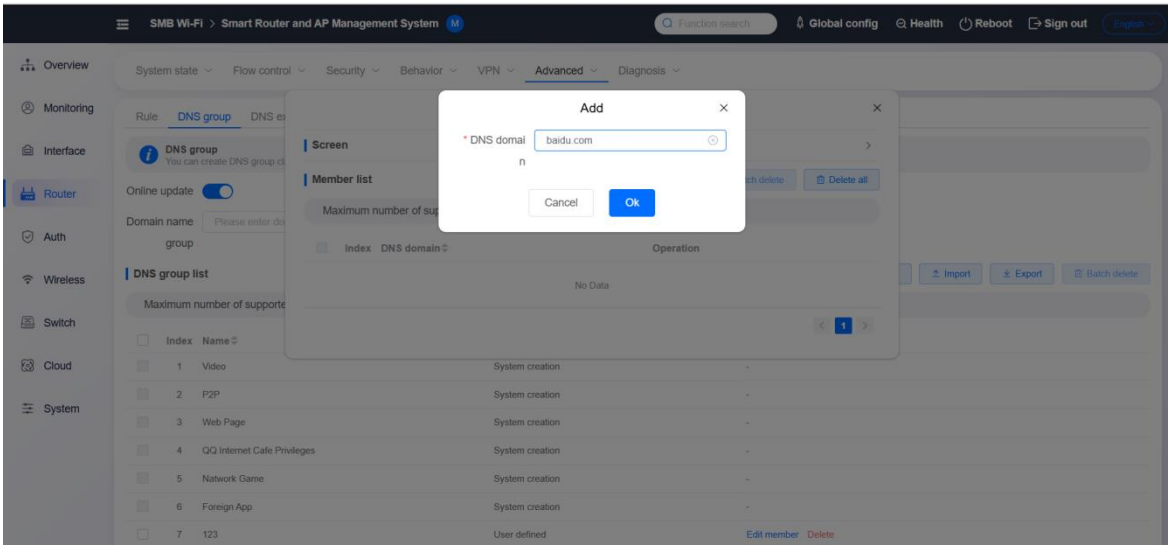
2. Click Edit Members of the DNS group to add the members to this DNS group



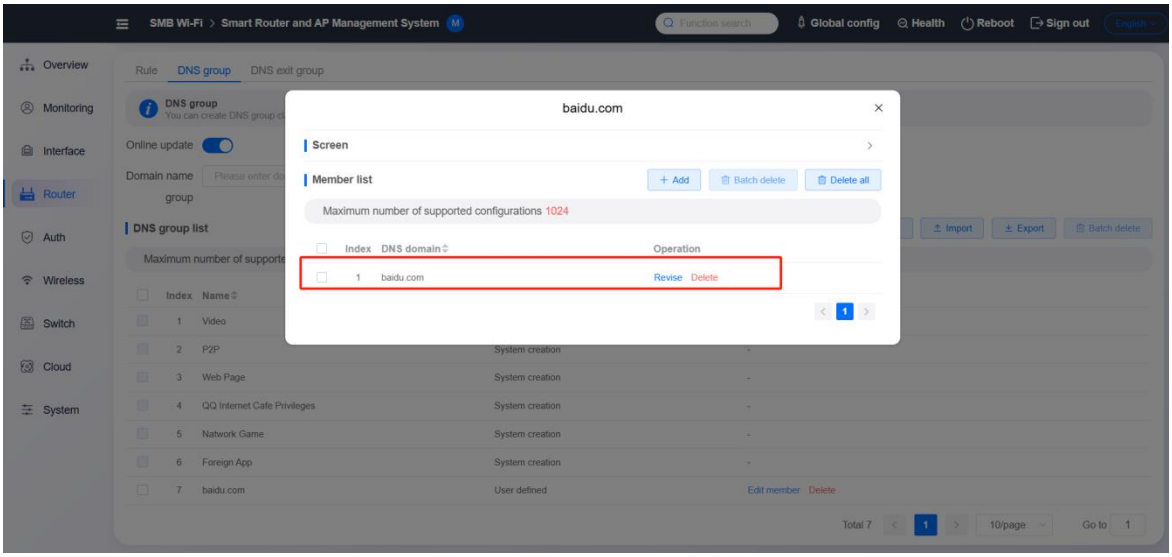
3. Add members



4. Enter the member's DNS domain name;

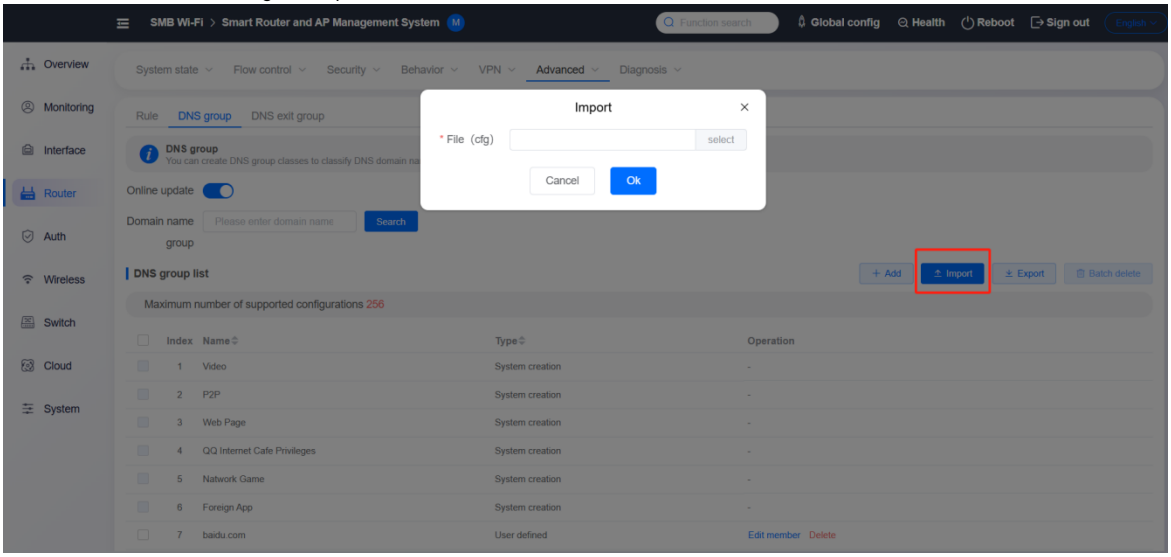


5. Added success

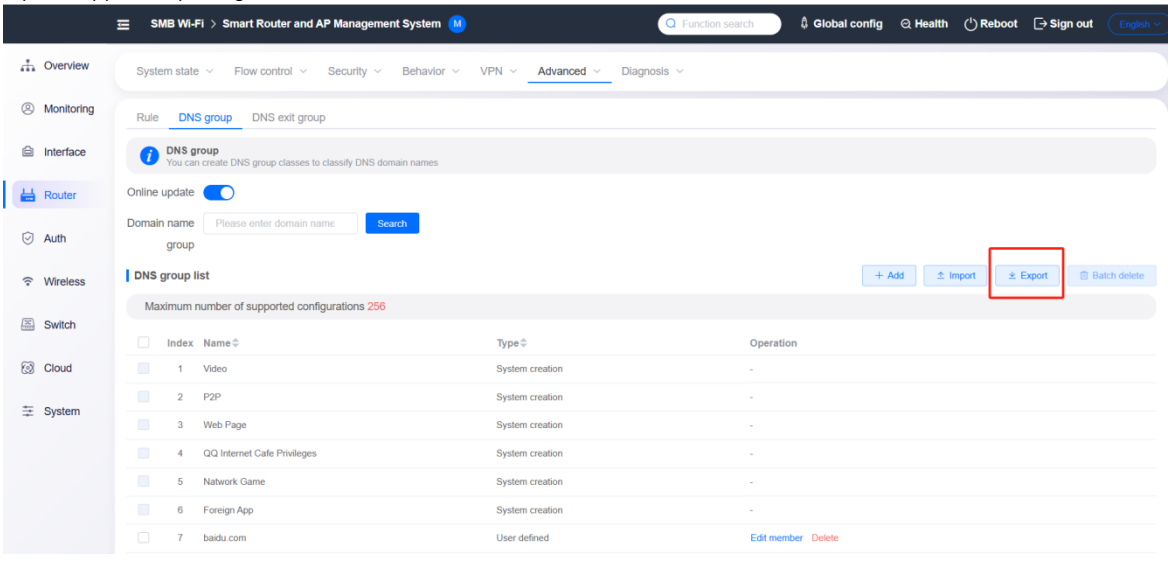


After successful addition, the DNS domain name can be used on the router for all functions related to the relevant options. During use, the DNS domain name cannot be deleted.

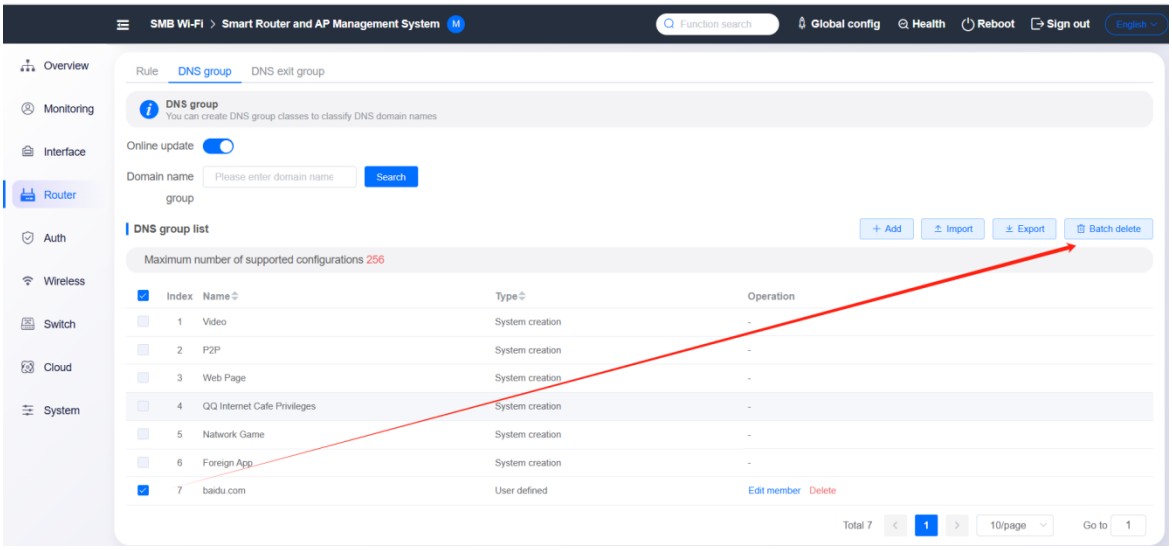
Import: Supports importing DNS groups with specified format file types. If the format is unclear, can export a rule file and then add it to the file before saving the import;



Export: Supports exporting DNS rules

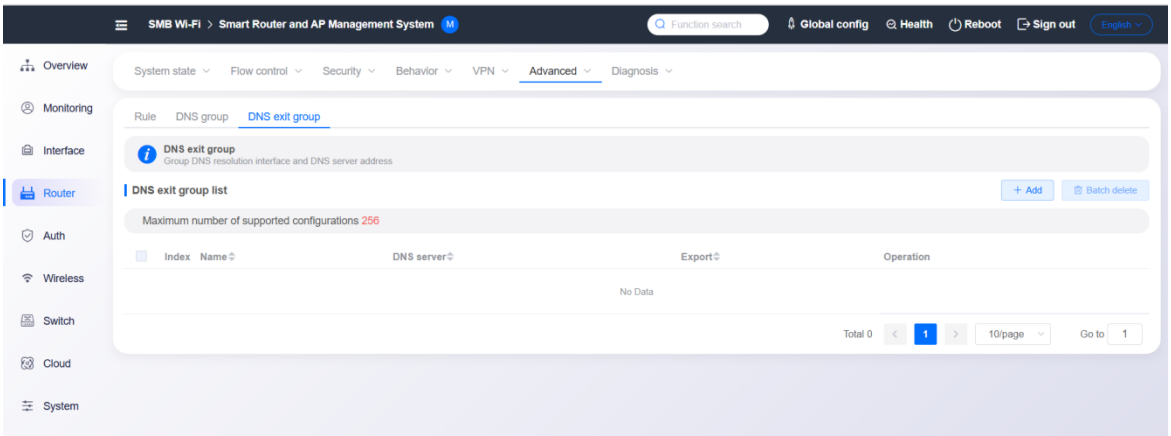


Batch deletion: Supports batch deletion of manually added DNS groups, but the system's built-in DNS groups do not support deletion.



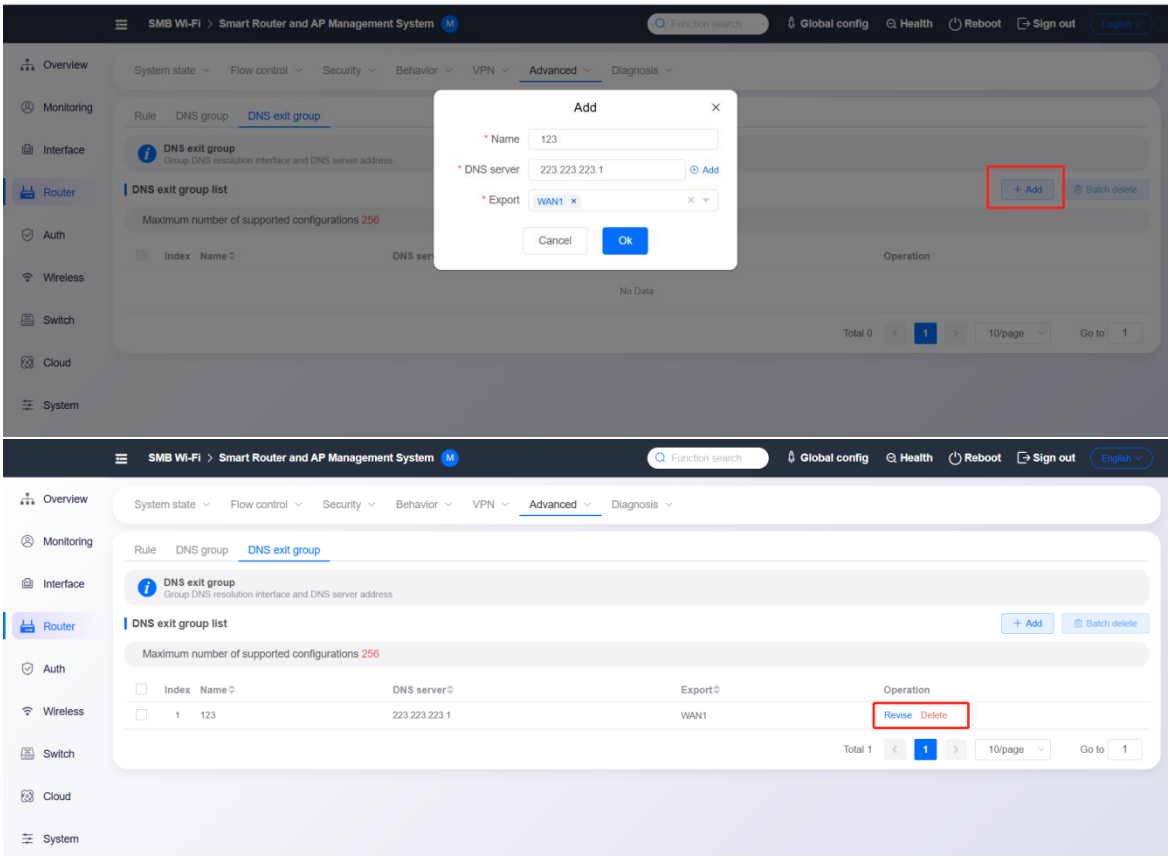
4.6.6.2 DNS exit group

Group DNS resolution interfaces and DNS server addresses.

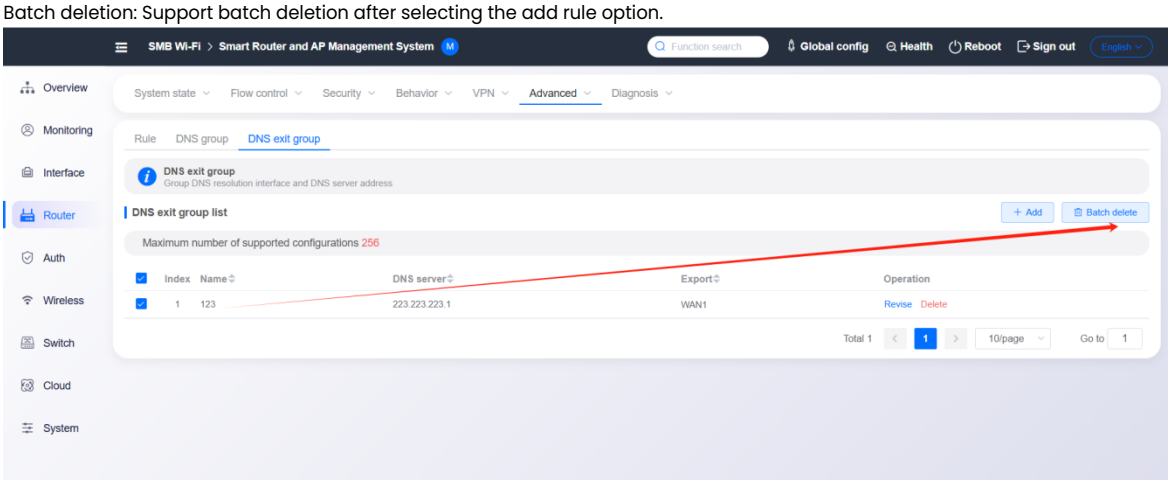


DNS exit group

Add: Fill in the DNS exit group name, DNS server address, and select exit port as required, all three conditions are mandatory;

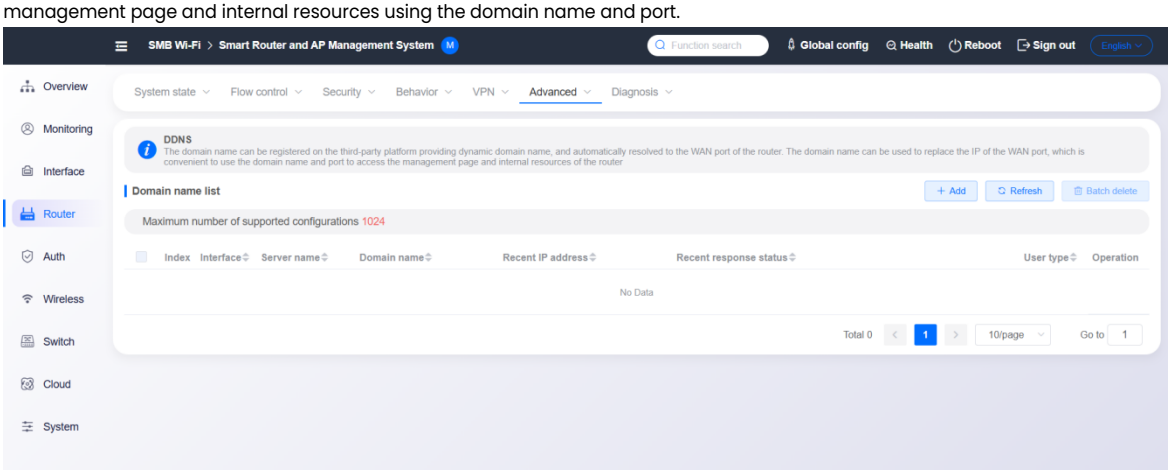


Revise: Modify the content of the currently added DNS group;
Delete: Delete the currently added DNS group;
Batch deletion: Support batch deletion after selecting the add rule option.



4.6.7 DDNS

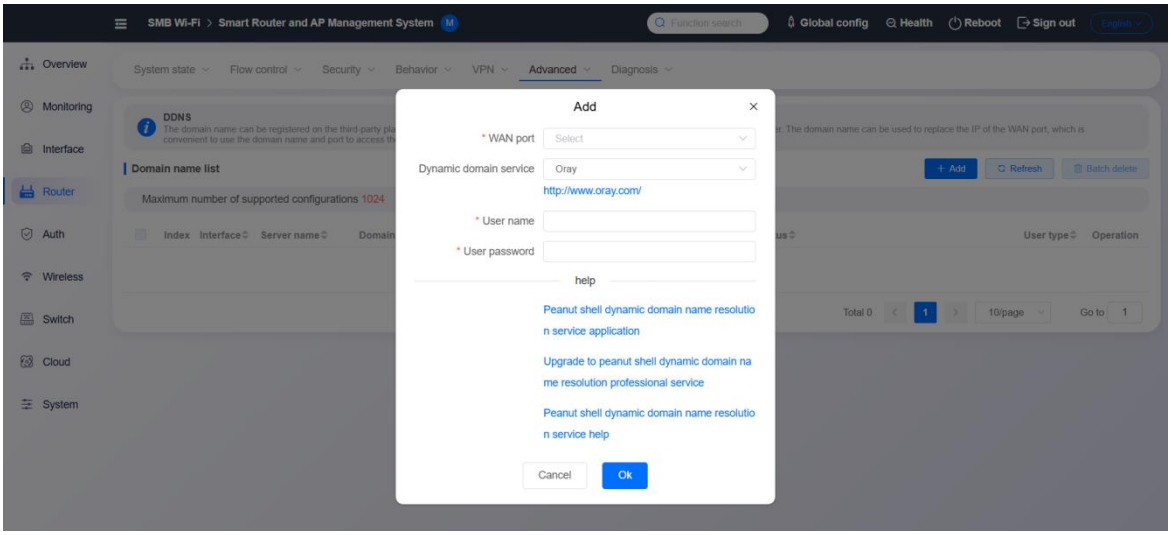
Dynamic domain names are mainly used to resolve a dynamic IP into a static domain name for network access. Before configure and use this feature, please first apply for domain registration on a third-party dynamic domain website and automatically resolve it to the WAN port of the router. Use this domain name instead of the IP address of the WAN port to access the router's management page and internal resources using the domain name and port.



Domain name list

Display a complete list of domain names and connection information.

Add

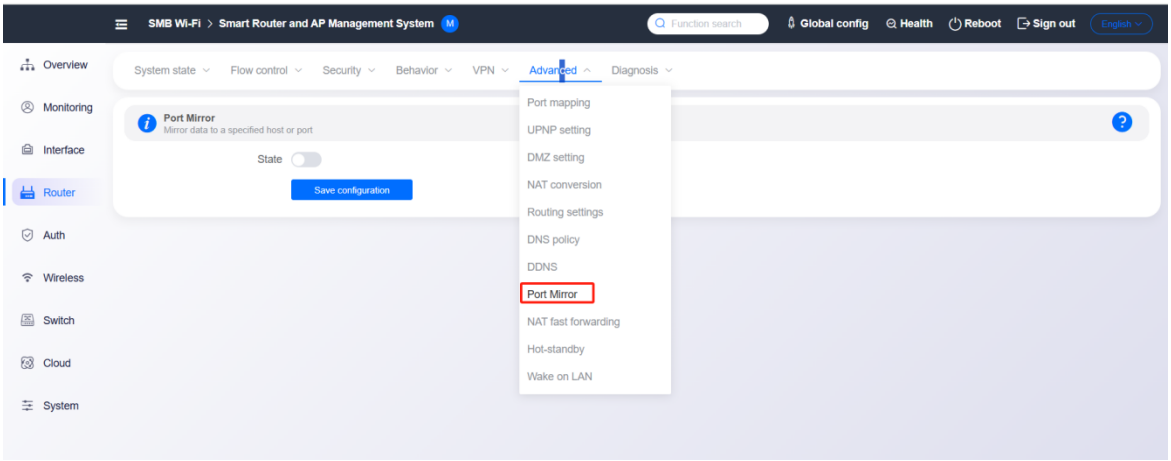


WAN port for domain name work: Select the WAN port will be used for the static domain name;
Dynamic Domain Service: Select the domain name server that is registered and resolved, click the expand button to view the domain name servers currently supported by the system;
User Name: Enter the user name registered on the domain name server;
User Password: Enter the user password registered with the domain name server.
Refresh: Refresh the list and the connection status in the list.

Batch Delete: Batch delete the binding information of multiple dynamic domain names.

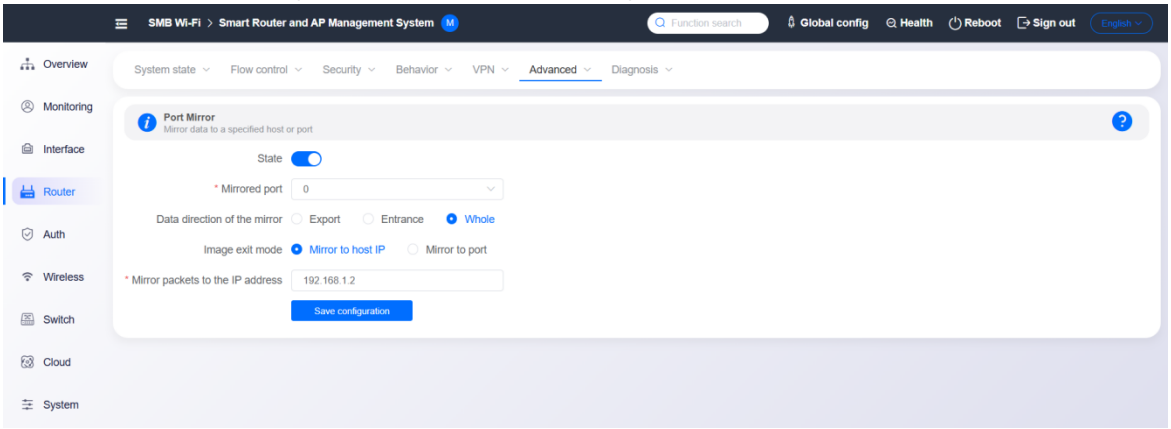
4.6.8 Port Mirror

The port mirror function is mainly used to mirror internal data to a specified port or host to facilitate management personnel to analyze network data.



Port Mirroring

Status: The default port mirroring function status is off. You can configure rules only after it is enabled.



Data direction of the mirror: Select the data direction to be mirrored, whether it is export data, import data, or both export and import data;

Image exit mode: Select the exit mode of the mirrored data, which can be simply understood as where the mirrored data is mirrored to - a host IP or a port;

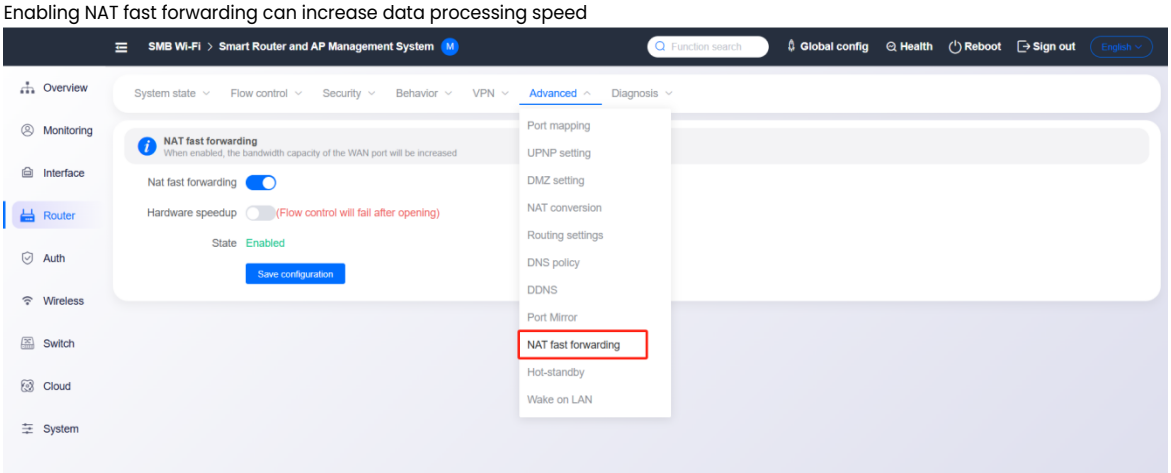
Mirror to Host IP: If the mirror export mode is selected as Mirror to Host IP, then fill in the IP address of the host here;

Mirror to port: If the mirror export mode is selected as mirror to port, please select the corresponding port here.

The port mirroring function can generally be used in conjunction with packet capture tools such as Cole.

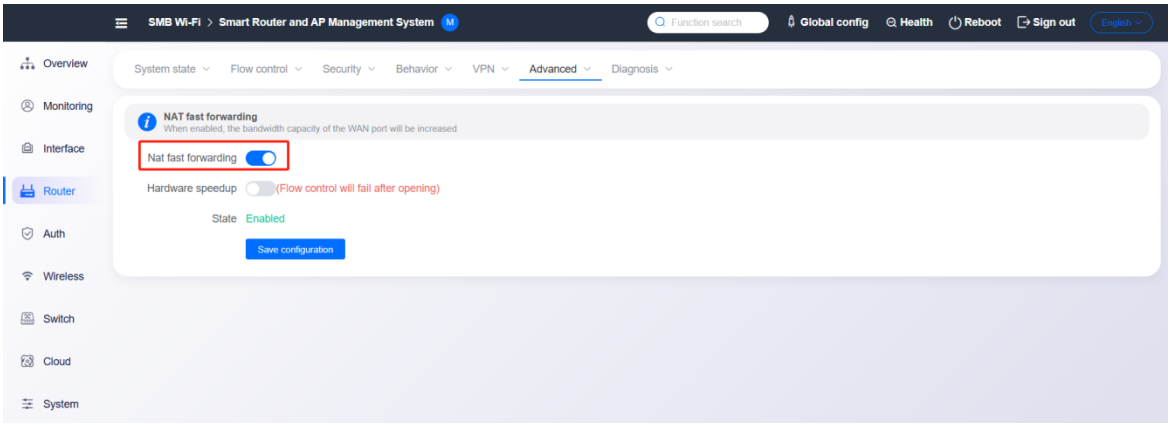
4.6.9 NAT Fast Forwarding

Enabling NAT fast forwarding can increase data processing speed

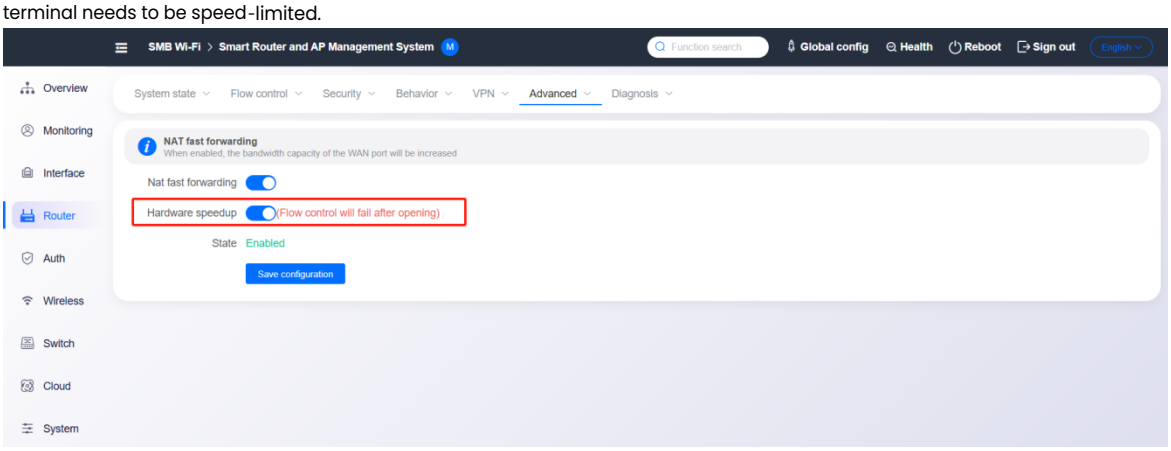


NAT fast forwarding

NAT Fast Forwarding: After it is enabled, the data processing speed can be improved , but the functions such as WEB keyword filtering, email monitoring, and 3G/4G Internet access will be invalid.

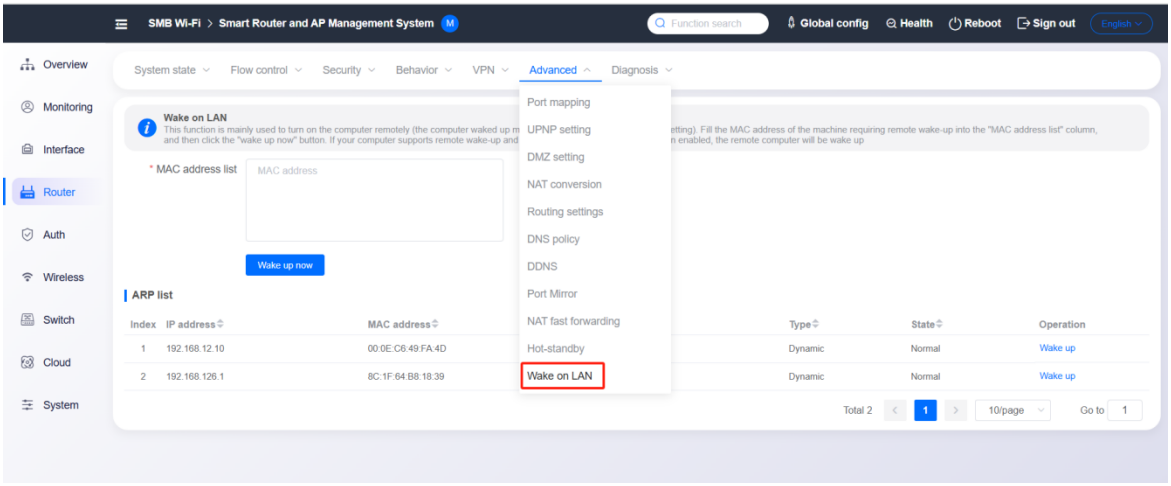


Hardware Speedup: Hardware speedup is a derivative function of NAT fast forwarding, which speeds up the forwarding capability of the device and improves the data processing speed . Because this function does not pass QoS, turning on hardware acceleration will cause the flow control rules to fail to take effect. Please disable this function in an environment where the terminal needs to be speed-limited.



4.6.10 Wake-up on LAN

This function is mainly used to remotely start a computer (the computer to be awakened must first enable the remote wake-up setting). Fill in the MAC address of the machine to be remotely awakened into the "MAC Address List" column, and then click the "Wake Up Now" button. If your computer supports remote wake-up and has enabled the remote wake-up function, the remote computer will be awakened



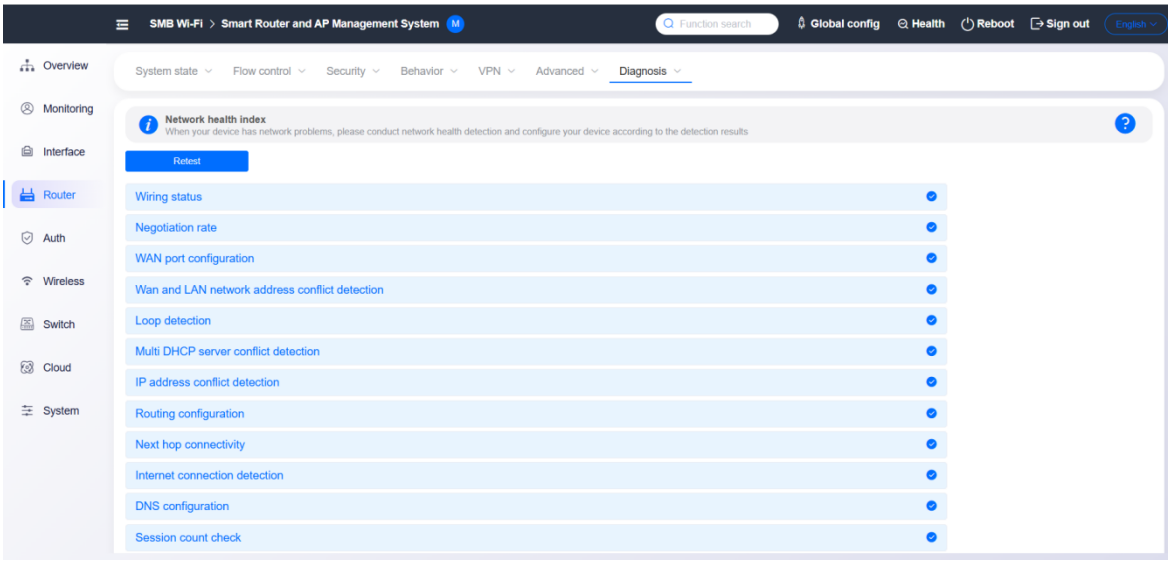
4.7 Troubleshooting

4.7.1 Network Health Index

This is network health detection: when there is a problem with the device or the local area network, you can enable "Start detection" to detect the network health and configure your device based on the detection results

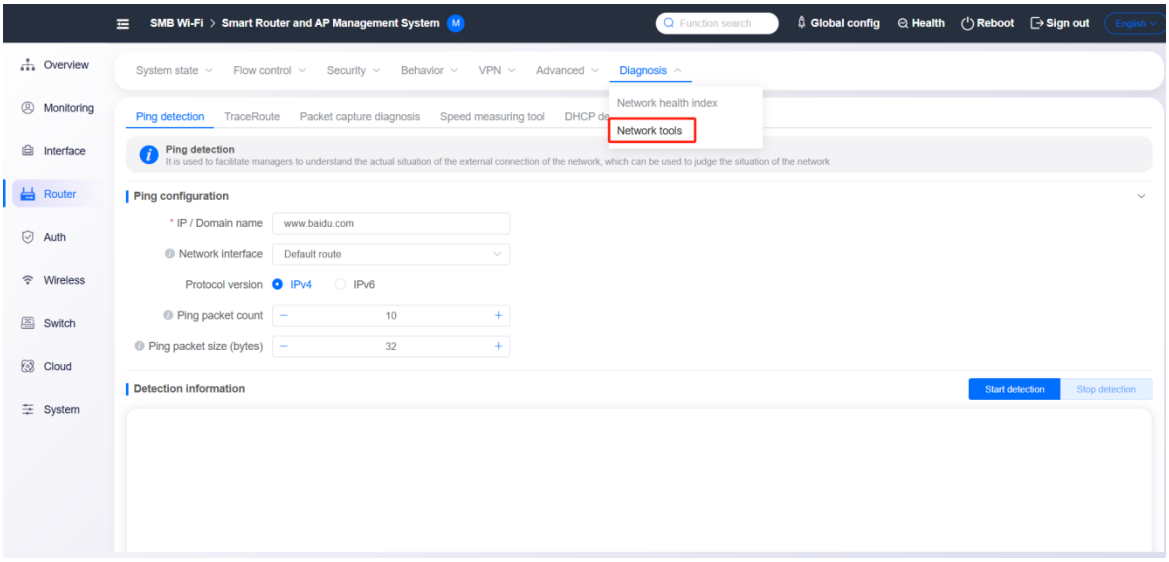
Network Health Index

Retest



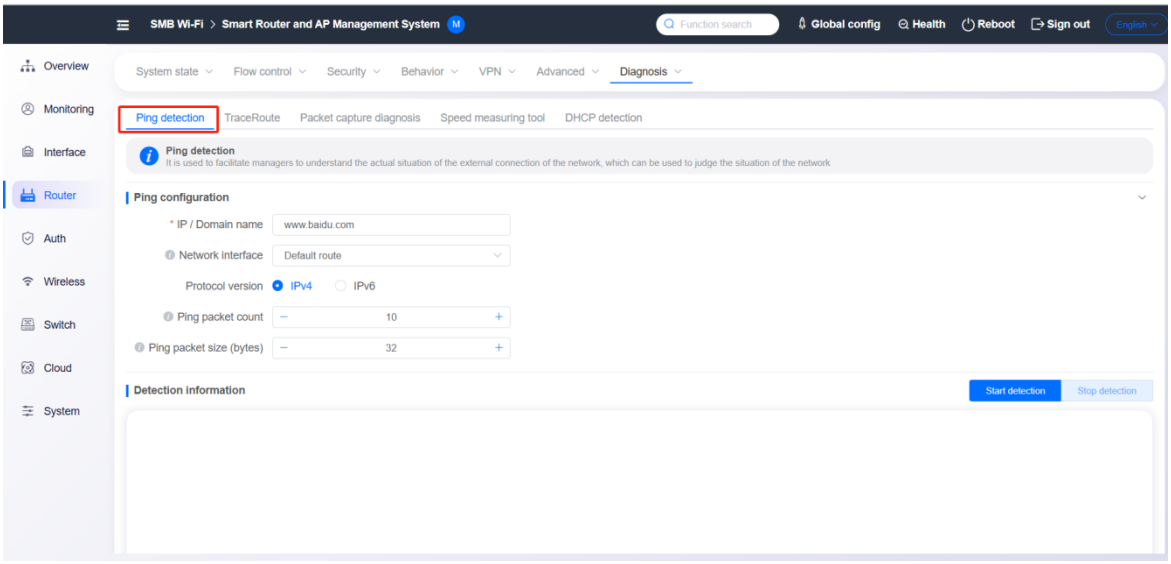
Wiring status: Check whether the interface is plugged into a network cable;
Negotiation rate: Check whether the negotiation rate of the interface is normal;
WAN port configuration: Check whether the WAN port is correctly configured/the IP address is obtained;
WAN and LAN network address conflict detection: detect whether there is a conflict between WAN and LAN network addresses;
Loop detection: detect whether there is a loop in the network;
Multiple DHCP server conflict detection: detect whether there are other illegal DHCP services in the intranet;
IP address conflict detection: detect whether there is an IP address conflict in the network;
Routing configuration: Check whether the routing configuration is normal and whether the configured routing can communicate with the external network;
Next hop connectivity: Check whether the next hop link of the default route is connected;
DNS configuration: Check whether a DNS server is configured or whether the DNS server link is connected;
Session number check: Check whether there are rules that limit the number of connections configured on the WAN port and the IP connection limit too low;
DHCP capacity check: Check whether the address capacity that can be allocated by the DHCP server at the LAN port is sufficient;
Flow control inspection: Check whether there are rules with too low speed limit in the flow control rules;
Cloud service configuration: Check whether the device is connected to the cloud server.

4.7.2 Network Tools



4.7.2.1 Ping detection

It is used to help administrators understand the actual status of the network's external connections. The Ping detection function can be used to determine the network status.



Ping Configuration

IP/Domain Name: Fill in the IP or domain name that needs to be pinged;

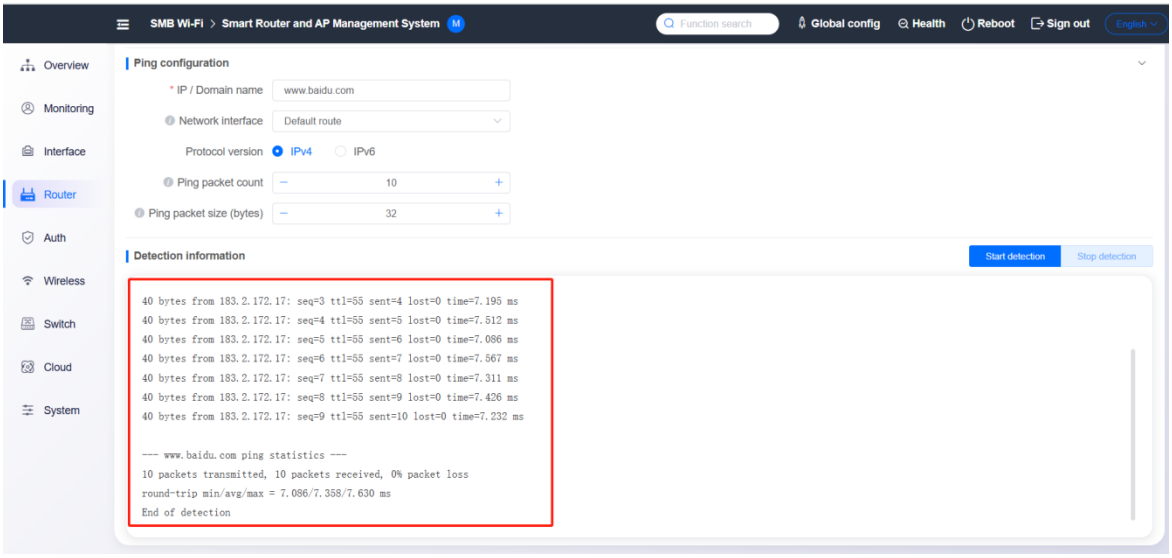
Network interface: Select the port from which the ping test is to be conducted;

Protocol version: Select the version to be detected, IPv4 or IPv6;

Ping Packet Count: Set the number of packets for each Ping detection, the default is 20, and the range is 1-1000;

Ping Packet Size (Bytes): Set the size of the packet for each Ping check. The default is 1024 and the setting range is 1-10240.

After configuring the rules, you can click " **Start Detection** " and the detection results will be displayed below. If you need to stop the detection, click " **Stop Detection** " .

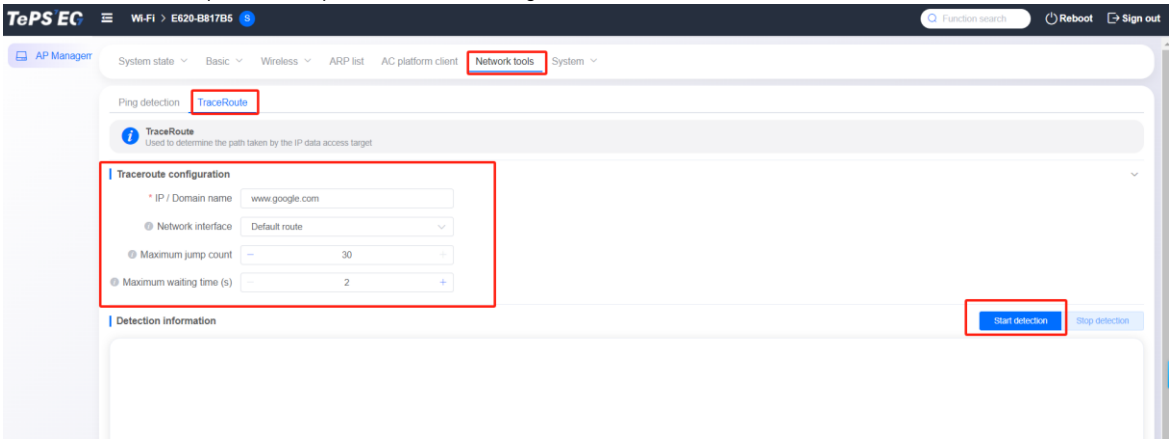


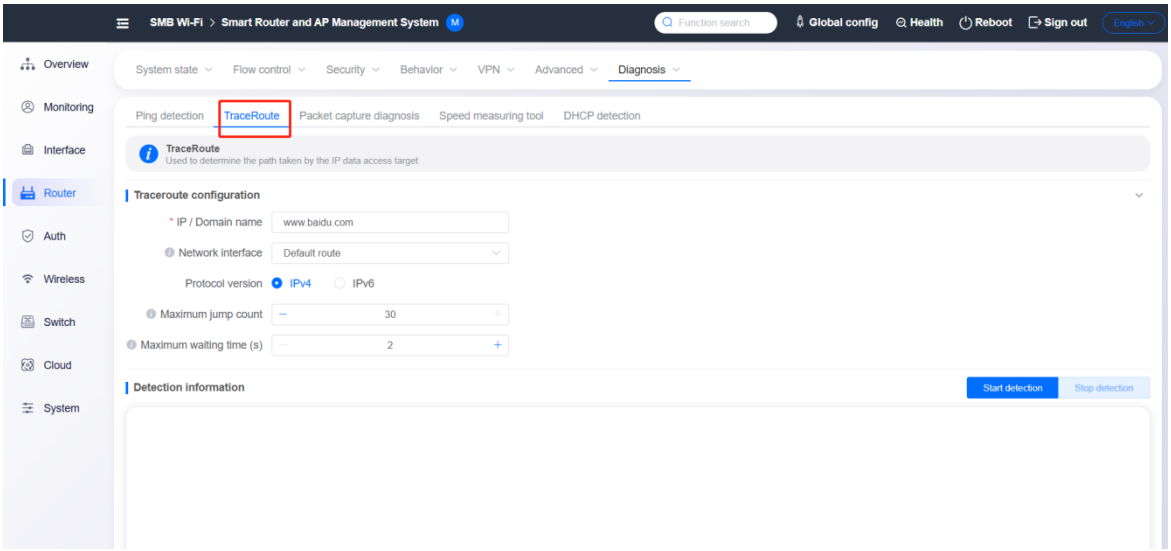
Detection information

Displays information after conditional Ping detection. The record is automatically cleared when exiting the page.

4.7.2.2 TraceRoute

Used to determine the path taken by IP data to reach a target.





TraceRoute Configuration

IP/Domain Name: Fill in the IP or domain name whose path needs to be determined;

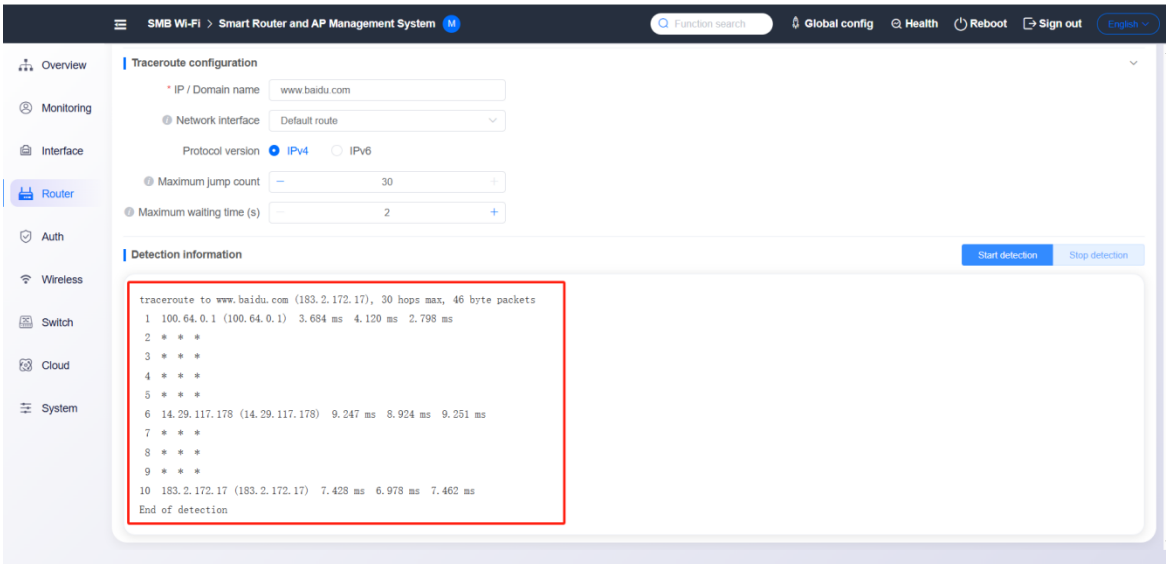
Network interface: select the port from which the data path will go out;

Protocol version: Select the version to be detected, IPv4 or IPv6;

Maximum jump count: Set the maximum jump count between data, the default is 30, the range is 2-30;

Maximum waiting time (seconds): Maximum waiting time setting, the default is 2 seconds, the range is 2-10.

After configuring the rules, you can click " **Start Detection** " and the detection results will be displayed below. If you need to stop the detection, click " **Stop Detection** ".

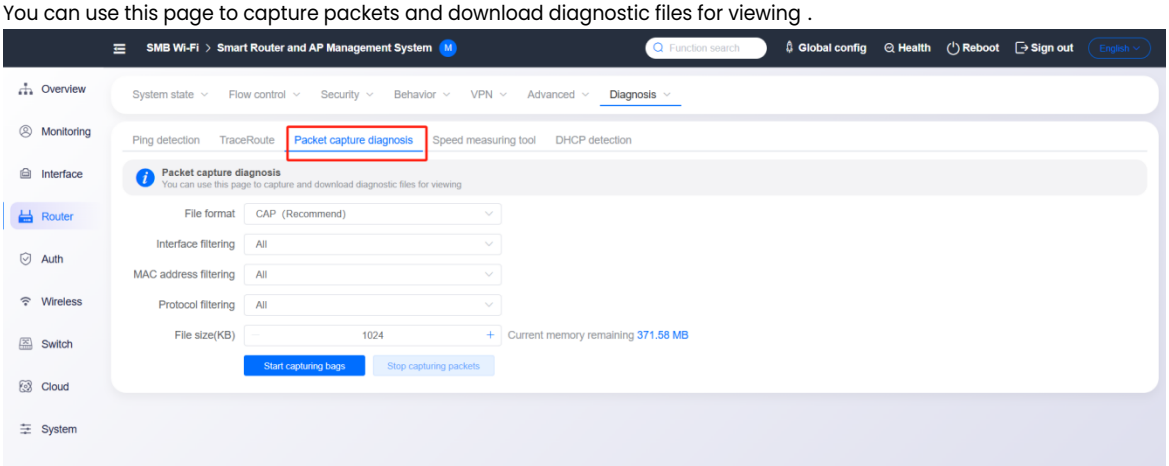


Detection information

Displays information after traceroute detection based on conditions.

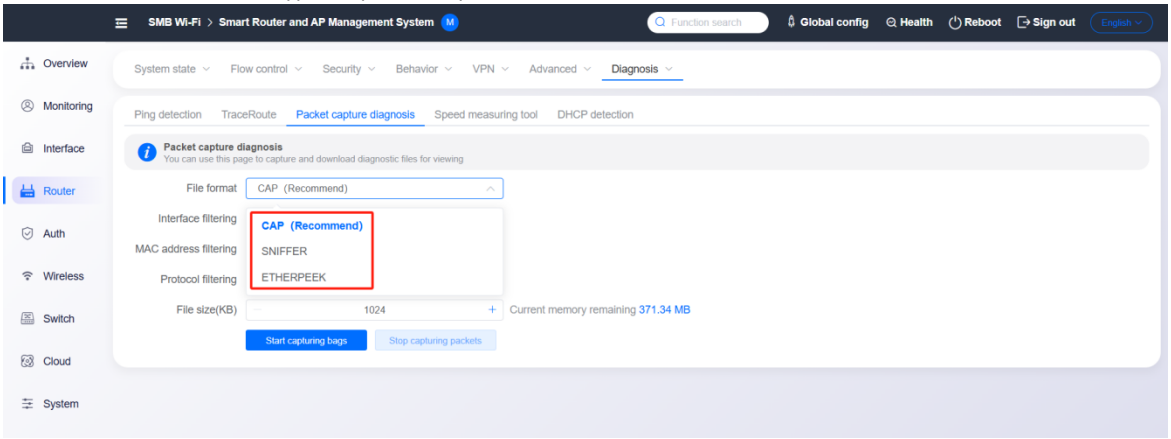
4.7.2.3 Packet Capture Diagnosis

You can use this page to capture packets and download diagnostic files for viewing .

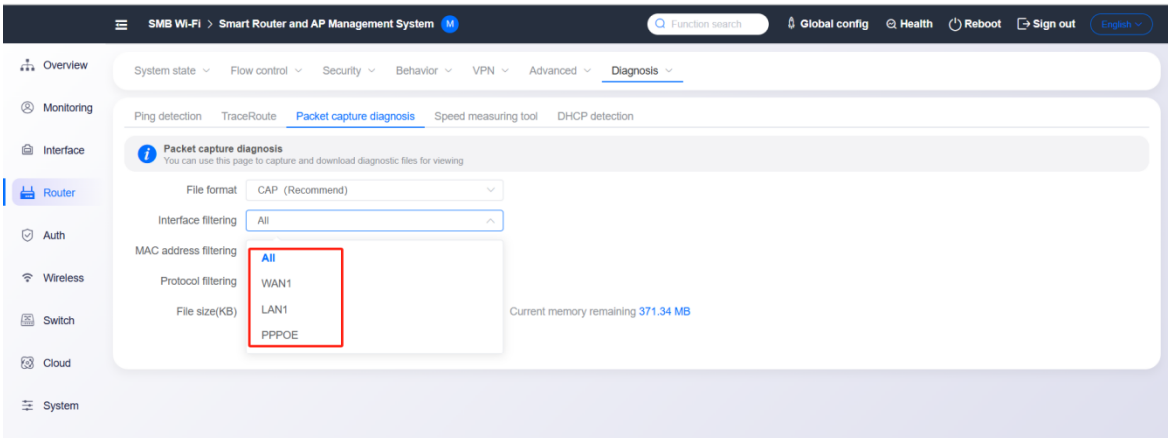


Packet capture diagnosis

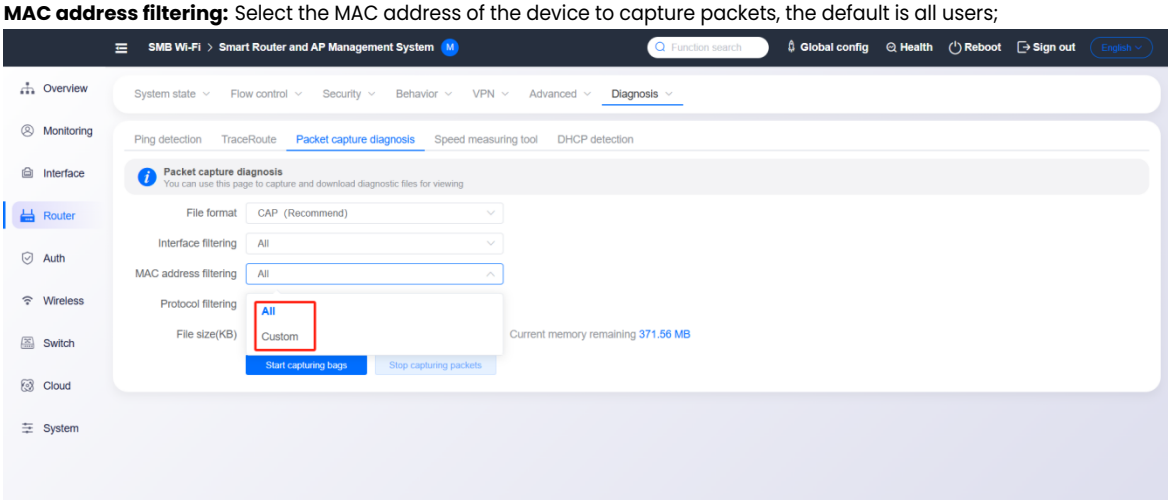
File format: There are three types of packet capture files to choose from: CAP, SNFFER, and ETHERPEEK ;



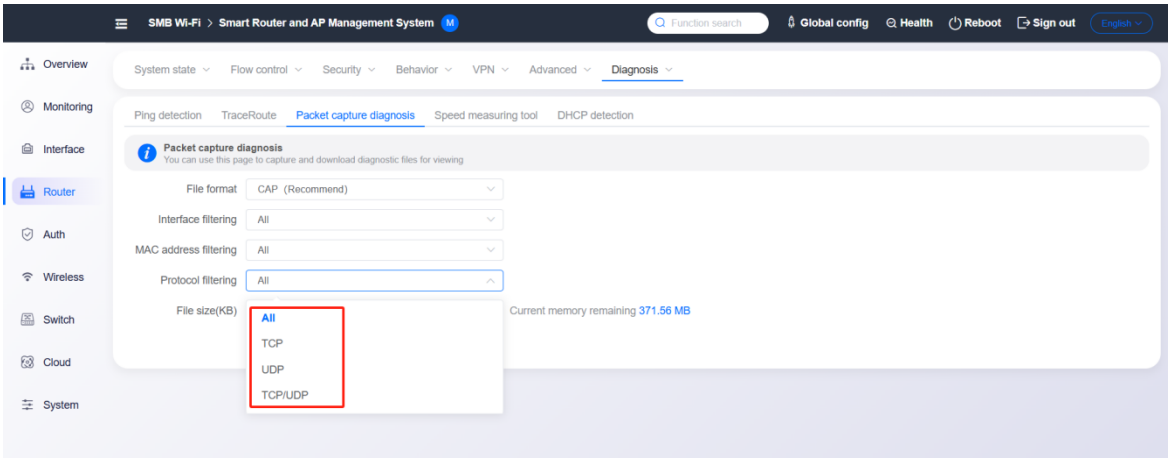
Interface filtering: select the data interface to capture packets;



MAC address filtering: Select the MAC address of the device to capture packets, the default is all users;

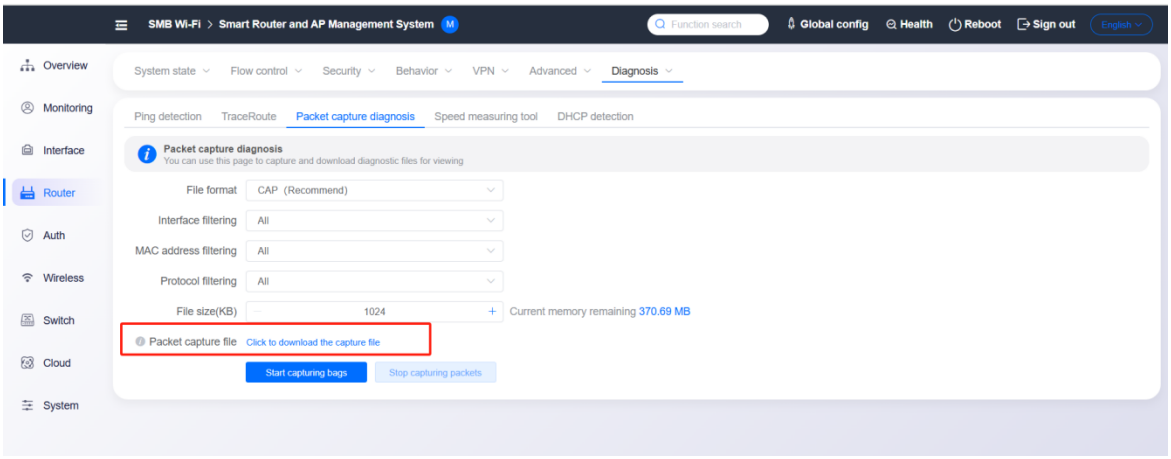


Protocol filtering: Select the protocol to capture packets;



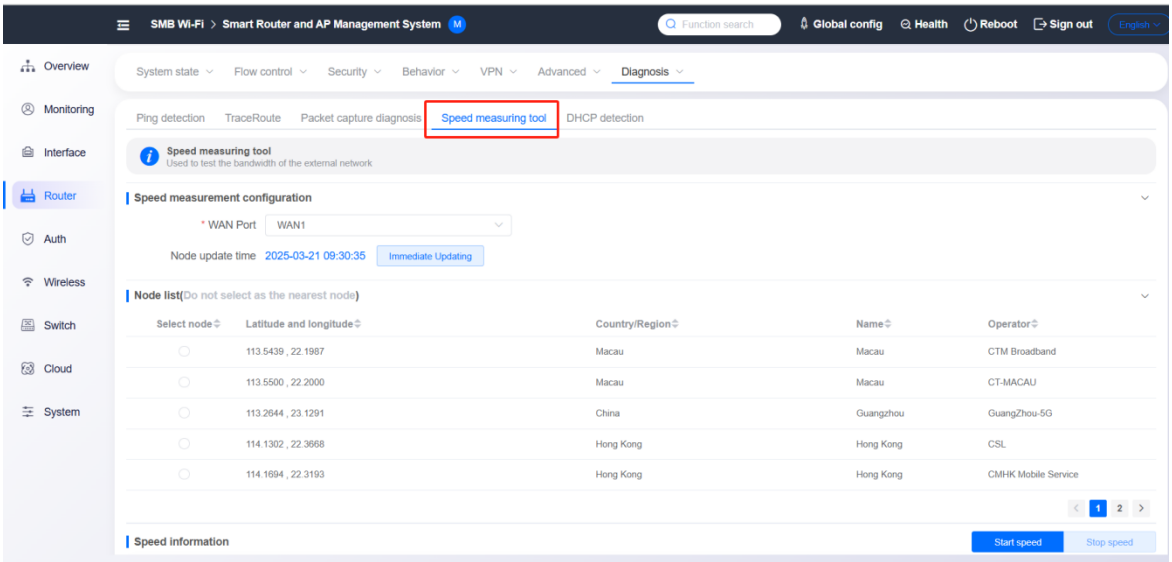
File size: the size of the captured file;

Packet capture file: Click to download the captured file. You can use special tools to open the downloaded file for analysis.



4.8.3.4 Speed Test Tool

Detect the upstream and downstream bandwidth of the WAN port. Select the WAN port that needs to be tested and click " **Start Speed**" . Can " **Stop Speed** " during the speed test .



Speed measurement configuration

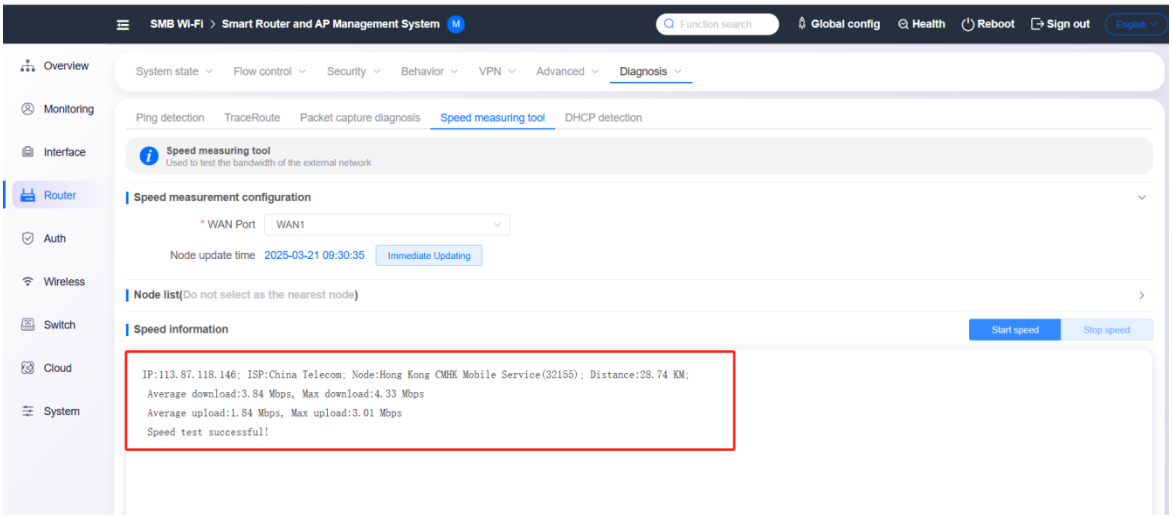
Select the WAN interface to test the speed.

Node list

Select the location passed during the speed test. If not selected, the nearest node will be automatically selected.

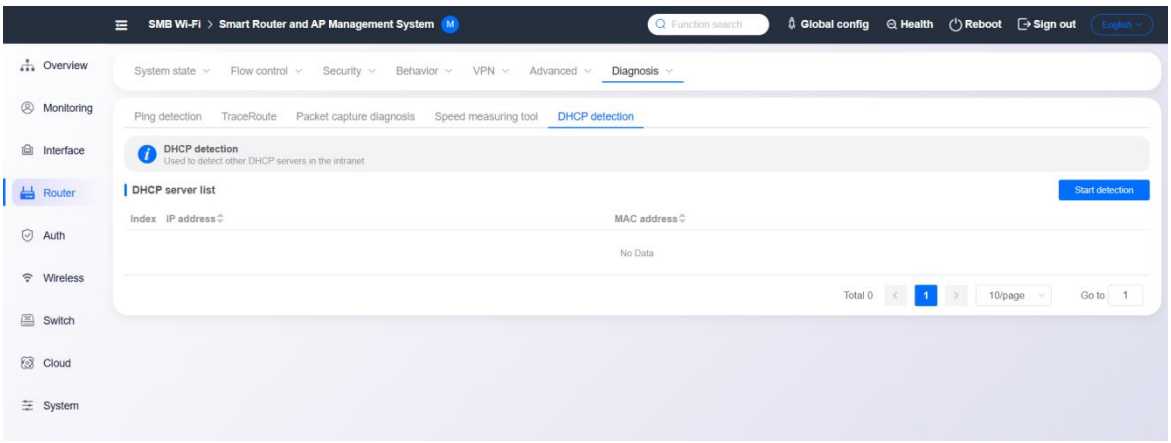
Speed information

Display the speed test information after detecting the corresponding WAN port according to the node. The record will be automatically cleared when exiting this page.



4.8.3.5 DHCP Detection

Used to detect other DHCP servers in the intranet.



DHCP Server List

After clicking Start detection, if other DHCP servers are found in the intranet, they will be displayed in the list. When you exit the page, the records will be automatically cleared.

五、 Authentication Management

Manage WEB users and PPPOE users, set user Internet authentication methods, and manage Internet notifications .

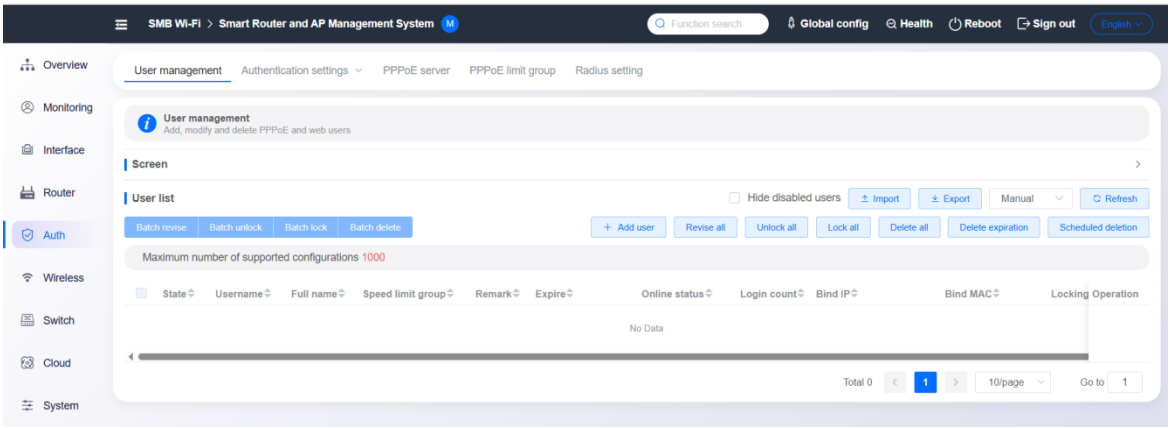
5.1 User Management

When WEB authentication and PPPOE functions are needed in the network environment, user accounts need to be created and managed. This menu mainly implements such functions.

Screen

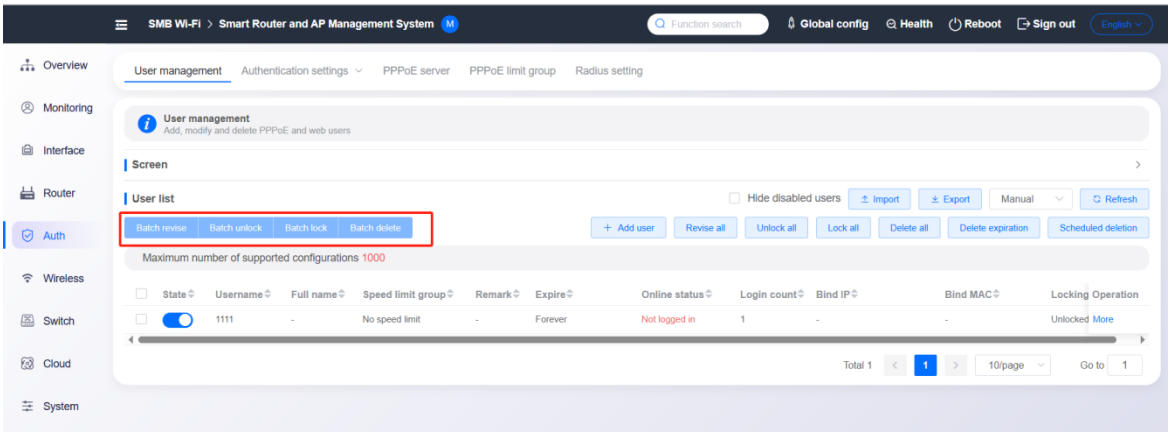
Added user accounts can be filtered by conditions to view the corresponding accounts

If the filtering conditions are incorrect or need to be changed, click the " **Clear** " button to clear the entered filtering conditions.



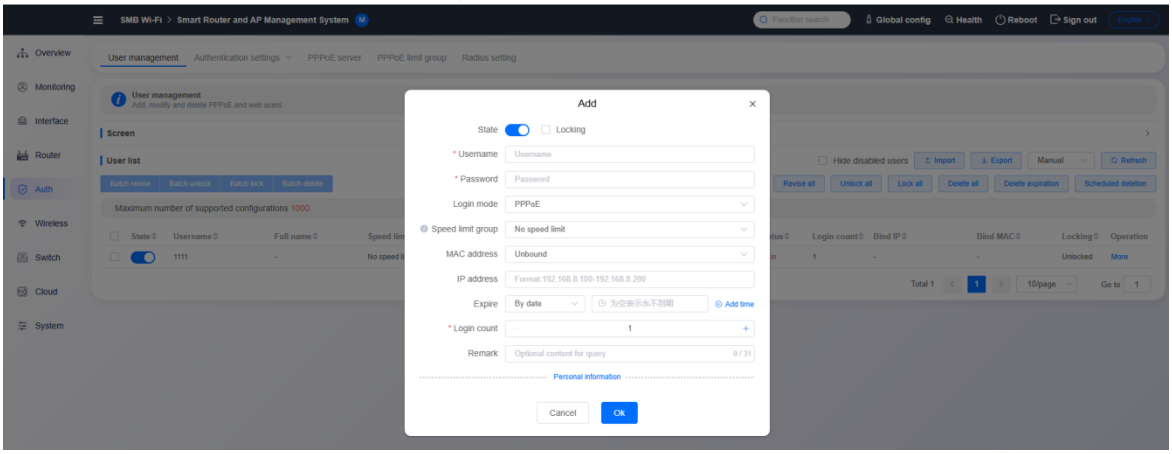
User List

Supports batch modification, batch unlocking, batch locking and batch deletion of user accounts.



添加用户：此处添加的用户（账号）认证仅适用于系统自带 WEB 认证和PPPOE 认证，不能用于云计费和智慧 WiFi 认证。

Add user: The user (account) authentication added here is only applicable to the system's built-in WEB authentication and PPPOE authentication, and cannot be used for cloud billing and smart WiFi authentication.



Status: The user account status is disabled or enabled. The accounts in disabled status cannot be used normally;

Locking: After checking, the account will be locked;

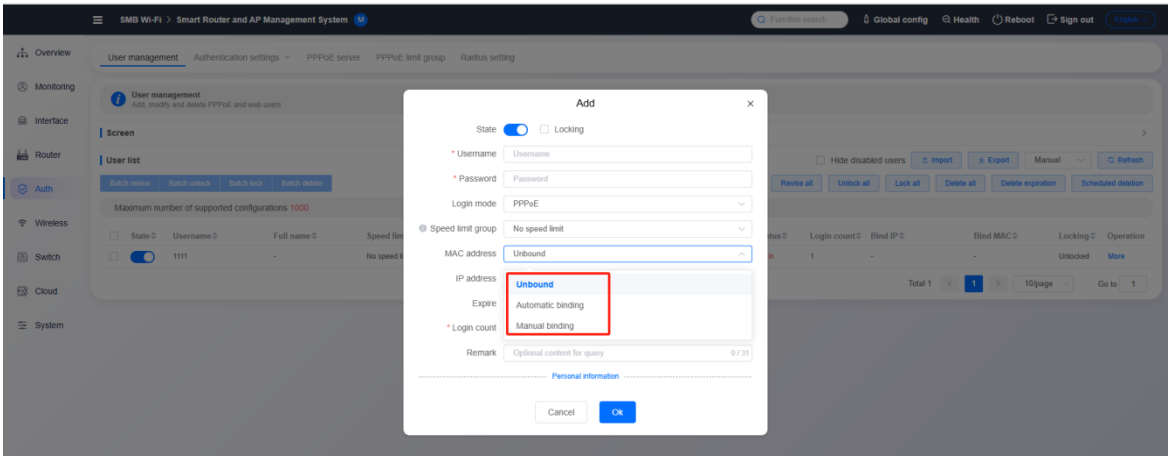
Username: Set the user account, which is usually letters, numbers or a combination of the two. The length cannot exceed 31 characters;

Password: Set the user authentication login password;

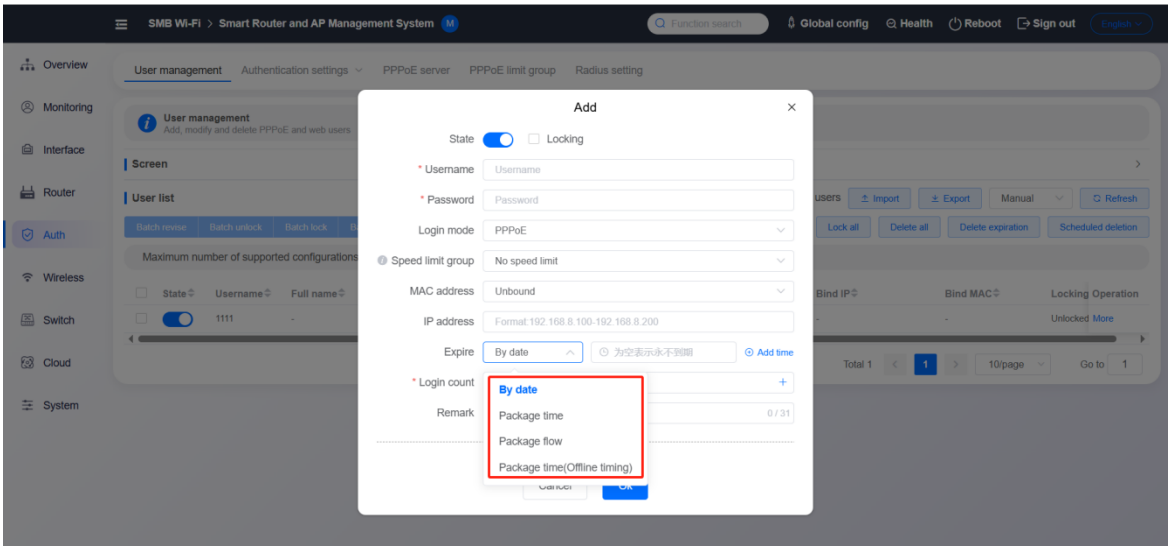
Login method: Select the authentication method for this account. Once the authentication method is selected, the account can only be used under this authentication method. For example, if the account selects WEB authentication, then it will not be used for PPPOE dial-up authentication;

PPPOE limit group: If the PPPOE dial-up method is used, there can be a PPPOE limit group where the account can be found. The system has no limit group by default, so "unlimited speed" is displayed here;

MAC address: whether the account is bound to the MAC address. The MAC address can be unbound,automatic binding, manually binding;

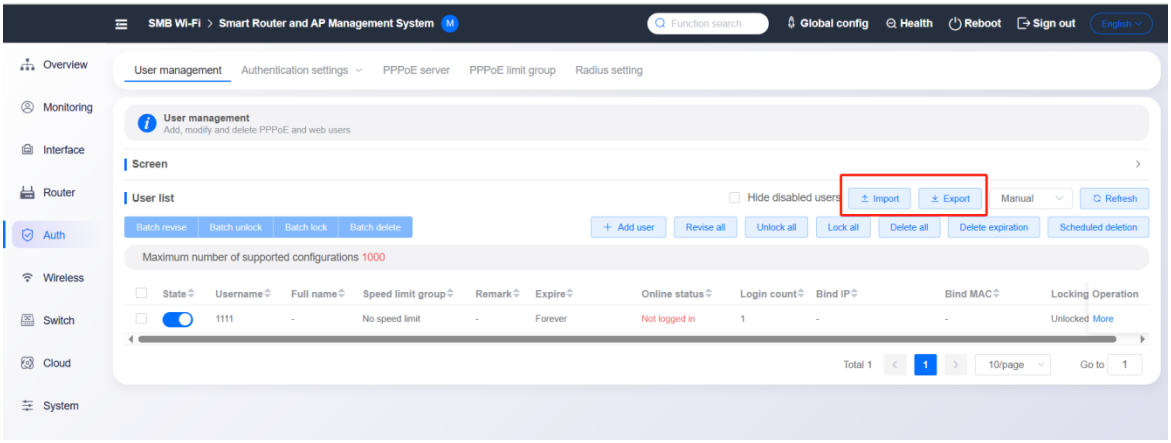


Automatic binding: When an account logs in to the Internet for the first time, it will automatically bind to the MAC address of the currently terminal in use, and then only the terminal with this MAC address can use this account. Otherwise, other terminals cannot use this account;
Manual binding: Banding the terminal' s MAC address after manually enter it. Only the terminal with this MAC address can use this account, and other terminals cannot use it.
IP address: If you fill in the IP address, it means that the account can only be used by the terminal with the IP address. Otherwise, the terminal with a non-filled IP address cannot use this account. If it is blank, it means it is not bound to the IP.
Expiration (time setting): Account expiration time setting. When the account expires, authentication fails and you need to contact the administrator to modify the expiration time. The expiration time can be set in different ways, as below:



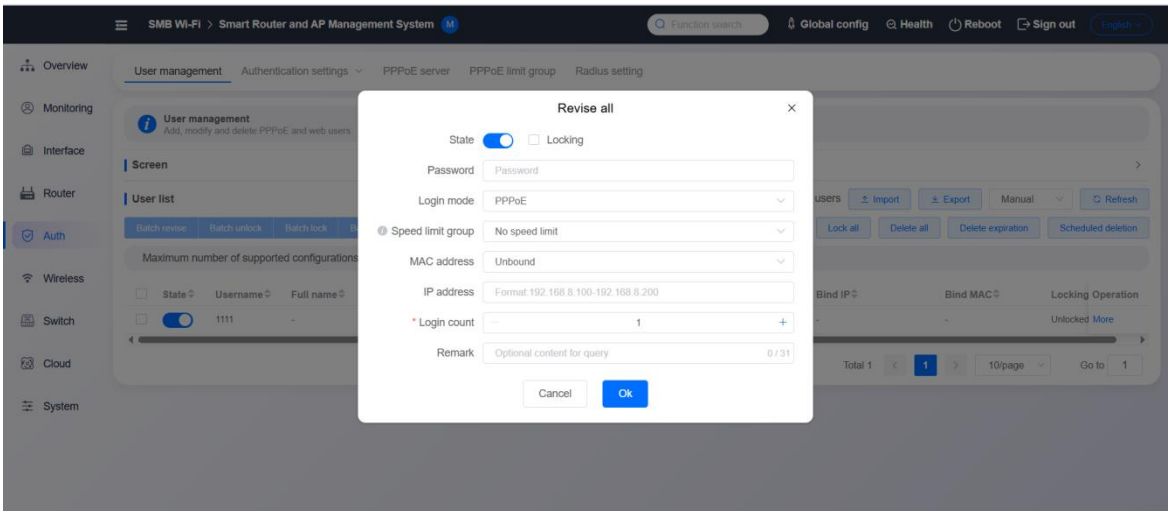
By date: After selecting a date on the page and submitting it, the account will expire on the set date and will no longer be able to authenticate and log in. When selecting a quick expiration date, the expiration date is calculated cumulatively based on the current date;
Package time: Indicates how long the account can be used. If the set time is exceeded, the authentication will fail. If "Repeat interval" is selected and the interval time is set, it indicates how often the account can be authenticated once. For example, the package time here is 1 hour, the interval time is 5 minutes, and 3 times a day. It means that the cumulative available time of this account is 1 hour. If the terminal disconnects from the network and needs to be authenticated when reconnecting, there are only 3 authentication opportunities per day, and each authentication time must be greater than or equal to 5 minutes, otherwise the authentication will not be successful. If Repeat is not checked, it means that there is no limit on the number of re-logins and the interval time for this account. For this type of package time, the time will not be accumulated after the account goes offline, and the time will only be counted when the account logs online;
Package flow: the total amount of traffic available for the account. After the traffic is used up, it cannot be used normally.
Package time, offline timing: Same as the package time package mentioned above, but the package time here will have speed control method: the uplink and downlink speed limit of the terminal using this account.
Login count: how many terminals are allowed to log in at the same time for one account. Entering 2 here means that two different terminals are allowed to log in at the same time without affecting each other.
Note: Give a brief description of the account;
Personal Information: Create a user account. If you need to fill in the account information, you can fill in the name, phone number, ID card information and remarks of the account holder here. This parameter is optional and is used for query.

Import: import user account information. If there is no user account in the current system, the export file content will be empty. You can add an account here and submit it before exporting. Add a new account to the export file content, save and import it.
Export: You can export the current accounts;

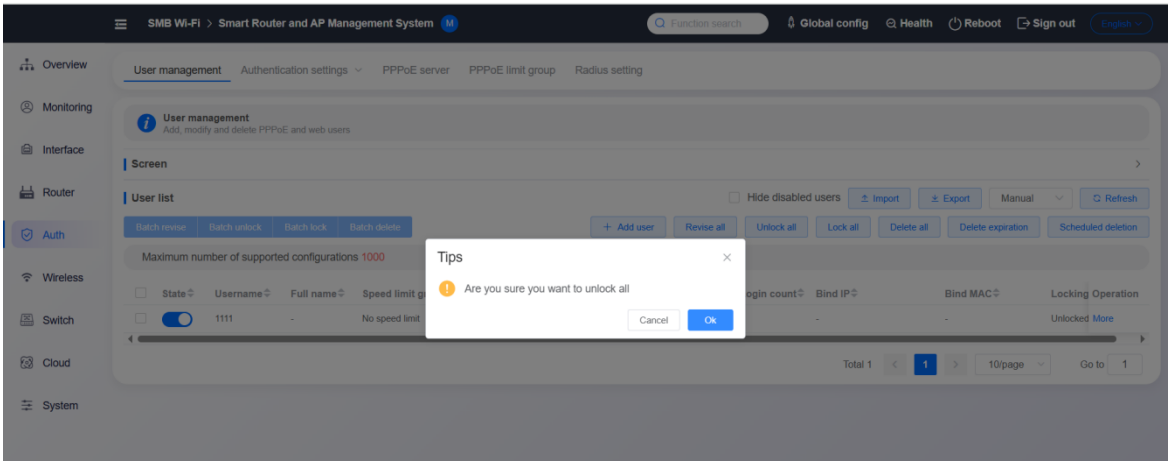


The list supports manual refresh and automatic fixed interval refresh;

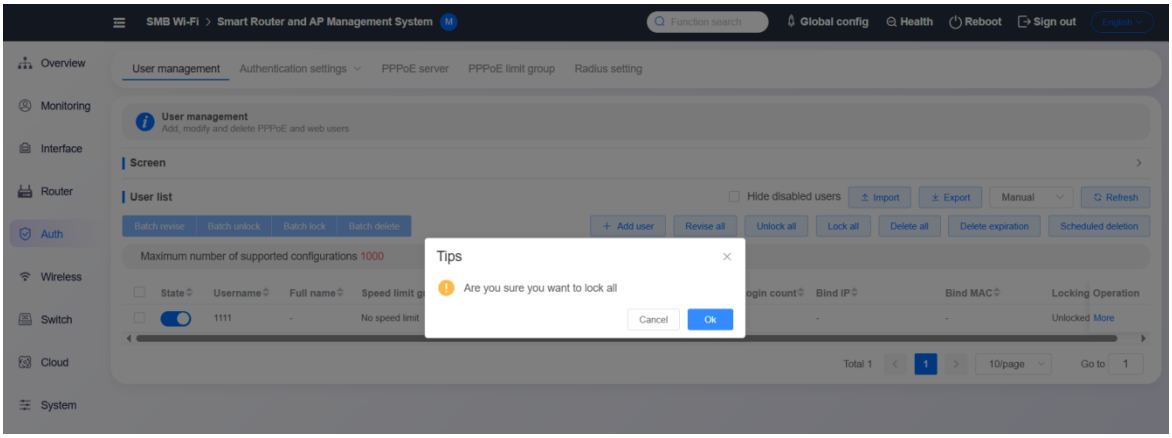
Modify All: No need to check and select the user accounts in the list. Click this button to modify part of the account content. Please check the figure below:



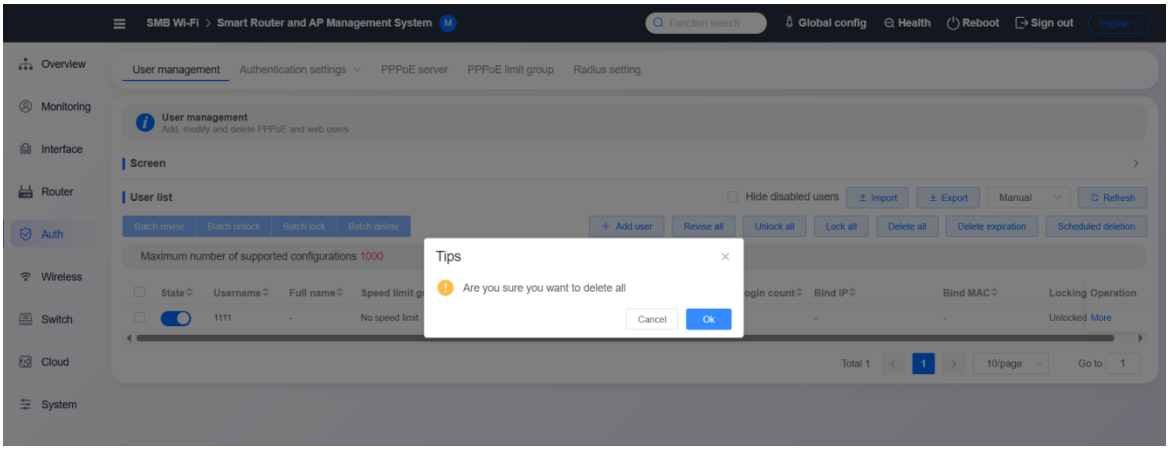
Unlock all: The premise of unlocking all is that the user account is in a locked state. The unlocked account can be deleted;



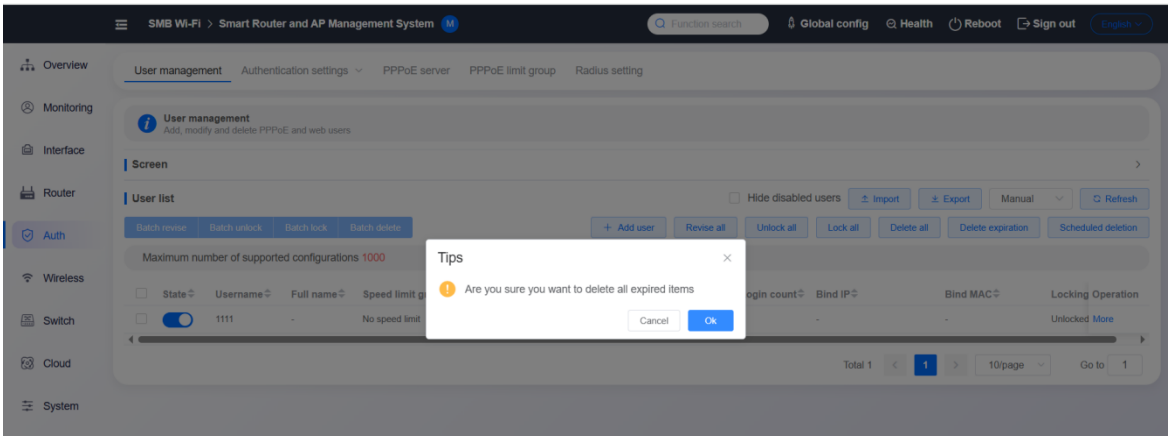
Lock all: locked accounts cannot be deleted or restored to default;



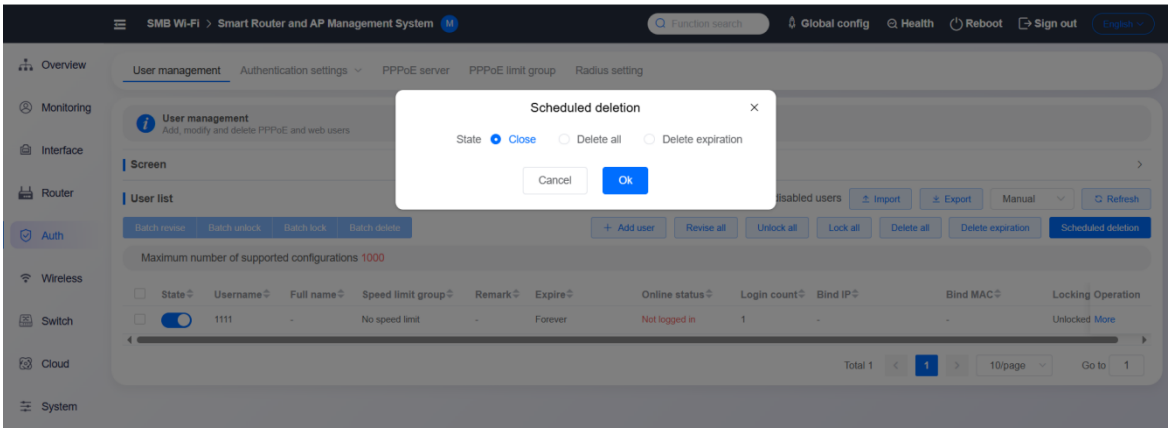
Delete All: Online accounts and locked accounts cannot be deleted, so clicking Delete All will only delete offline, expired, and unlocked accounts ;



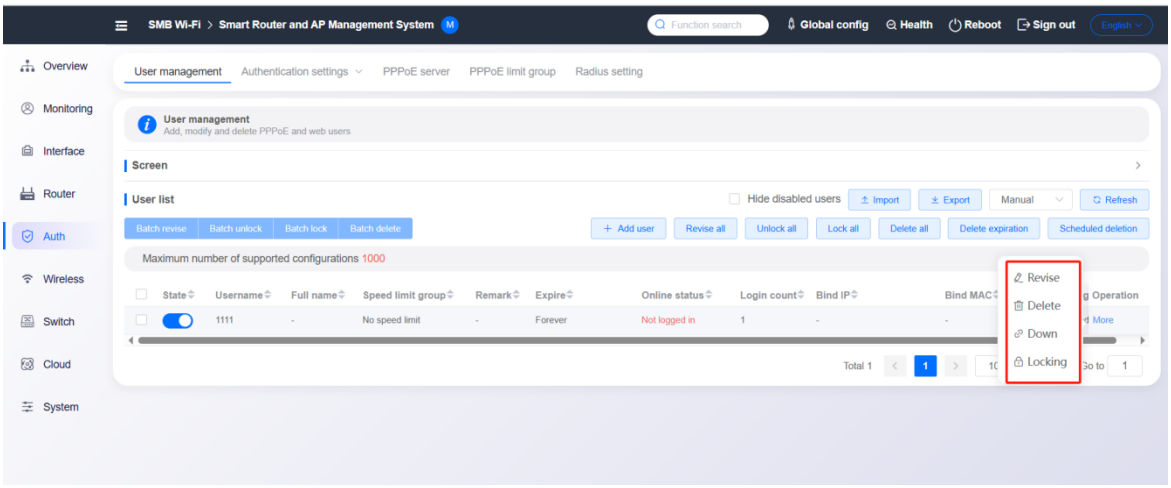
Delete expiration: delete expired accounts in batches;



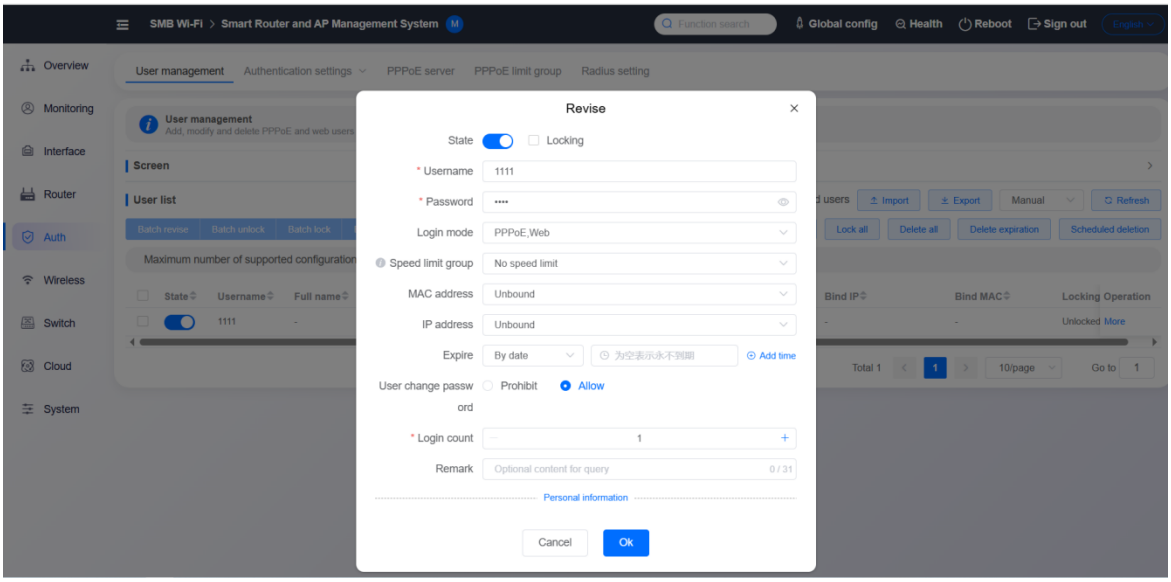
Scheduled deletion: Scheduled deletion of all accounts or expired accounts;
Close: Do not enable the scheduled deletion function;
Delete all: delete all accounts;
Delete Expiration: Delete the account that has expired.



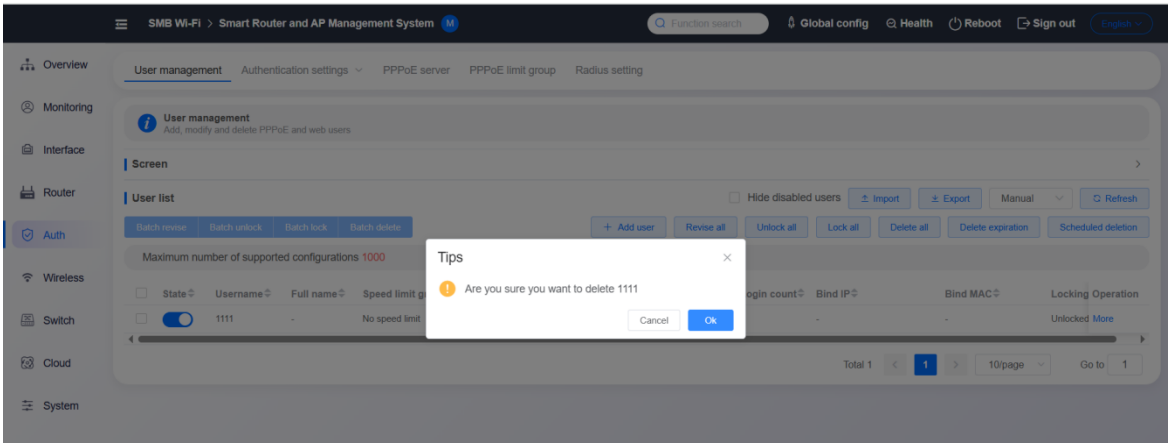
More user list operation bars: support modification , deletion, status disconnection and unlocking of individual user accounts .



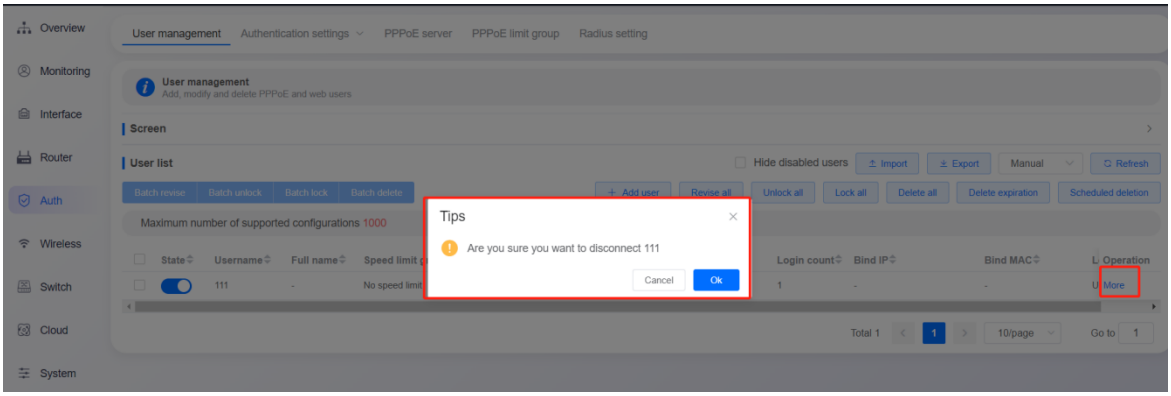
Modify: Modify the configuration parameters of the account. If the online user status is set to disabled or the username and password are modified, the terminal logged in by the account will be offline immediately. The locked account cannot be modified its login username, should be unlocked before it can be modified;



Delete: Delete the user account. The deleted account cannot be restored. Online and locked users cannot be deleted . Locked accounts cannot be deleted before unlocked it.



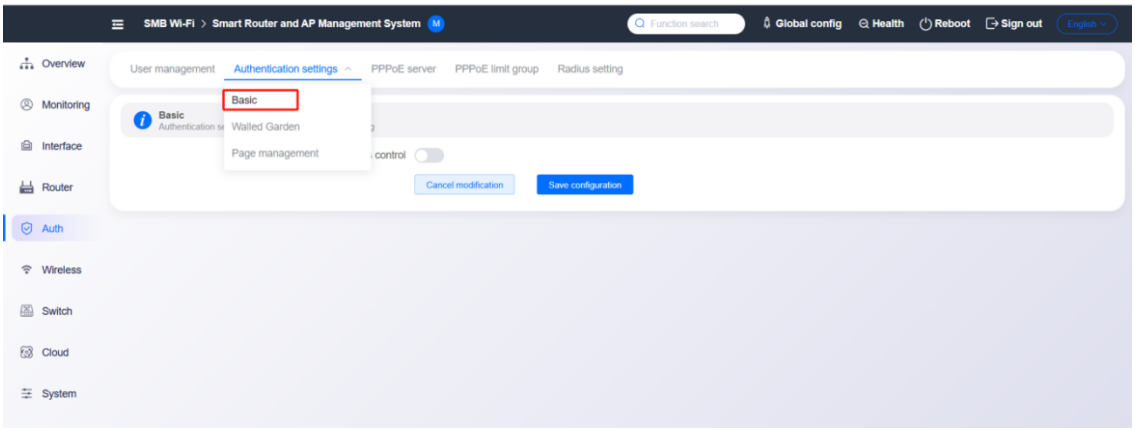
Down: If the current account online status is "logged in", click the down button to disconnect, and the corresponding end users will also be offline;



5.2 Authentication Settings

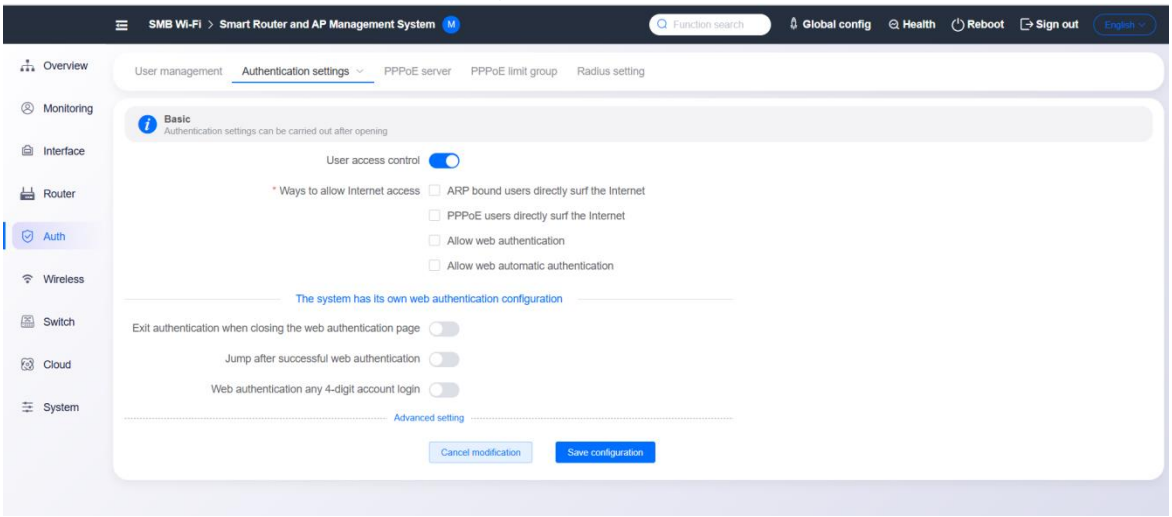
5.2.1 Basic Settings

Can set up authentication after enable authentication function.



Basic Settings

For the local WEB authentication function, check to select it, no need to enable other authentications ways . Just check and select "Allow WEB authentication" in this menu in basic settings.



User access control: When it is enabled, can proceed to the next step of rule configuration, the user Internet access method control will be automatically turned on .

Ways allow Internet access: Select the ways to the allow the users to access the Internet, " ARP binding users to access the Internet directly ", "PPPOE users to access the Internet directly", "Allow WEB authentication to access the Internet", "Allow WEB automatic authentication to access the Internet" .

ARP-bound users directly surf the internet: Users whose IP and MAC addresses have been bound can access the Internet directly;

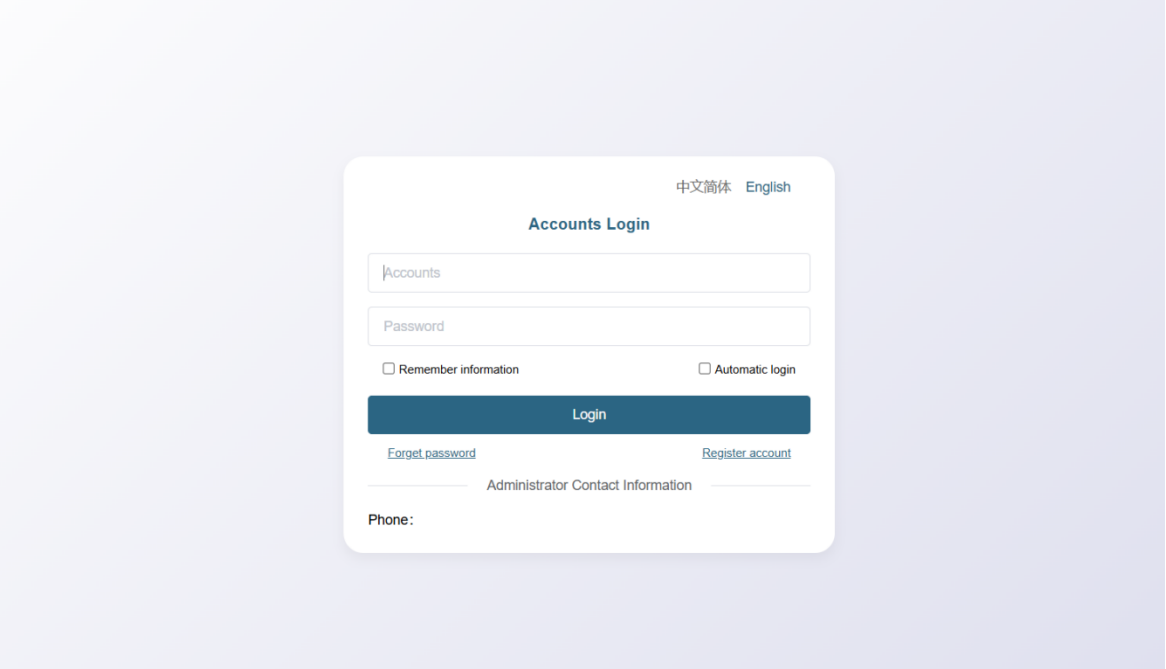
PPPoE users directly surf internet: Users who dial up to the router using the PPPoE protocol can access the Internet only after passing verification;

Allow WEB authentication: Only users who have logged in through web authentication information can access the Internet ;

Allow WEB automatic authentication: Users will be authenticated when they connect to the router for the first time. No need to authenticate it again before the router is restarted.

Generally, if the authentication way is WEB (page) authentication, please check "Allow WEB authentication" and "Allow WEB automatic authentication". "Allow WEB authentication" is to enable the WEB page portal to pop up normally, and "Allow WEB automatic authentication" means that when the terminal connects to the original network within the MAC aging time range, no need to fill in the account and password authentication.

WEB authentication type : The system comes with WEB authentication. Select "Allow WEB authentication" or "Allow WEB automatic authentication" in the authentication method. The terminal connected to this network in the LAN will pop up the following portal:

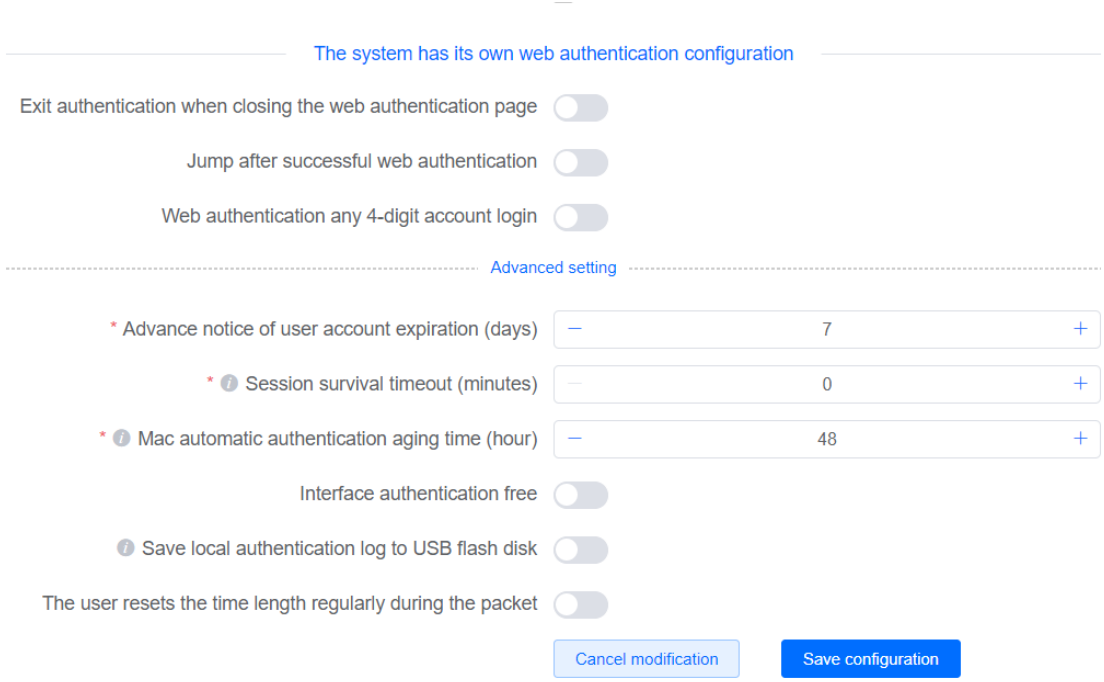


The system has its own web authentication configuration:

Exit authentication when closing the WEB authentication page: Disable or enable

Jump after successful WEB authentication: Disable or enable

Log in with any 4-digit account via WEB authentication: disable or enable.



Advanced Setting

Advance notice of user account expiration (days) : How many days should be set to start pushing expiration notifications before the account will be expired

Session survival timeout (minutes) : How long does it take for a user to be detected online and then forcibly re-authenticated, the maximum is no more than 1440 minutes;

MAC automatic authentication aging time (hours) : 0 means no aging;

Interface authentication free : Select an interface that can access the Internet directly without authentication. The interfaces can be distinguished by wired and SSID.

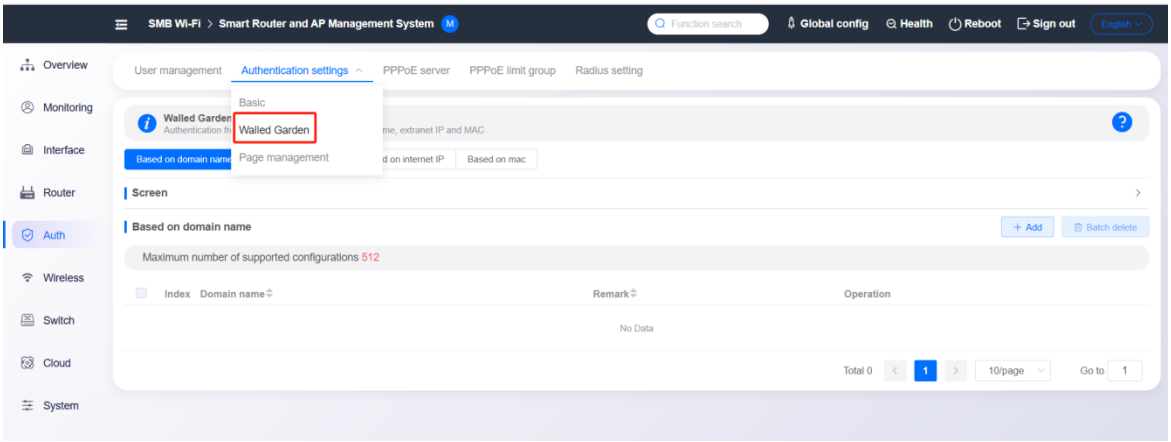
Save local authentication log to USB flash disk : log file path /auth_log/ ;

The user resets the time length regularly during the packet : this is the settings for hour by hour users, when a package is sent, the users is scheduled to clear the remaining time and then restart a new package.

5.2.2 Auth Free

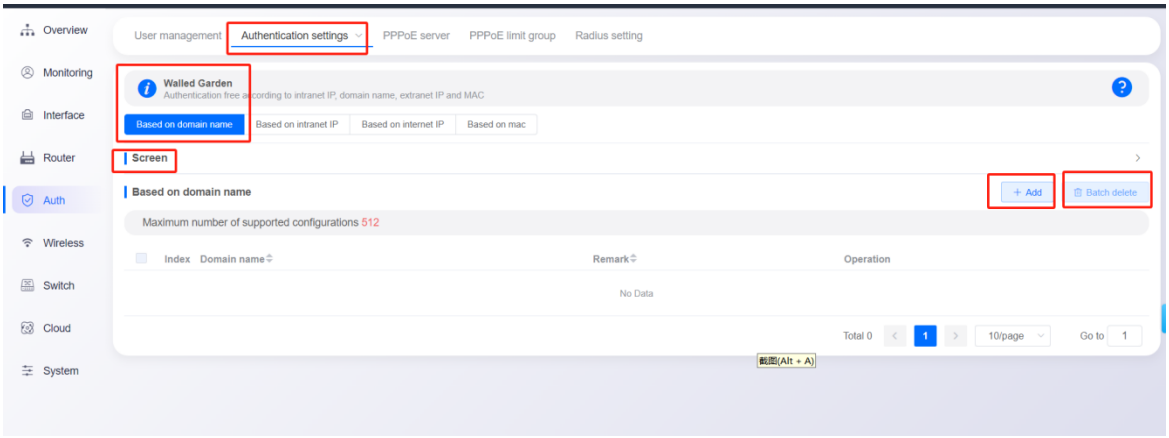
Authentication free method

By using methods such as internal IP, domain name, external IP, MAC, etc. for authentication free access, user can directly access the internet without any authentication.



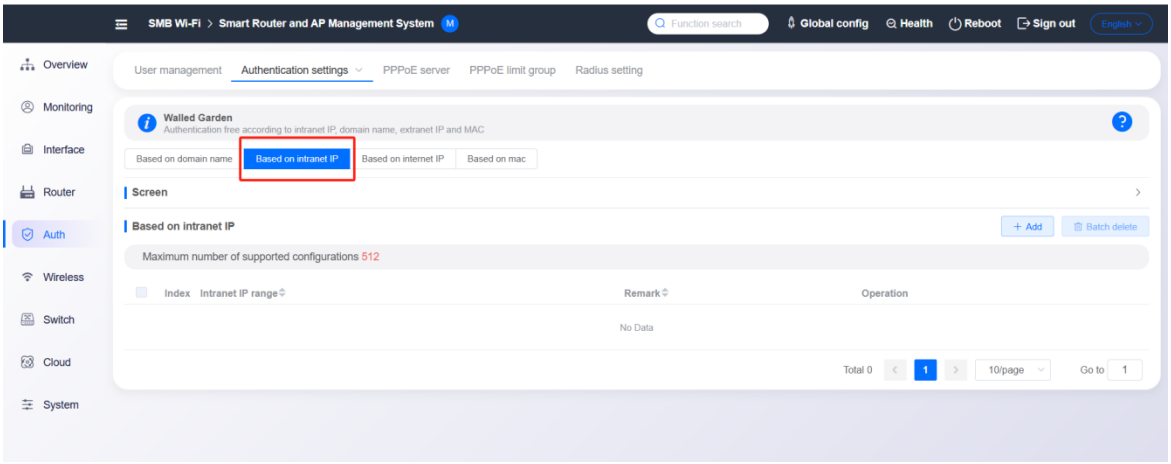
1. **Based on domain name**

If any authentication method is enabled , the terminals in the LAN will fail to access all URLs. However, the domain name is added in here will not be blocked when the terminal accesses it, and it can be directly access. The format of the domain name is added in must comply with the standard format and cannot be filled in arbitrarily. Only one domain name can be filled in at a time in the input space. If there are multiple domain names will be configured in the whitelist, please add a few more rules. If there are whitelist domain names that need to be deleted in batches, check and click "Batch Delete" to confirm. Please note that the deleted domain names cannot be restored.



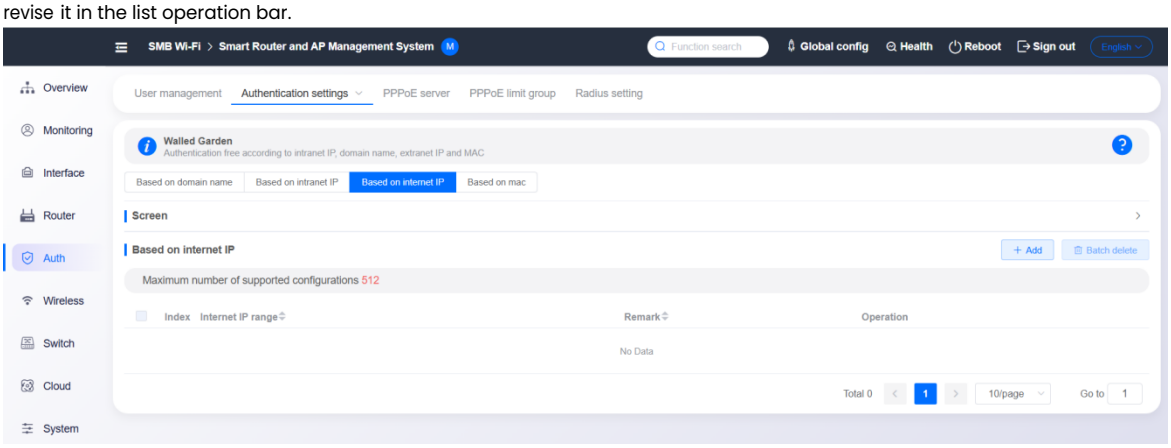
2. Based on intranet IP

Release the whitelist of user IP addresses within the local area network. For example, if the IP obtained by the mobile phone at this time is 192.168.1.101 , after the system turns on the authentication function, the terminal with IP 1.101 will be allowed to access the Internet without authentication. Users in the whitelist are displayed as "Allowed" in the "User List" and "Internet Status" of the host monitoring. When adding an intranet IP, it can be either a single IP address or an IP address segment. If you need to delete one or some intranet IP whitelists, check it then delete it, or click "Batch Delete".



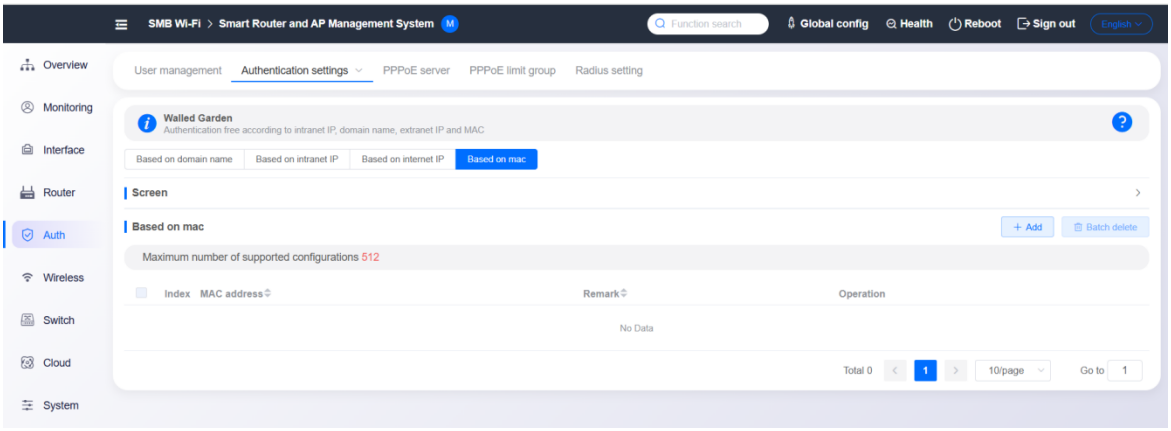
3. Based on external IP

Similar to making a whitelist based on domain names, if you need to make a whitelist for external IPs, just fill in the external IP addresses that need to be released in this menu. The input box supports filling in a single IP or a certain IP segment. If you need to delete the external IP whitelist, please check it first, then delete or batch delete it; If you need to modify the filled IP address, revise it in the list operation bar.



4. MAC-based

Because the intranet IP address often changes due to the terminal user disconnecting and reconnecting, the whitelist based on the intranet IP is not effective. As a result, the whitelist based on the MAC address was born. The MAC address here refers to the MAC address of the terminal, which will not change. Similarly, the terminal users filled in the MAC whitelist can be allowed to access the Internet without authentication. If you need to delete the MAC address whitelist, please check it first, delete or "Batch Delete" it. If you need to modify the filled MAC address, revise t in the list operation column.



Screen

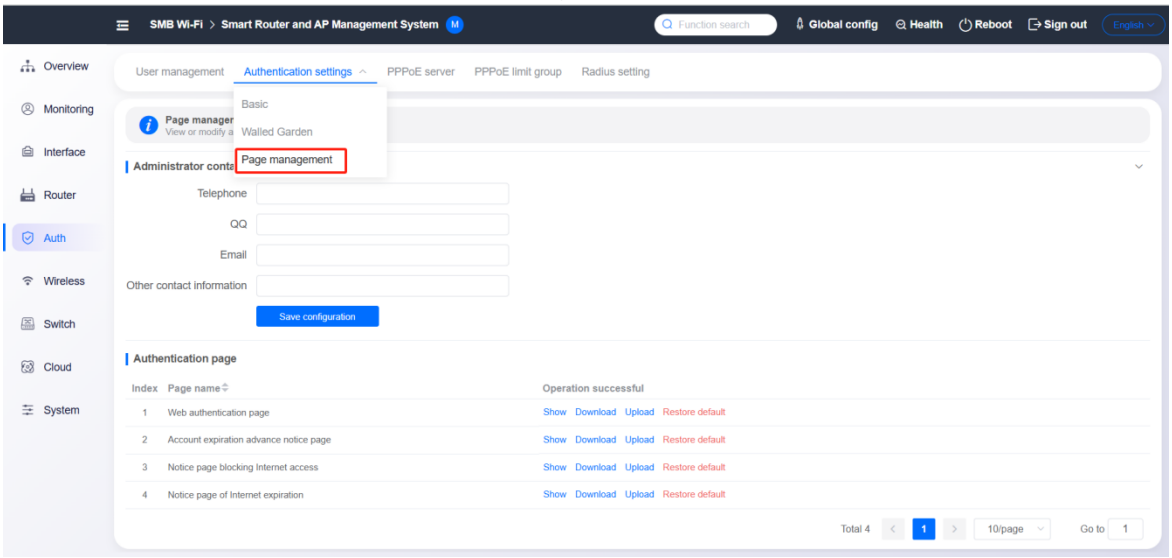
Based on domain name: filter by domain name;
Based on intranet IP: filter by intranet IP range;
Based on external IP: filter by external IP range;
MAC-based: Filter by MAC address range.

Screen display list

Based on domain name: Display all domain names that are exempt from authentication or that meet the conditions for filtering;
Based on intranet IP: Display all intranet IPs that are exempt from authentication or those that meet the conditions;
Based on external IP: Display all external IPs that are exempt from authentication or those that meet the conditions;
Based on MAC: Displays the MAC addresses of all devices that are exempt from authentication or that meet the filtering criteria.

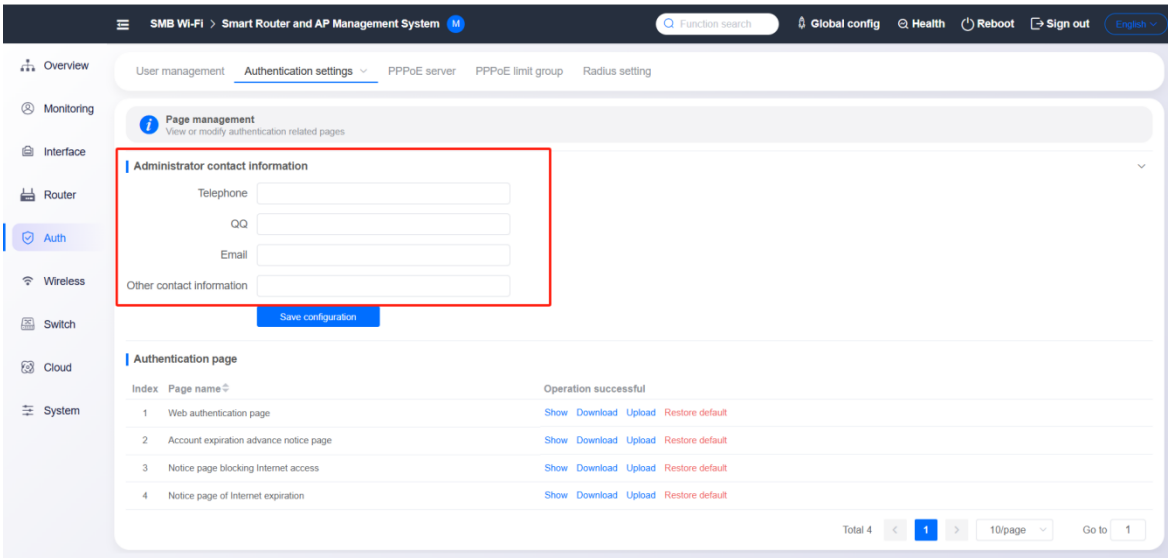
5.4.3 Page Management

This function is to view or modify all authentication related pages .



Administrator contact information

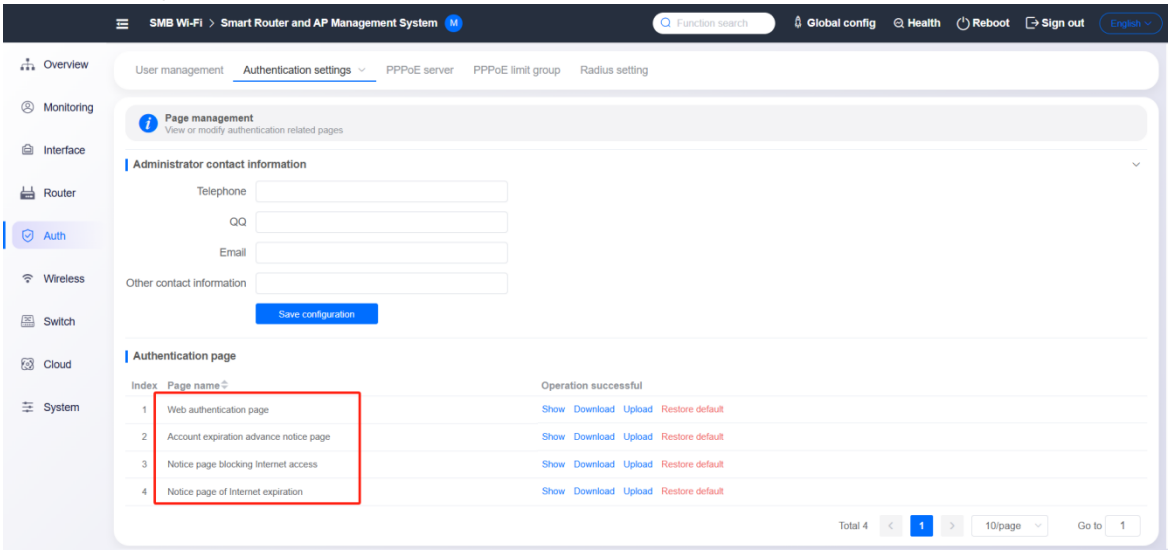
Used to provide administrator contact information so that customers can contact the administrator when their account expires or they cannot access the Internet.



Authentication page

Supports view (preview), download, upload, and restore default operations for the following page types:

1. Web authentication page;
2. Account expiration advance notice page;
3. Notice page blocking Internet access;
4. Notice page of Internet expiration;

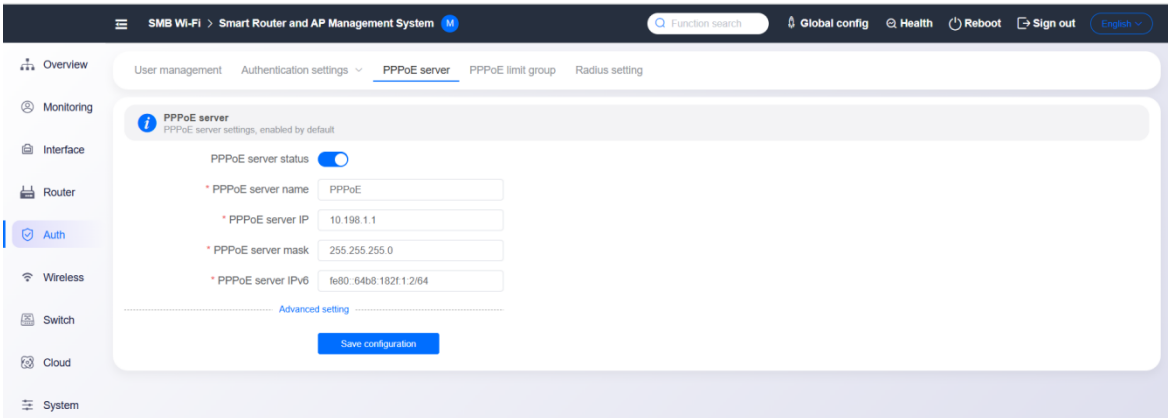


5.5 PPPoE server

PPPoE function is required in the network configuration and it serves as a PPPoE server , please set it here.

PPPoE Server

PPPoE server settings, enabled by default .



PPPoE server status: Generally, the system turns on the PPPOE server by default. If it is disabled, the PPPOE user will fail to dial;

PPPoE server name: Customize the PPPoE server name, normally use the default name;

PPPoE server IP: The address of the PPPoE server. PPPoE users can access the server settings WEB login page through this address. If the PPPoE server address of the lower-level device is the same as the upper-level server address, please modify one of the address to avoid conflict;

PPPoE server mask: The mask address of the PPPoE server, which can be modified according to environmental requirements;

PPPoE server IPv6: If the IPV6 function of PPPoE is required in the environment, the IPV6 address can be configured here. Generally, the default address can be used. If there is an address conflict, please modify it as needed;

Advanced Settings

Allow any server name to access: If this function is enabled, the server name filled in by the client during dial-up will not be verified. Otherwise, the server name needs to be verified.

Only PPPOE access is allowed: After it is enabled, only users who dial up via PPPoE can access the router and surf the Internet, and only the PPPoE server address can be used to access the router WEB interface. If the LAN port IP is used, the router WEB interface cannot be accessed;

Preferred DNS server: The DNS server address assigned by the PPPOE server to the client;

Alternate DNS server: The DNS server address assigned by the PPPoE server to the client.

Idle detection time (seconds): After the set time, if there is no data communication between the client and the server, it will start to detect whether the client is offline. The default value is 3 seconds, and the range is 3-180;

Disconnect if request error: How long time of the detection requests are not responded before disconnection, fill the time here, if the client has no data communication response in this time, its connection will be disconnected. The default value is 3, and the range is 3-180 seconds;

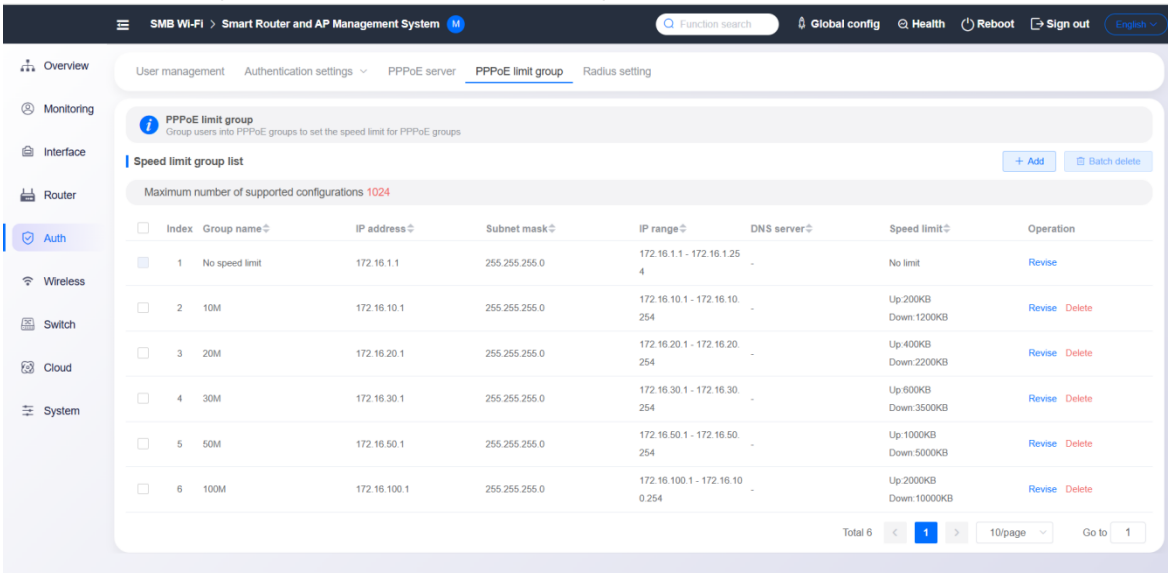
Authentication method: Different authentication methods can be used for different application environments. For general PCs, PAP mode is used. If a lower-level router is used for dialing, can check all authentication methods;

Log in with any account: After enabling this function, please do not check the MS-CHAP v2 encrypted authentication in "Authentication method". Then the server will no longer accurately verify the dial-up account information of the terminal, and the user can pass the authentication by entering any account and password.

Login with any account: Allow login but prohibit Internet access, this function can be enabled or disabled as needed only after the authentication account login function is enabled.

5.6 PPPoE Limit Group

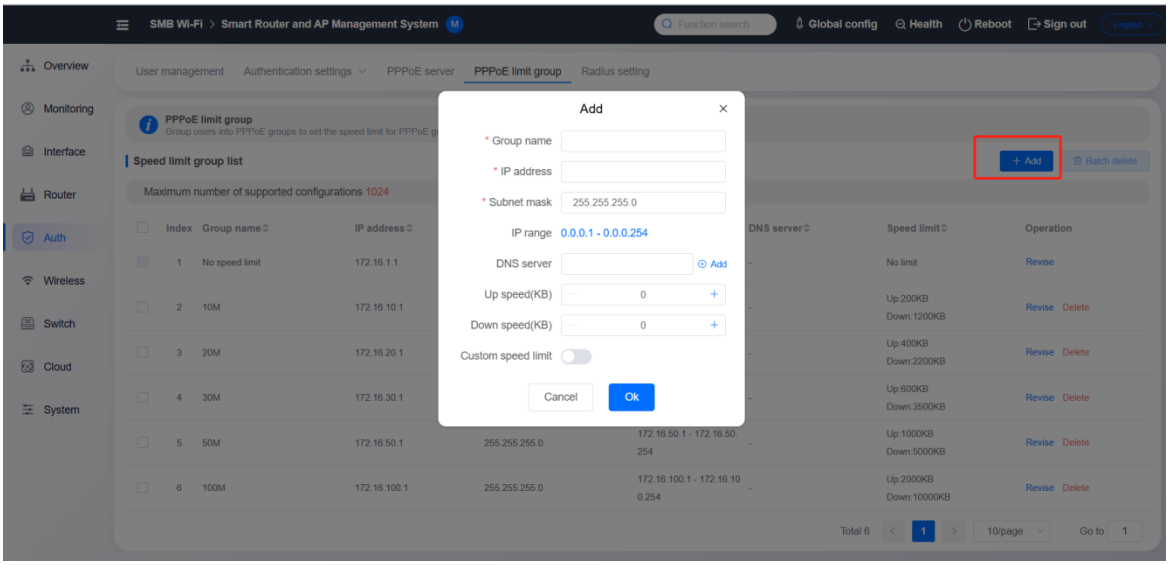
Divide users into PPPoE groups and set speed limits for the PPPoE groups.



Speed limit group list

Display all speed limit groups;

Add: Add multiple PPPoE speed limit groups, which are generally used to distinguish different types of users, making it easier to perform bandwidth restrictions or access restrictions on different types of users.



Group name: Notes and description of the group, so that managers can easily understand the difference between groups;

IP address: Set an IP address for the group;

Subnet mask: Set the mask corresponding to the IP address of the grouped network segment;

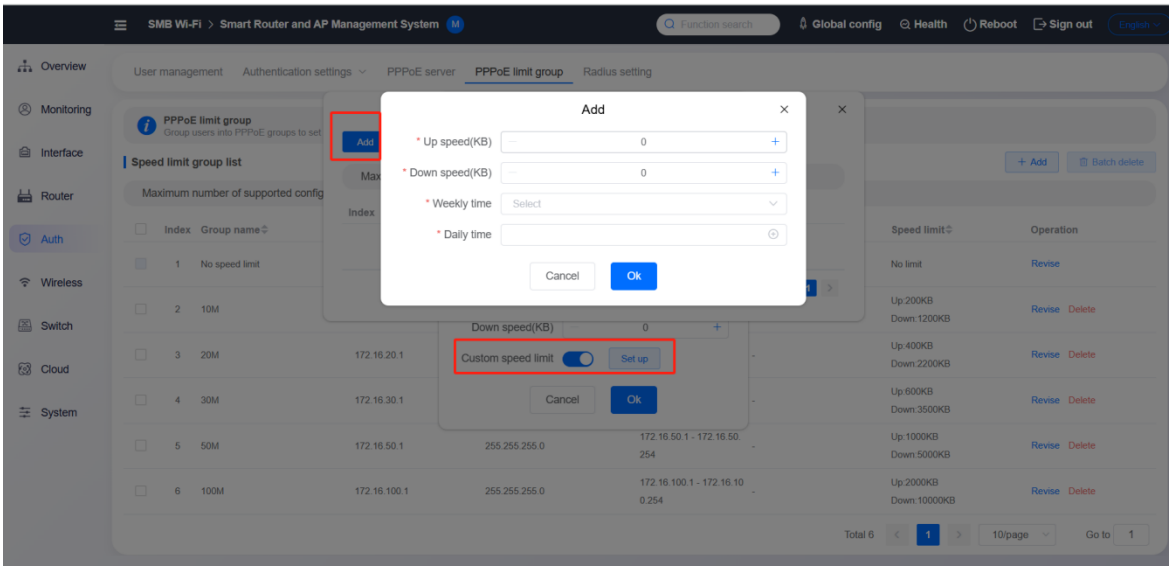
IP range: the available IP range calculated by IP address and subnet mask;

DNS server: Set an independent DNS server for this group, otherwise it will be automatic.

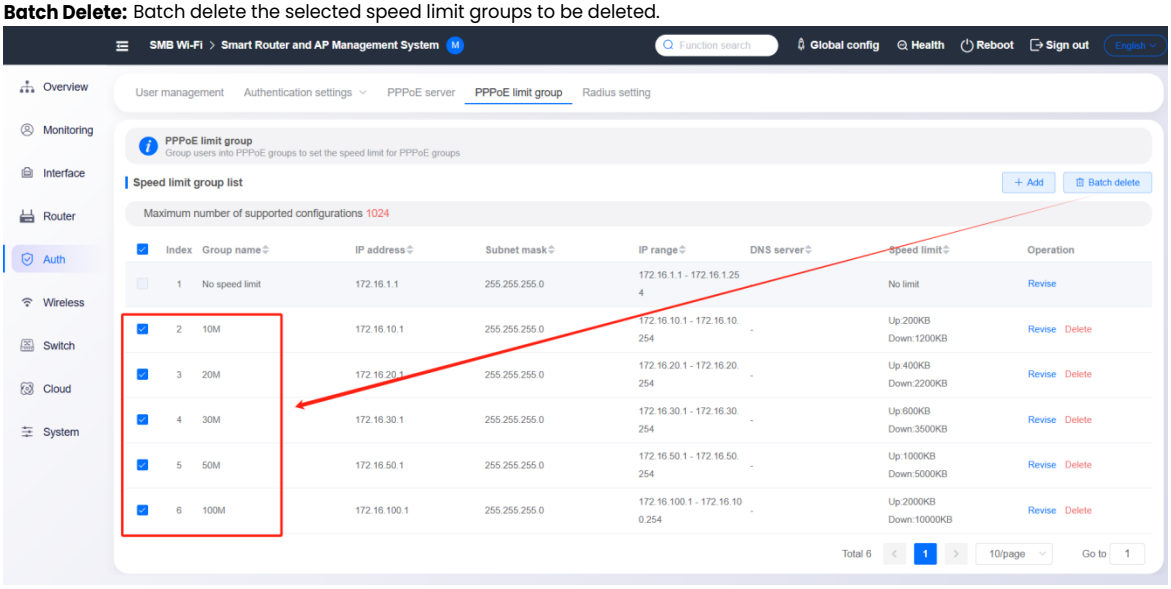
Up speed (KB): The upload speed limit of users in this group;

Down speed (KB): The download speed limit for users in this group;

Custom speed limit: Can set different speed limits for different time periods based on custom time.

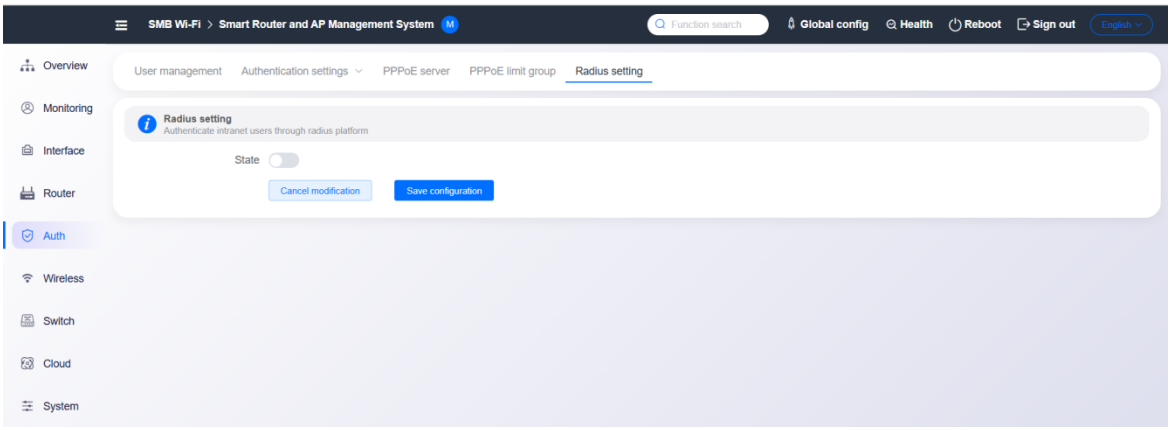


Batch Delete: Batch delete the selected speed limit groups to be deleted.



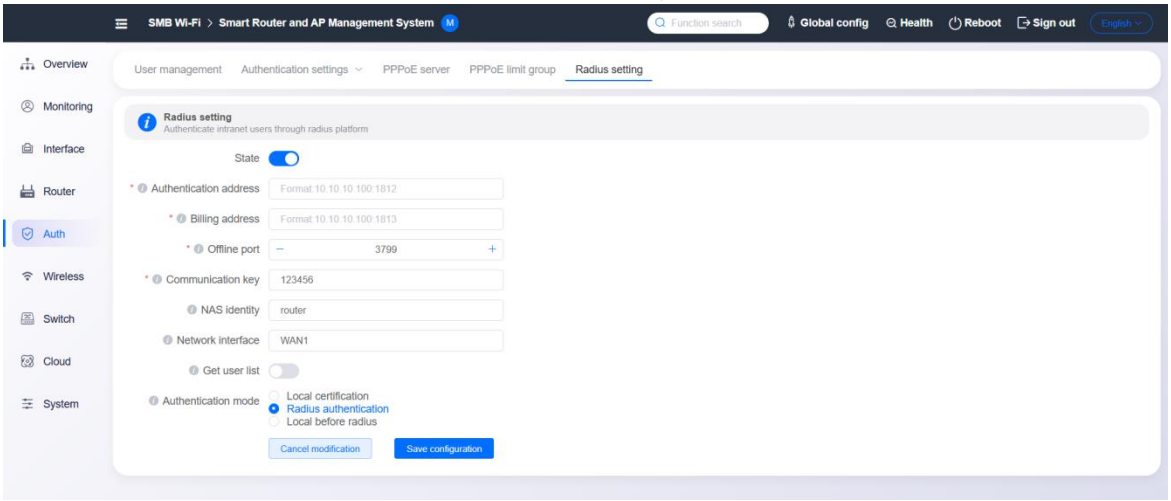
5.7 Radius Settings

The system's built-in standard RADIUS protocol can be connected to the standard RADIUS server on the market for authentication and billing



Radius Settings

Intranet users are authenticated and allowed to access the Internet through the Radius platform .



State: Radius authentication is disabled by default. Can configure rules after enable it. After enabling, Please click "Save Configuration", otherwise the configuration parameters will not be saved.

Authentication address: The authentication server address and port of the Radius server. Keep it consistent with the information provided by the server. The format is: 10.10.10.1:1812;

Billing address: The billing server address and port of the Radius server. Keep it consistent with the information provided by the server. The radius server can be accessed through this address and port. The format is: 10.10.10.1:1813 ;

Offline port: The Radius server sends the offline command to this port. Please check the port number with the server when filling in the form;

Communication key: Keep it consistent with the communication key provided by the server and need to be confirmed with the server;

NAS identity: Enter the ID of the target server;

Network interface: that is, the interface from which the radius data goes out of the current system, such as LAN, WAN1, WAN2, VPN1, VPN2, OVPN. Please specify multiple interfaces by English commas ", " to separate them;

Get user list: After enable it, the user account list will be obtained from the server. Only PAP encryption is supported;

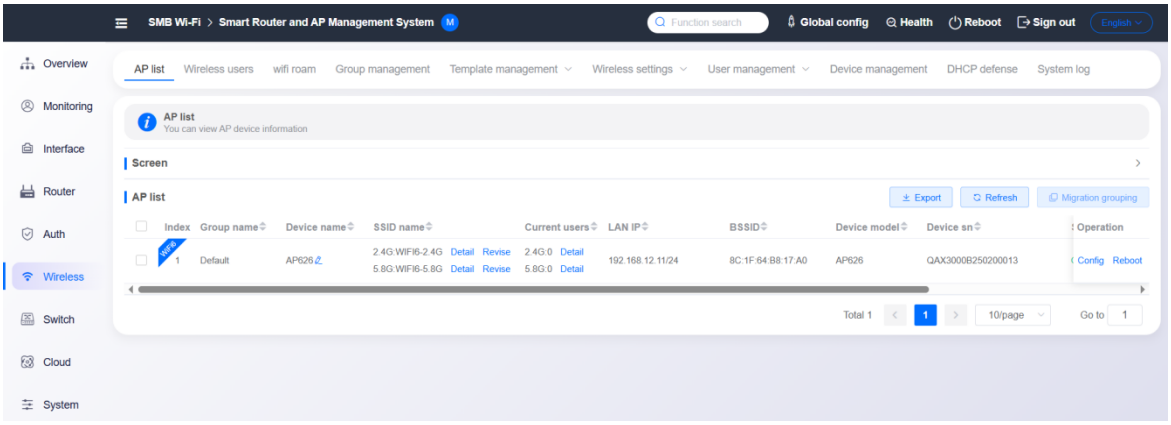
Authentication mode: Please select the router itself or the Radius server for authentication. The speed limit issued by Radius takes precedence over the local one.

六、 Wireless

In this part, mean this device is work as AP controller, to manage the wireless access point.

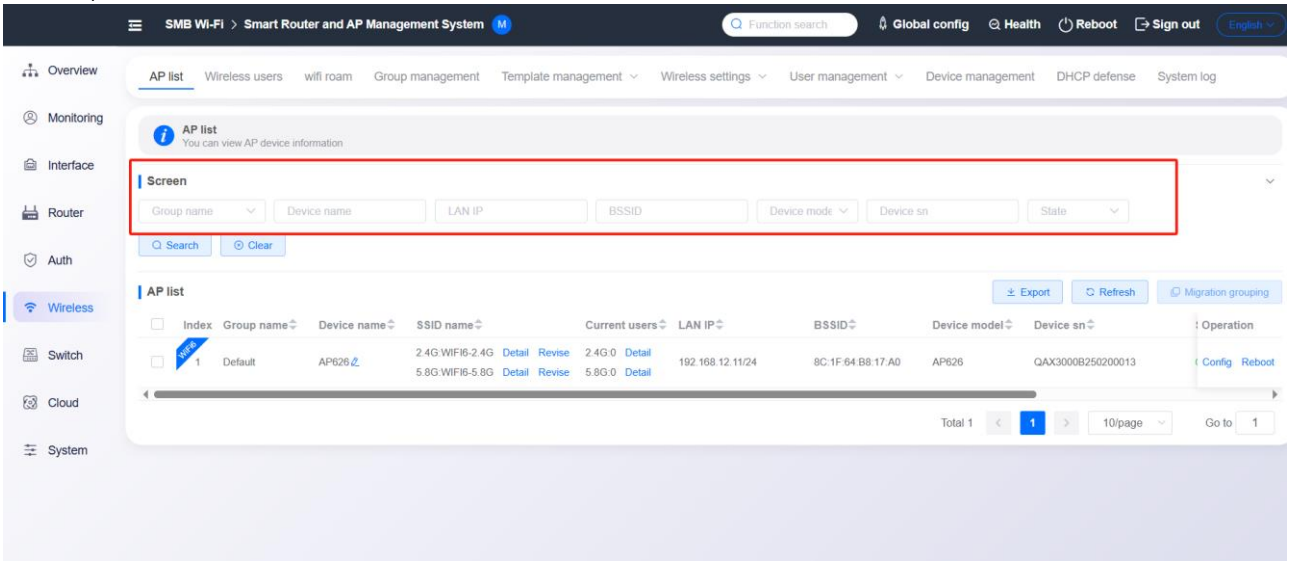
6.1 AP list

Displays the AP devices that has connected or in connecting to the main device. Supports logging into the corresponding AP management page through "Config" button in the AP list. In the AP list, can view information such as AP model, SSID name, running time, remaining memory, etc.



Screen

When there are multiple AP devices connected to the AP controller, can filter them by currently supported conditions to accurately find the AP will be viewed



AP List

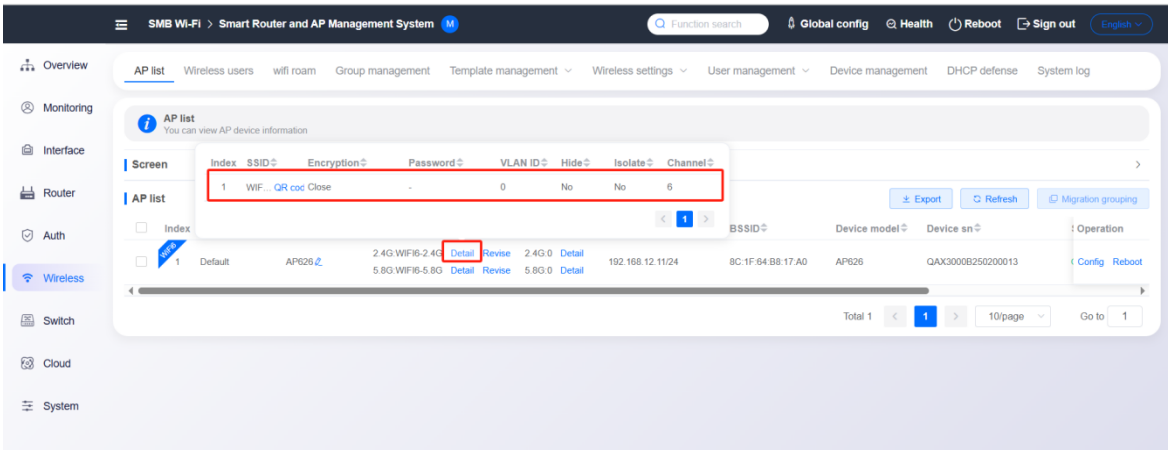
Displays information such as SSID, current number of users, LAN IP, BSSID and online status of all current APs.

Migration grouping: The administrator needs to create AP groups first. If there are no groups, migration is not possible. APs connected to the main device are summarized in the "Default Group". Administrators often group devices for easy management. After checking the device, click "Migrate Group" - select the group name and submit.

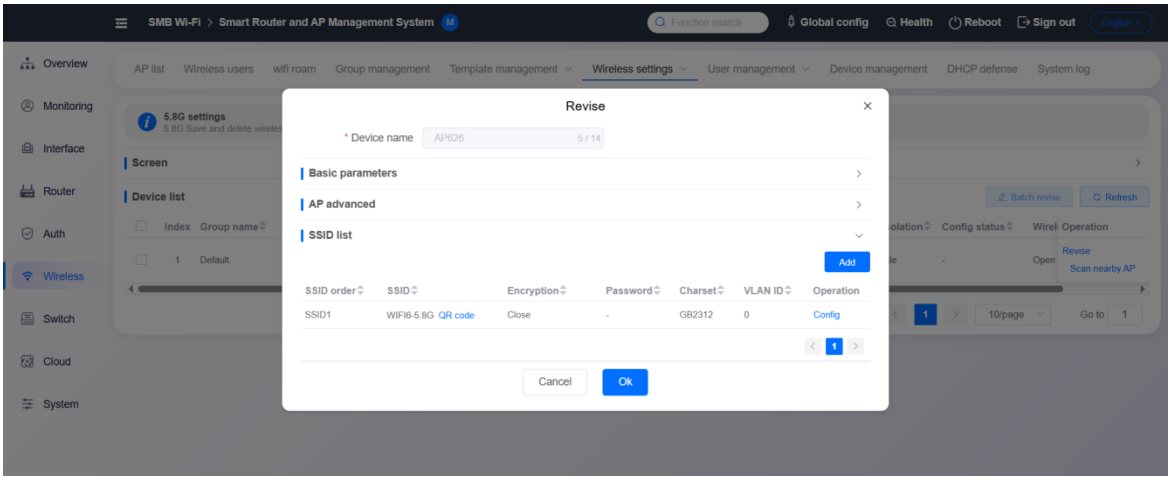
Refresh: refresh the current list information display;

Export: export the current list information;

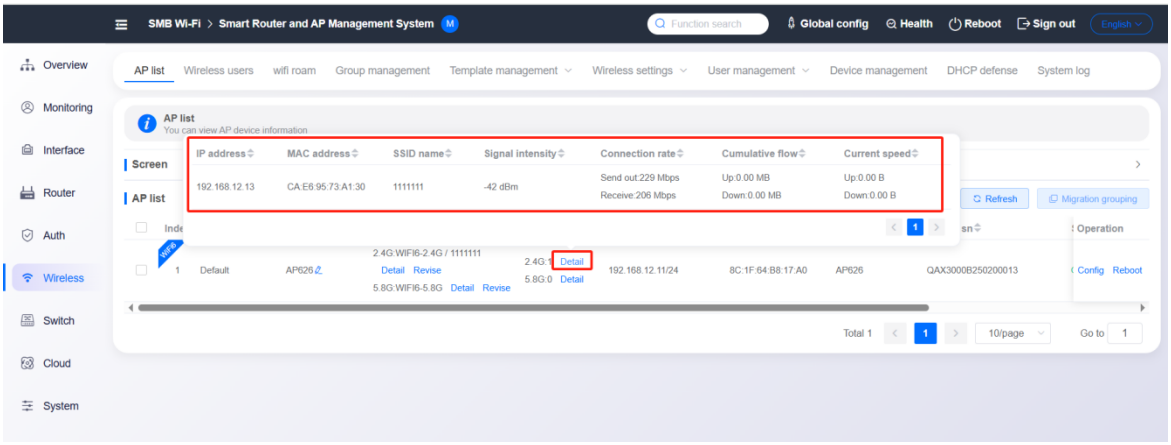
SSID name: can view the SSID information from “details” in below picture, the 2.4G and 5.8G wireless names are displayed separately, as shown below:



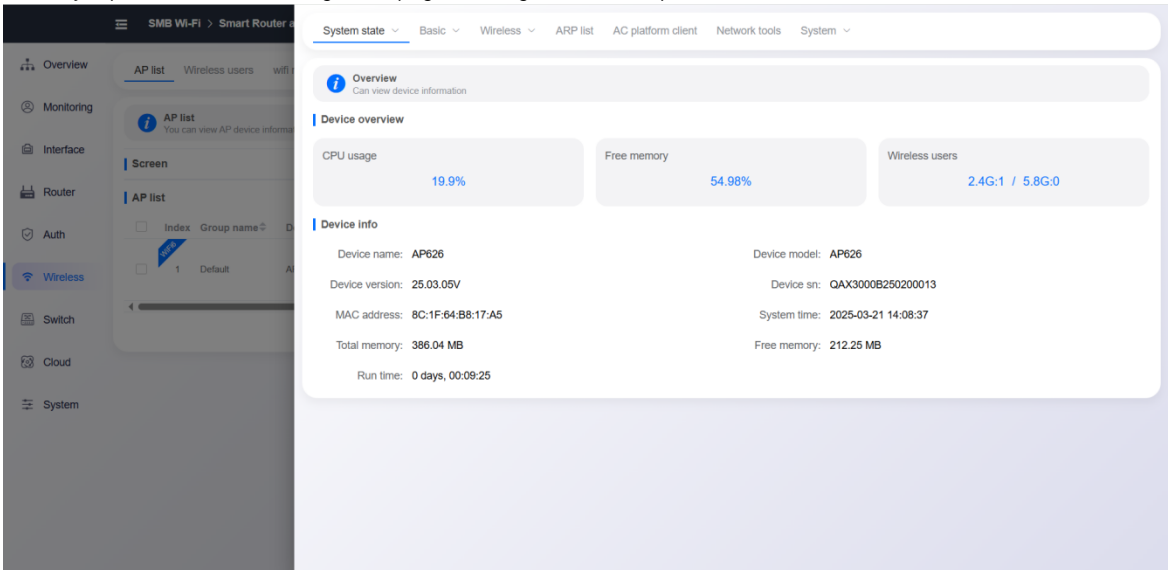
SSID name revise: Click “revise” in above picture to modify the wireless parameters of the current AP, such as device name, basic wireless parameter and advanced parameters, add a SSID or delete the current SSID and other information;



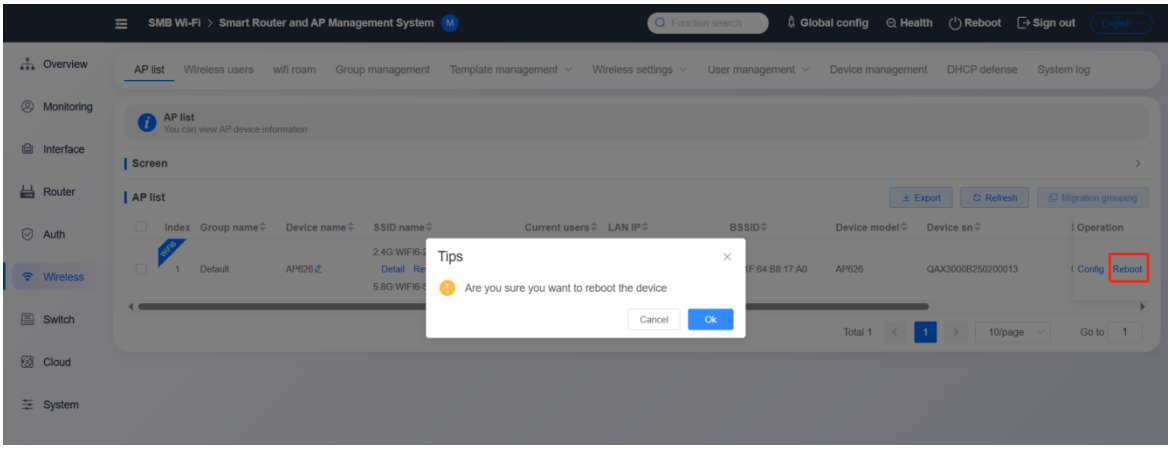
Current users : can view the detailed information of the current wireless connected users;



Config: jump to the AP's WEB management page to configure or view AP parameters;

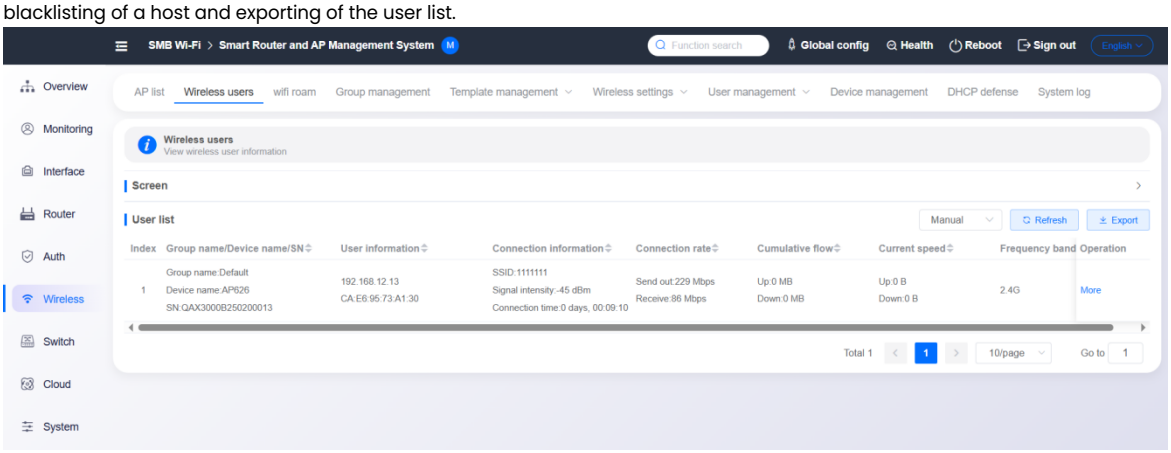


Reboot: After clicking the Reboot button, the current AP will restart immediately.



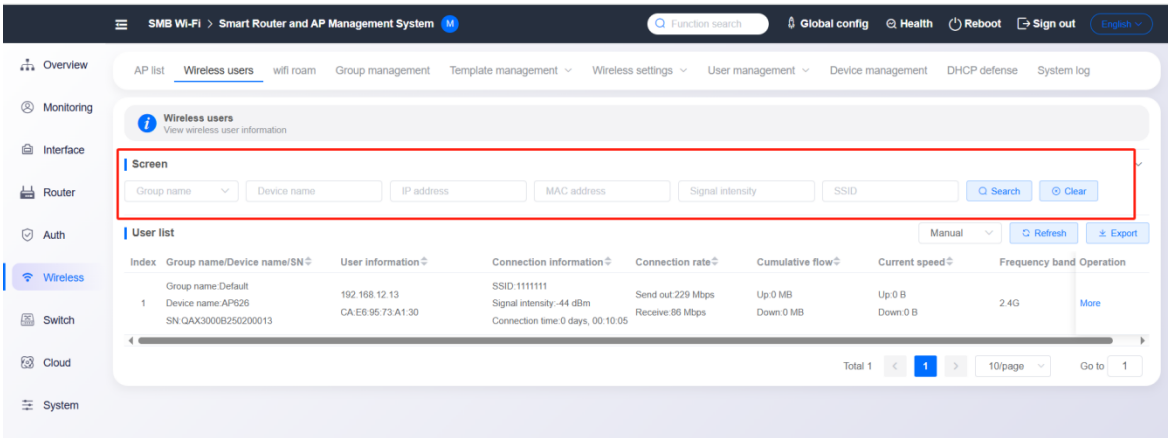
6.2 Wireless Users

When a wireless user is connected to the wireless AP, can view the user's connection status in this menu. Screen and locate users according to conditions. If the conditions are entered incorrectly, click the "Clear" button. In addition, the user list also supports blacklisting of a host and exporting of the user list.



Screen

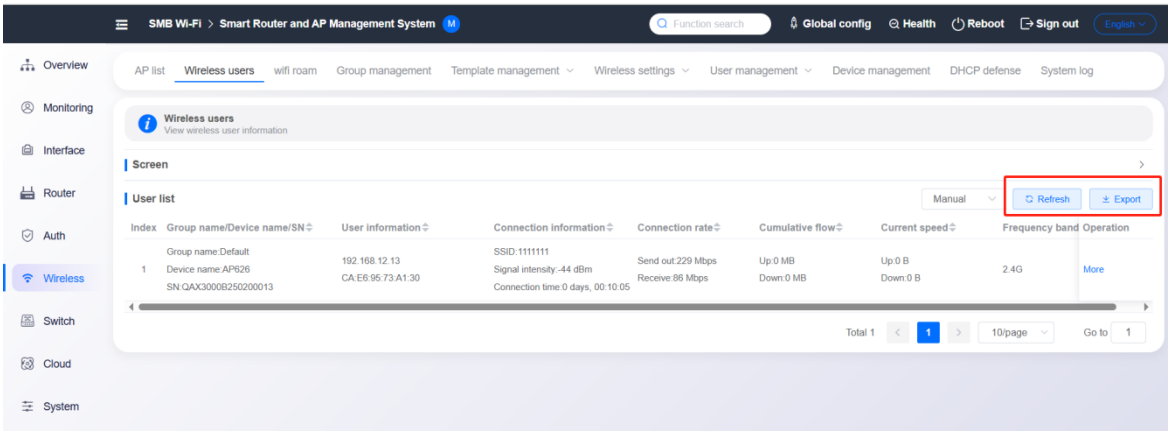
When there are multiple AP devices connected to the router, can filter users by currently supported conditions to accurately find the user information that needs to be viewed for the current AP.



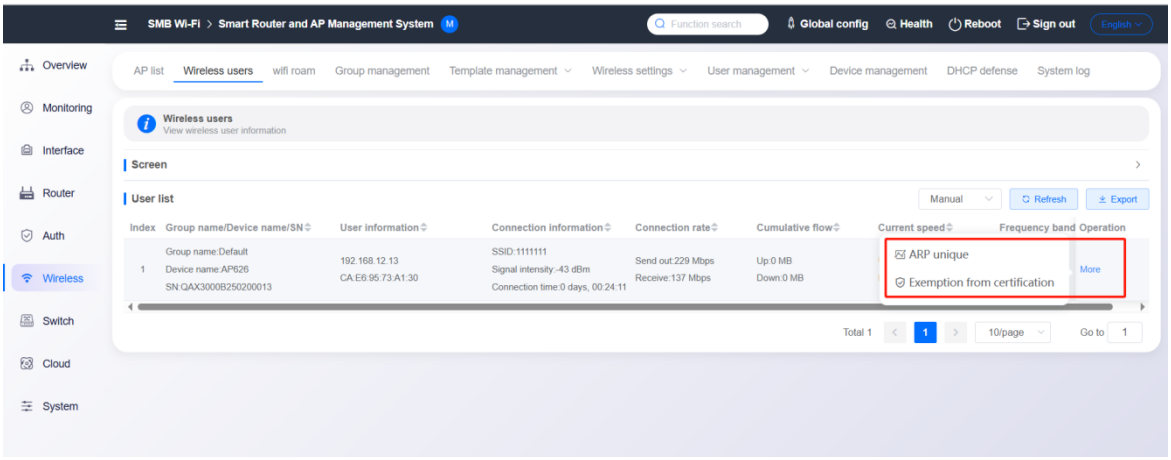
User List

Export: Export all currently connected wireless user tables;

Refresh: supports manual refresh and automatic refresh at fixed intervals;



More: Support operations on a single wireless user;

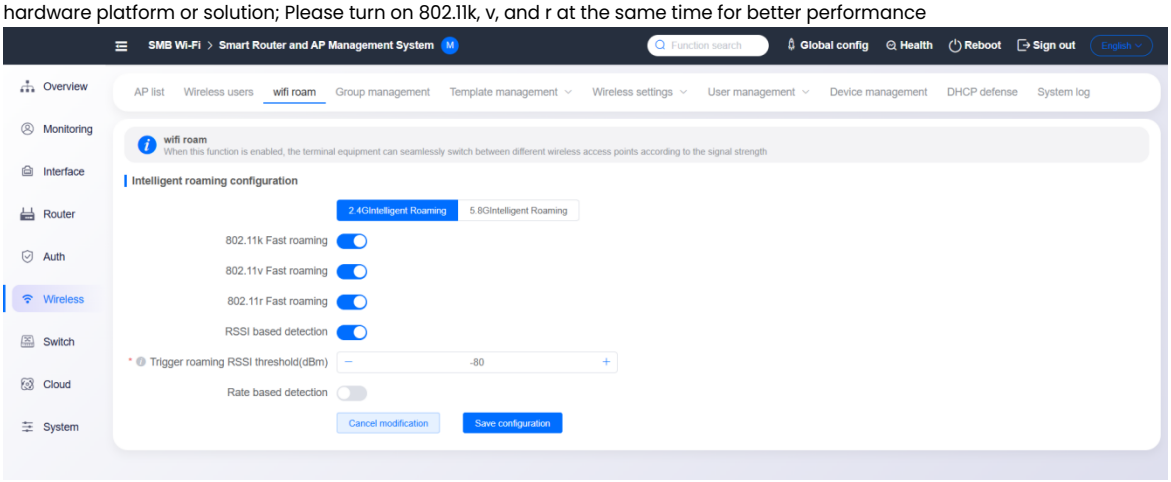


ARP unique: Set the current mobile phone IP and MAC address as ARP unique binding. The binding result can be viewed in "Router" - "Security" - " ARP List";

No authentication required: When the main device has enabled the authentication function, if want to set a wireless user as no authentication required (whitelist), click this button to add it to the no authentication required list. The result can be viewed by going to "Auth" - "Authentication settings" - "Auth Free" - "Based on MAC ".

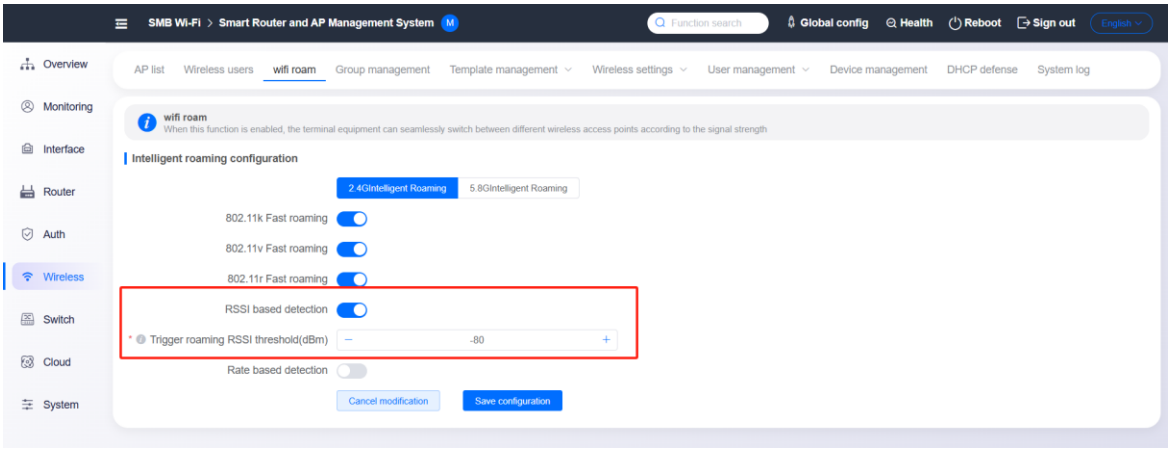
6.3 WiFi Roaming

When this function is enabled, the terminal device can seamlessly switch between different wireless access points according to the signal strength. To improve the roaming effect, please try to use the seamless roaming function in wireless APs with the same hardware platform or solution; Please turn on 802.11k, v, and r at the same time for better performance

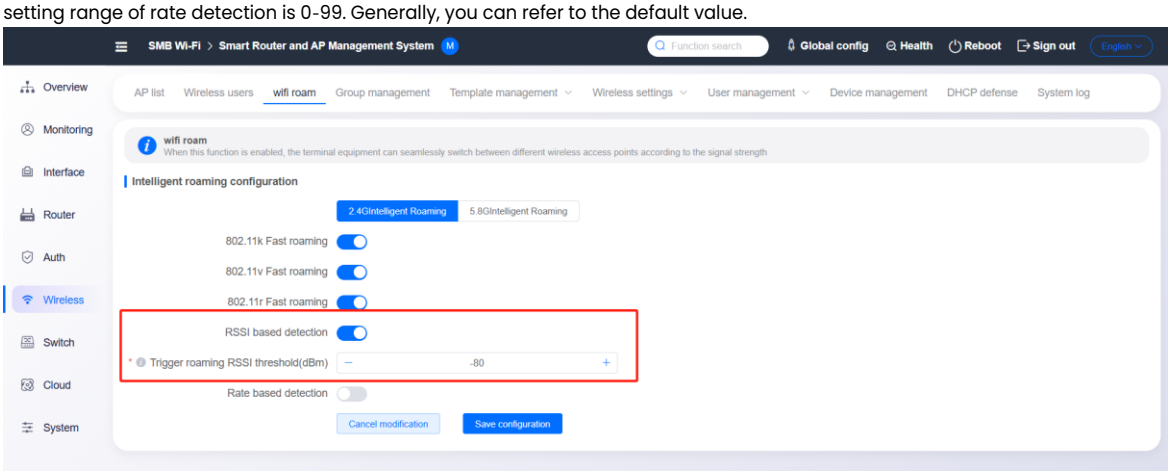


Intelligent roaming configuration

Trigger roaming RSSI threshold: Switch the wireless roaming based on the signal strength of the wireless terminal. If the trigger roaming RSSI threshold is set to -70 and the terminal signal strength is -80, the system will automatically disconnect the wireless network and switch the terminal wireless network to a wireless network with better signal strength. The signal strength range is -95 to -50, and a value of 0 means that signal strength detection switching is not enabled;



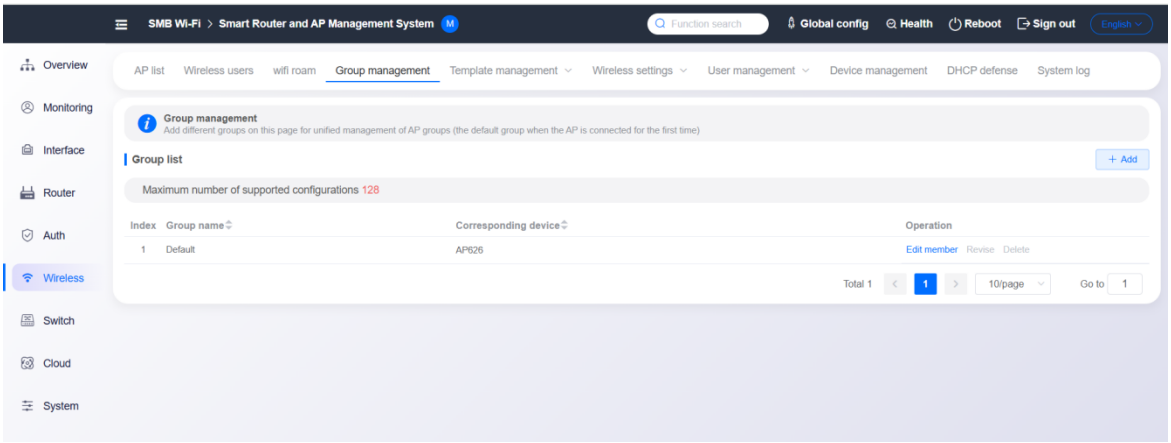
Based on rate detection: The principle is the same as RSSI threshold signal strength detection, but the standard is different. The setting range of rate detection is 0-99. Generally, you can refer to the default value.



5.8G also supports the same configuration. Generally, it is not recommended to set up detection for 5.8G smart roaming.

6.4 Group Management

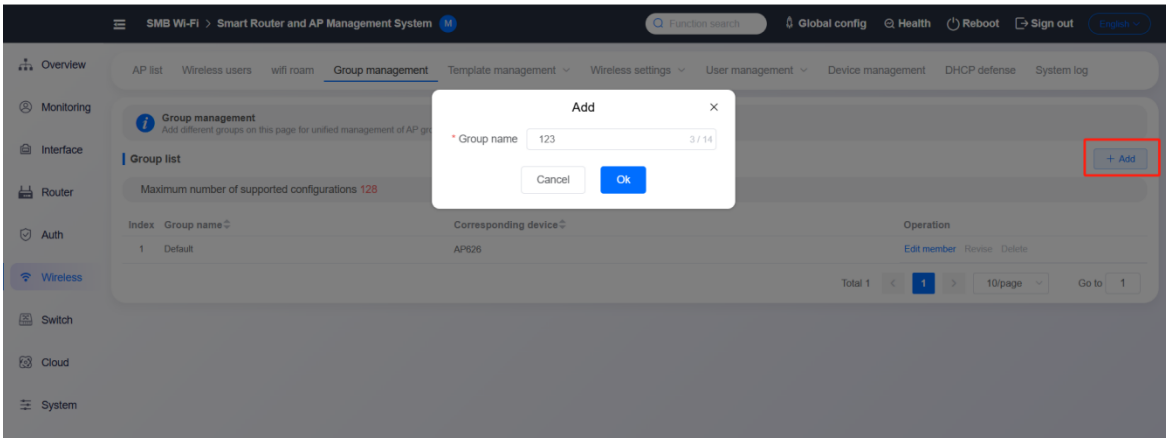
Add an AP group. After adding the group, can choose to group the devices on the AP management page for easier management. By default, there is only one "default group" and all connected APs belong to this group.



Group List

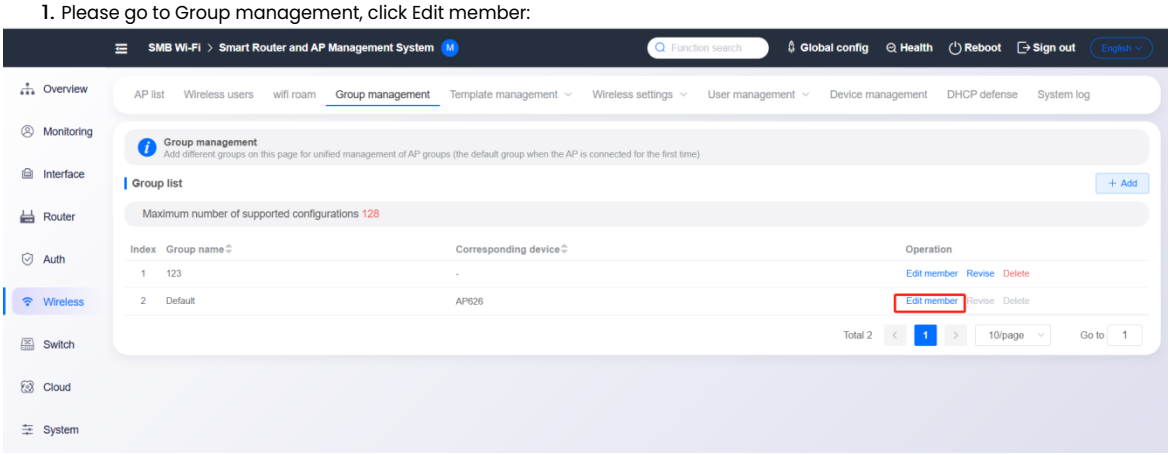
Add different groups on this page to manage APs in groups (the default group is used when the AP is connected for the first time)

Add: Create a new group.

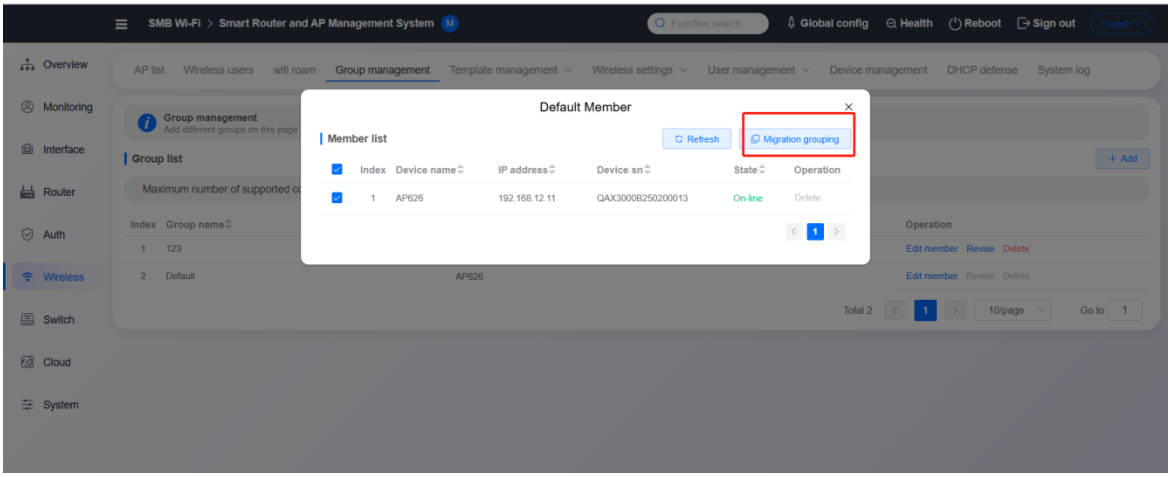


Group Migration Demo

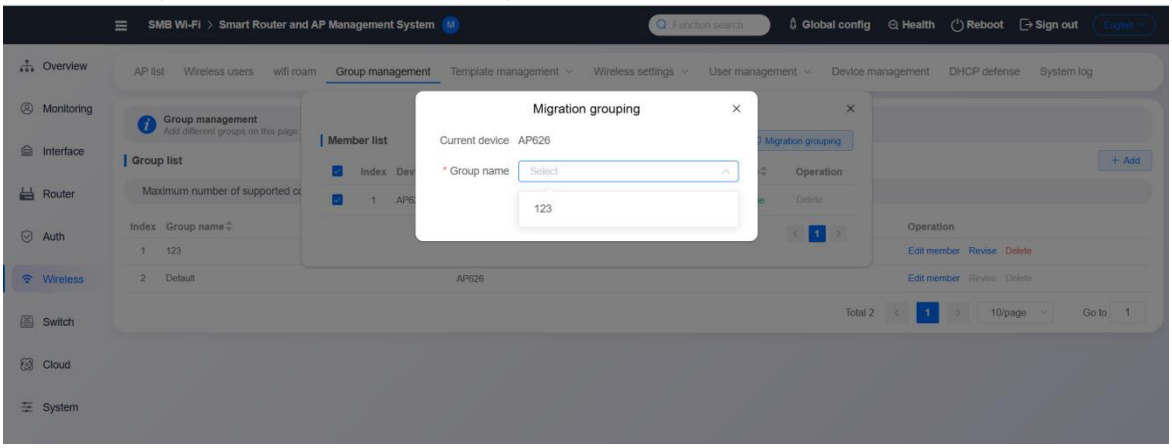
1. Please go to Group management, click Edit member:



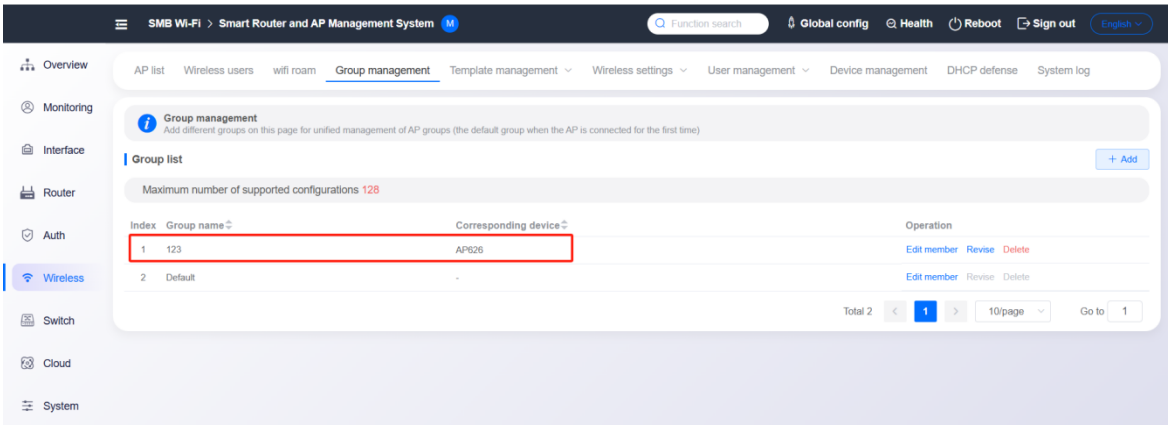
2. Select the device to be operated and click Migration Grouping:



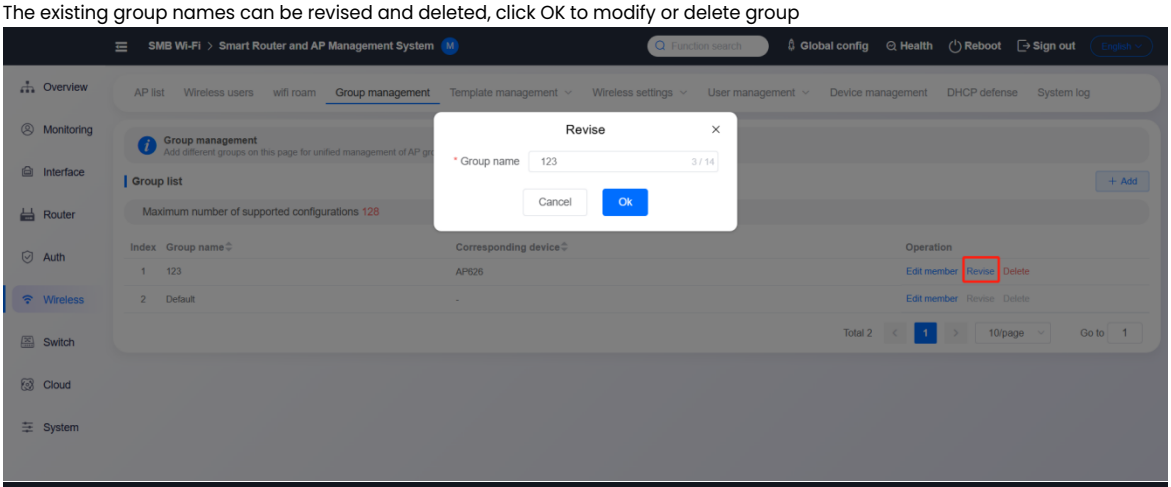
3. Select the group name this wireless AP will be migrated, click OK to finish it.

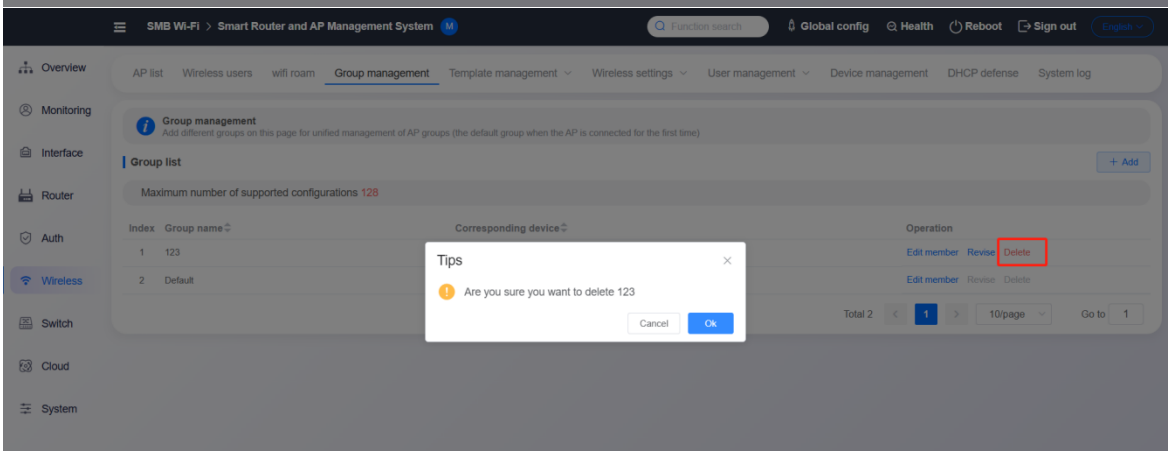


4. Finally go to the group list to view the group name of this AP



The existing group names can be revised and deleted, click OK to modify or delete group

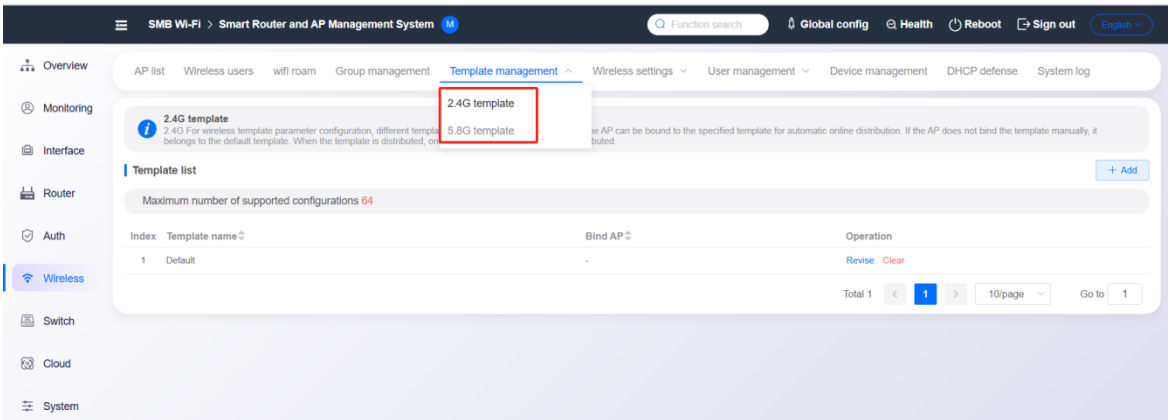




6.5 Template Management

Template refers to the template formed by configuring preset parameters for wireless AP. The parameters will be sent to the AP devices are connected. There are 2.4G templates and 5.8G templates:

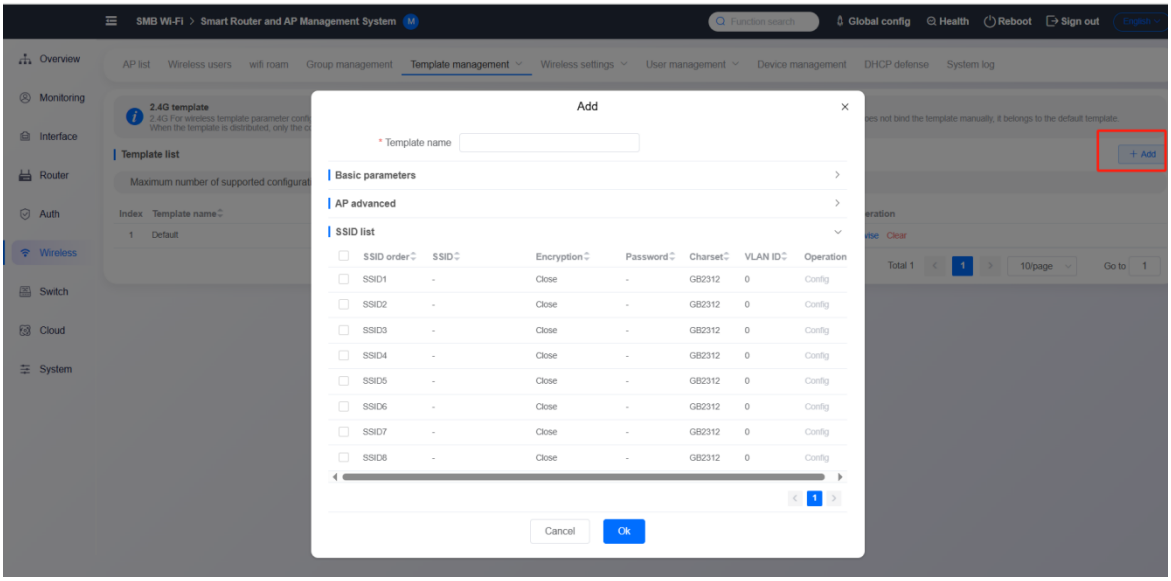
6.5.1 2.4G Template



Template List

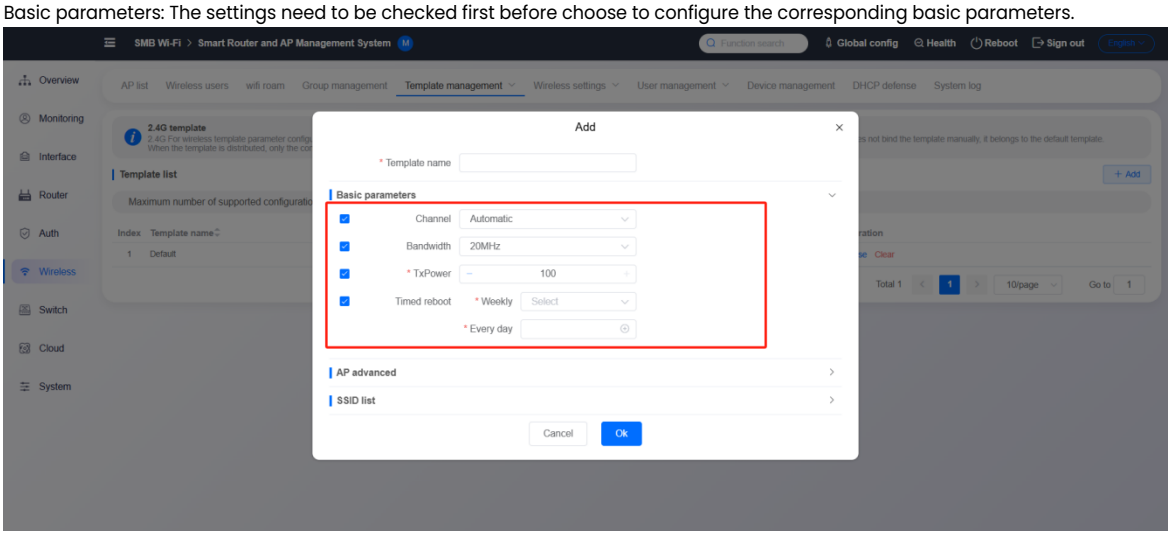
The maximum number of supported configurations varies depending on the model and is displayed with restrictions.

Add template



Template name: name the template to facilitate differentiation among many templates;

Basic parameters: The settings need to be checked first before choose to configure the corresponding basic parameters.



Channel: Select the default wireless channel for this template. The template channels for 2.4G and 5.8G are inconsistent;

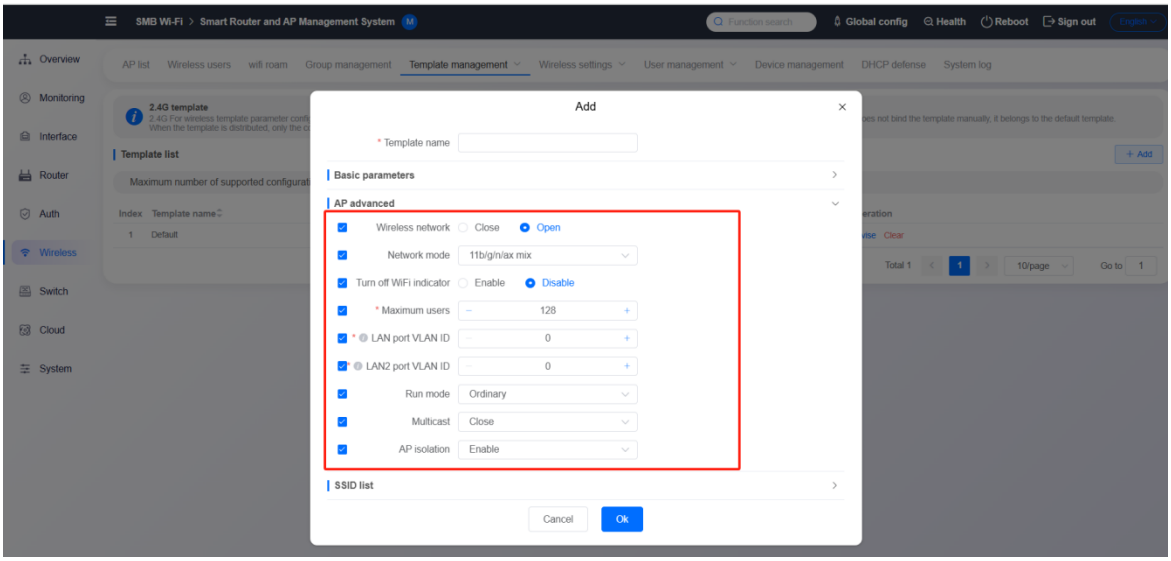
Bandwidth: Select the bandwidth for this template, 20MHz or 20/40MHz;

VHT BandWidth: The high throughput bandwidth for 5.8G;

TxPower: the wireless transmit power setting of the wireless AP, with an upper limit of 100. When setting this value, please consider the installation distance and gap between APs. If the distance between adjacent APs is close and the transmit power values are high, it is easy to cause poor wireless effect as Wi-Fi interface.

Timed reboot: The AP that receives this template will automatically restart according to the set time. Please fill in the time after checking this option. Please uncheck it If do not want to set this option;

AP Advanced: Advanced wireless parameter settings.



Wireless network: Can close or open the wireless function. Generally, the AP wireless function is opening by default. If the template is closed, the AP' s wireless function will turn off after successfully receiving parameters from the template. The performance is: When the wireless AP automatically restarts; the users cannot search for the wireless name of the AP. Similarly, after the wireless state is changed from close to open, the AP' s wireless function will be enabled and the user can search for the wireless name and can connect normally;

Network mode: refers to the highest supported bandwidth. Generally, please use the default 11b/g/n/ax mixed;

Turn off WiFi indicator light: Can set the wireless indicator light on the AP hardware. If enabled, the AP wireless light will be on normally; if disabled, the AP wireless light will be off.

Maximum users: refers to the maximum number of terminal users that can be accessed by the AP's 2.4G (or 5.8G)

LAN port VLAN ID: If the upper-level device has set a VLAN ID, please fill in the corresponding VLAN ID here;

LAN2 port VLAN ID: If the upper-level device has set a VLAN ID, please fill in the corresponding VLAN ID here. The ID here cannot conflict with the VLAN ID above. If the AP hardware has a LAN2 port, configuring the LAN2 port VLAN ID will be effective.

Run mode: wireless performance mode selection, ordinary or enhance, ordinary in default.

Multicast: Enable or close multicast;

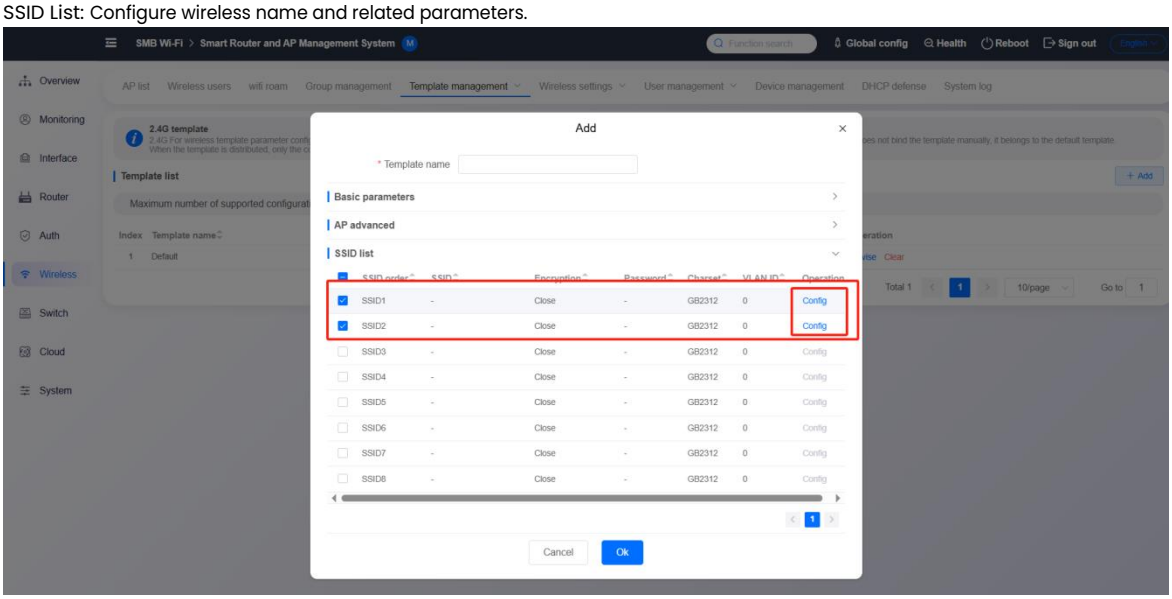
Close, the multicast function is closed and does not take effect;

Multicast-to-multicast can achieve the purpose of transmitting data to all target nodes at once or only transmitting data to specific objects;

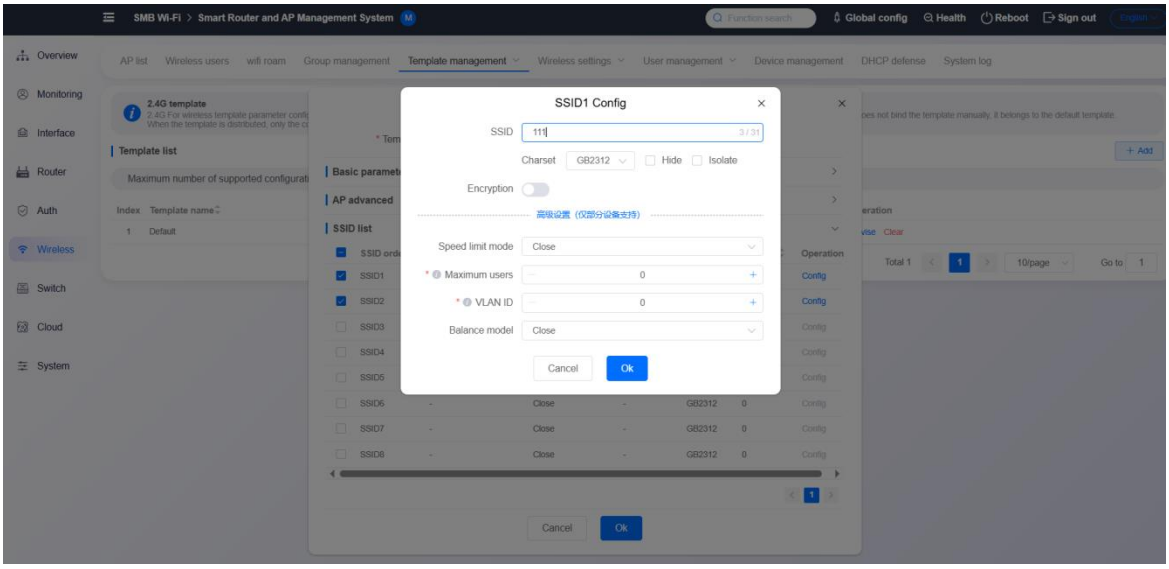
Multicast to unicast is generally used in multicast videos to make the video smoother;

AP Isolation: Enable or disable AP isolation;

SSID List: Configure wireless name and related parameters.



If SSID will be modified, please check the SSID and click "Config" to set the corresponding parameters:



SSID: Set SSID (wireless name). Wireless terminal users can use this name to find the wireless network and connect to it. The naming rule is 1-31 characters, letters, numbers and _-!@#$%^&*().;

Charset: Generally, the default is GB2312. If the SSID contains Chinese characters, please select UTF-8 charset if mobile phone or tablet terminals will be accessed. If the SSID does not contain Chinese characters, can directly select GB2312 encoding.

Hide: The wireless network is hidden, and the terminal will not be able to search for the wireless name;

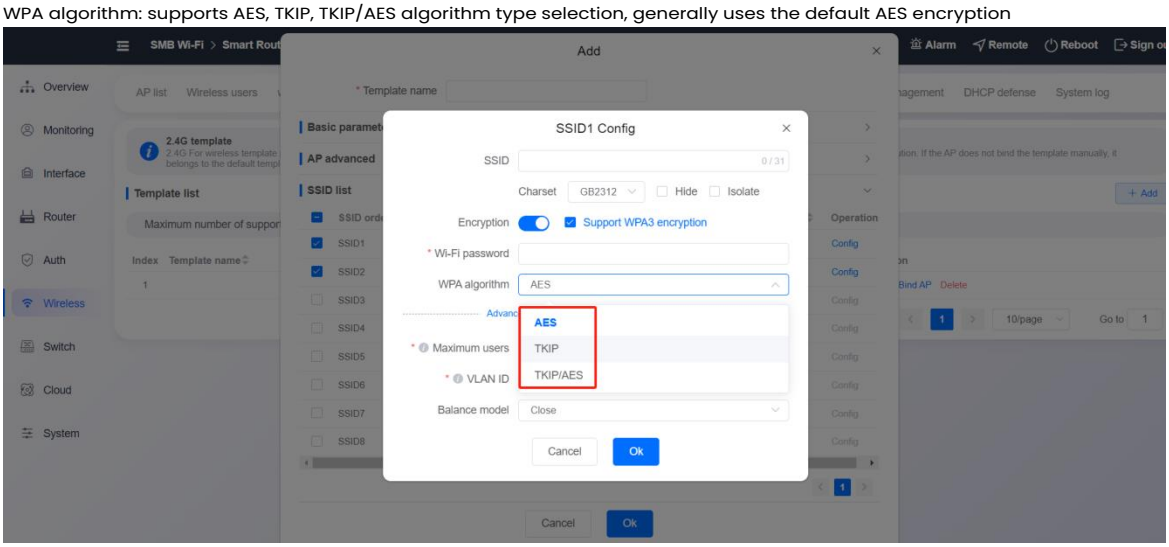
Isolate: After submitting, terminal users of APs in the same network segment cannot access each other;

Encryption: whether to enable wireless encryption mode;

Disable: The terminal user can connect to the wireless network without Wi-Fi password.

Enable: The users should enter the corresponding Wi-Fi password before connecting to the wireless network

WPA algorithm: supports AES, TKIP, TKIP/AES algorithm type selection, generally uses the default AES encryption



Maximum users: The maximum number of users that the AP device can support to connect. 0 means no limit.

VLAN ID: The range is 0-4080;

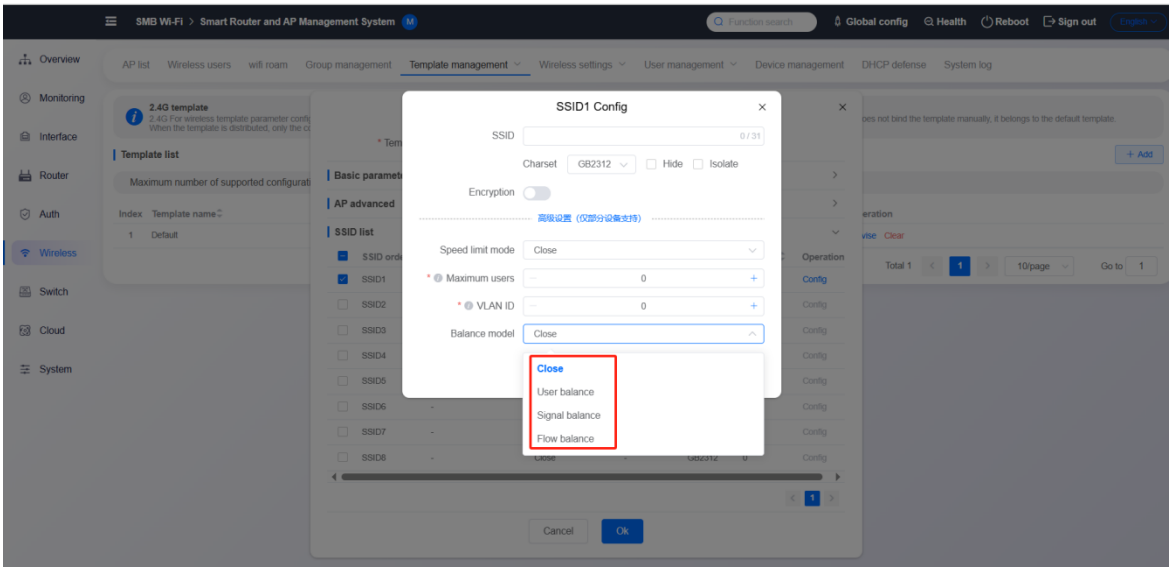
Balanced mode:

Close: No balancing mode is used between APs;

User Balanced: APs are evenly allocated according to the number of users;

Signal balance: APs are evenly distributed according to the terminal signal strength;

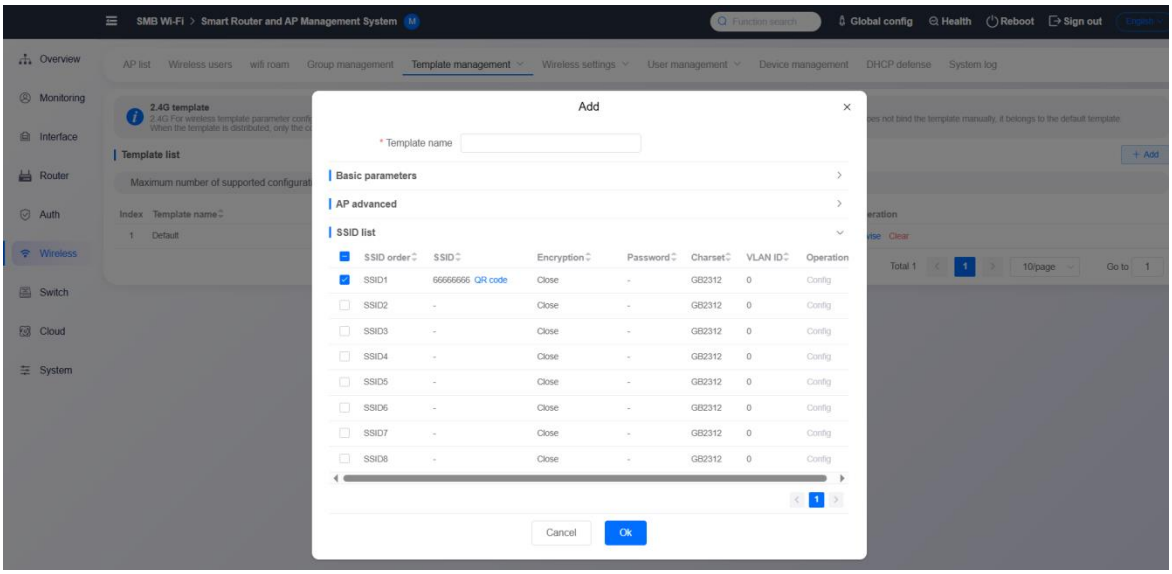
Flow balance: APs are evenly distributed based on traffic usage.



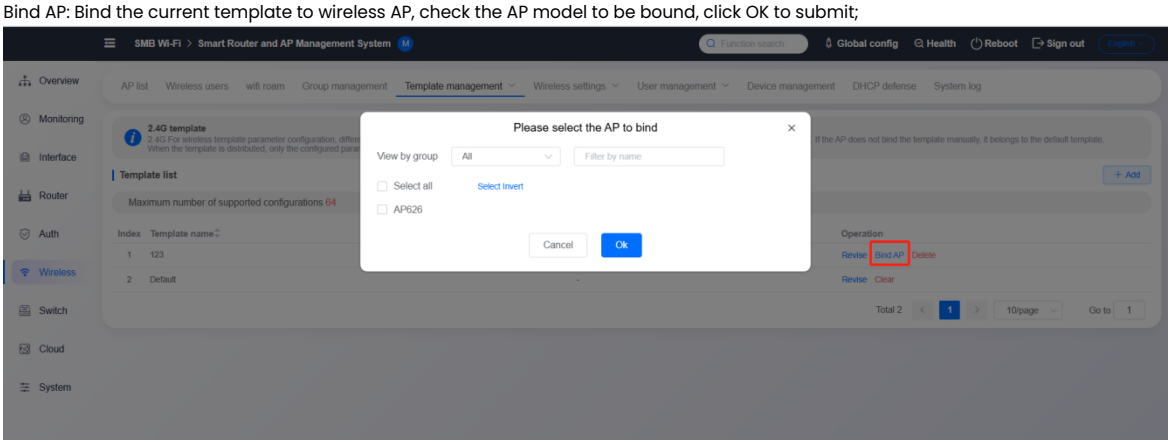
Template List Operation

Supports template operations, including Revise, Bind AP, Delete

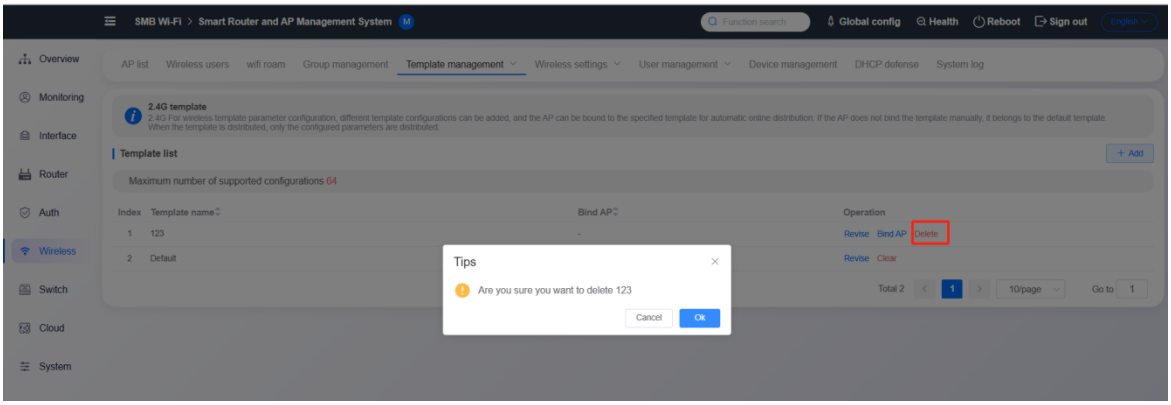
Revise: refers to modifying template parameters. Including template name, basic parameters, AP advanced parameters and SSID. After modification, click OK save. The modified template will be automatically sent to the bound AP device. Generally, the AP will automatically restart.



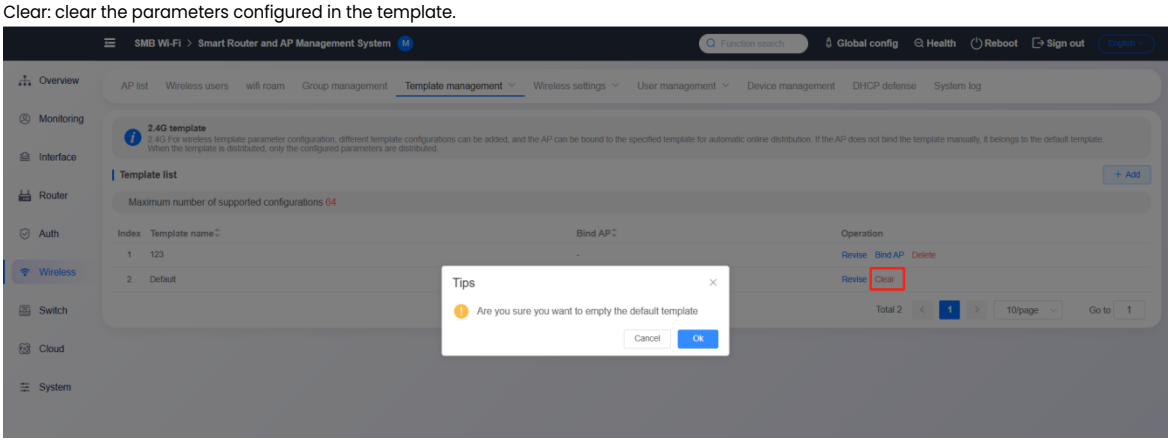
Bind AP: Bind the current template to wireless AP, check the AP model to be bound, click OK to submit;



Delete: Delete the template. After deleting the template, the parameters that have been sent to the device will not be cleared. The APs that are connected later will NOT receive the parameters of the deleted template, and the deleted template cannot be restored.



Clear: clear the parameters configured in the template.



6.5.2 5.8G Template

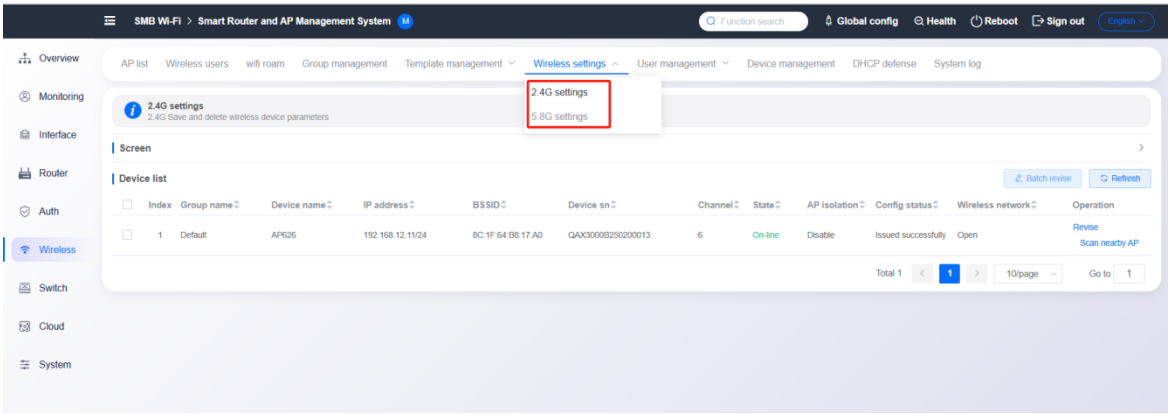
The 5.8G template setting process is the same as the 2.4G template setting process. Please refer to the 2.4G template configuration for 5.8G template settings. It should be noted that after the 2.4G template is created, it will not automatically synchronize parameters to the device. The device needs to be bound, and the 2.4G template only synchronizes 2.4G parameters to the device, and will not automatically synchronize 5.8G parameters.

6.6 Wireless Settings

Including 2.4G settings and 5.8G settings

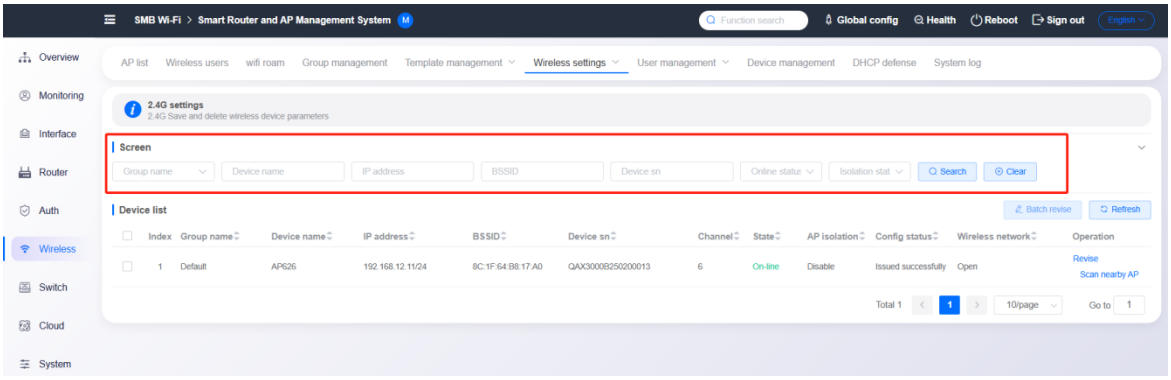
6.6.1 2.4G Wireless Settings

On this page, can modify the 2.4G wireless parameters of the online AP



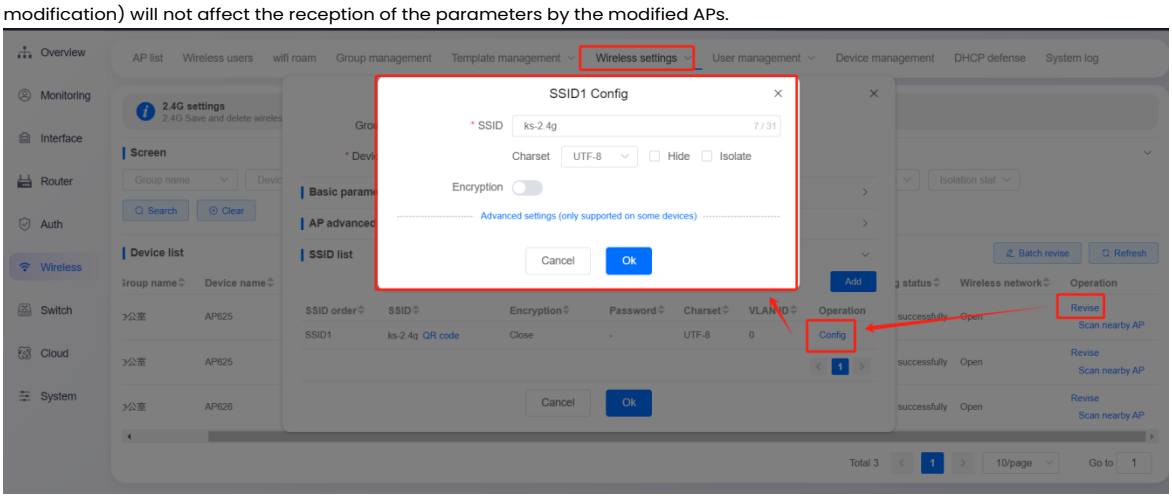
Screen

Filter out APs by specifying conditions. If the filtering conditions are incorrect or need to be modified, click the "Clear" button to clear the selected conditions;



Device List

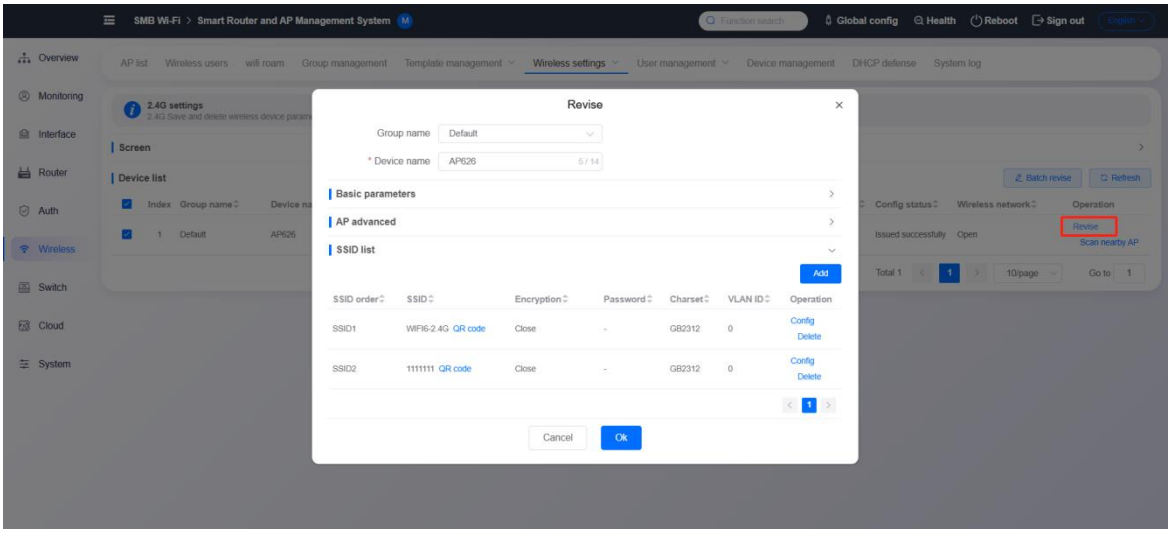
Batch modification: Check the APs in the list and click Batch Modify to modify the parameters of the selected APs in batches. If the device has received the parameters sent by the template, modifying the parameters (including batch modification or single modification) will not affect the reception of the parameters by the modified APs.



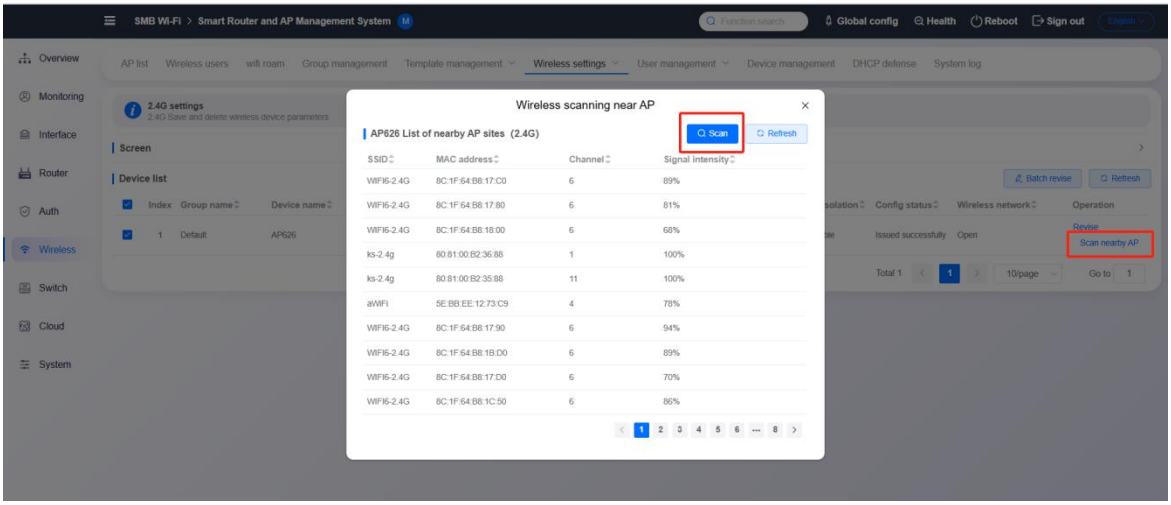
Config: To modify the wireless parameters of the online AP device, please select the parameter item will be modified, input the parameters based on request.

Refresh: Refresh the current AP list.

Revise: Modify the parameters of the selected AP separately.



Scan nearby AP: Scan the SSID, MAC addresses, channels and signal strength information of all nearby wireless signals;



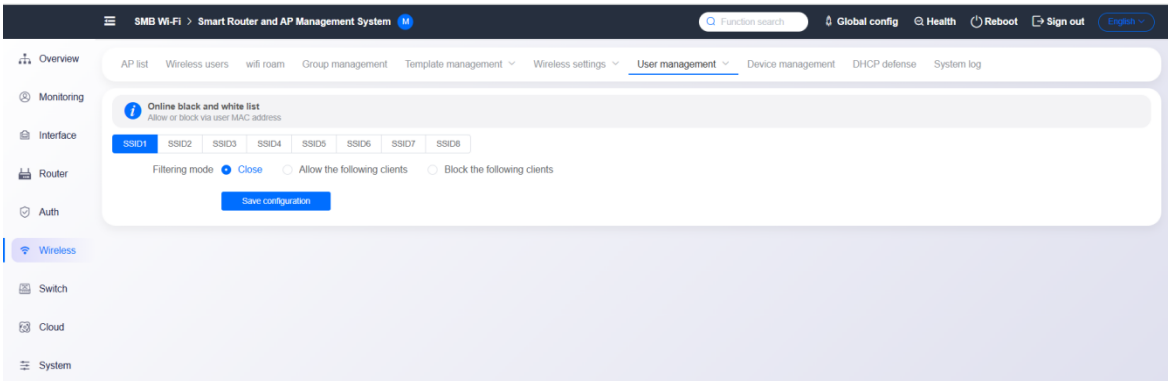
6.6.2 5.8G Wireless Settings

The wireless settings of 2.4G and 5.8G are basically the same, please refer to 2.4G wireless settings to set the 5.8G wireless. Before configuration, please confirm which wireless(2.4G/5.8G) is set.

6.7 User Management

6.7.1 Online black and white list

Allow or block wireless users by MAC address.



Online black and white list

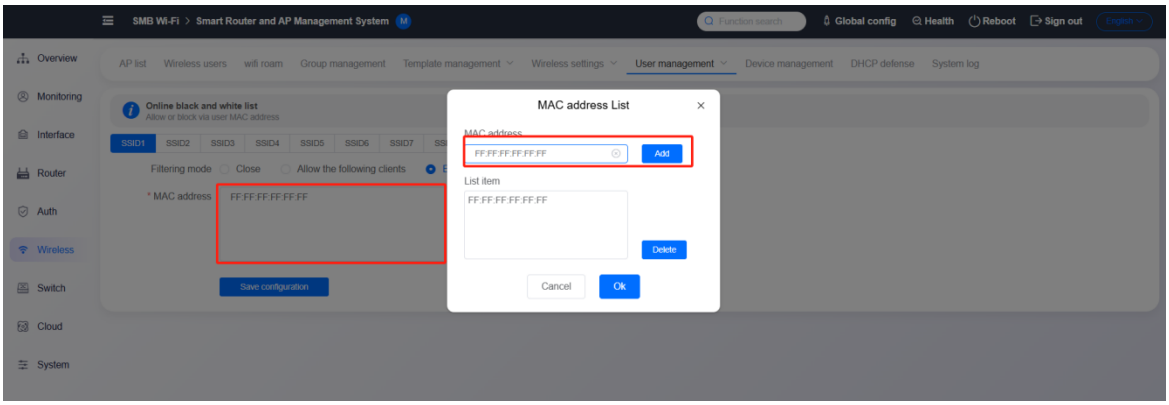
Filtering method: Setting the filtering method for wireless user MAC;

Close: Close the filtering function, and all the users are connected to this router can be used;

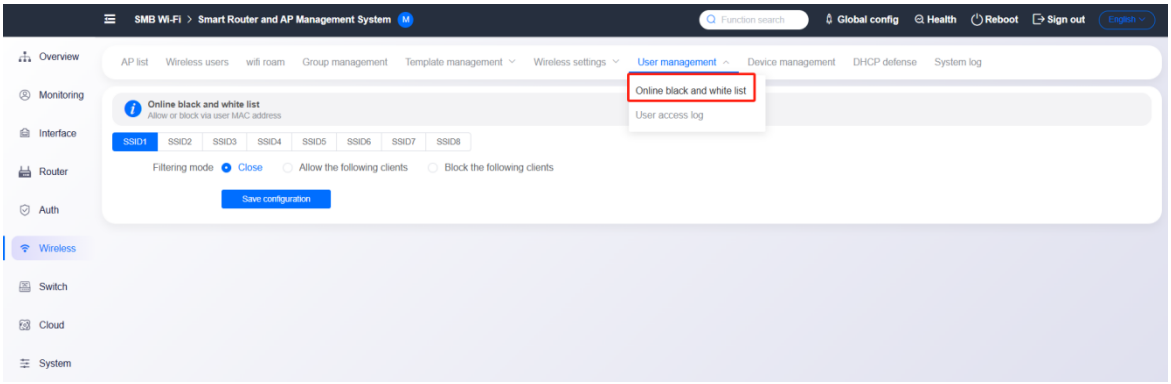
Allow the following clients: Enter the corresponding client MAC address. After the Allow the following client filtering mode is turned on, the filled MAC can connect normally, and the unfilled MAC address can not allowed to access;

Block the following clients: Enter the corresponding client’ s MAC address. After the blocking the following client filtering mode is turned on, the filled MAC will not be able to connect to the wireless network, and the unfilled MAC address can pass.

When the mobile phone uses multiple virtual MAC addresses, if MAC1 used by the mobile phone to connect to SSID1 is listed as a blocked client here, the wireless connection cannot be successful; if the mobile phone is connected to SSID2, the mobile phone may use MAC2 address to access the network. At this time, MAC2 is not blocked, and the terminal can connect to the network normally.



Please note that the filtering method is configured for each SSID individually, and the default for an unconfigured SSID is that no blacklist or whitelist exists.

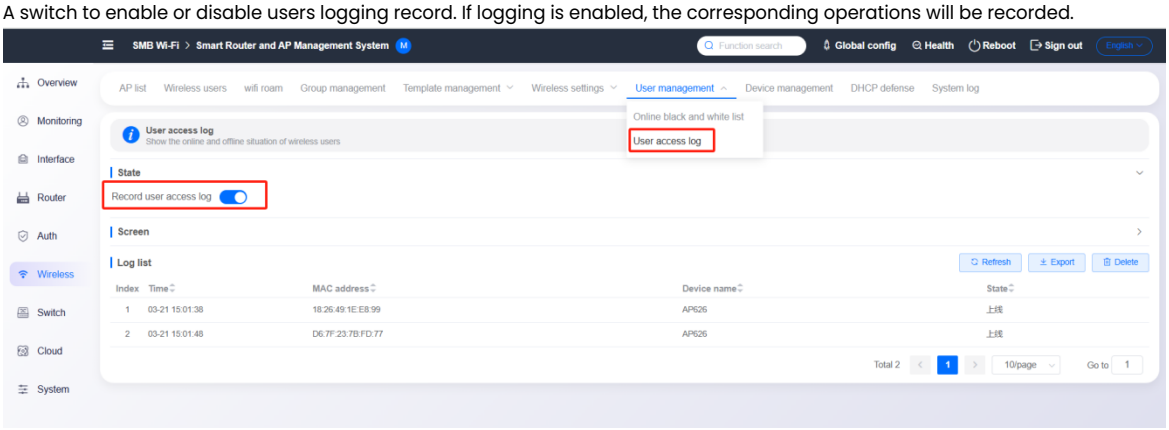


6.7.2 User access log

When wireless users online or offline, the user access log records are displayed.

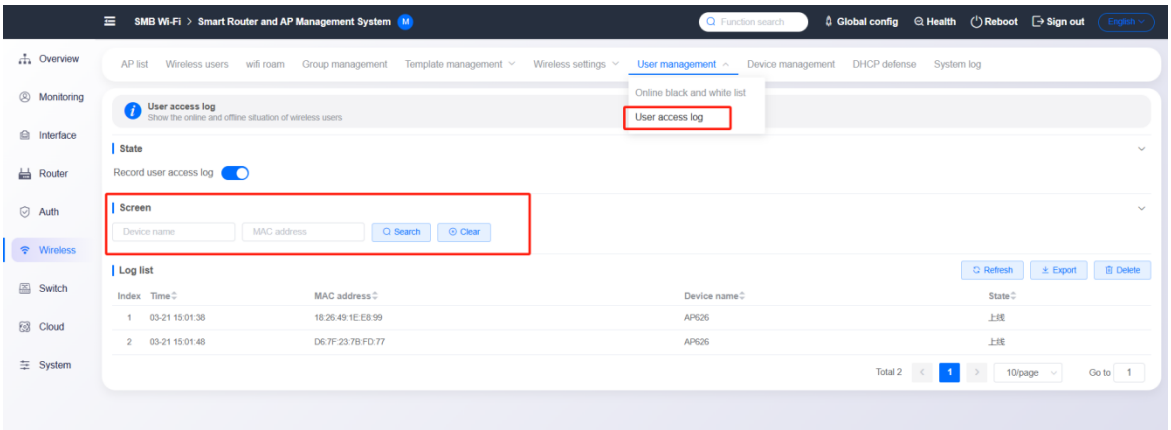
State

A switch to enable or disable users logging record. If logging is enabled, the corresponding operations will be recorded.



Screen

Filter device name and MAC address by specifying conditions. If the filtering conditions are incorrect or need to be modified, click the "Clear" button to clear the selected conditions.



Log List

Displays the online and offline log records of all wireless users

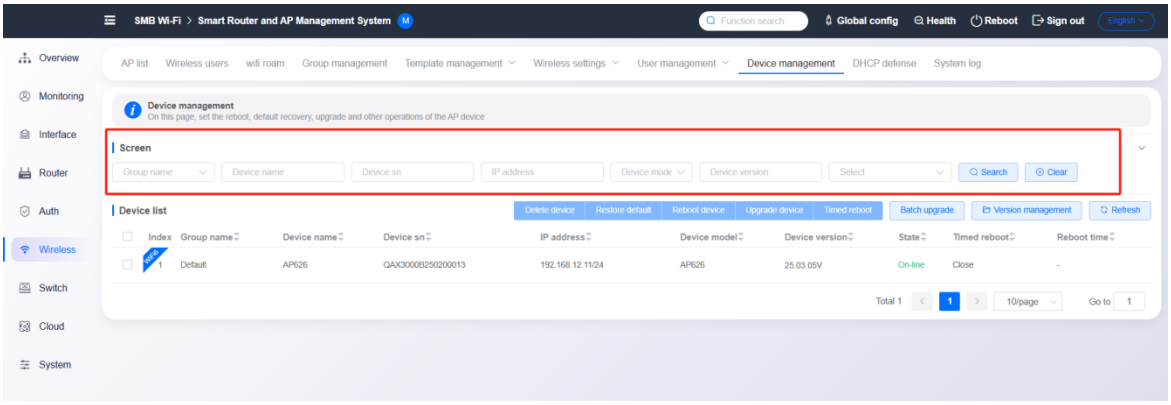
6.8 Device Management

On this page, set the reboot, default recovery, upgrade and other operations of the AP device

6.8.1 Device Management

Screen

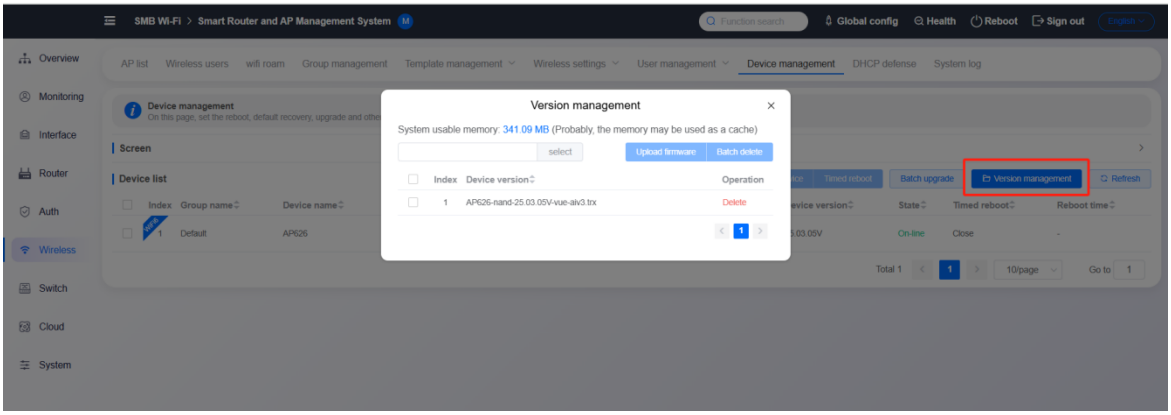
Filter out AP devices by specifying conditions. If the filtering conditions are incorrect or need to be modified, click the "Clear" button to clear the selected conditions.



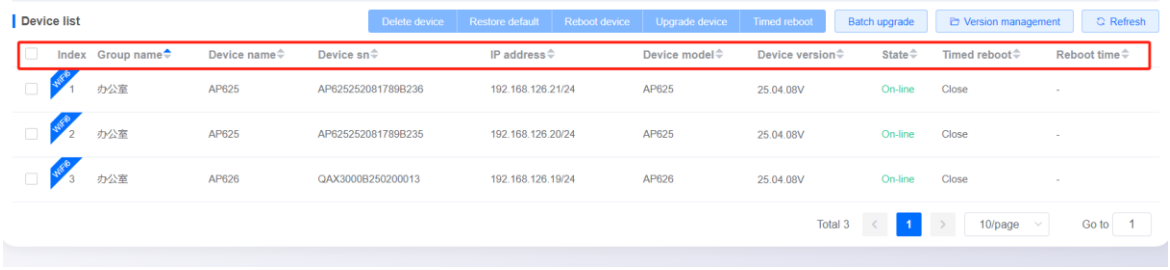
Device List

Displays all AP corresponding information.

Check the corresponding device in device list, can delete, restore to default, reboot, upgrade firmware, timed reboot operations for the device. To upgrade the device version through this page, pls upload the firmware of the AP through the version management button first.

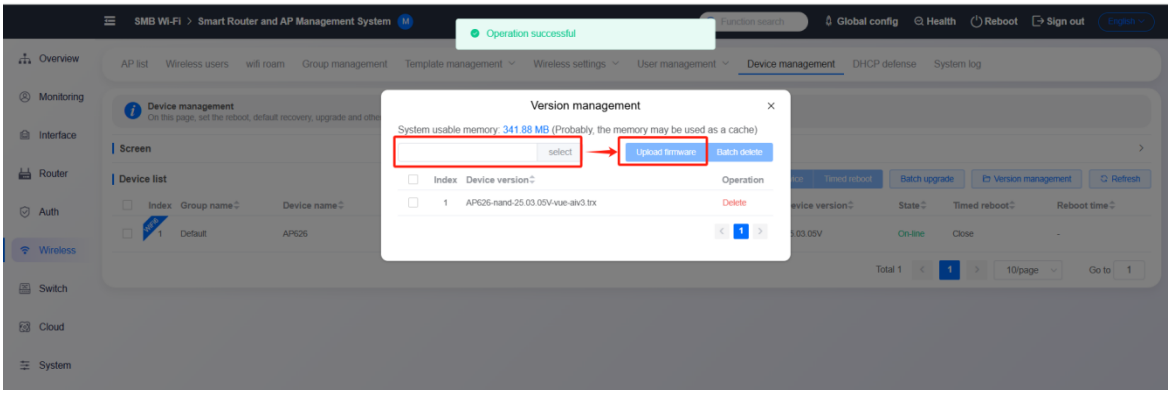


If there are many APs in the device list, can also use the up and down buttons in the following figure to filter APs and select multiple APs at once for operation

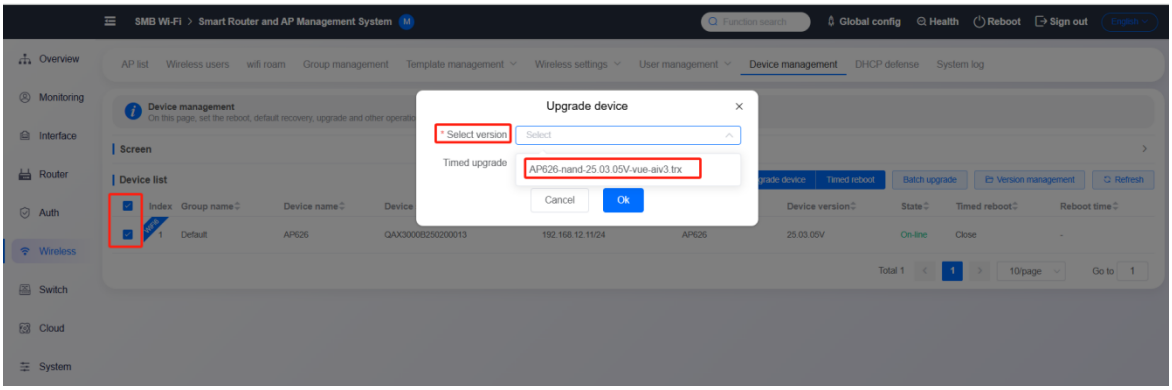


6.8.2 Demonstration: AP upgrade process

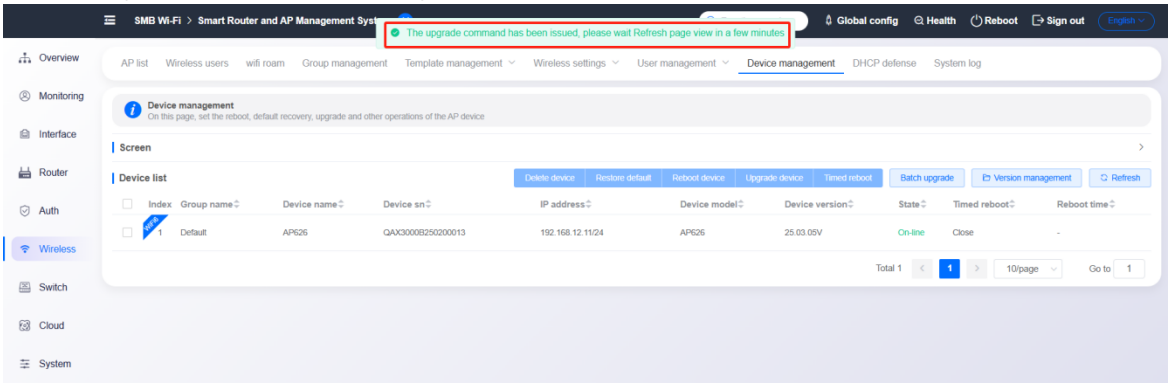
1. Upload firmware:



2. Select the firmware version will be uploaded:

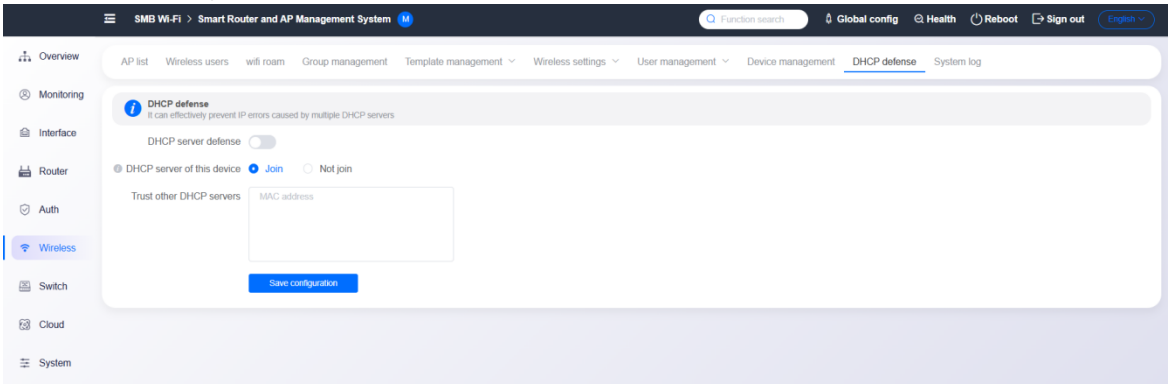


3. The upgrade is successful, please waiting for the automatic restart:



6.9 DHCP Defense

This function can effectively prevent the wrong IP caused by multiple DHCP servers. If there are other DHCP servers in the LAN, the terminal user may get an incorrect IP address. Please enable this function and set the device to join the DHCP server.



DHCP Defense

DHCP server defense: Enable or disable, generally disabled by default;

DHCP server of this device: join or not join;

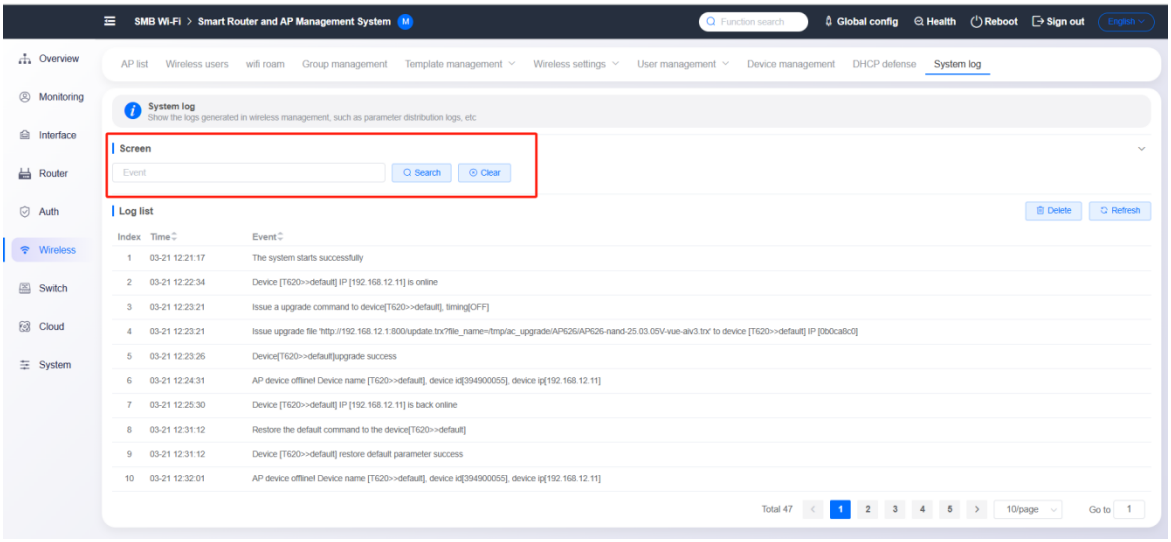
Add: This device will provide DHCP service to the terminal device;

Not join: This device will not provide DHCP service to terminal devices.

Trust Other DHCP servers: Can add other trusted DHCP servers, which can also be used normally when the defense function is enabled.

6.10 System Log

Displays logs generated in wireless management, such as parameter delivery logs.



Screen

Search: Start filtering to list display;

Clear: Clear the previous filter conditions.

Log List

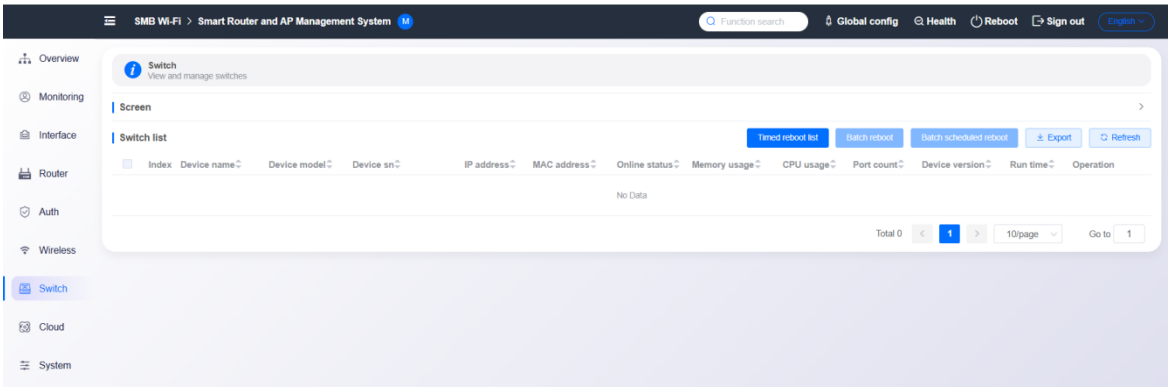
Refresh: refresh the log display information;

Delete: Delete all log information.

七、 Switch Management

This is functions to manage the L2/L3 managed switch, in improving.

Will update it when functions are finished.

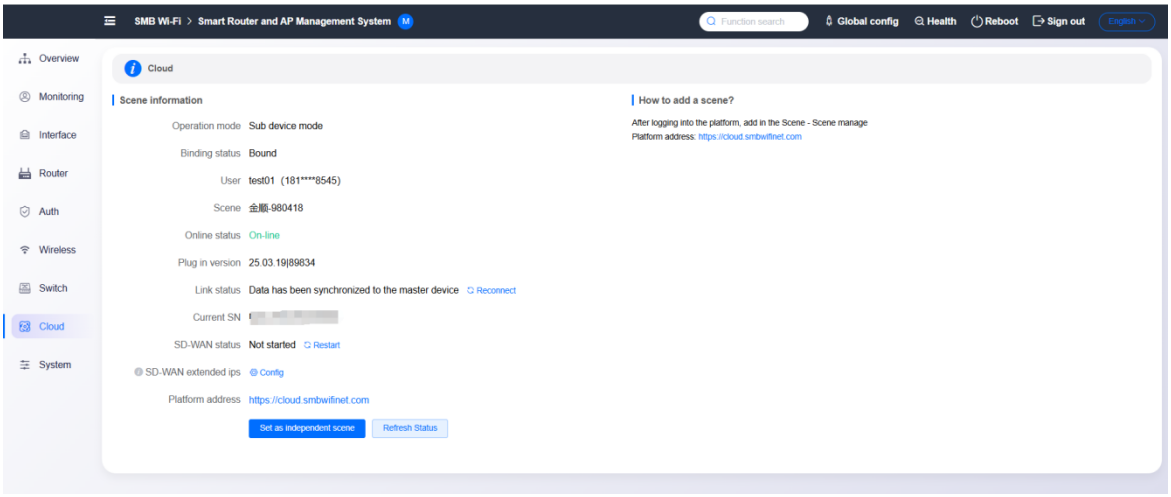


八、 Cloud

The SMB Wi-Fi cloud manage platform is a scenario-based centralized cloud management of devices. Support central and remote management of routers, wireless APs at this period, It support special features such as network topology, SD-WAN, and scenario reports. User analysis and alert.

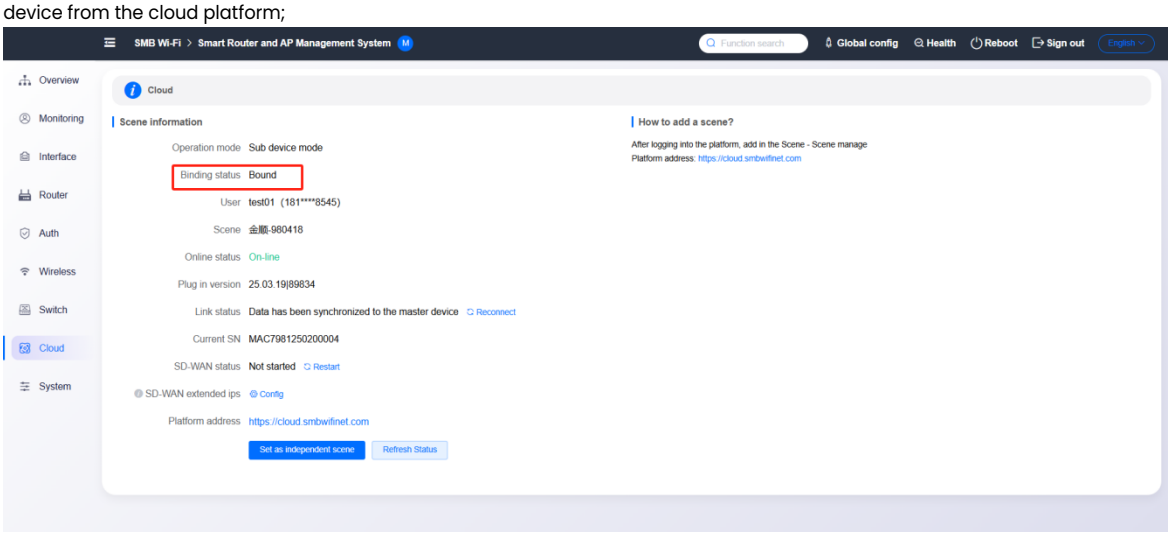
8.1 Cloud Platform

Scene Information



Operation mode: Master device mode and slave device mode. When a device is bound to the cloud as a upper-level device, the master mode will be displayed in operation mode. If the sub-level device is also bound to the cloud, the slave mode will be displayed in operation mode.

Binding status: After the device banding to the cloud, it will show "Bound" status here. Can click Unbinding to unbind the device from the cloud platform;



After clicking Unbinding, the countdown will start. After the countdown ends, enter the device login password to successfully unbind this device from cloud.

User: The cloud login account that is used to band the device to cloud;

Scene: The name of the scene for this device created on the cloud platform;

Online status: The on-line and off-line information of the device is band to the cloud platform;

Plug in version: the firmware version information of the device which is band to the cloud platform;

Link status: whether the device is successfully connected to the cloud platform;

Current SN: the authorized serial number of the device;

SD-WAN status: the status if started SD-WAN function after the device is connected to cloud platform;

SD-WAN extended IPs: Can configure other local intranet segments that need to be accessed (such as the network segment assigned by the three-layer switch). After configuration, it will be automatically added to the SD-WAN routing table and synchronized to other nodes;

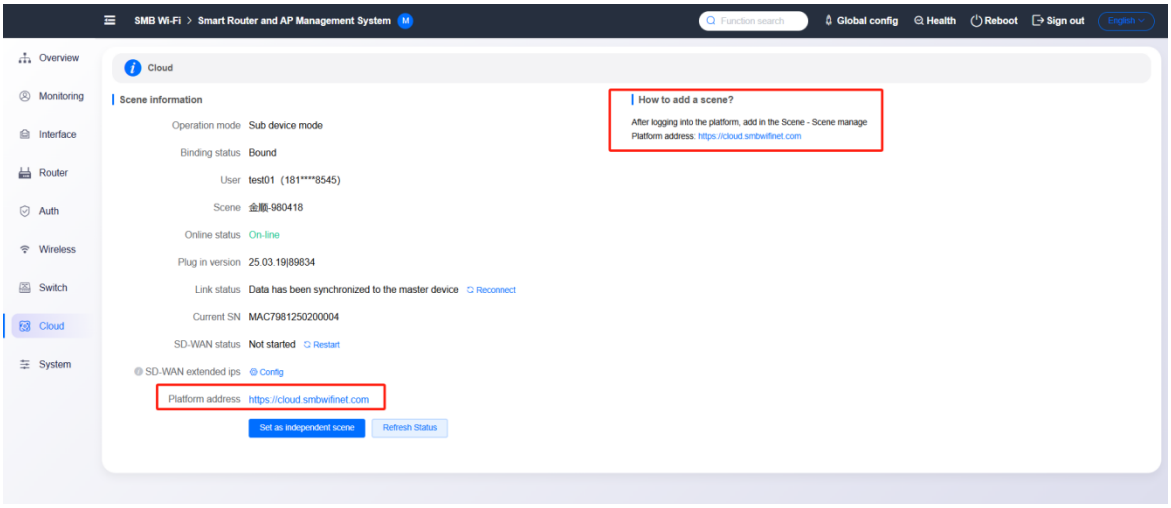
Platform address: the domain address of the cloud platform.

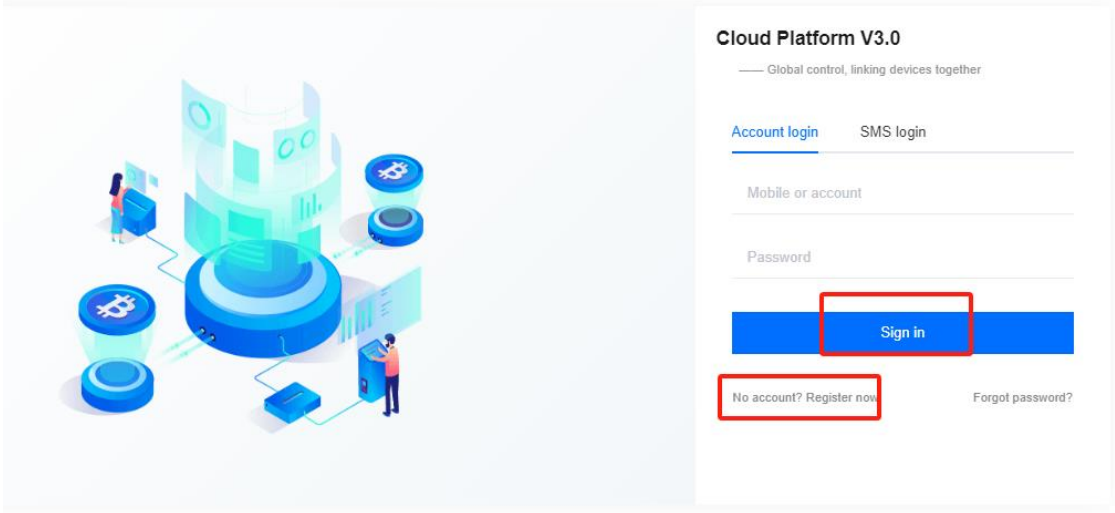
8.2 Adding devices to the cloud platform

There are two methods to add devices to platform modes:

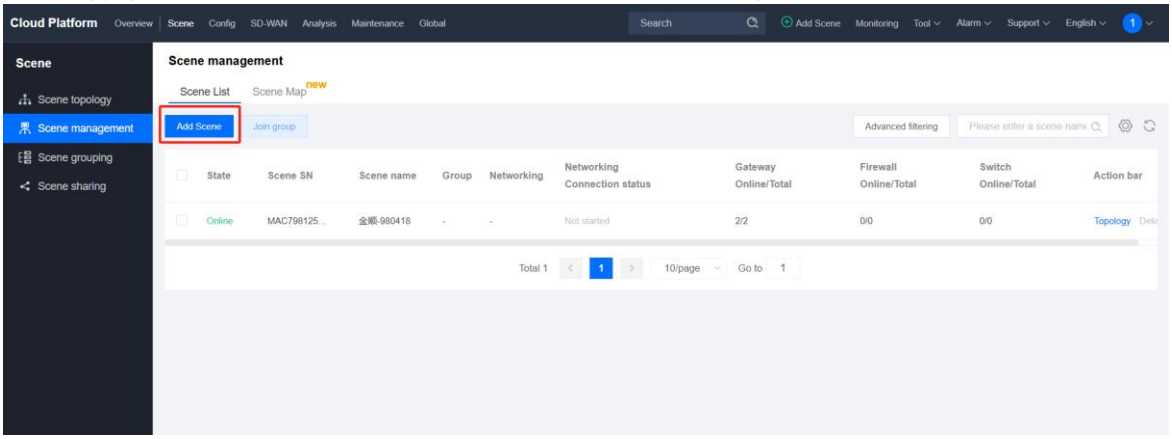
Method 1: Log in to the cloud platform and add devices

1. To access the cloud platform, please register a cloud platform account on the cloud login page:https://cloud.smbwifinet.com; If you already have one, log in the cloud platform;

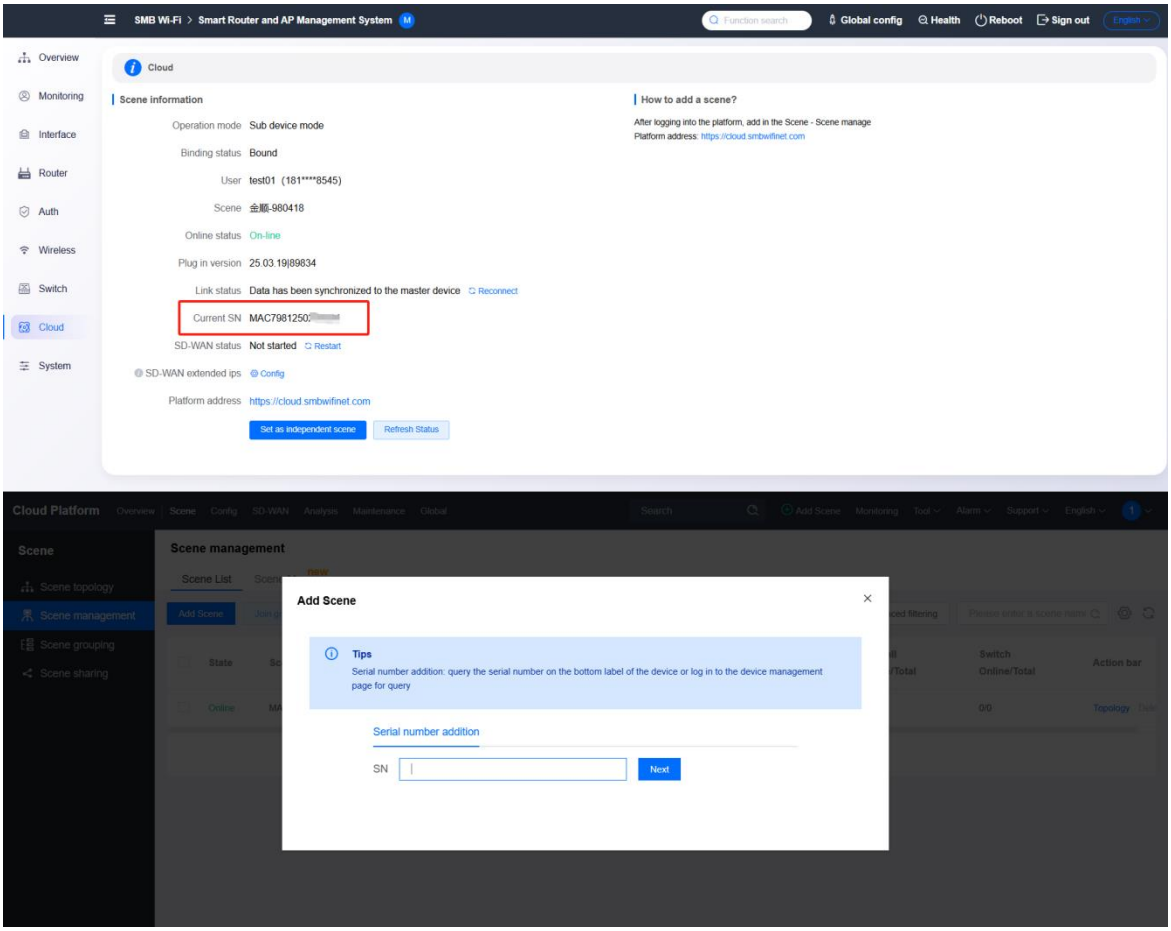




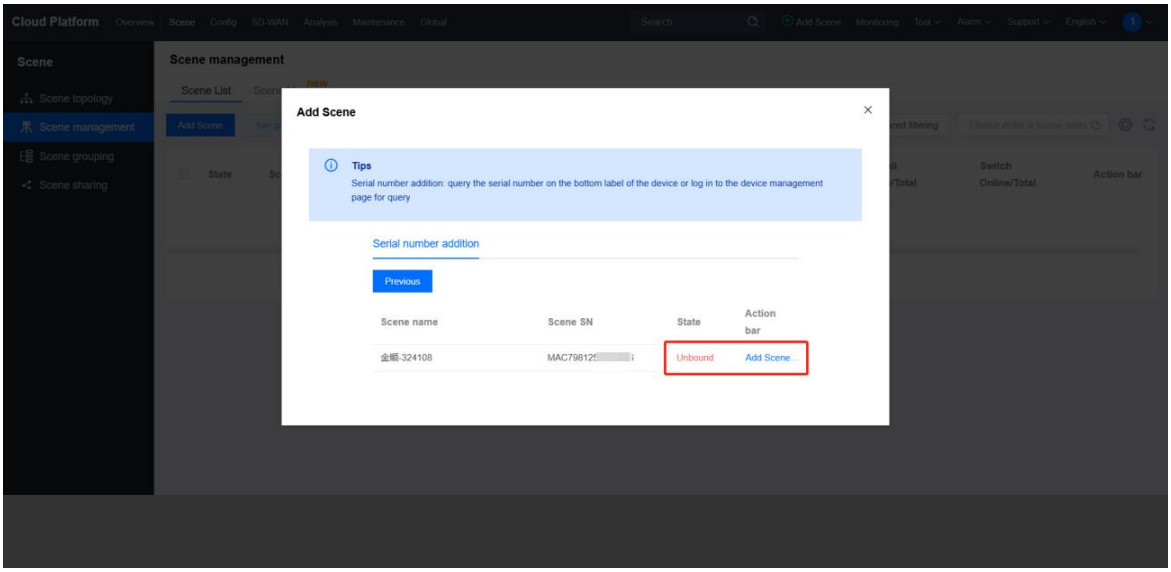
2. After logging in to the cloud platform, please add a network scene in Scene Management



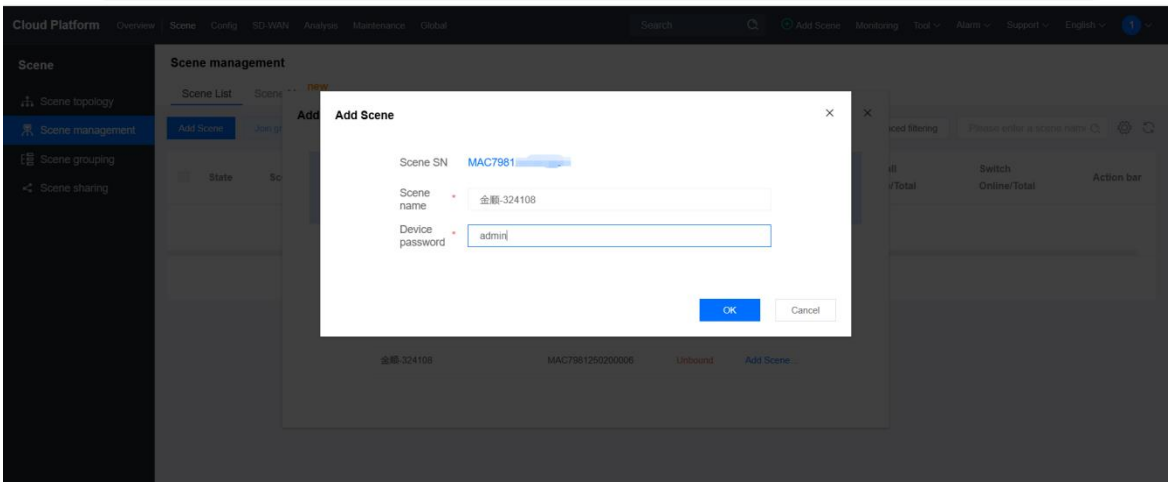
3. Find the device SN from device web interface or from the sticker on the back side of product, copy or input it in below picture to band device to cloud



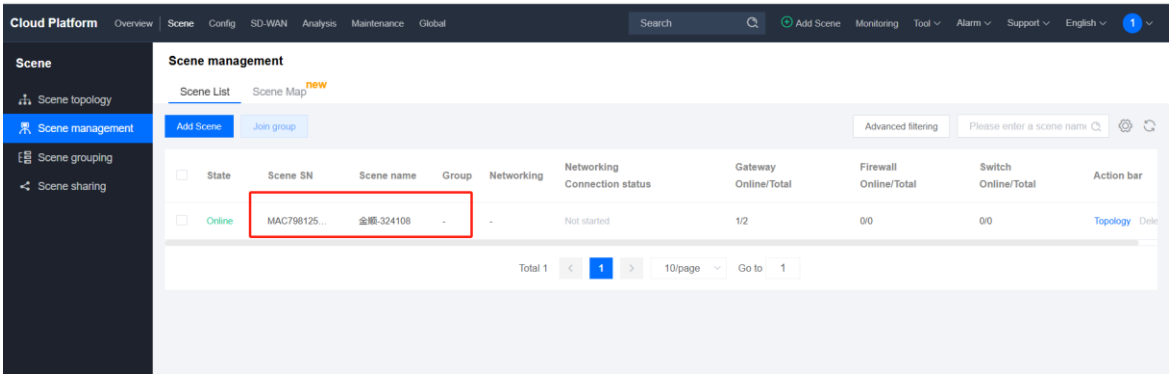
Here we show the serial number addition method. Fill in the SN in "Serial Number Addition" and click Next.



If the state is unbound, the device can be added to cloud. Click "Add Scene", input the scene name, and then enter the router login password and OK to add.



Finally the device will be successful to display in Scene list



九、 System

9.1 Remote Maintenance

Enabling this function will generate a link for remote control of the device. Can use this link to remotely control the device. After entering the account and password, can login the WEB management page to debug the device.

Manual Application

That is, manually apply for a control link .

Apply now : The page will automatically generate a control link, can go to the management page of the device by accessing the link. It should be noted that the default account does not support the application of control link generation. Please change the login password of the router first. The new password cannot be admin ;

Refresh: refresh the current connection status;

Remote control status: Displays whether the current control application is enabled or disabled.

Automatic application

When the device is restarted, the original application link will become invalid and a new generated link will be needed. At this time, the automatic application function is needed. The automatic application function is disabled by default and needs to be enabled before the rules can be configured;

Device ID: Fill in the device name or other identification for the control link application to facilitate identification when receiving;

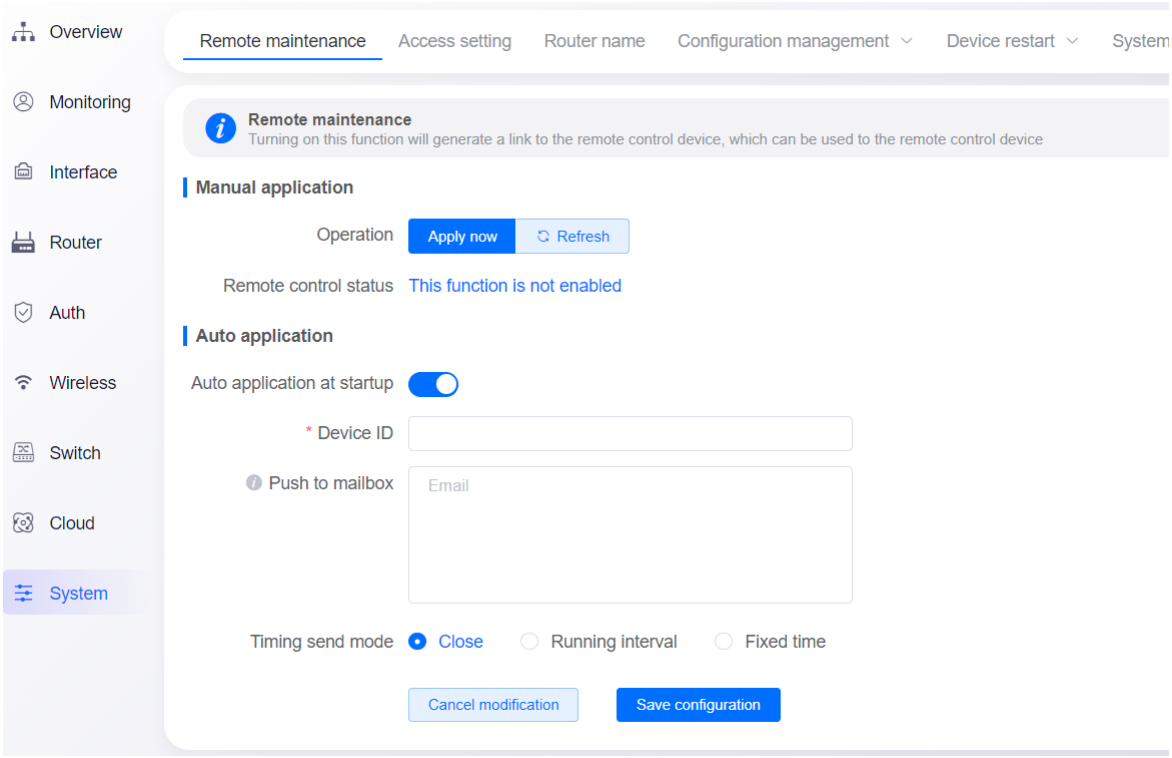
Push to mailbox: When the device restarts, the updated application control link is sent to the specified mailbox;

Timing send mode:

Close : In this state, the application control link will be sent to the specified mailbox only after this rule is saved;

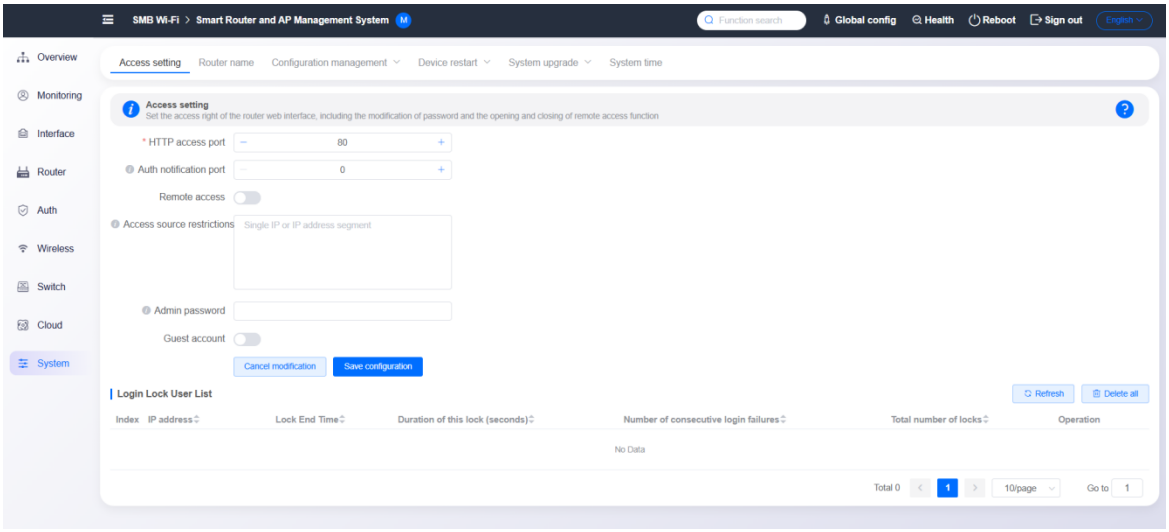
Running interval : When the device runs to the time set here, it will automatically send the application control link to the specified mailbox;

Fixed time : Specify the time to send the application control link, and the link will not be sent actively at other times.



9.2 Access setting

Set the access right of the router web interface, including the modification of password and the opening and closing of remote access function



HTTP access port: The port used by the local area network to access the router. The default value is 80;

Auth notification port: 0 means the same as the management port;

Remote access: Enable means activating remote access. After activation, the router WEB control interface can be accessed in the WAN, which is convenient for administrators to perform remote maintenance. It is disabled by default;

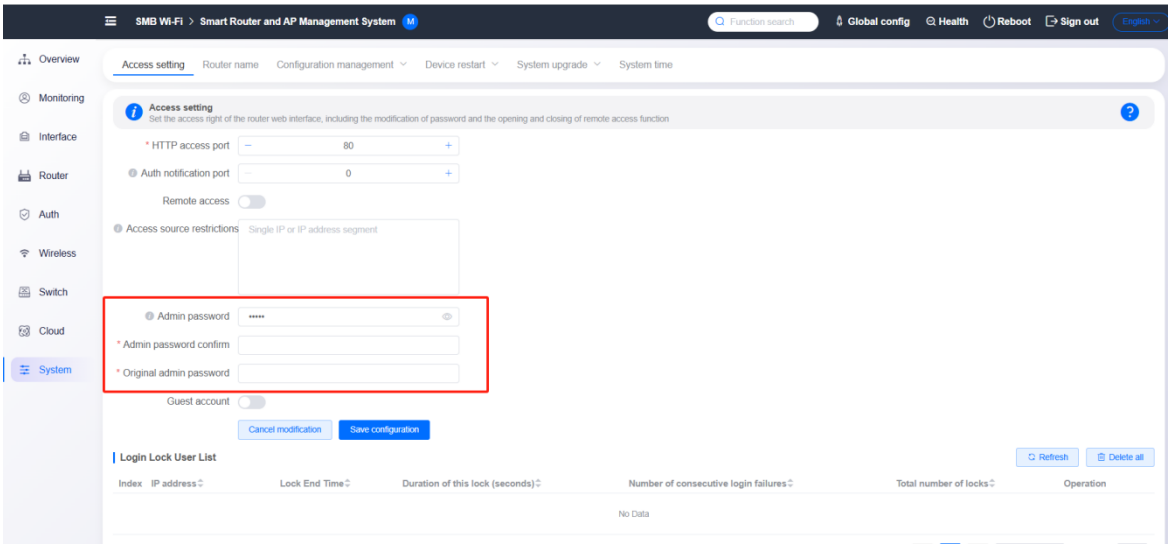
Access source restriction: The filled address will not be able to access the remote address of the system;

Admin Password:

A custom administrator password , which has the highest management privileges for the router ;

By default, there is no need to set or modify the account in this system, and the account is always “admin” by default ;

To change the password, directly enter the new password in "Admin Password", then enter "Admin Password Confirmation" and "Original Admin Password", and submit to complete the change.



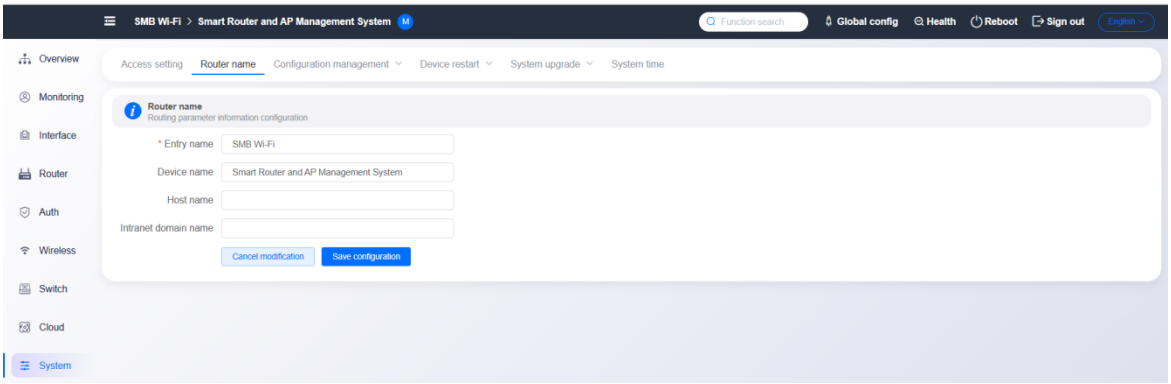
Guest account: A guest account refers to an ordinary administrator account. The ordinary administrator account does not have the highest authority, so the owner of this account can only view the system configuration and has no authority to operate and modify the system.

After enabling the guest account, please enter the "Guest Password" and "Guest Password Confirm" and save configuration to finish it.

9.3 Router Name

Routing parameter information configuration.

Router Name



Entry name: The name of the entire network to be built with our equipment;

Device name: the name of the device currently in use;

Host name: The default is SMB Wi-Fi, which generally does not need to be modified or defined;

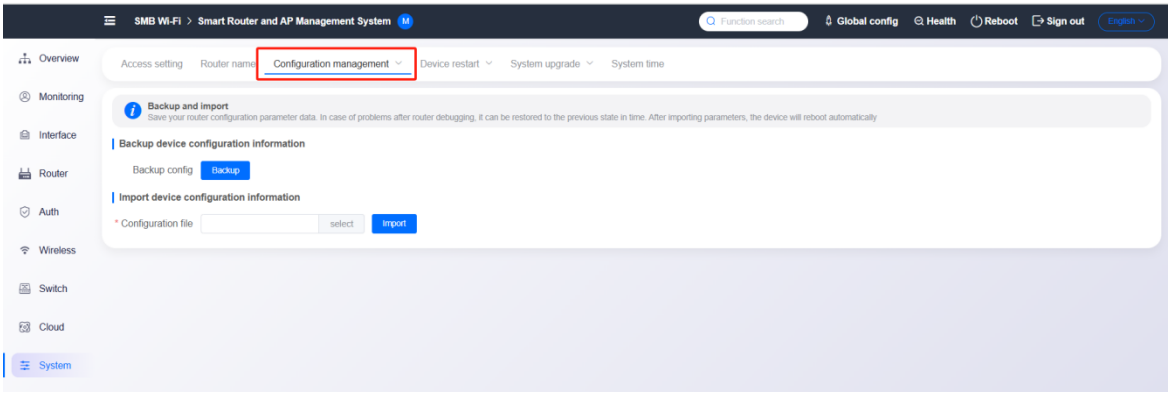
Intranet domain name: Intranet users can log in to the device management interface through this domain name.

The above names can be modified manually. There is no need to modify the parameters and just keep the default values.

9.4 Configuration Management

9.4.1 Backup and Import

The router configuration parameter data can be saved so that the router can be restored to the previous configuration state in time if problems occur after debugging . Please noted that the device will automatically restart after importing the parameters.



Backup device configuration information

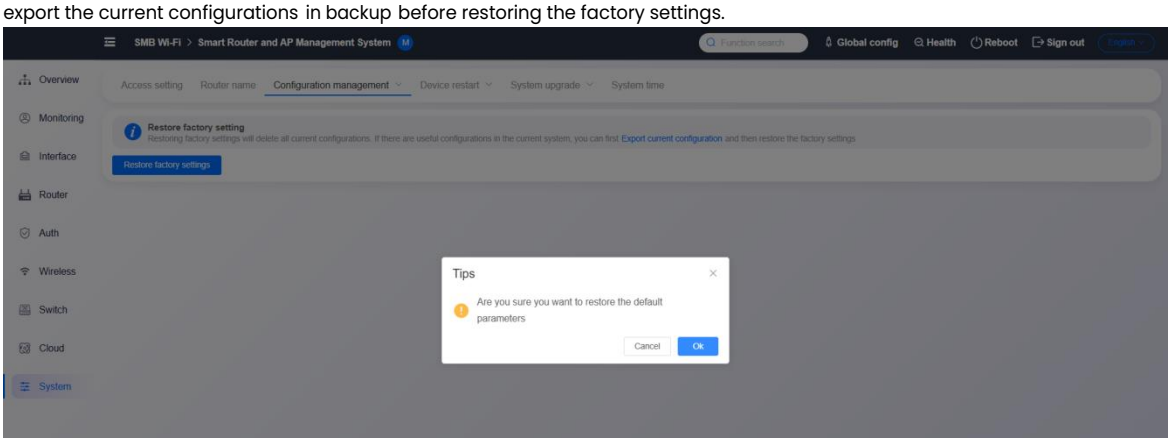
If want to back up parameters, click the "Backup" button and the parameters will be downloaded to the browser. Please view or move the downloaded files in the "Download" menu.

Import device configuration information

If the device needs to restore parameters after being restored to default, click "Select" to select the saved parameter file, and then click "Import". The device will automatically restart after the parameters are restored .

9.4.2 Restore factory setting

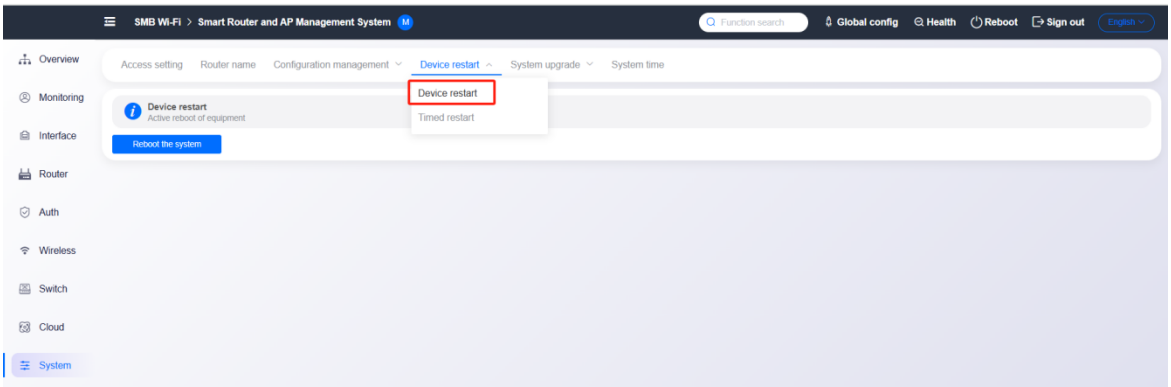
Restoring the factory settings will delete all current configurations. If there are useful configurations in the current system, please export the current configurations in backup before restoring the factory settings.



9.5 Device Restart

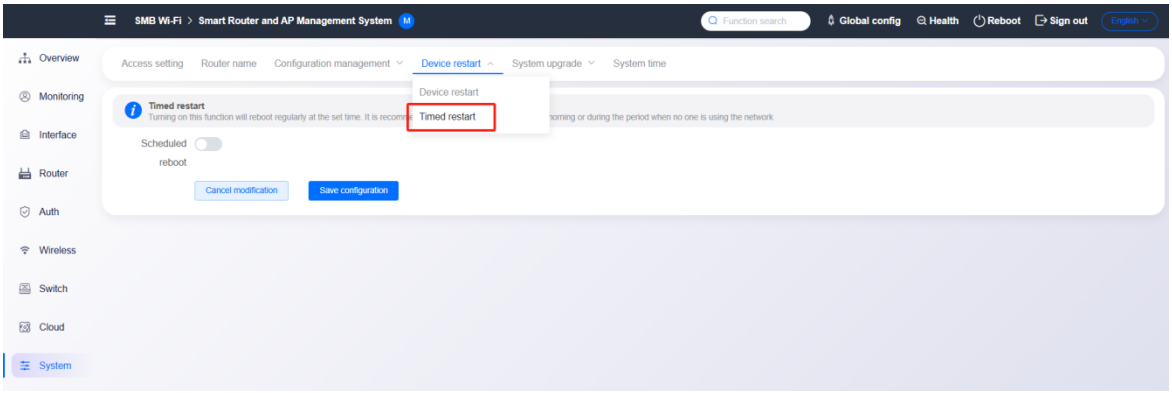
9.5.1 Device Restart

Manually restart the device in the software. Restarting the device will not clear the configured parameters. The network will be automatically disconnected during the device restart process . Please operate it with caution.



9.5.2 Timed Restart

Turning on this feature will schedule to restart the device at the set time. It is recommended to schedule a reboot in the early morning or when no one is using the network. Scheduled reboot is disabled by default and can only be created after it is enabled.



Timed restart

Scheduled reboot: confirm whether the rule is enabled or disabled. When the scheduled restart status is disabled, the scheduled restart rule will not take effect.

Mode:

Running days : When the system runs for the set number of days, the device will be restarted at the specified time on that day;

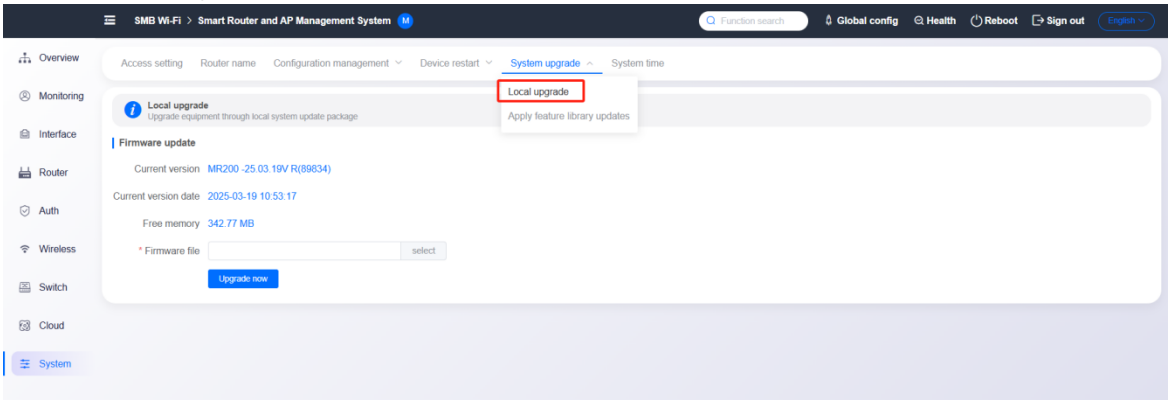
Fixed time : Specify a fixed restart time, day and hour of the week .

After setting the scheduled restart rule, please be sure to save the configuration, otherwise the rule will not take effect.

9.6 System Upgrade

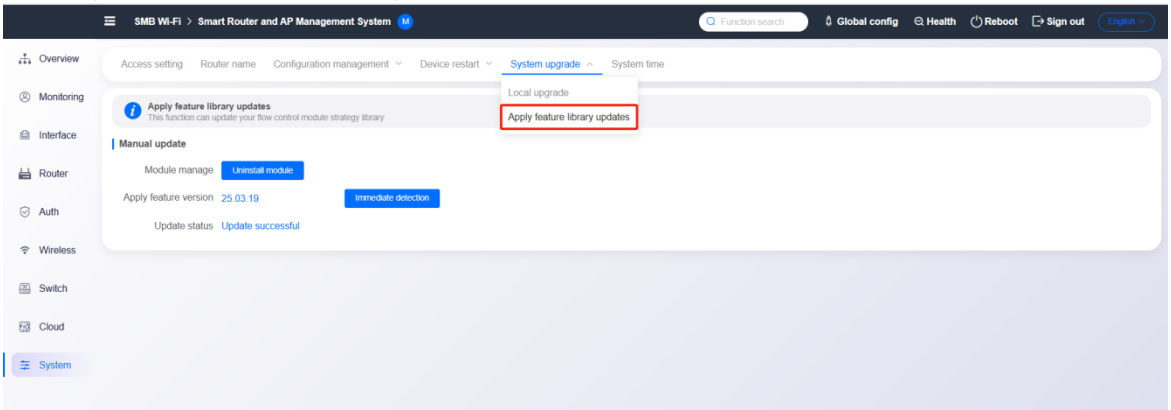
9.6.1 Local Upgrade

When there is a new firmware that needs to be upgraded or downgraded, select local upgrade. After select the firmware, click " **Upgrade Now** " and wait for the firmware upgrading to complete; " **Upgrade Later** " means that the firmware will be upgraded only when the device is restarted (software restart or power off restart). To upgrade the firmware later, please select the upgrade firmware and click Upgrade Later.



9.6.2 Apply feature library update

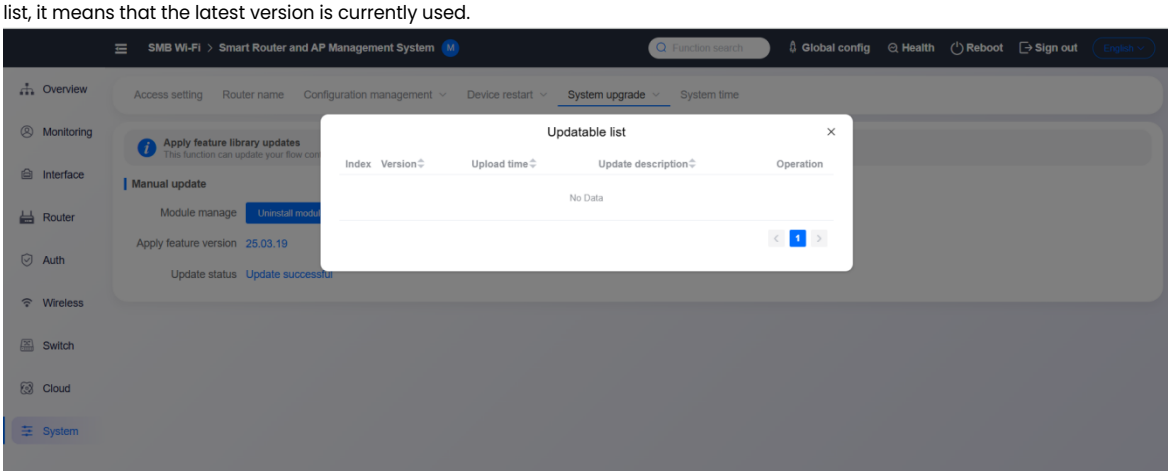
The settings to update the application recognition feature library



Manual Update

Module manage: The default state feature library module is automatically loaded and used. If you click "Uninstall module", the identification rules involved in policy routing, flow control settings, etc. will no longer take effect, and the terminal host applications will not be identified;

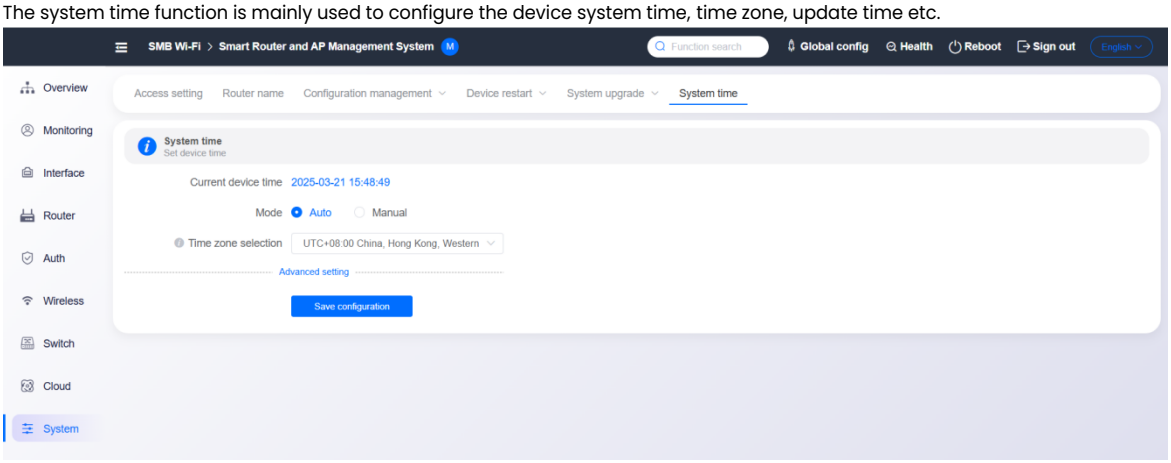
Apply feature version: Displays the version date of the current signature database. Click "immediate detection". If the service provider has updated the latest signature database version, can update it to the latest version. If there is no content in the update list, it means that the latest version is currently used.



Update status: indicates whether the signature database is updated successfully;

9.7 System Time

The system time function is mainly used to configure the device system time, time zone, update time etc.



System time

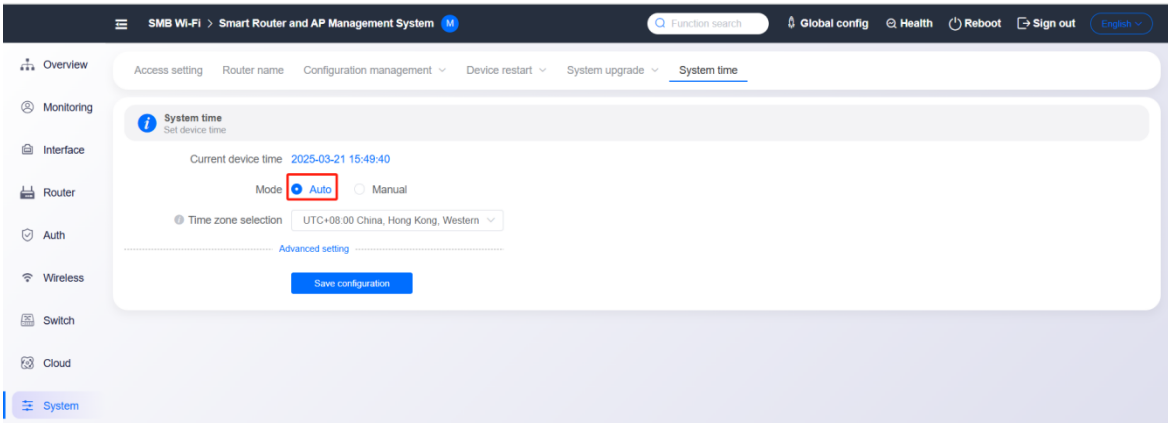
Set the device time.

Current device time : Displays the current real-time time of the device.

Mode

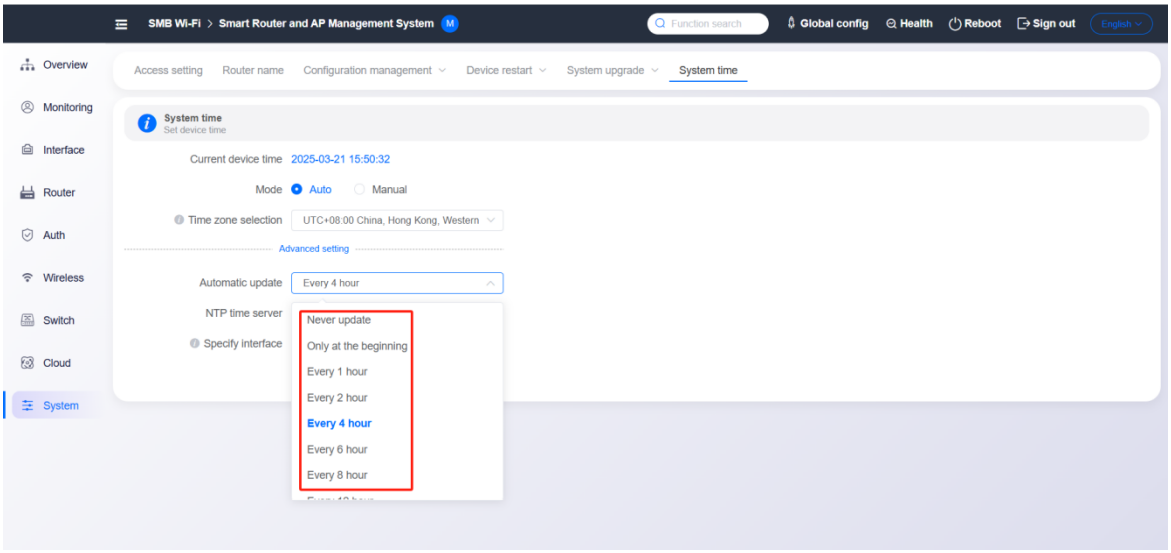
Auto: After the device is connected to the Internet, it will automatically update the time according to the selected time zone.

Manual: After the device is connected, update the system by specified time.

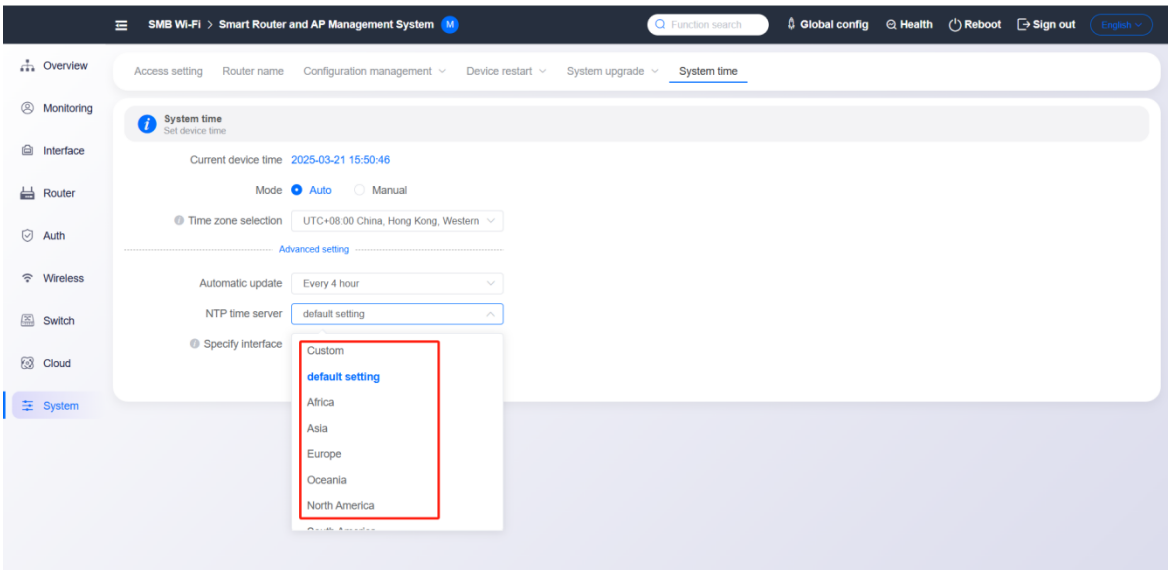


Advanced Settings

Automatic update: Set the frequency of automatic update, that is, the automatic update time every few hours;



NTP time server: supports manual selection, select the time server in which region to update the time, the default is the Asian time zone;



Specify interface: Select the specific external network line update time. If it is left blank, it means the default WAN port. If specify multiple interfaces, please add English commas to separate them, for example: "WAN1, WAN2".