User Guide For Gateway

www.wireless-tek.com

CONTENTS

1. Overview

Applicable product models are as follows:

WI-AC500 WI-AC150, WI-AC105P V1/V2, WI-AC108P V1/V2, WI-ER205

Note: The software interface is based on v5.0.build20230629-1419-c71c5a0 after.

Revision History:

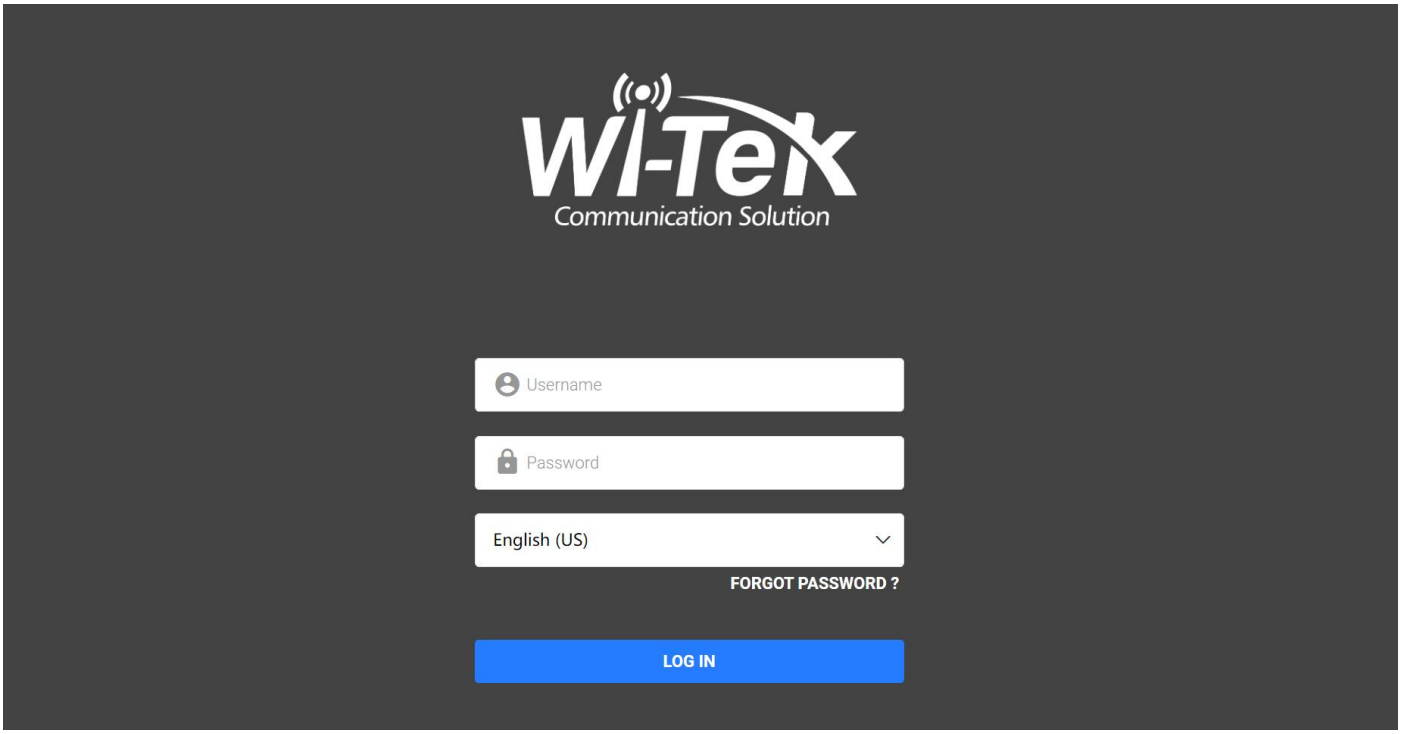
Date	Doc Version	Description
June 2023	V1.0	Initial version
April 2024	V1.1	Correction of errors in section 14.1

2. Log in to the gateway

1) Connect the computer to the LAN port of the gateway using a network cable. If your computer is configured with a fixed IP address, please change it to 'Automatically obtain IP address'.

2) Open a web browser and type the default management address **http://192.168.10.1** inthe address field of the browser, then press the Enter key.

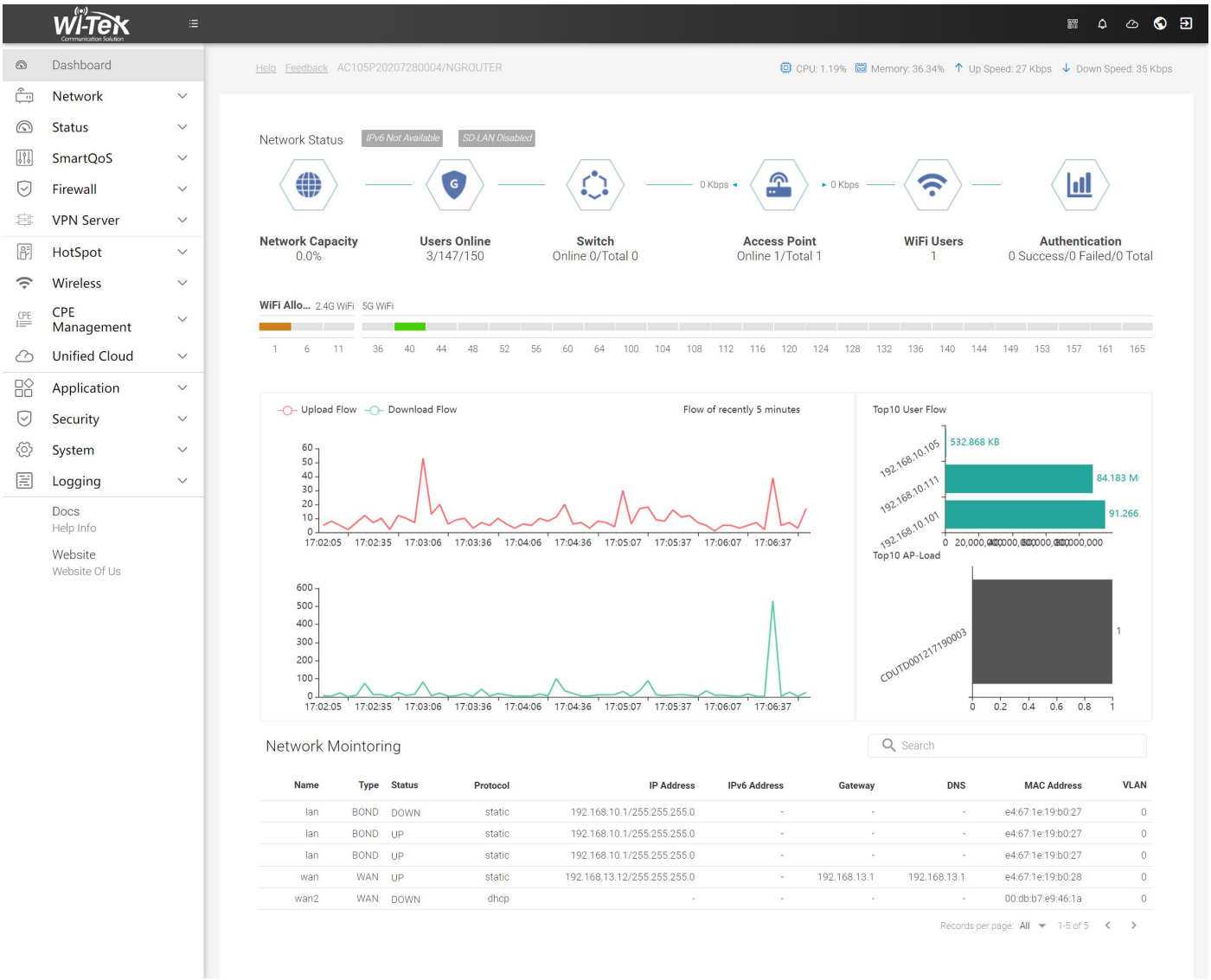
3) Enter the default username: **admin**, password: **admin.**



After a successful login, you can configure the function by clicking the setup menu on the l eft side of the screen.

3. Dashboard

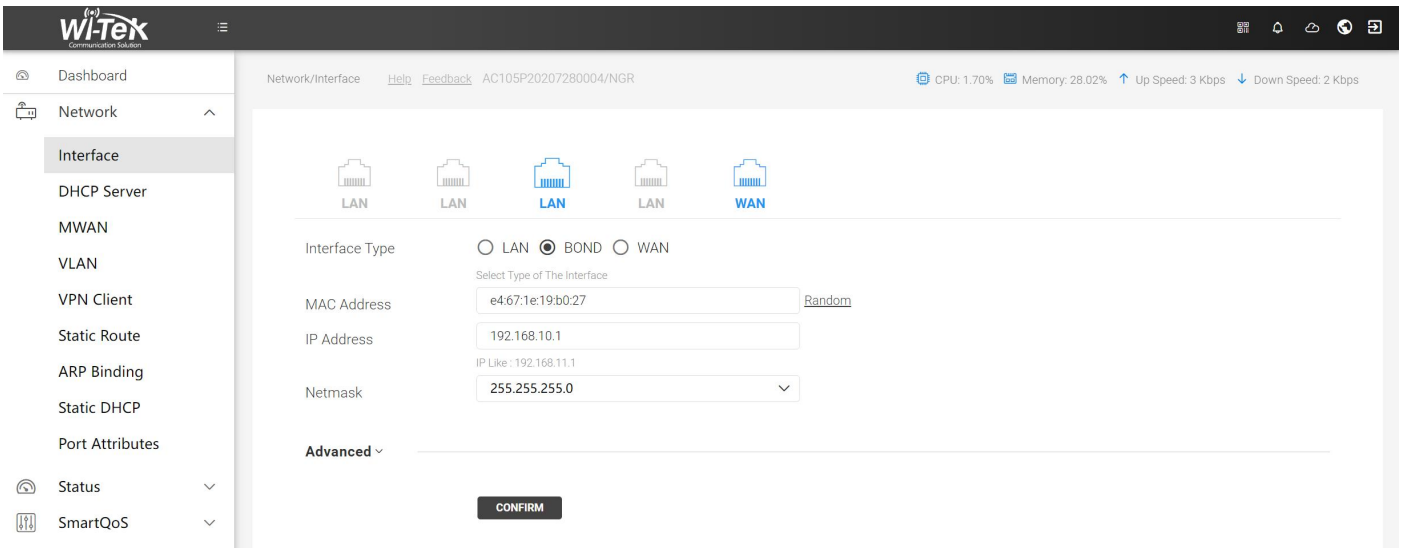
The dashboard page displays basic system information (such as network status, WiFI information, and system time) and operational information (such as traffic statistics, interface status, memory utilization, and CPU utilization).



4. Network

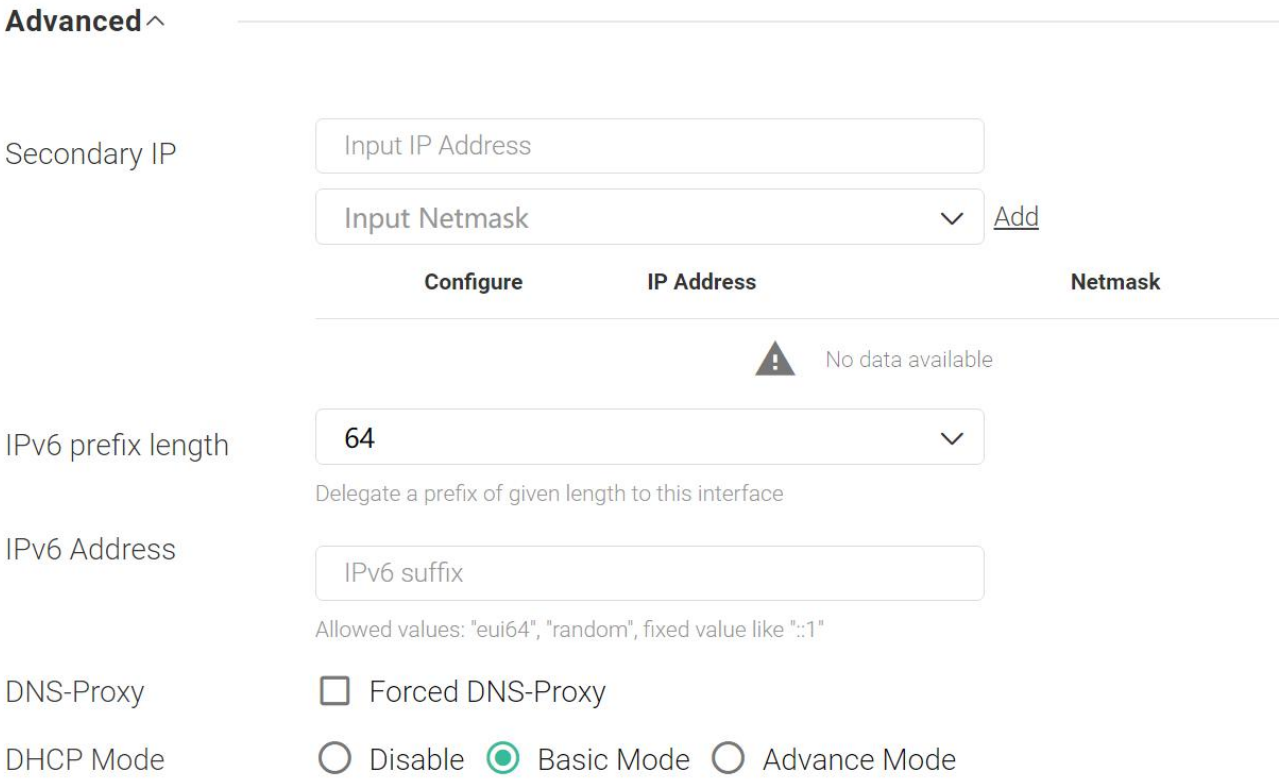
4.1. Interface

Choose the menu **Network** > **Interface** to load the following page.

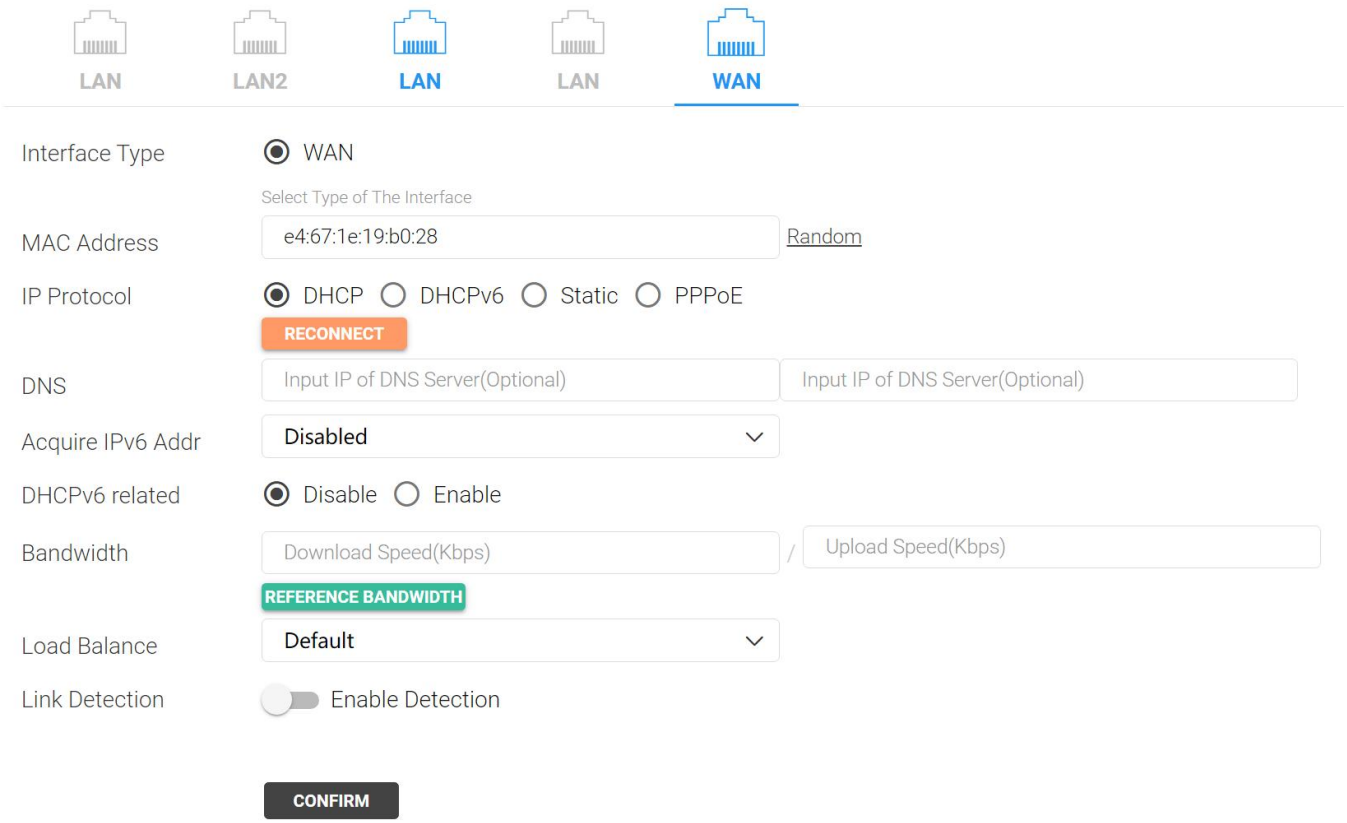


Parameter	Describe
Interface Type For LAN	**LAN**:Each port is a separate physical interface and can be assigned to a separate network segment. Note: Supports up to 4 LAN ports. **BOND**:Combine multiple LAN ports into a switch group and and can be assigned to a separate network segment. Note: For AC108P, it cannot be split into multiple independent LAN ports.

Then click on the **Advanced** option to load the following page.



Parameter	Describe
Secondary IP	Add an IP or network segment to the specified LAN port.
IPv6 prefix length	Delegate a prefix of given length to this interface.
IPv6 Address	Specify an IPv6 address for the interface.
DNS-Proxy	Check it to force the use of local DNS for domain name resolution
DHCP Mode	Disable: Select it to disable the DHCP server under this interface. Basic Mode:Specify the range of IP address allocation, total number of IPs, and IP address lease term. Advance Mode: In addition to the basic mode, you can specify the subnet mask and gateway.

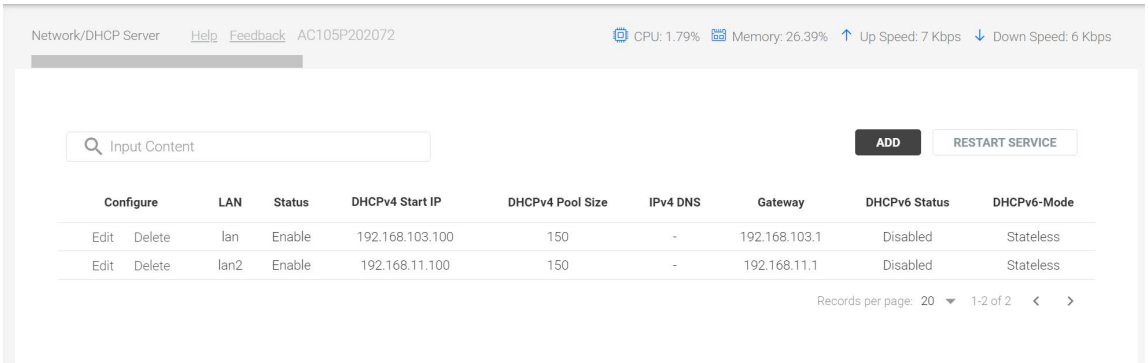


Parameter	Describe
Interface Type For WAN	WAN:The port used for internet connectivity. Note:Supports up to 4 WAN
MAC Address	Randomly generate MAC addresses.
IP Protocol	DHCP: Automatically obtain the IP address of IPv4 DHCP v6: Automatically obtain the IP address of IPv6 Static: Enter normal IP address, mask, gateway,etc. PPPoE: Enter the broadband account and password provided by your ISP.
DNS	Optional. Enter the IP address of the DNS server provided by your ISP.
Acquire IPv6 Addr	The default is disabled. If auto is selected, it will detect whether the upper network has an IPv6 IP address.
DHCPv6 related	The default is disabled. Select Enable to set the corresponding mode.

Bandwidth	Select a value greater than or equal to the actual bandwidth.
Load Balance	The realization of load balancing requires multiple WAN to be in one group.
Link Detection	For the network topology with multiple WAN accesses, enable it, enter the corresponding parameters, and automatically kick off the offline WAN port from the load balancing group.

4.2. DHCP Server

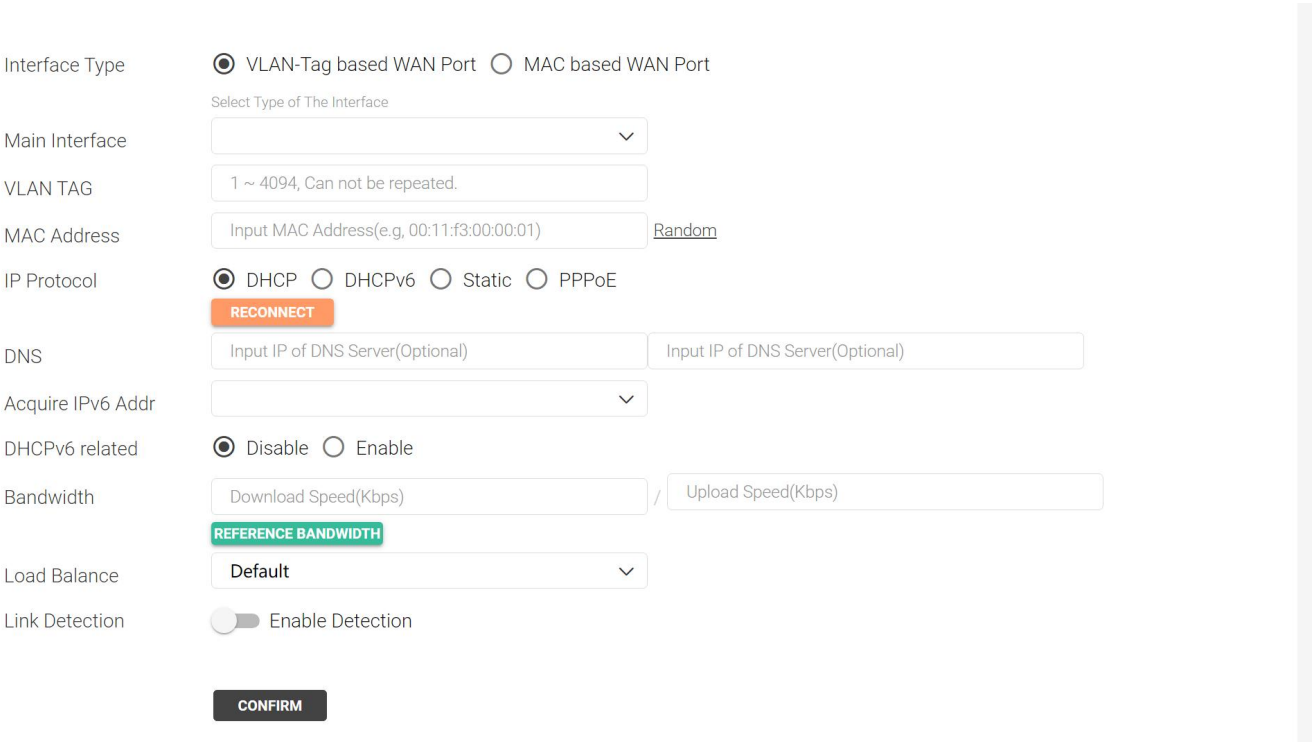
Choose the menu **Network** > **DHCP Server** to load the following page.You can add or edit the parameters of the DHCP server.



4.3. MWAN

In special scenarios where the number of WAN connections exceeds the available WAN ports on the gateway, the MWAN (Multi-WAN) feature can be used in conjunction with a managed switch that supports the 802.1q protocol. This allows for an expansion of the WAN port capacity beyond the physical limitations of the gateway.

Choose the menu **Network** > **MWAN** to load the following page.



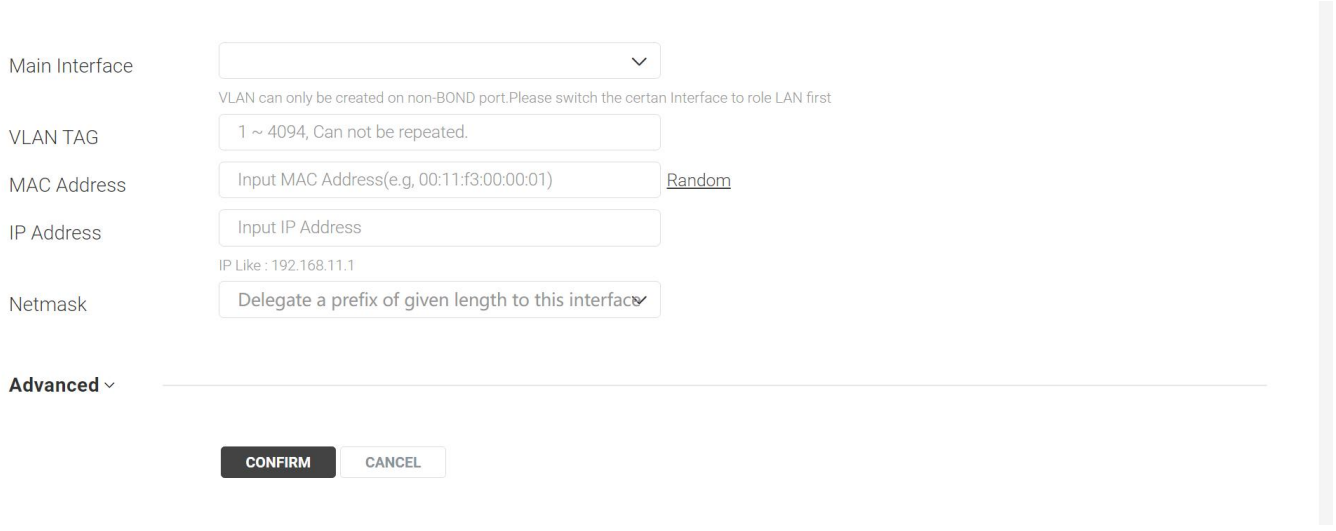
Parameter	Describe
Interface Type	**VLAN-Tag based WAN Port** Select it, select the corresponding WAN port, and enter the VLAN ID of the corresponding port created on the managed switch.  **MAC based WAN Port** Select it, select the corresponding WAN port, and enter any number in the Port Index without repeating it. 

Follow the WAN settings described in section **3.1** for other functions.

4.4. VLAN

This feature allows the creation of VLANs based on physical interfaces, enabling a single p hysical interface to accommodate multiple subnets.

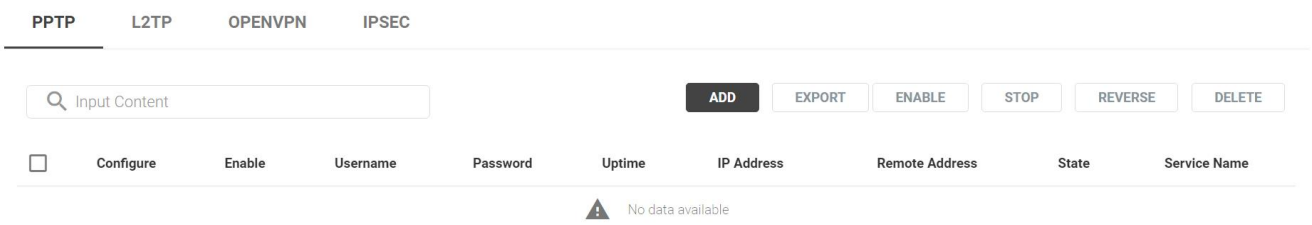
Choose the menu **Network** > **VLAN** to load the following page.



Parameter	Describe
Main interface	VLAN can only be created on non-BOND port.Please switch the certan Interface to role LAN first.
VLAN TAG	Enter VLAN ID, In actual networks, it will be used in conjunction with managed switches and APs.
Follow the LAN settings described in section 3.1 for other functions.	

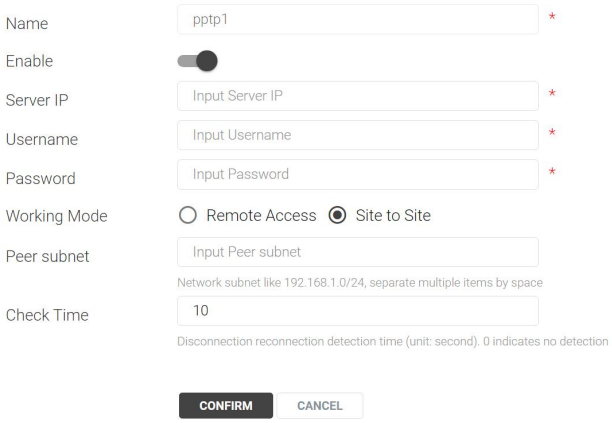
4.5. VPN Client

Choose the menu **Network** > **VPN Client** to load the following page.



For PPTP Client

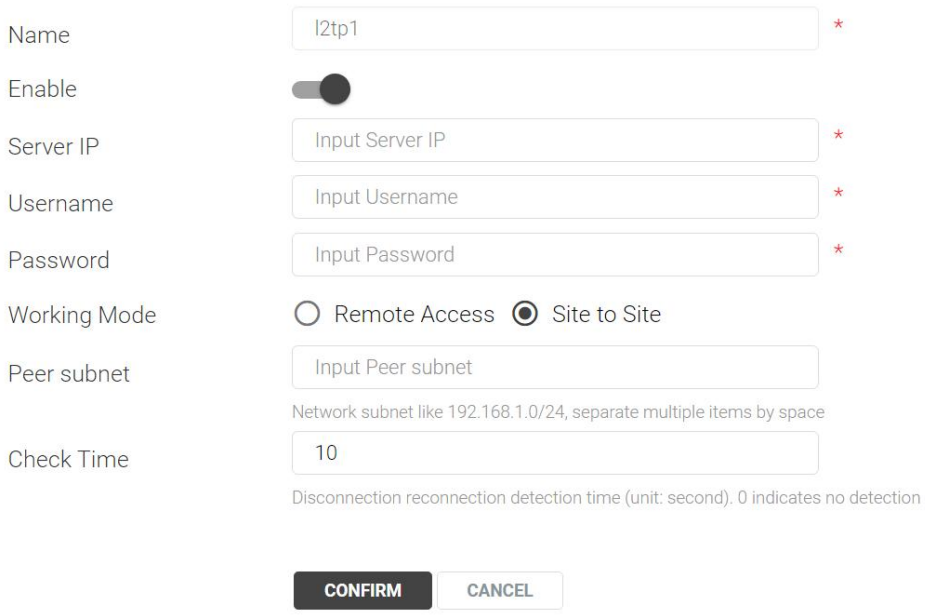
Choose the menu **Network > VPN Client > PPTP** and click **ADD** to load the following pag e.



Parameter	Describe	
Name	Enter any name for easy recognition.	
Enable	Enable or disable PPTP Client.	
Server IP	Enter the IP or domain name provided by the VPN server.	
Username	Enter the account provided by the VPN server.	
Password	Enter the password provided by the VPN server.	
Working Mode	Remote Access (Client to Site)	It is a type of VPN that connects a single device, such as a laptop or smartphone, to a remote network, such as a corporate or cloud network.
	Site to Site	It is a type of VPN that connects two or more networks, such as branch offices or data centers, over the internet.
Peer subnet	Enter as the internal subnet of the VPN service gateway.	
Check Time	Disconnection reconnection detection time (unit: second). 0 indicates no detection.	

For L2TP Client

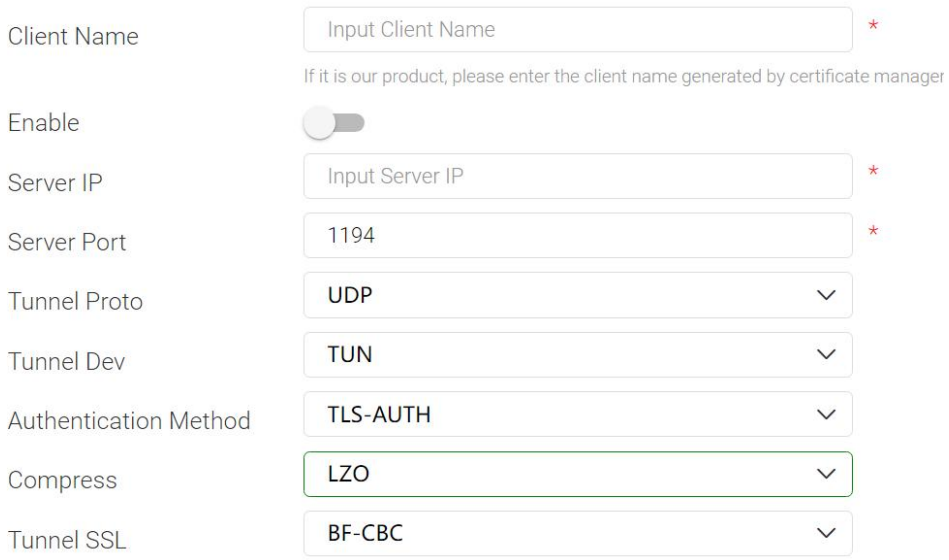
Choose the menu **Network > VPN Client > L2TP** and click **ADD** to load the following page.

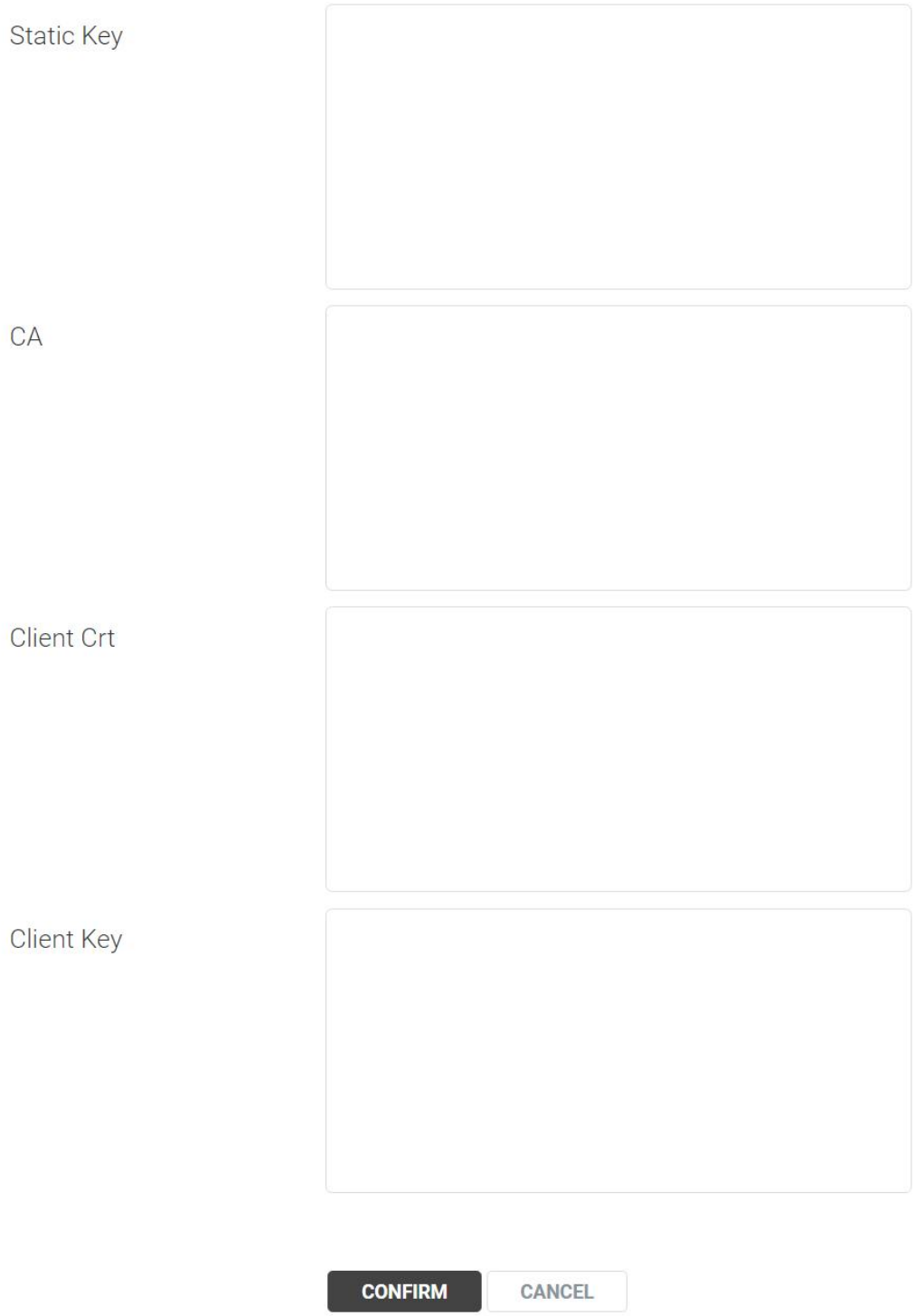


Parameter	Describe	
Name	Enter any name for easy recognition.	
Enable	Enable or disable PPTP Client.	
Server IP	Enter the IP or domain name provided by the VPN server.	
Username	Enter the account provided by the VPN server.	
Password	Enter the password provided by the VPN server.	
Working Mode	Remote Access (Client to Site)	It is a type of VPN that connects a single device, such as a laptop or smartphone, to a remote network, such as a corporate or cloud network.
	Site to Site	It is a type of VPN that connects two or more networks, such as branch offices or data centers, over the internet.
Peer subnet	Enter as the internal subnet of the VPN service gateway.	
Check Time	Disconnection reconnection detection time (unit: second). 0 indicates no detection.	

For OPENVPN

Choose the menu **Network > VPN Client > OPENVPN** and click **ADD** to load the following page.



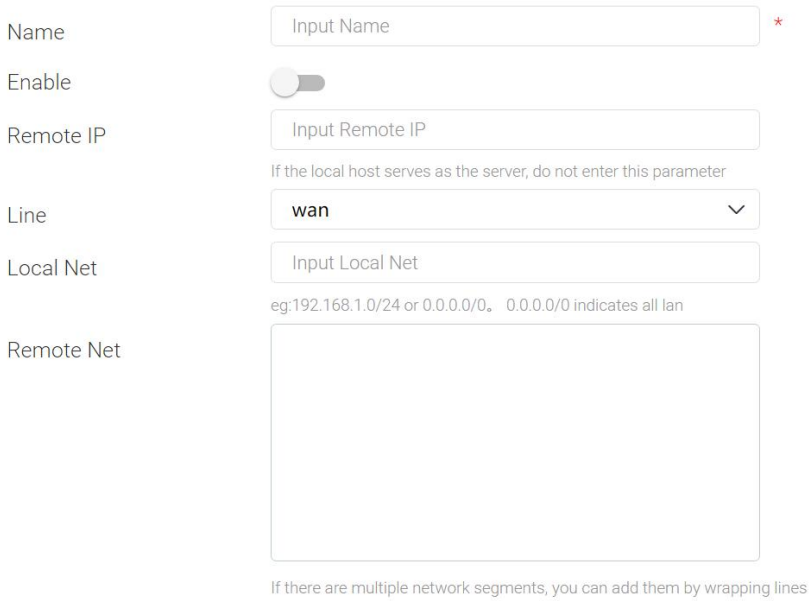


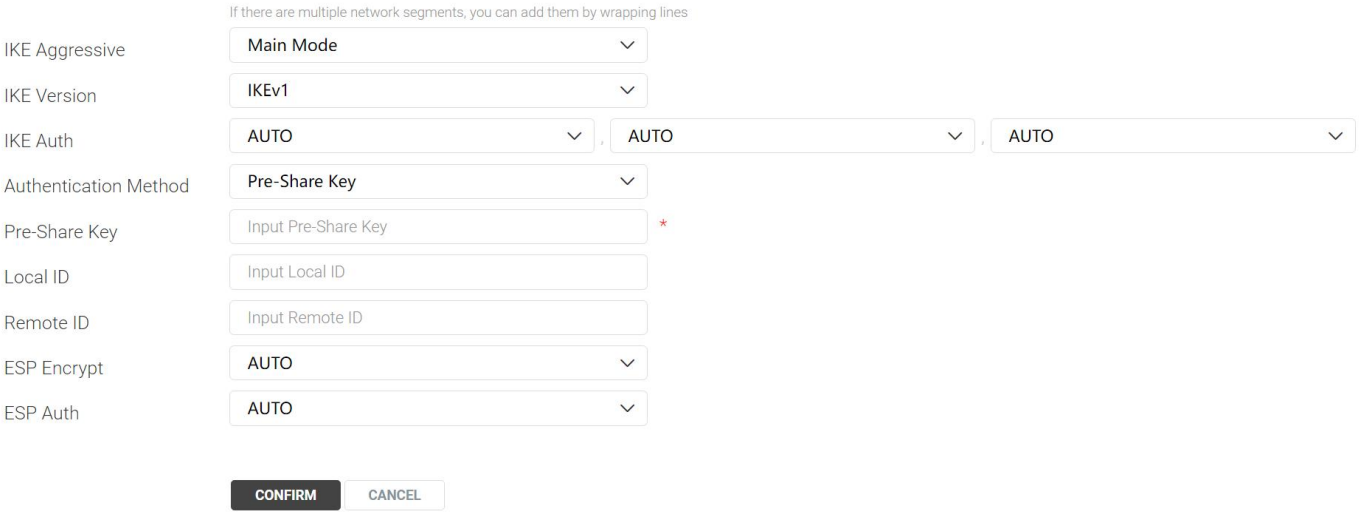
Parameter	Describe
Client Name	If the VPN service side is built by a Wi Tek gateway,please enter the client name generated by certificate management.
Enable	Enable or disable VPN client.
Server IP	Enter the public IP or domain name of the VPN server.

Server Port	Specify UDP port number.(Default :1194)
Tunnel Proto	Specify Tunnel protocol.
Tunel Dev	Support TAP and TUN mode, TAP is similar to bridge mode, TUN is similar to routing mode, and the selection of client and server should be consistent.
Authentication Method	TLS_AUTH and TLA_CRYPY are supported. Make sure the server and client choose the same.
Compress	A data compression algorithm that supports LZO and LZ4 modes.Make sure the server and client choose the same.
Tunnel SSL	Specify the encryption algorithm type.Make sure the server and client choose the same.
Static Key	Maintain consistency with the static key of the VPN server.
CA	Maintain consistency with the CA of the VPN server.
Client Crt	Create a client crt file from the VPN server side
Client Key	Create a client key from the VPN server side

For IPSEC

Choose the menu **Network** > **VPN Client** > **IPSEC** and click **ADD** to load the following pa ge.



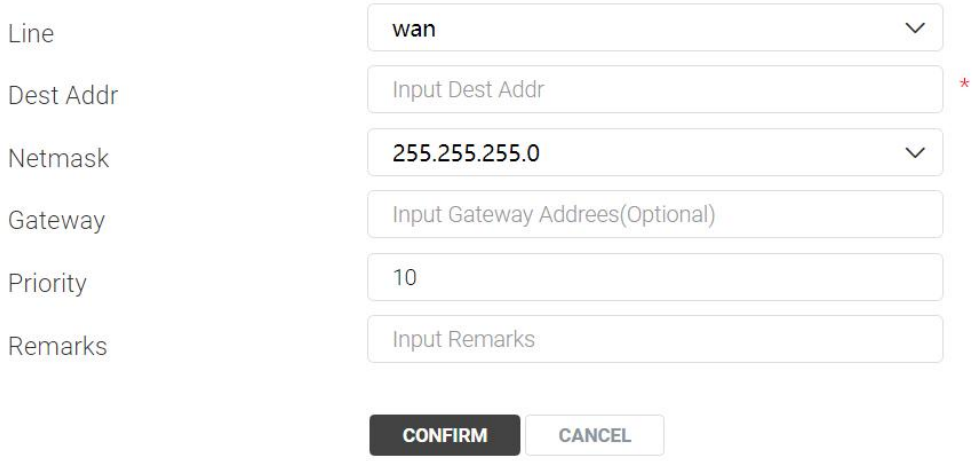


Parameter	Describe
Name	Enter any name for easy recognition.
Enable	Enable or disable IPsec.
Server IP	Enter the public IP or domain name of the VPN server.
Line	Specify tunnel establishment at interface.
Local Net	Specify the local network.
Remote Net	Specify the remote network.
IKE Aggressive	Specify the IKE Exchange Mode as **Main Mode** or **Aggressive Mode**. By default, it is Main Mode. **Main Mode**: Main mode provides identity protection and exchanges more information.which applies to scenarios with higher requirements for identity protection. **Aggressive Mode**: Aggressive Mode establishes a faster connection but with lowersecurity, which applies to scenarios with lower requirements for identity protection.
IKE Version	Specify the IKE version.Ensure that the local and remote selection versions are consistent.

IKE Auth	Specify the IKE authentication.Ensure that the local and remote IKE authentication are consistent.
Authentication Method	**Pre-Share Key** and **Self-signed certificate** are supported.
Pre-Share Key	Specify the unique pre-shared key for both peers' authentication.
Local ID	Specify the Local ID. Fill in local ID and remote ID each other.
Remote ID	Specify the remote ID. Fill in local ID and remote ID each other.
ESP Encrypt	Specify the ESP encryption algorithm used by the SA.Ensure that the local and remote ESP Encrypt are consistent.
ESP Auth	Specify the ESP authentication algorithm used by the SA.Ensure that the local and remote ESP authentication are consistent.

4.6. Static Route

Choose the menu **Network** > **Static Route** and click **ADD** to load the following page.

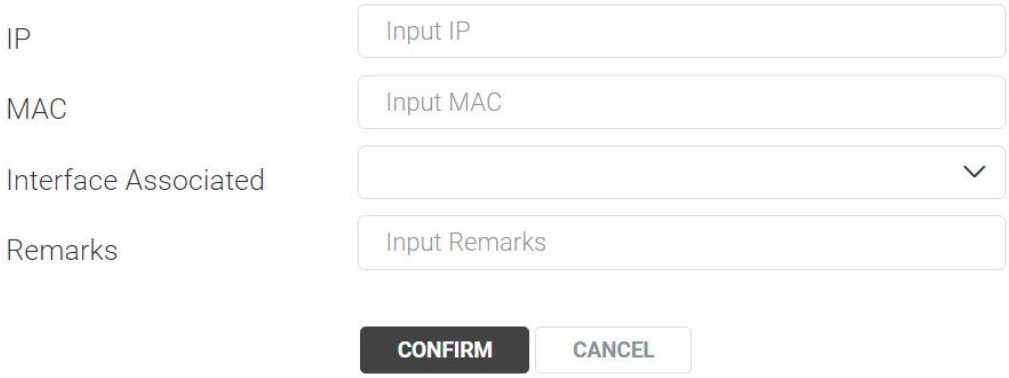


Parameter	Describe
Line	Specify the physical network interface through which this route is accessible.
Dest Addr	Specify the destination IP address the route leads to.
Netmask	Specify the subnet mask of the destination network.

Gateway	Specify the IP address to which the packet should be sent next
Priority	Define the priority of the route. A smaller value means a higher priority. The default value is 10. It is recommended to keep the default value.
Remaks	Give a remarks for identification.

4.7. ARP Binding

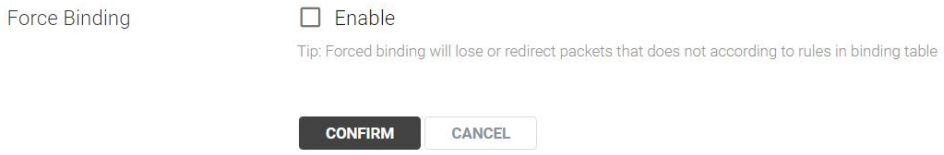
Choose the menu **Network** > **ARP Binding** and click ADD to load the following page.



Parameter	Describe
IP	Enter an IP address to be bound.
MAC	Enter an MAC address to be bound.
Interface Associated	Select the specified interface.
Remarks	Give a remarks for identification.

To complete Anti ARP Spoofing configuration, there are two steps. First, add IP-MAC Binding entries to the IP-MAC Binding List. Then enable **BINDING POLICY** for these entries.

Click the **BINDING POLICY** button to load the following image.

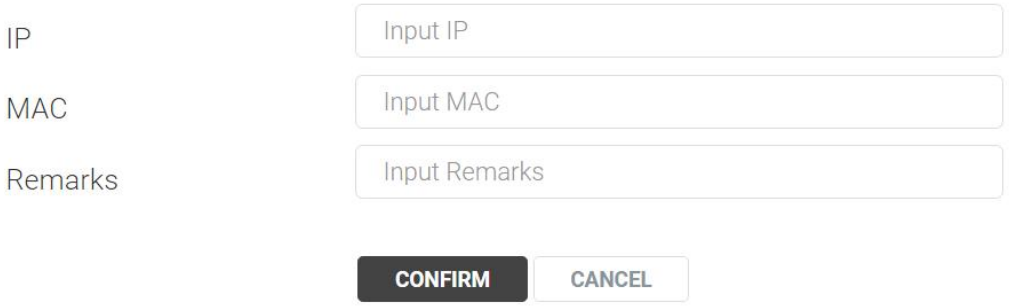


Tick the **enable** button, Forced binding will lose or redirect packets that does not according to rules in binding table.

4.8. Static DHCP

Static DHCP will be needed if you want an device to always have the same IP address.So metimes required for certain programs, this feature is useful if other people on your LAN kn ow your IP and access your PC using this IP. Static DHCP should be used in conduction with Port Forwarding. If you forward an external WAN TCP/UDP port to a port on a server running inside your LAN, you have to give that server a static IP, and this can be achieved easily through Static DHCP.

Choose the menu **Network** > **Static DHCP** and click **ADD** to load the following page.



Parameter	Describe
IP	Enter an IP address.
MAC	Enter an MAC address.
Remarks	Give a remarks for identification.

4.9. Port Attributes

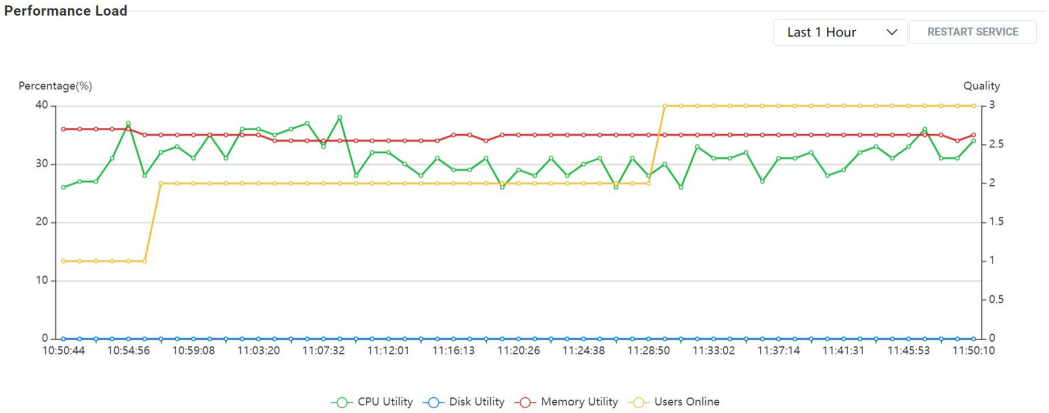
Port attributes page displays the basic port information (like the link status, speed and in/out packets).

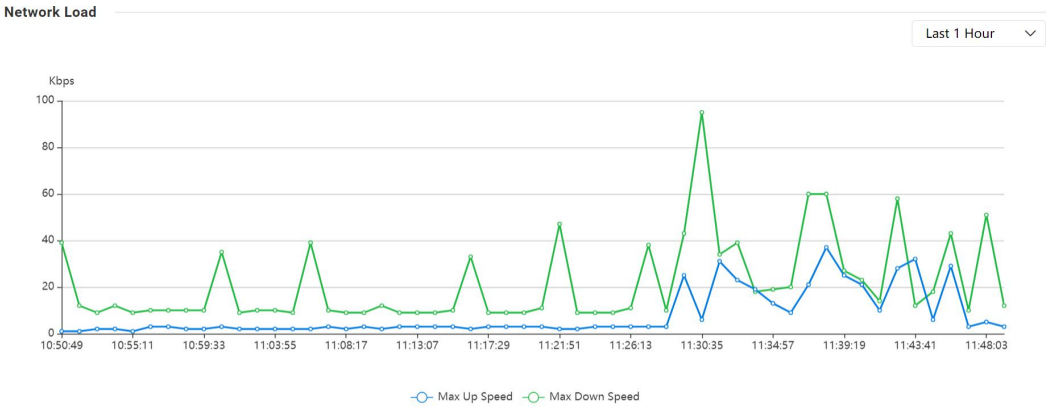
Choose the menu **Network** > **Port Attributes** to load the following page.

5. Status

5.1. Load Monitoring

You can choose different time intervals to observe the device load situation. Choose the menu **Status** > **Load Monitoring** to load the following page.

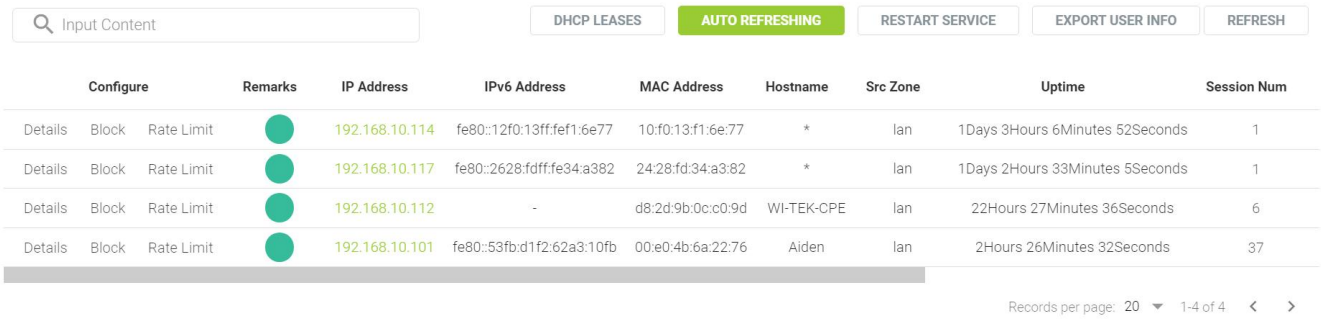




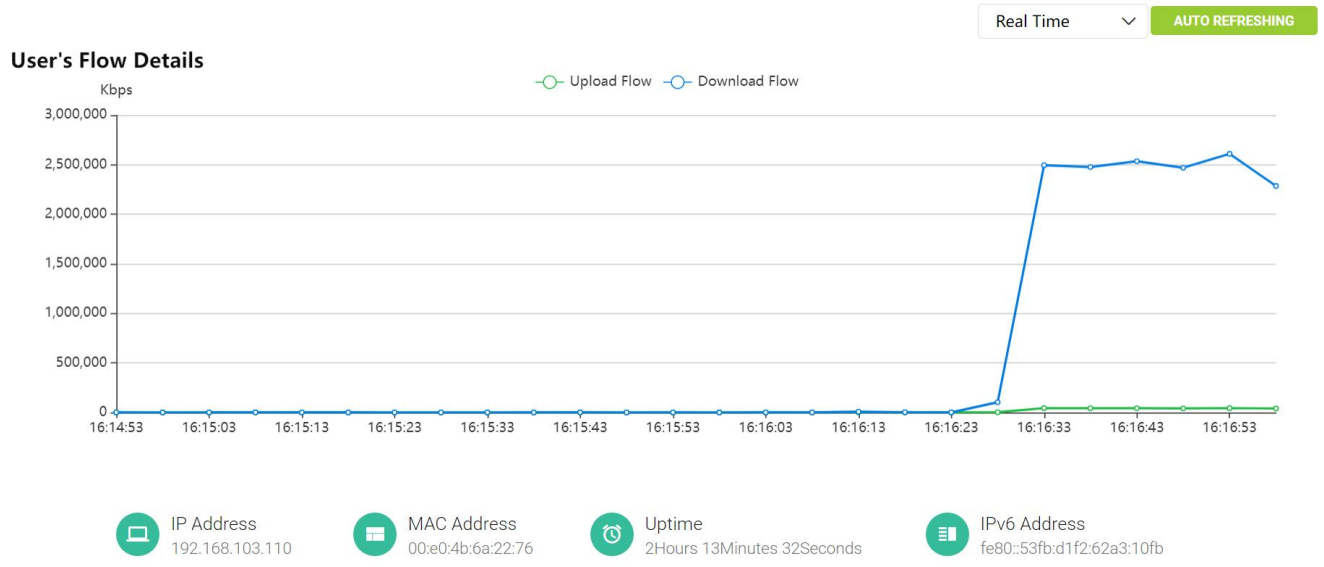
5.2. User Info

You can observe the basic information of each user, such as IP address, MAC address, source area, online duration, etc.

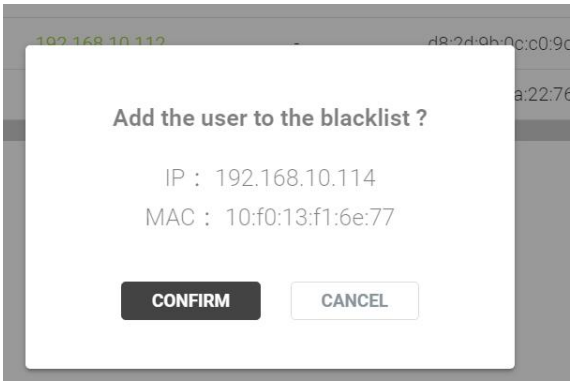
Choose the menu **Status** > **User Info** to load the following page.



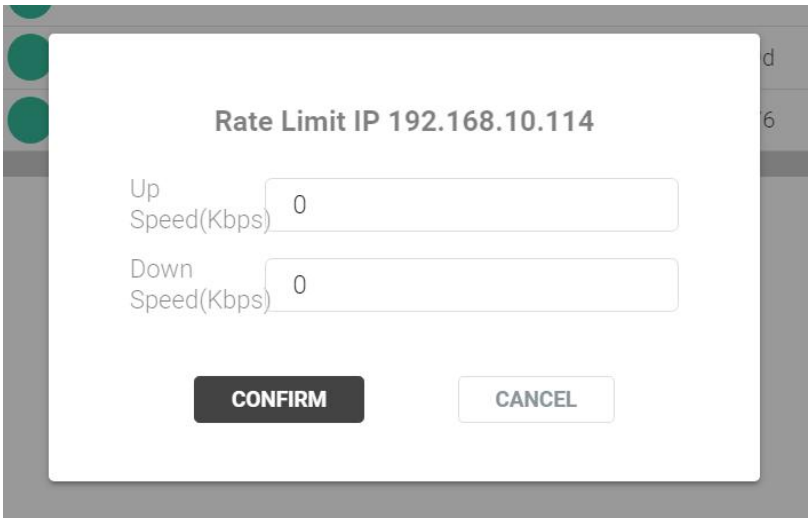
If you want to view the traffic of a specified user, please click the **Details** button to load the following image.



Clicking **Block** allows users to join the blacklist and block access to the network.



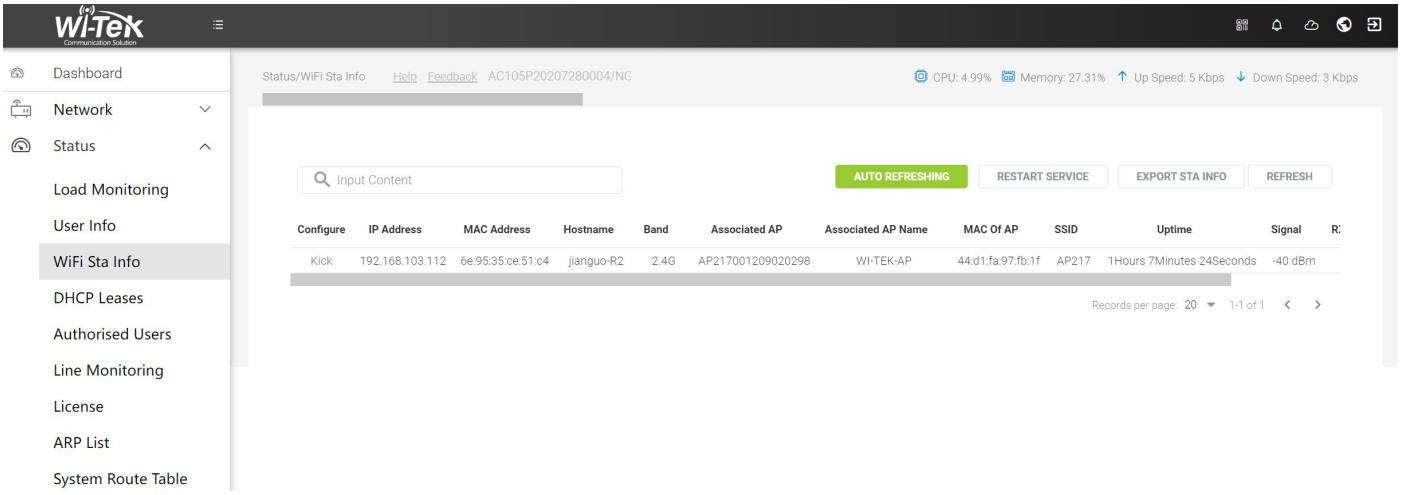
Clicking on **Rate limit** can limit users' upload and download speeds.



5.3. WiFi Sta Info

You can observe the basic information of wireless users and click **Kick** to kick off the wirel ess client.

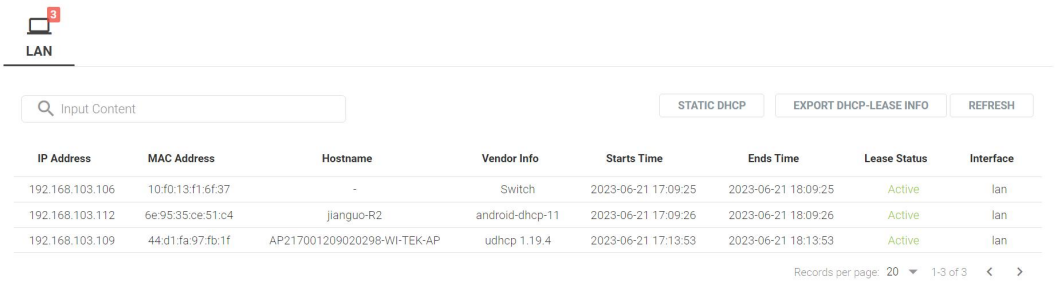
Choose the menu **Status** > **WiFi Sta Info** to load the following page.



5.4. DHCP Leases

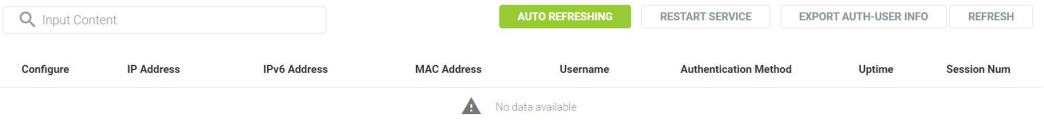
You can view the DHCP client list. If you want to schedule an IP address for a specified cl ient to use, you can click the **STATIC DHCP** button to go to the specified page and add a n IP address.

Choose the menu **Status** > **DHCP Leases** to load the following page.



5.5. Authorised Users

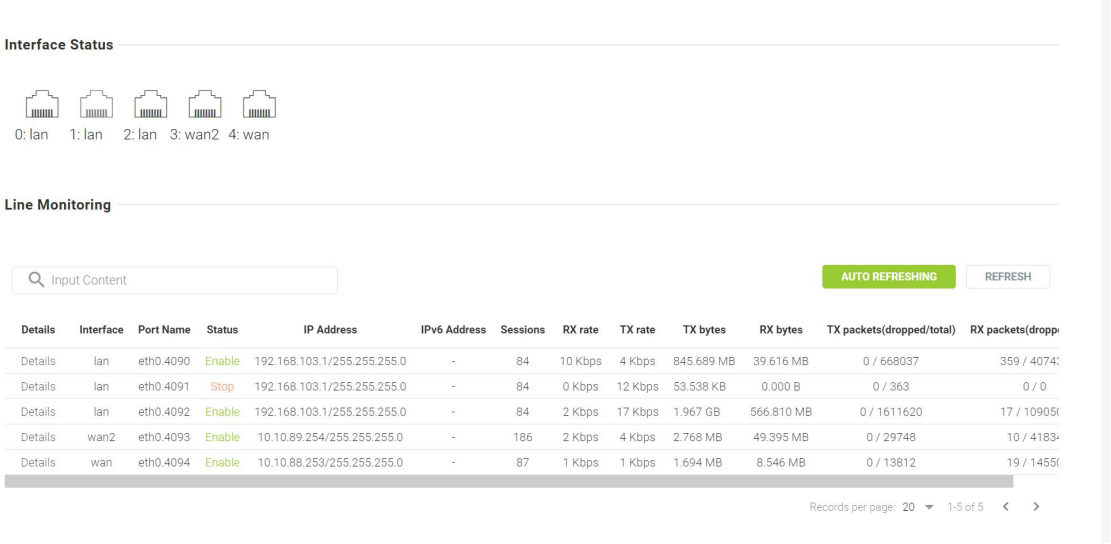
Choose the menu **Status** > **Authorised Users** to load the following page.



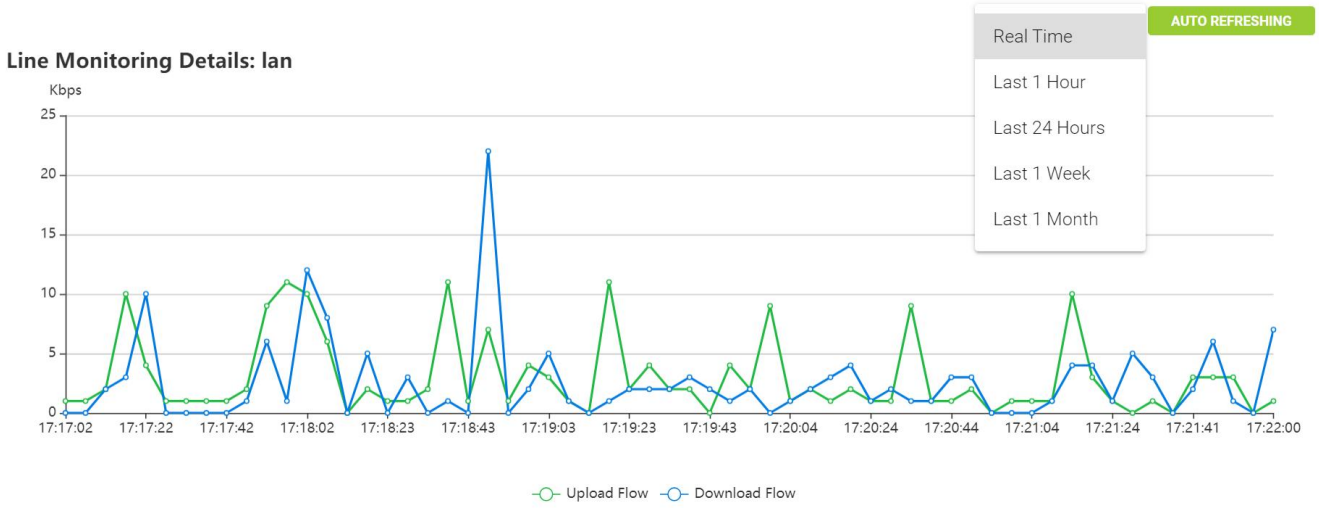
5.6. Line Monitoring

Line monitoring will collect statistics on line status and receive and transmit data packets, p roviding visual basis for IT administrators.

Choose the menu **Status** > **Line Monitoring** to load the following page.



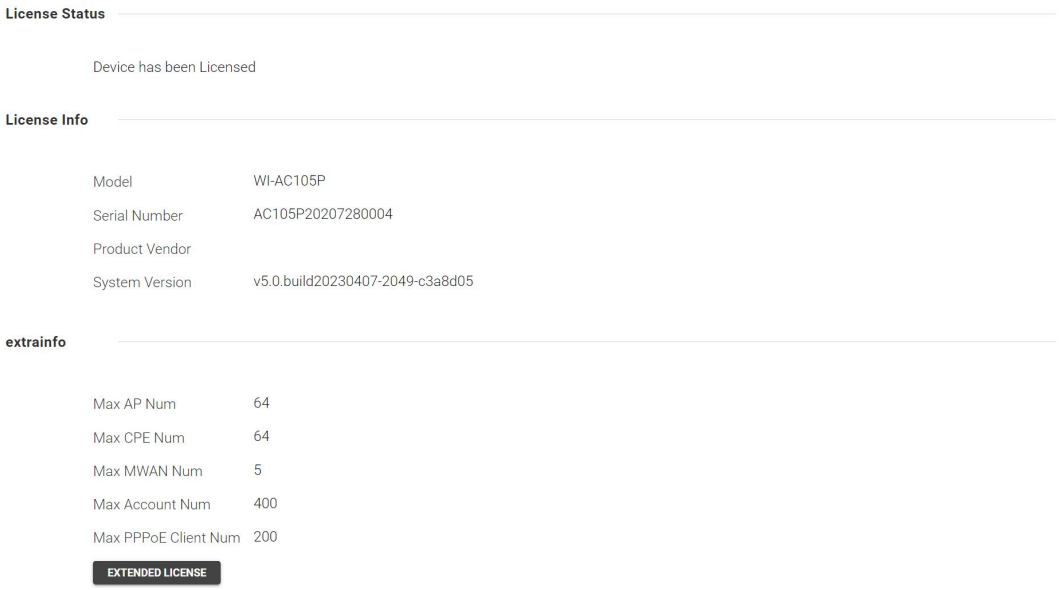
Click the **Details** button to load the following image.



5.7. License

The device has been activated at the factory, and you can view information such as the de vice model, SN, and the number of manageable APs.

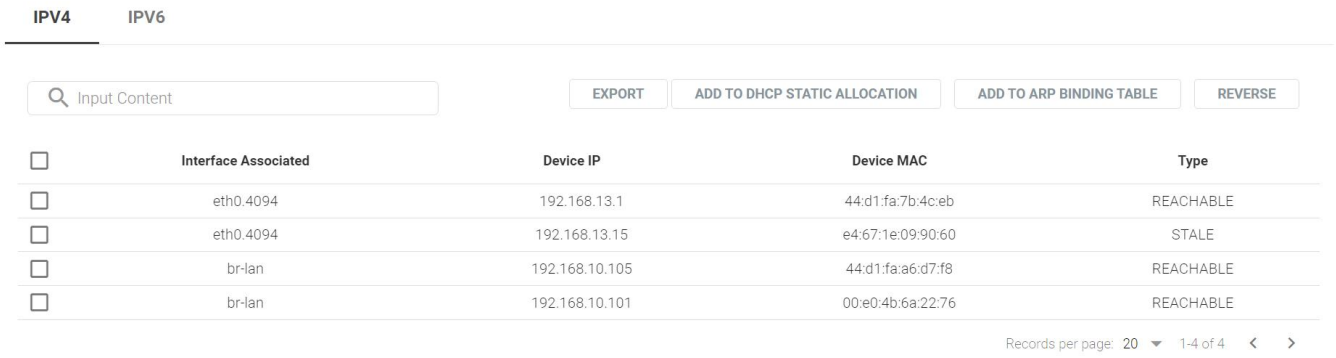
Choose the menu **Status** > **License** to load the following page.



5.8. ARP List

ARP List to view and bind the ARP Scanning entries. The ARP Scanning list displays all th e historical scanned entries.

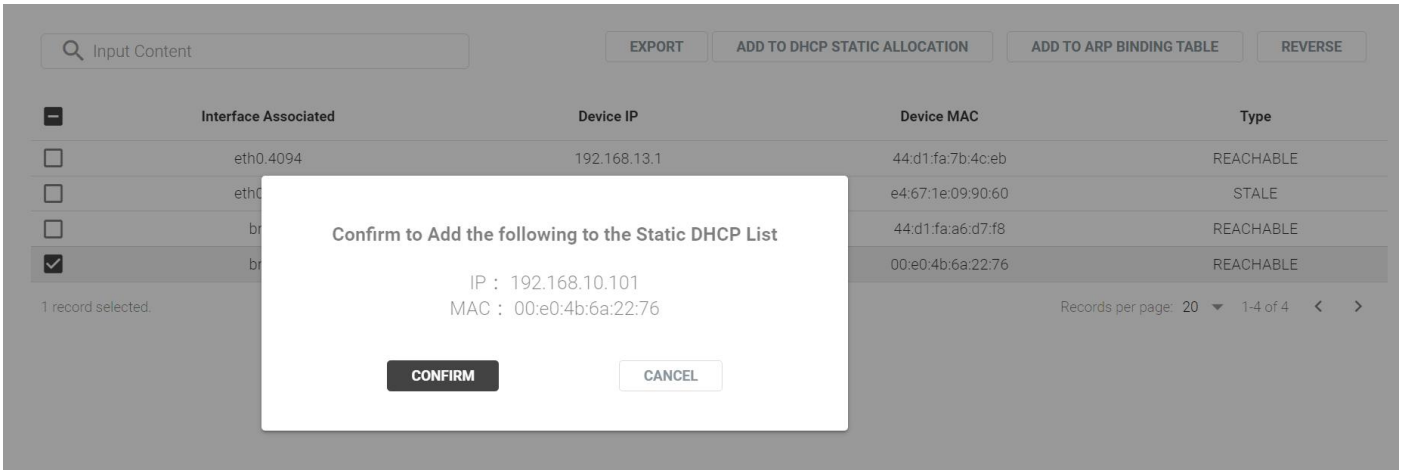
Choose the menu **Status** > **ARP List** to load the following page.



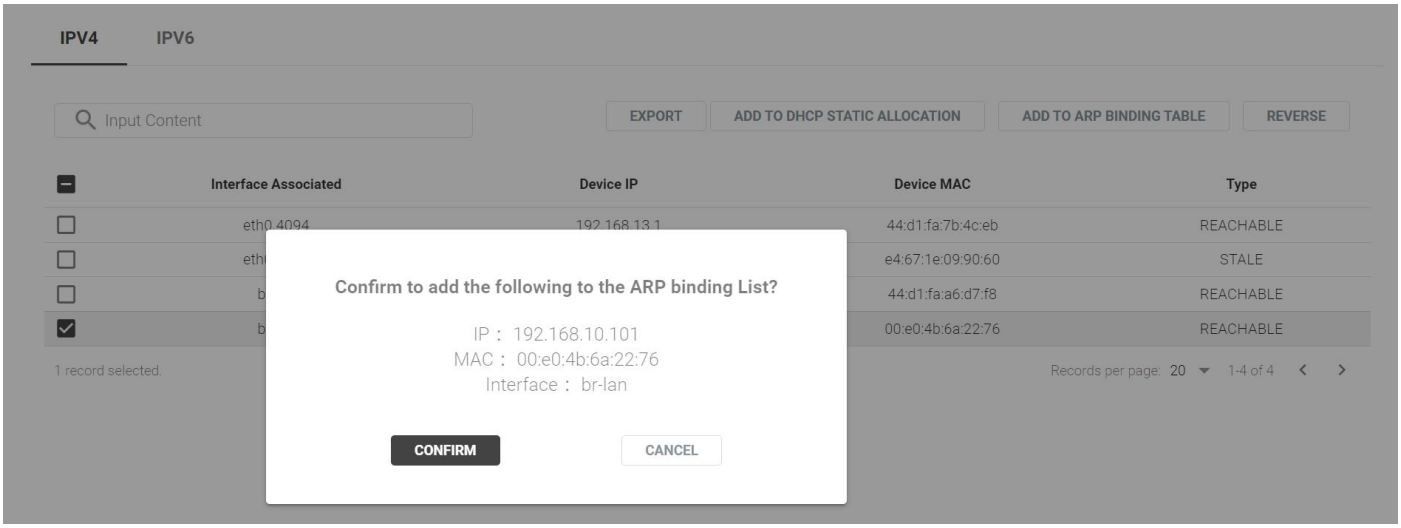
Parameter	Describe

Interface Associated	Displays the network interface of an ARP entry.
Device IP	Displays the IP address of an ARP entry.
Device MAC	Displays the MAC address of an ARP entry.
Type	Displays the type of an ARP entry.

Select the entry and click the **ADD TO DHCP STATIC ALLOCATION** button to add static DHCP list.

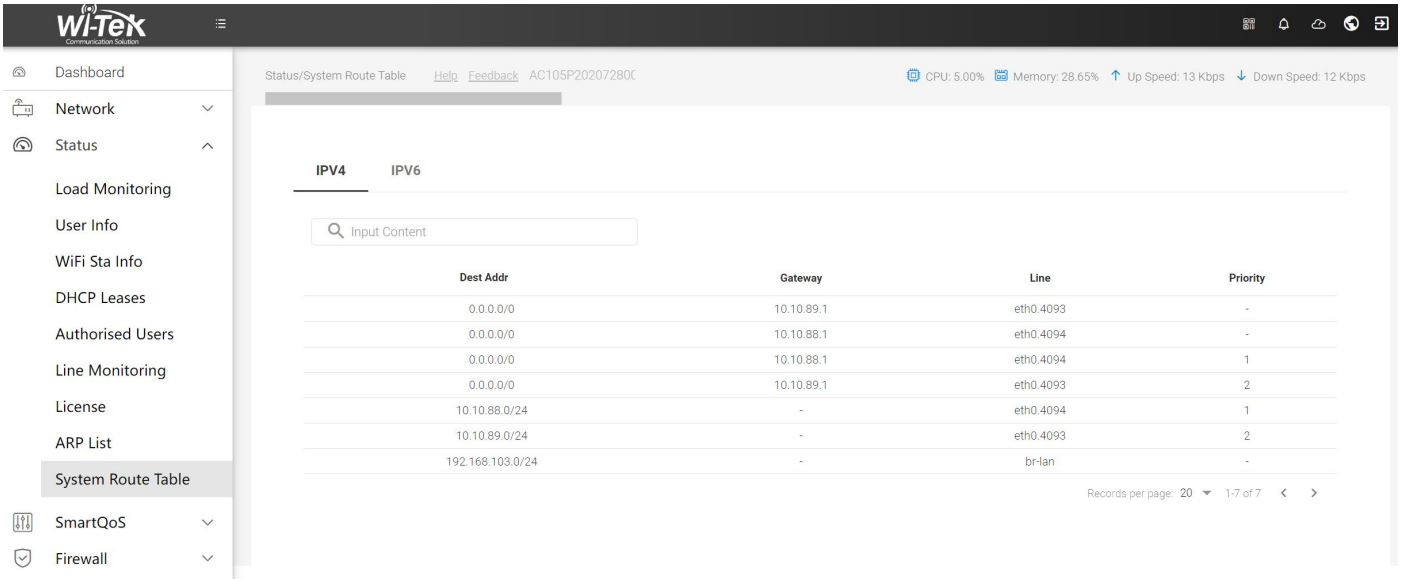


Select the entry and click the **ADD TO DHCP BINDING TABLE** button to add static DHCP list.



5.9. System Route Table

Choose the menu **Status** > **System Route Table** to load the following page.



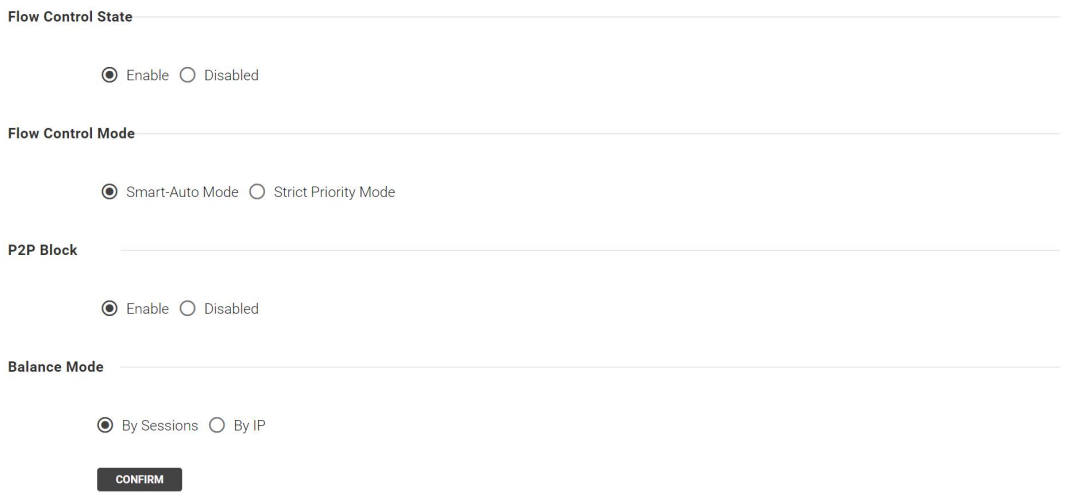
Parameter	Describe
Dest Addr	Specify the destination IP address the route leads to.
Gateway	Specify the IP address to which the packet should be sent next.
Line	Specify the physical network interface through which this route is accessible.
Priority	Define the priority of the route. A smaller value means a higher priority.

6. Smart QoS

6.1. Qos Configuration

Enabling QoS functionality can improve service quality in situations where WAN bandwidth resources are small and there are a large number of users. Intelligent QoS is Automatically adjust usage priority based on traffic usage. The more forwarded traffic, the lower the priority.

Choose the menu **SmartQoS** > **QoS Configuration** to load the following page.

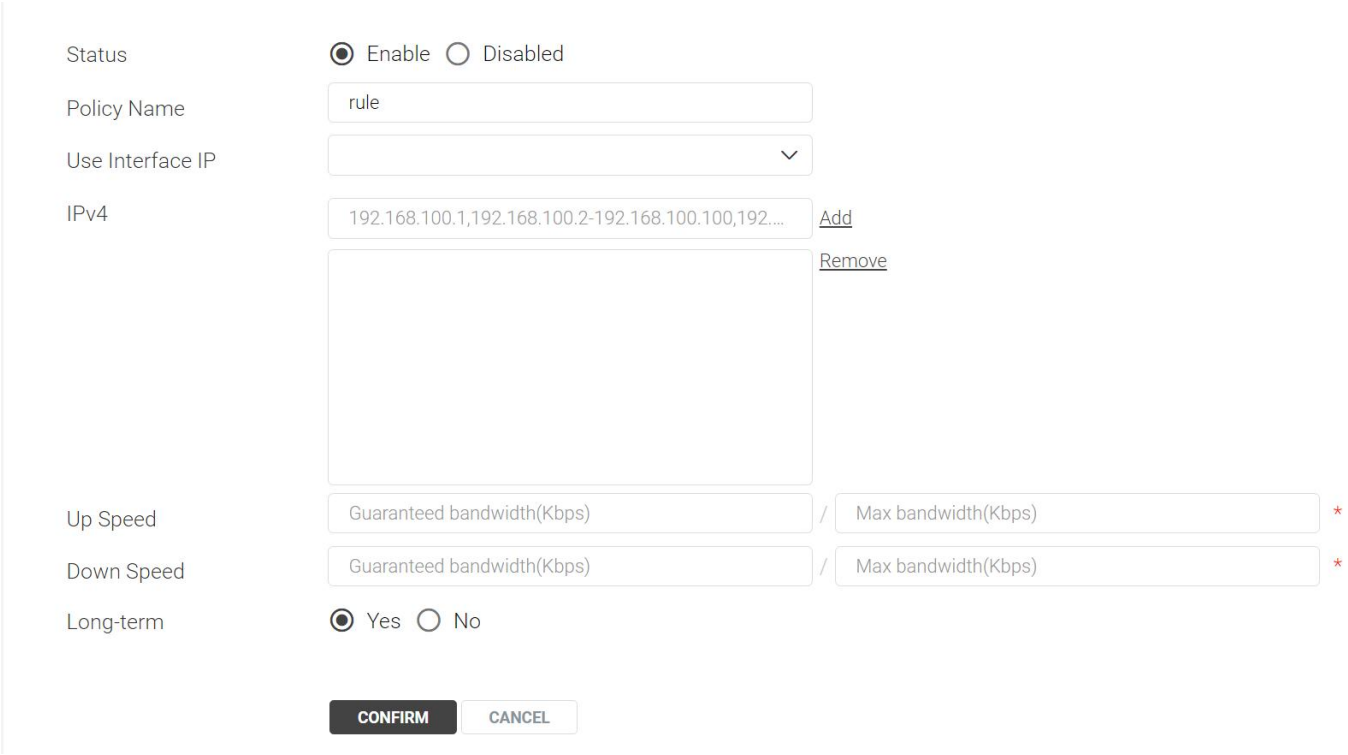


Parameter	Describe
Flow Control State	Enabling or disabling the Smart QoS feature.
Flow Control Mode	Smart-Auto Mode:For application scenarios with low bandwidth and high concurrency requirements. Strict Priority Mode: For application scenarios with low bandwidth, high concurrency, and low latency requirements.
P2P Block	Enable or disable P2P blocking.
Balance Mode	When the gateway is connected to multiple WANs, within the default balance group, select **by session** type will allocate sessions based on weight.Select **by IP** mode, and it will be assigned sequentially.

6.2. Flow Control

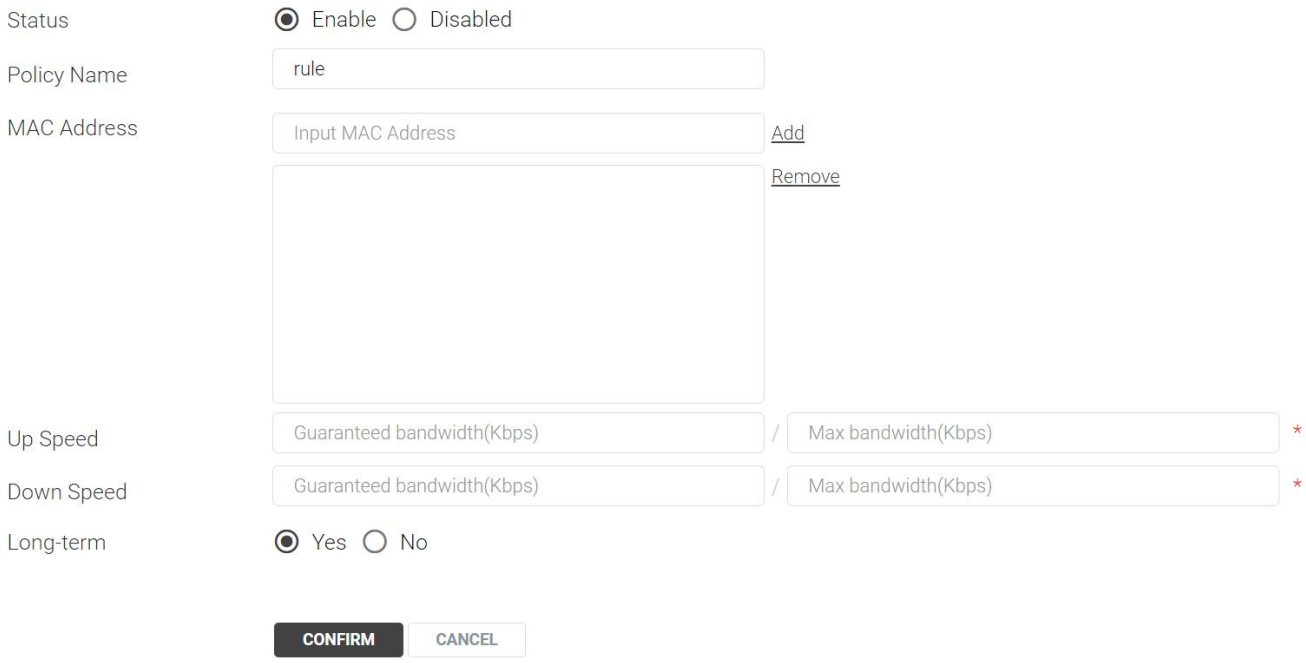
You can control uplink and downlink bandwidth for IP or IP range.

Choose the menu **Flow Control > Flow Control > IP-BASED** and click **ADD** to load the following page.



Parameter	Describe
Status	Enable or disable rules.
Policy Name	Specify a name for easy identification.
Use Interface IP	Specify the Interface for the rule to define the controlled users.
IPv4	Specify the IP address for the rule to define the controlled users.
Up Speed	Specify the Upstream Bandwidth in Kbps for the rule.
Down Speed	Specify the Downstream Bandwidth in Kbps for the rule.
Long-term	Specify the time for the rule to take effect.

Choose the menu **Flow Control > Flow Control > MAC-BASED** and click **ADD** to load the following page.

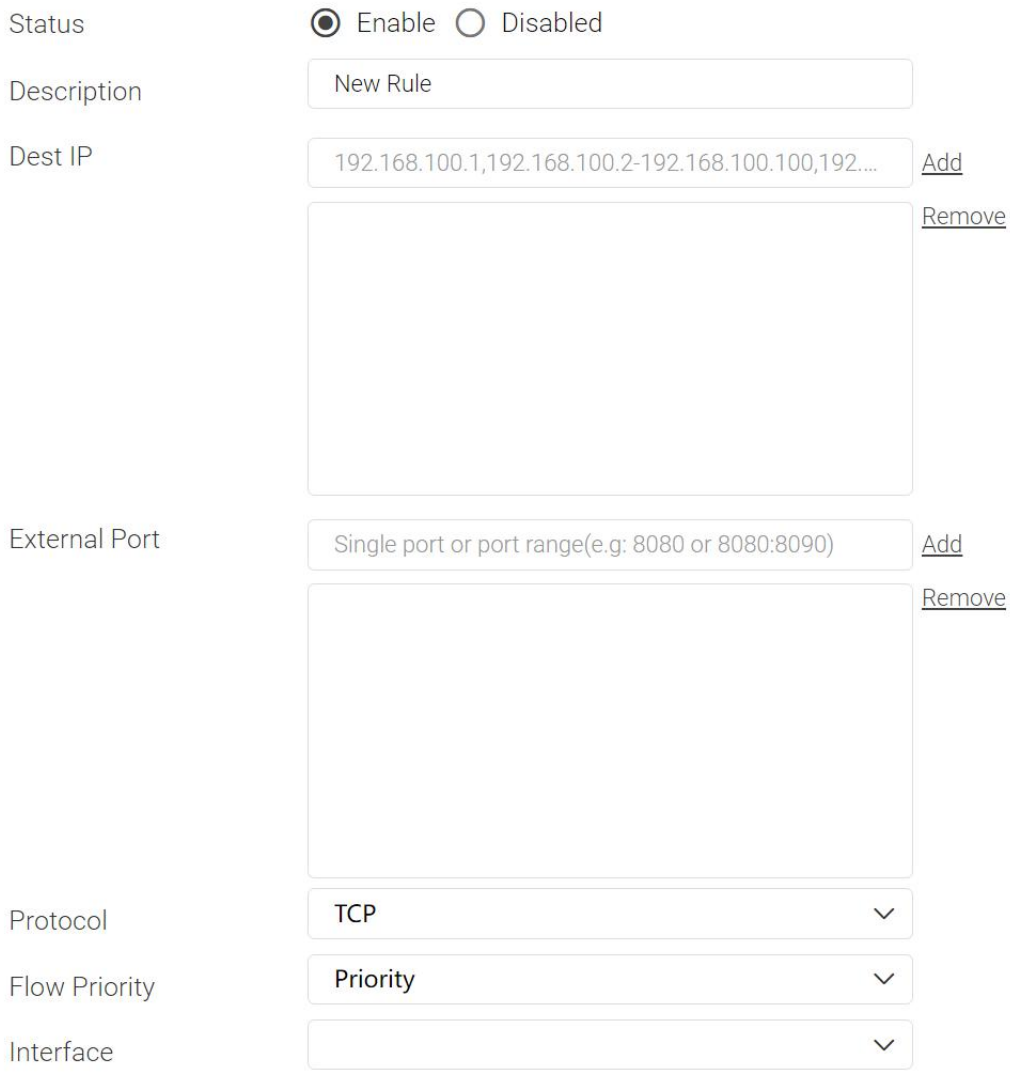


Parameter	Describe
Status	Specify the bandwidth control enable or disabled for rule.
Policy Name	Specify a name for easy identification.
Use Interface IP	Specify the Interface for the rule to define the controlled users.
IPv4	Specify the IP address for the rule to define the controlled users.
Up Speed	Specify the Upstream Bandwidth in Kbps for the rule.
Down Speed	Specify the Downstream Bandwidth in Kbps for the rule.
Long-term	Specify the time for the rule to take effect.

6.3. Port Route

You can create port based policy routing here.

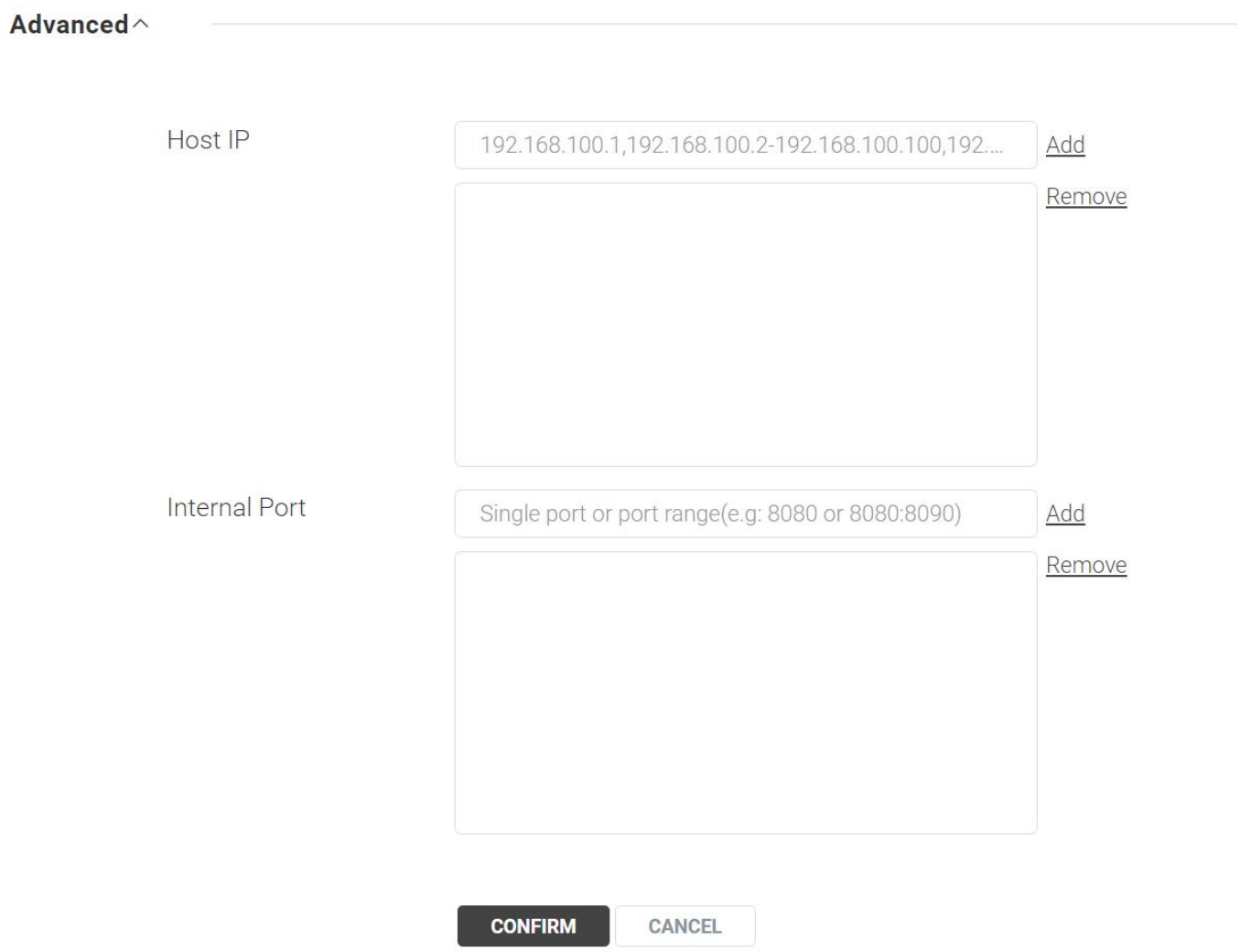
Choose the menu **SmartQoS** > **Port Route** and click **ADD** to load the following page.



Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Dest IP	Specify the destination IP or IP range for the rule.
External Port	Specify the destination port or port range for the rule.
Protocol	Specify the protocol for the rule.

Flow Priority	Specify Priority for the rule.
Interface	Specify the effective port for the rule.

Then click on the **advanced** button to load the following page.

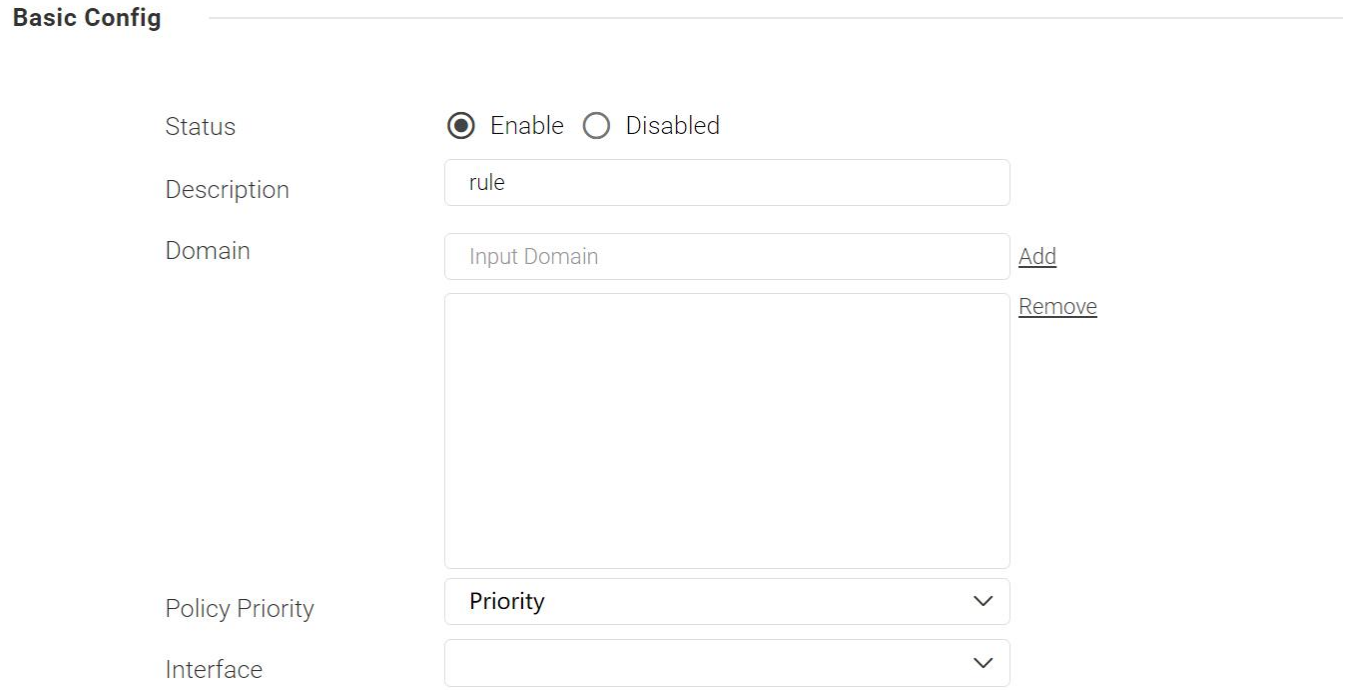


Parameter	Describe
Host IP	Specify the source IP or IP range for the rule.
Internal Port	Specify the source port or port range for the rule.

6.4. Domain Route

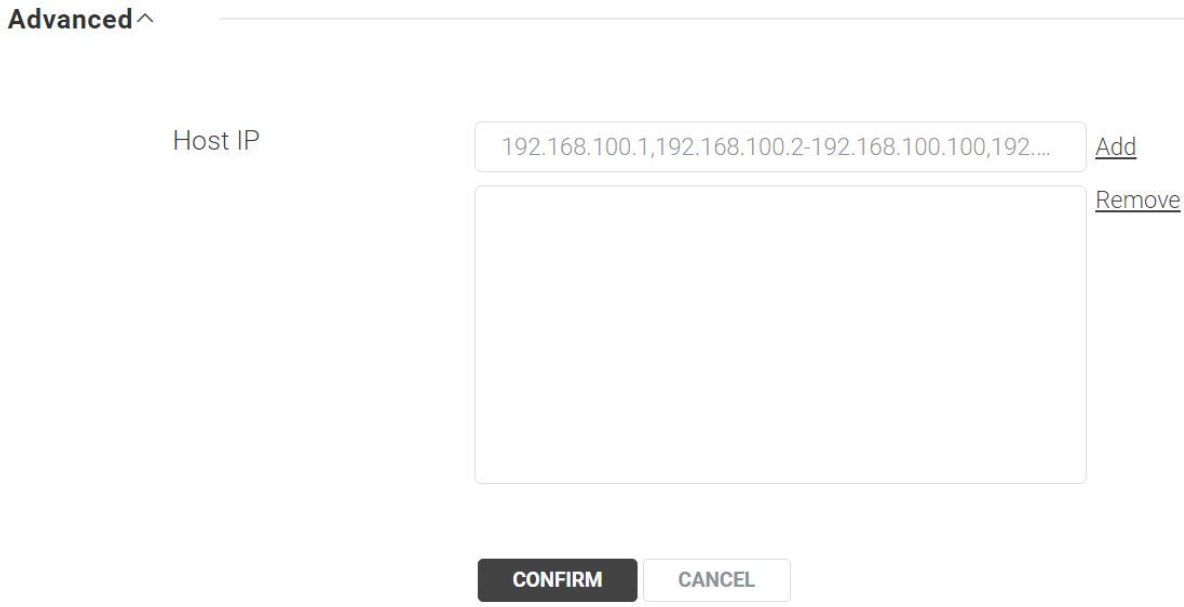
You can create domain based policy routing here.

Choose the menu **SmartQos** > **Domain Route** and click **ADD** to load the following page.



Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Domain	Specify the destination domain for the rule. Note: Support domain format, for example: www.xxxx.com.
Policy Priority	Specify Priority for the rule.
Interface	Specify the effective port for the rule.

Then click on the **advanced** button to load the following page.

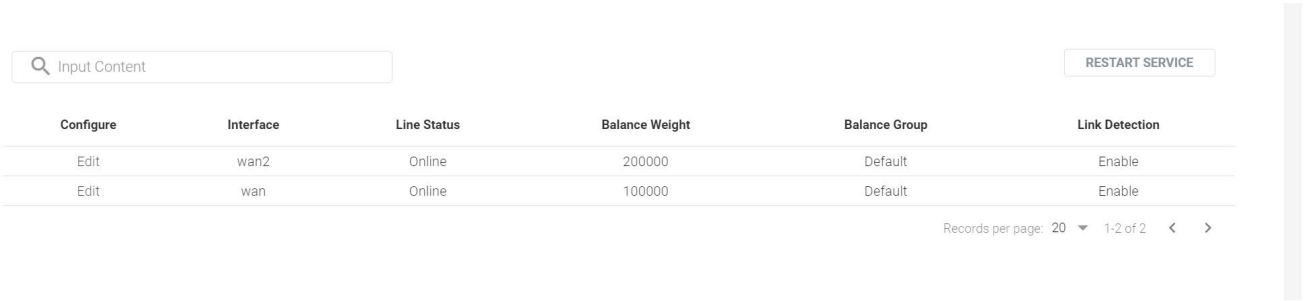


Parameter	Describe
Host IP	Specify the source IP or IP range for the rule.

6.5. Load Balance

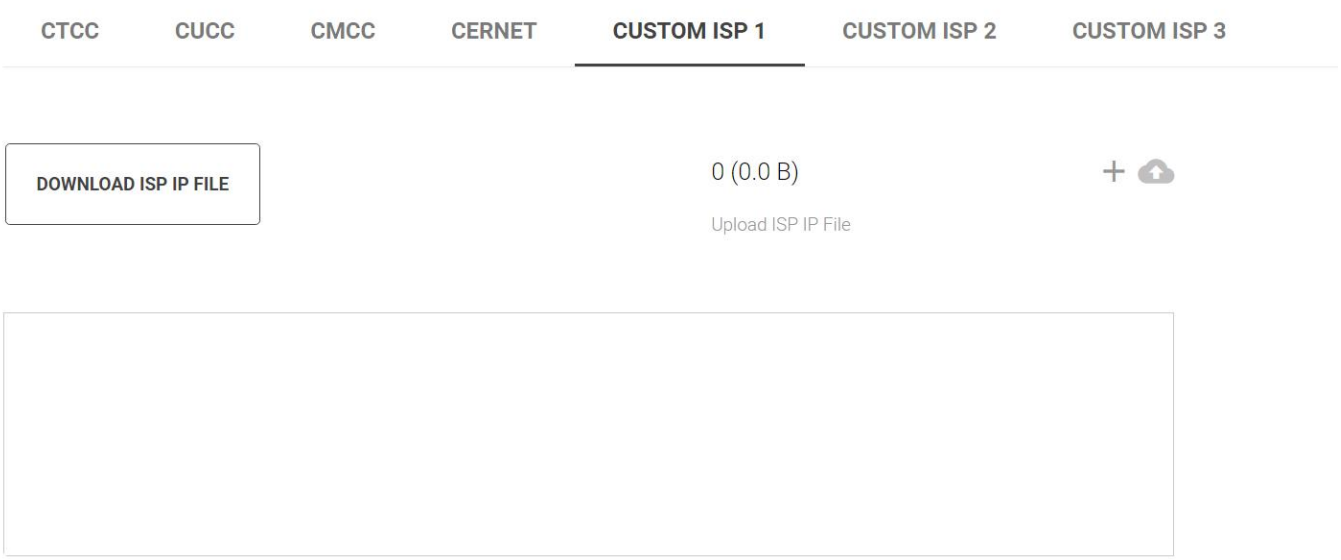
You can manually modify the balance ratio of WAN lines.

Choose the menu **SmartQos > Load Balance** to load the following page.



6.6. ISP Segment

If you can collect IP addresses used by different ISPs, generate an IP file in a format and upload it, combined with the policy routing function.

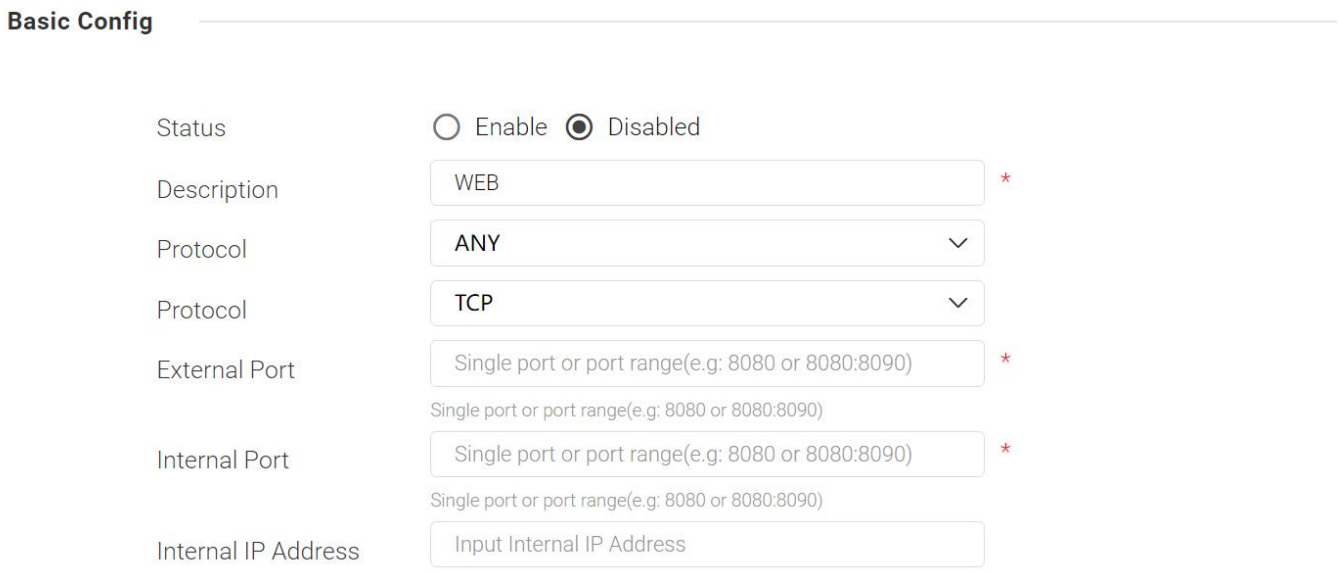


7. Firewall

7.1. Port Mapping

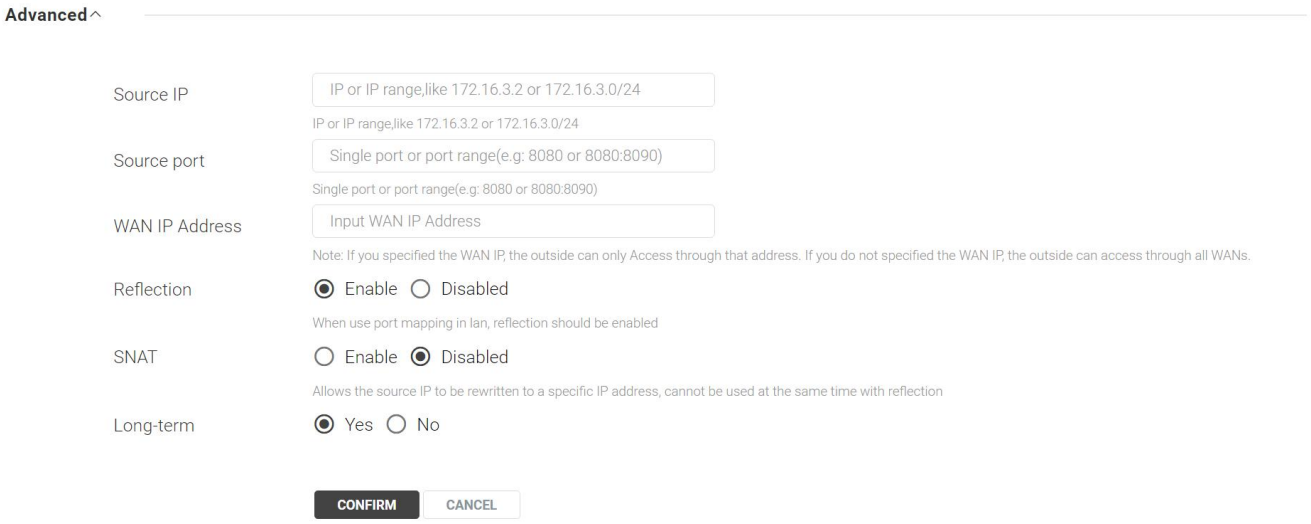
Port mapping allows extranet access to a intranet server (such as to a WWW server or FT P server on an extranet). The private IP address and service port of an intranet server are mapped into a public IP address and port, so that users from the extranet can access the i ntranet server. With port mapping, the public IP address but not the private IP address is vi sible to the users.

Choose the menu **Firewall** > **Port Mapping** and click ADD to load the following page.



Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Protocol	Specify the trigger protocol for the trigger port.
External Port	Specify a port range used by extranet users to access the intranet server.
Internal Port	Specify the port or port range used by the Internal Services.
Internal IP Address	Specify the IP address of the intranet server.

Then click on the **advanced** button to load the following page.

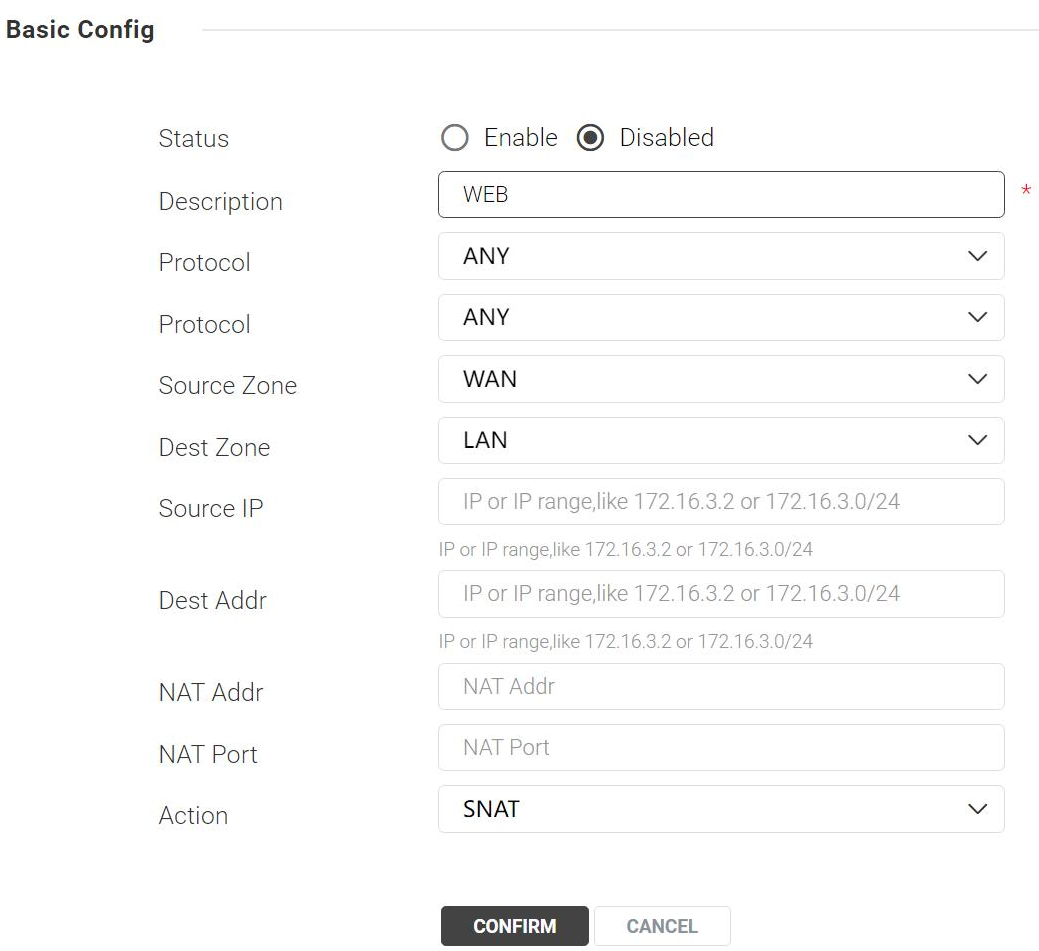


Parameter	Describe
Source IP	Specify the source IP input range.
Source port	Specify the source port input range.
WAN IP Address	If you specified the WAN IP, the outside can only Access through that address. If you do not specified the WAN IP, the outside can access through all WANs.
Reflecion	When use port mapping in lan, reflection should be enabled.
SNAT	Allows the source IP to be rewritten to a specific IP address, cannot be used at the same time with reflection.
Long-term	Specify the effective time of this rule.

7.2. NAT

Network Address Translation generally involves "re-writing the source and/or destination addr esses of IP packets as they pass through a router or firewall".

Choose the menu **Firewall** > **NAT** and click **ADD** to load the following page.



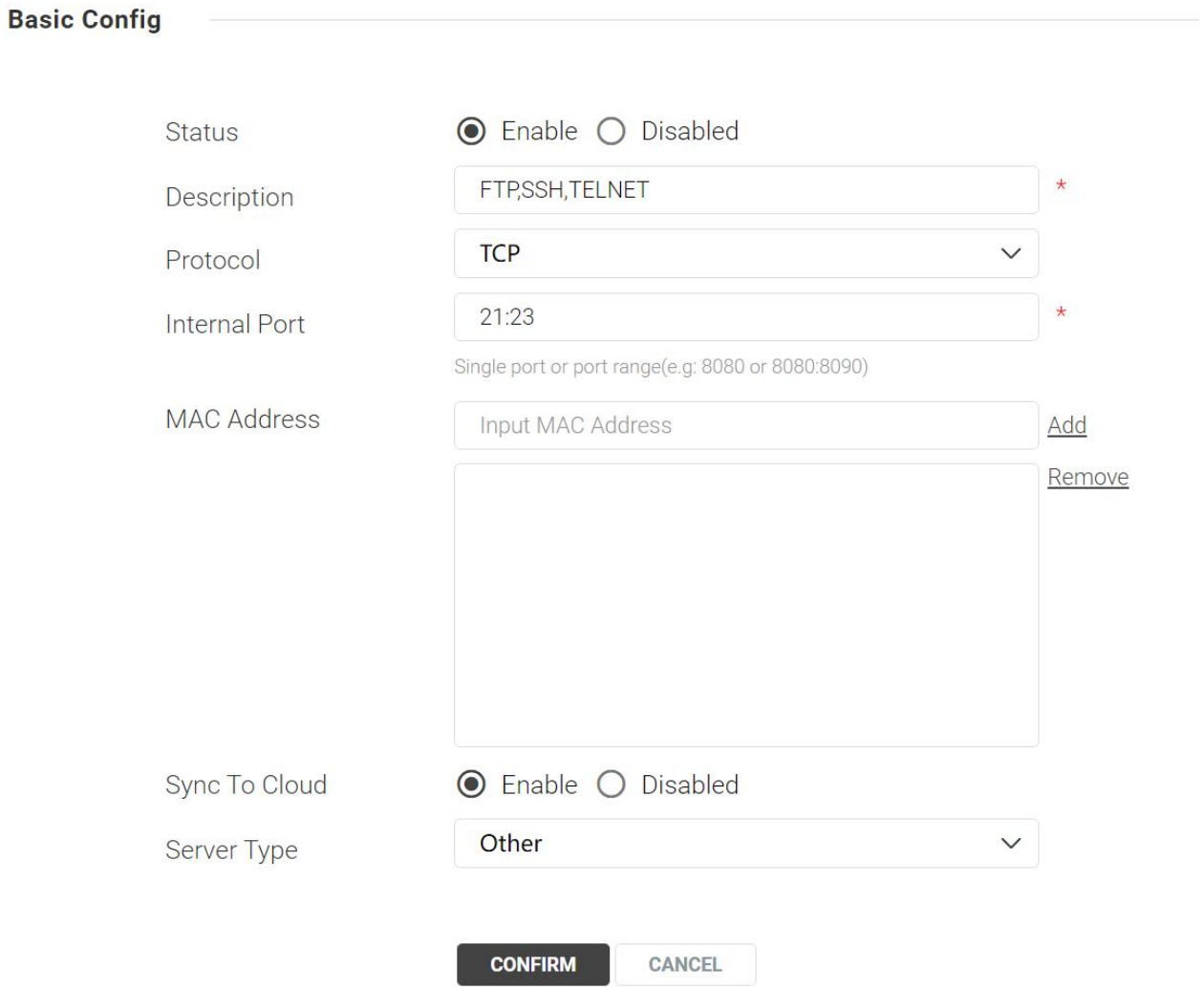
Parameter	Describe
Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Protocol	Specify the trigger protocol for the trigger port.
Source Zone	Specifies the traffic source zone(ROUTER, LAN or WAN).
Dest Zone	Specifies the traffic destination zone(ROUTER, LAN or WAN).
Source IP	Specifies the traffic source IP (IP or IP Range).

Dest Addr	Specifies the traffic Dest Addr (IP or IP Range).
NAT Addr	For SNAT rewrite the source address to the given address.For DNAT, match incoming traffic directed at the given destination ip address.
NAT Port	For SNAT, match traffic directed at the given ports.For DNAT, redirect matched incoming traffic to the given port on the internal host.
Action	NAT target (DNAT or SNAT) to use when generating the rule.

7.3. Host Mapping

Using IPv6 for internal networks,when the host IPv6 address changes, the host MAC addre ss can be used as a condition for open internal services.

Choose the menu **Firewall** > **Host Mapping** and click **ADD** to load the following page.



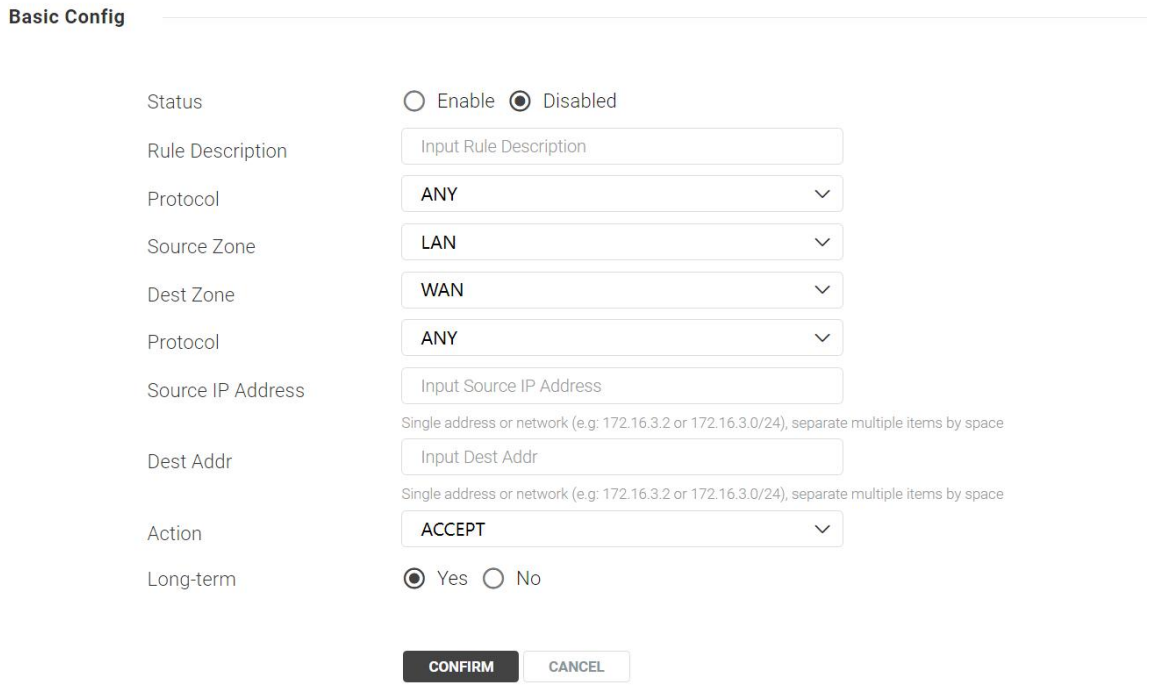
Parameter	Describe

Status	Enable or disable this rule.
Description	Specify a name for easy identification.
Protocol	Specify the trigger protocol for the trigger port.
Internal Port	Matching and mapping internal port of internal network hosts
MAC Address	Matching and mapping MAC addresses of internal network hosts.
Sync To Cloud	the latest IPv6 address of servers can be seen through cloud platform or wx-app.
Server Type	Server Type (WWW, FTP, Email or SNAT) to use when generating the rule.

7.4. Access Control List

Access control lists (ACLs) can control the traffic entering a network. When you configure ACLs, you can selectively admit or reject inbound traffic, thereby controlling access to your network or to specific resources on your network.

Choose the menu **Firewall** > **Access Control List** and click **ADD** to load the following page.



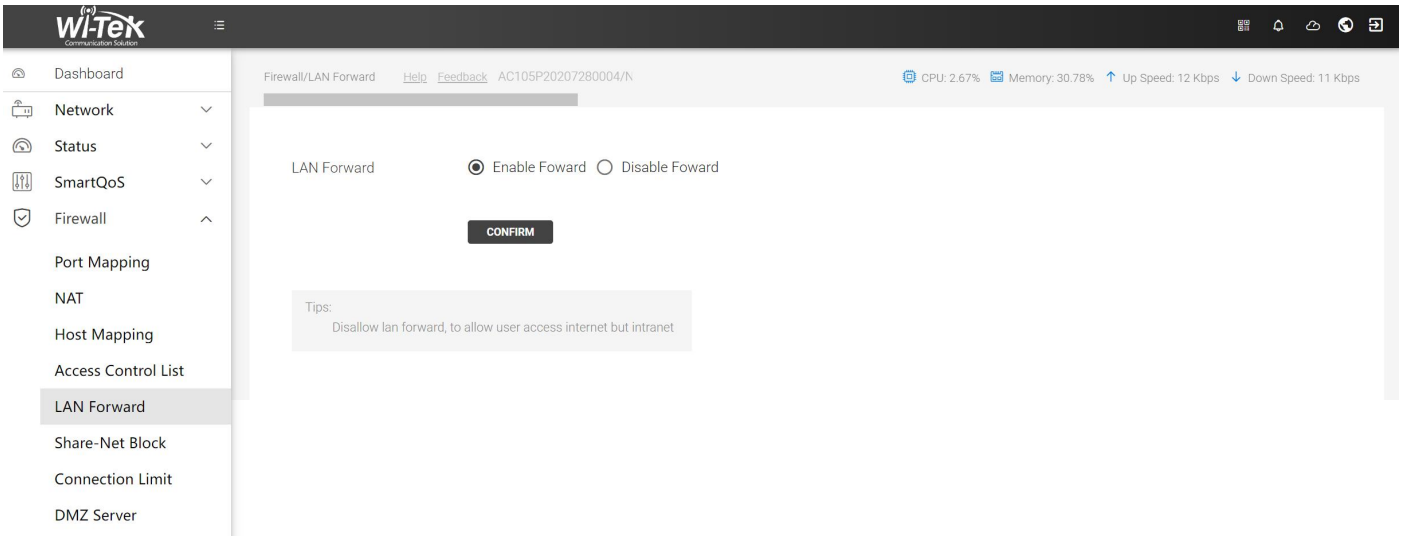
Parameter	Describe

Status	Enable or disable this rule.
Rule Description	Specify a name for easy identification.
Protocol	Protocol family (ipv4, ipv6 or any) to generate ACL rules for.
Source Zone	Specifies the traffic source zone(ROUTER, LAN or WAN).
Dest Zone	Specifies the traffic destination zone(ROUTER, LAN or WAN).
Protocol	Protocol family (TCP, UDP, ICMP or any) to generate ACL rules for.
Source IP Address	Specifies the traffic source IP (IP or IP Range).
Dest Addr	Specifies the traffic Dest Addr (IP or IP Range).
Action	ACL target (ACCEPT, REJECT, DROP) to use when generating the rule.
Long-term	Specify the effective time of this rule.

7.5. LAN Forward

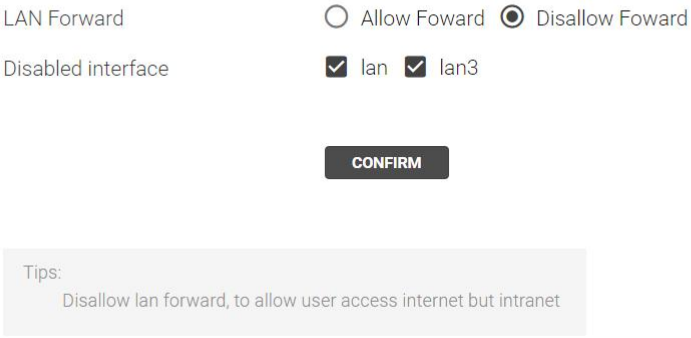
You can block inter LAN access with just one click, and the default is to allow forwarding b etween LANs.

Choose the menu **Firewall** > **LAN Forward** to load the following page.



If you set up multiple subnets in the gateway and select the Disable Forward option, the fol lowing page will be loaded.

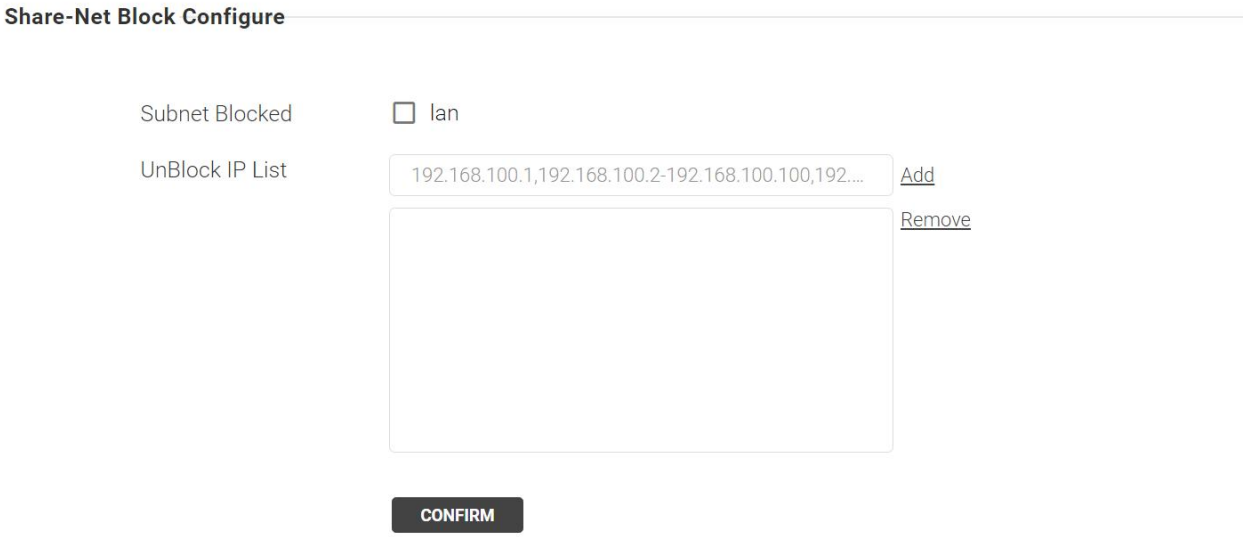
Select the **Disallow Forward** button and check the blocked subnet.



7.6. Share-Net Block

You can prevent the secondary router from accessing the internet.

Choose the menu **Firewall** > **Share-Net Block** to load the following page.

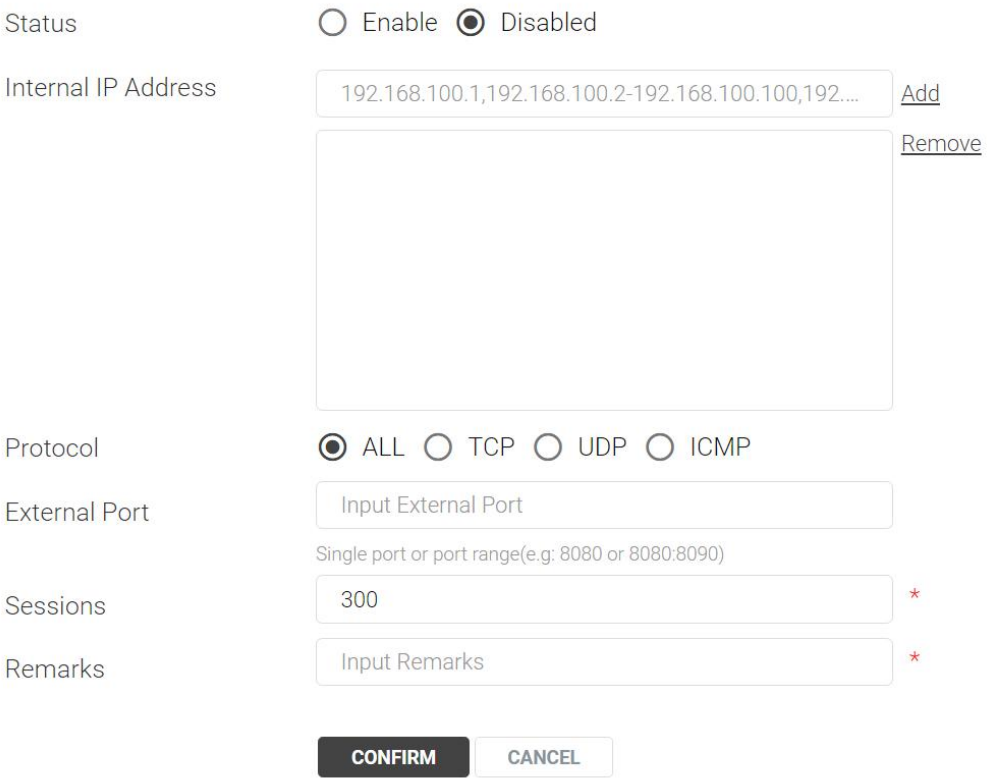


Parameter	Describe
Subnet Blocked	Select it, the secondary router under this subnet cannot access the internet.
Unblock IP List	Unblock IP or IP range.

7.7. Connection Limit

Session Limit feature allows Network Administrator to limit the number of sessions that a LAN client can use. This feature will prevent the router's resources from being occupied by a single host, especially who are downloading using P2P software.

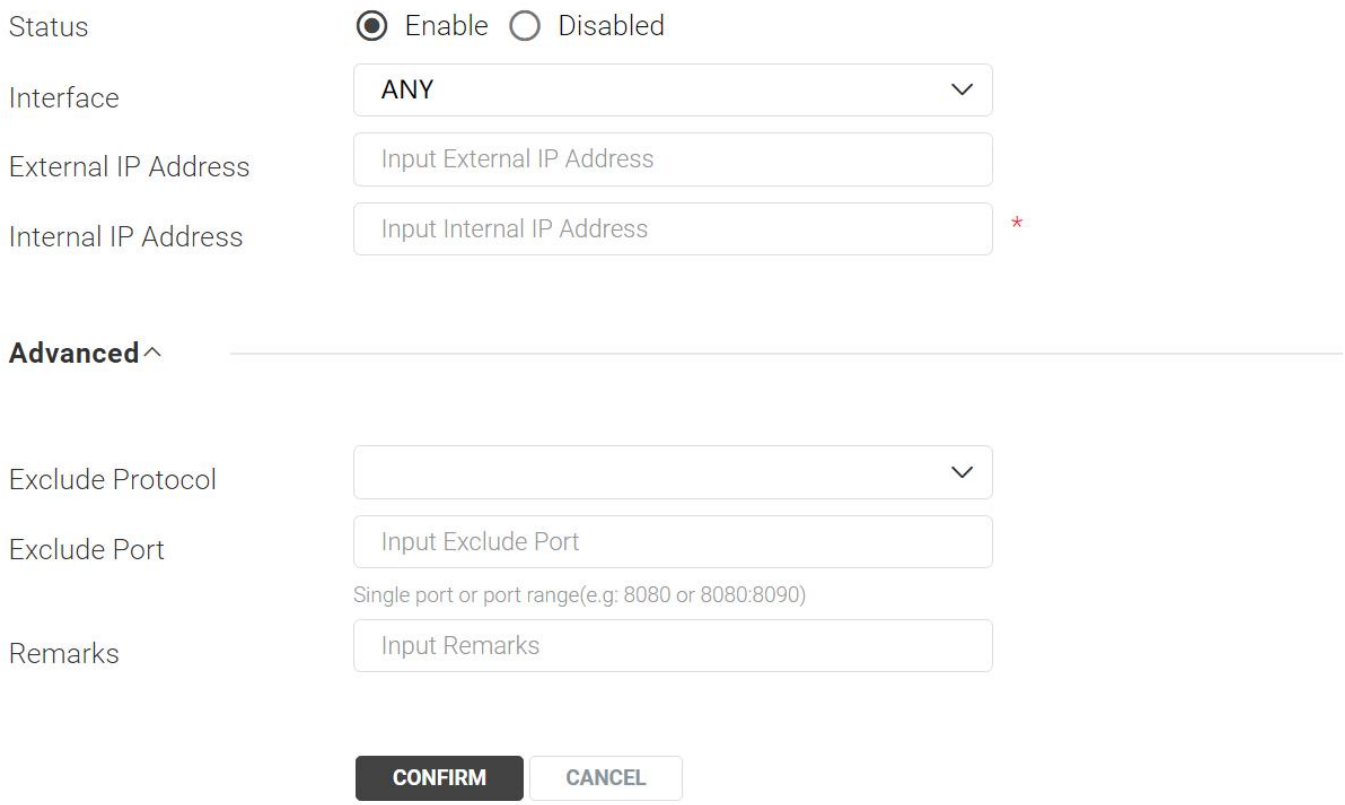
Choose the menu **Firewall** > **Connection Limit** and click **ADD** to load the following page.



Parameter	Describe
Status	Enable or disable this rule.
Internal IP Address	Restrict sessions for IP
Protocol	Select protocol type for the rules.
External Port	Restrict sessions for external port,
Sessions	Specify the max sessions for the IP
Remarks	Specify a name for easy identification.

7.8. DMZ Server

Choose the menu **Firewall** > **DMZ Server** and click ADD to load the following page.

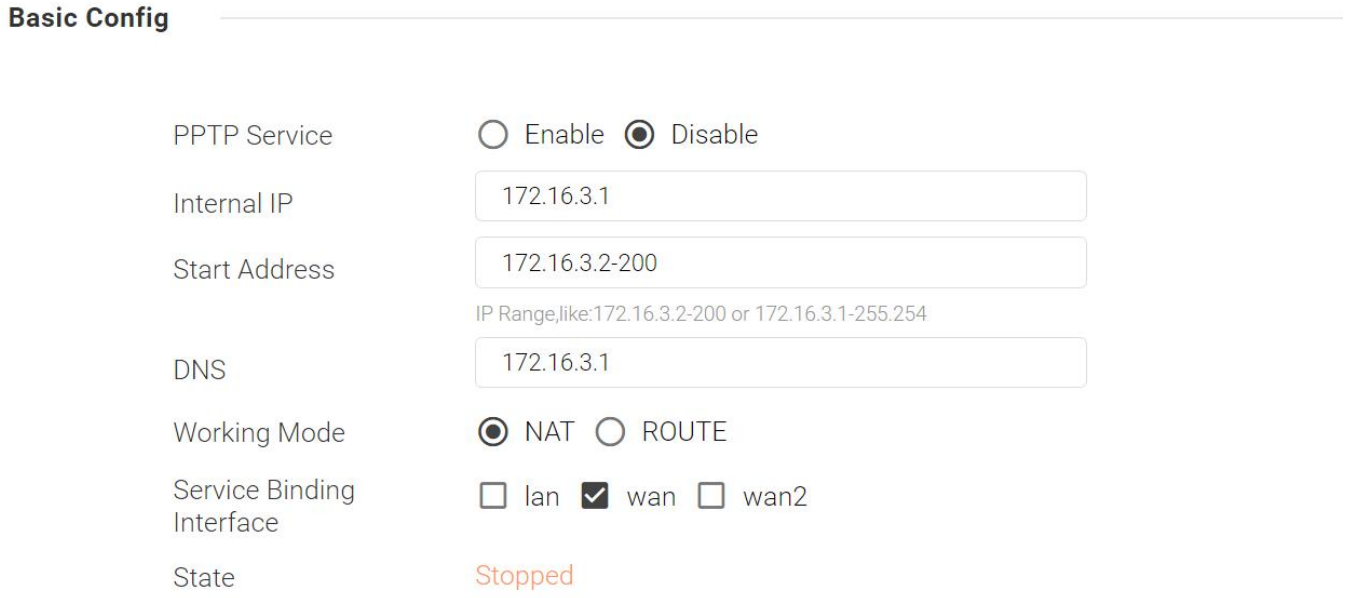


Parameter	Describe
Status	Enable or disable this rule.
Interface	Specify the effective interface for the rule.
External IP Address	If you choose Any, you need to specify the WAN port public IP address.
Internal IP Address	Enter the IP address of the host specified as DMZ server.
Exclude Protocol	Exclude protocol not participating in DMZ services
Exclude Port	Exclude ports from participating in DMZ services
Remarks	Specify a name for easy identification.

8. VPN Server

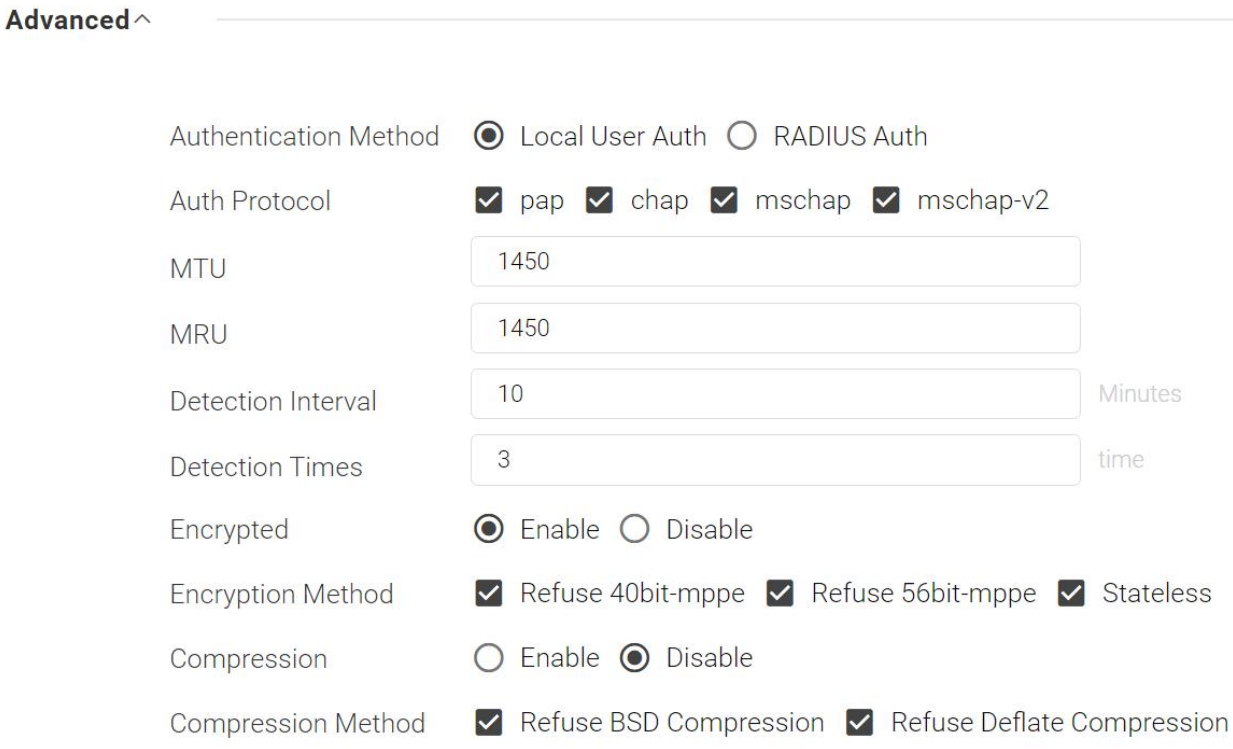
8.1. PPTP Service

Choose the menu **VPN Server > PPTP Service** to load the following page.



Parameter	Describe
PPTP Server	Enable or disable this rule.
Internal IP	Local IP of VPN tunnel (Cannot conflict with other subnets)
Start Address	IP pool assigned for VPN clients.
DNS	Provide DNS resolution for PPTP clients.
Working Mode	Traffic forwarding mode.
Service Binding Interface	Specify the WAN port used for PPTP tunnel.

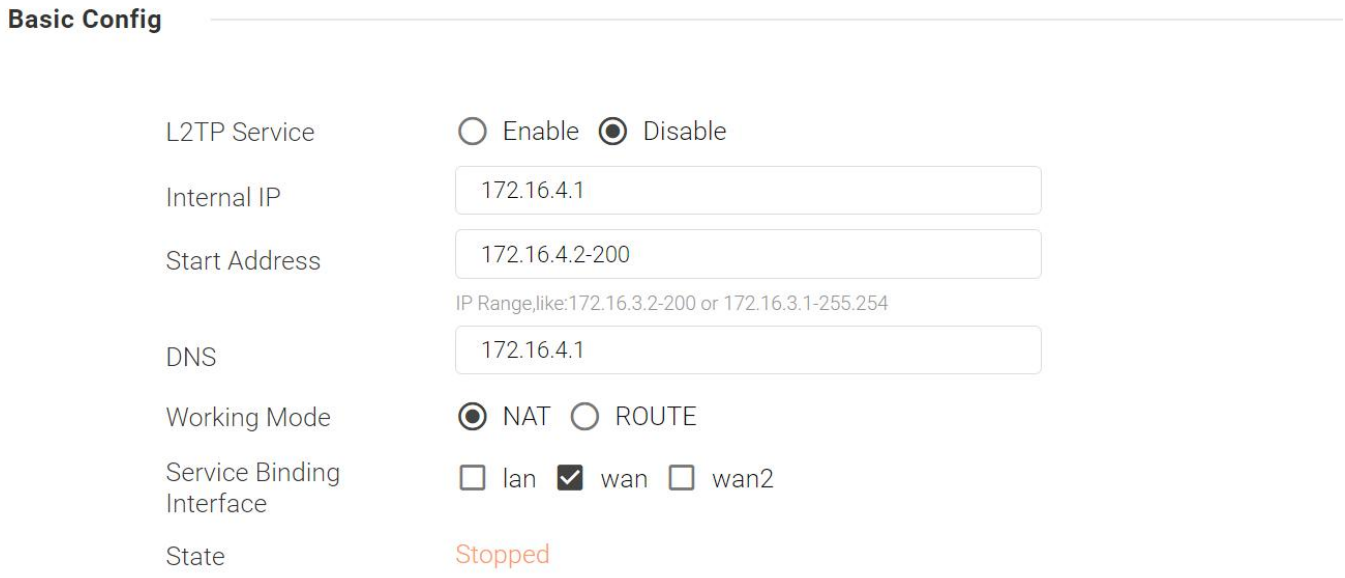
Then click on the **advanced** button to load the following page.



Parameter	Describe
Authentication Method	Authentication method that server will accept.
Auth Protocol	Authentication protocol that server will accept.
MTU	Maximum Transmission Unit.You can keep the default value for this setting.
MRU	Maximum Receive Unit.You can keep the default value for this setting.
Detection Interval	Detect VPN tunnel “heartbeat ”time interval.The default value is 600 seconds.
Detection Times	Detect VPN tunnel “heartbeat ”count. The default value is 3.
Encrypted	Provide encryption for VPN tunnels.The default is enabled.
Encryption Method	Specify tunnel encryption type.
Compression	Provide compression types for data.
Compression Method	Specify compression method.

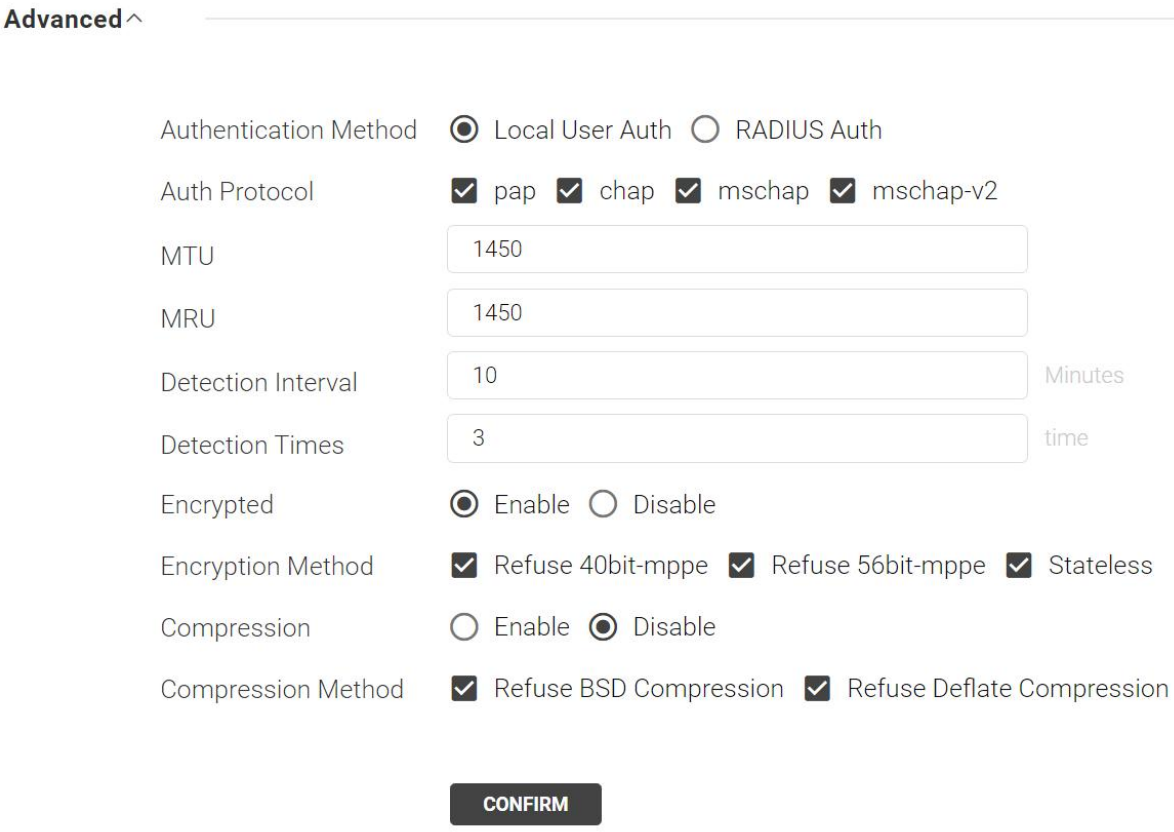
8.2. L2TP Service

Choose the menu **VPN Server > L2TP Service** to load the following page.



Parameter	Describe
L2TP Server	Enable or disable this rule.
Internal IP	Local IP of VPN tunnel (Cannot conflict with other subnets)
Start Address	IP pool assigned for VPN clients.
DNS	Provide DNS resolution for PPTP clients.
Working Mode	Traffic forwarding mode.
Service Binding Interface	Specify the WAN port used for L2TP tunnel.

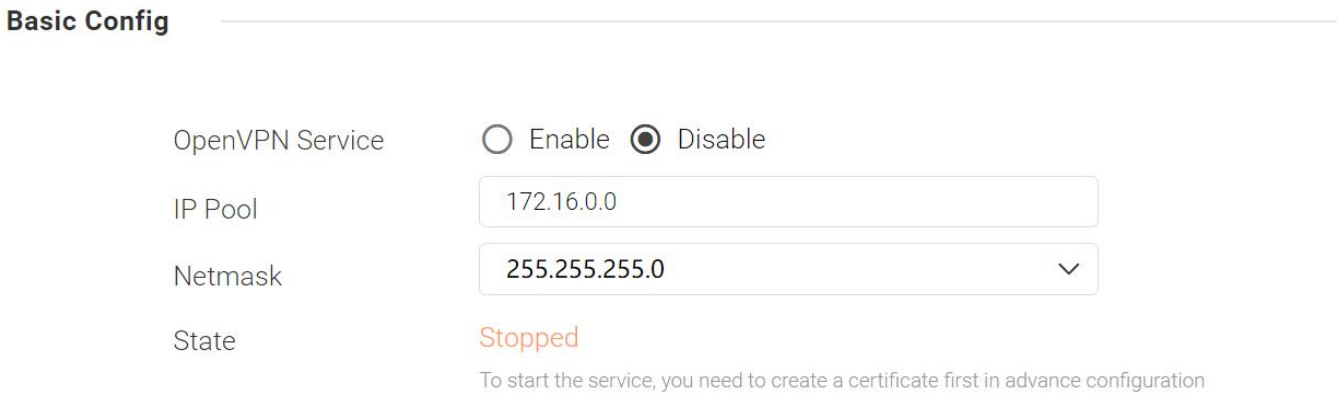
Then click on the **advanced** button to load the following page.



Parameter	Describe
Authentication Method	Authentication method that server will accept.
Auth Protocol	Authentication protocol that server will accept.
MTU	Maximum Transmission Unit.You can keep the default value for this setting.
MRU	Maximum Receive Unit.You can keep the default value for this setting.
Detection Interval	Detect VPN tunnel “heartbeat ”time interval.The default value is 600 seconds.
Detection Times	Detect VPN tunnel “heartbeat ”count. The default value is 3.
Encrypted	Provide encryption for VPN tunnels.The default is enabled.
Encryption Method	Specify tunnel encryption type.
Compression	Provide compression types for data.
Compression Method	Specify compression method.

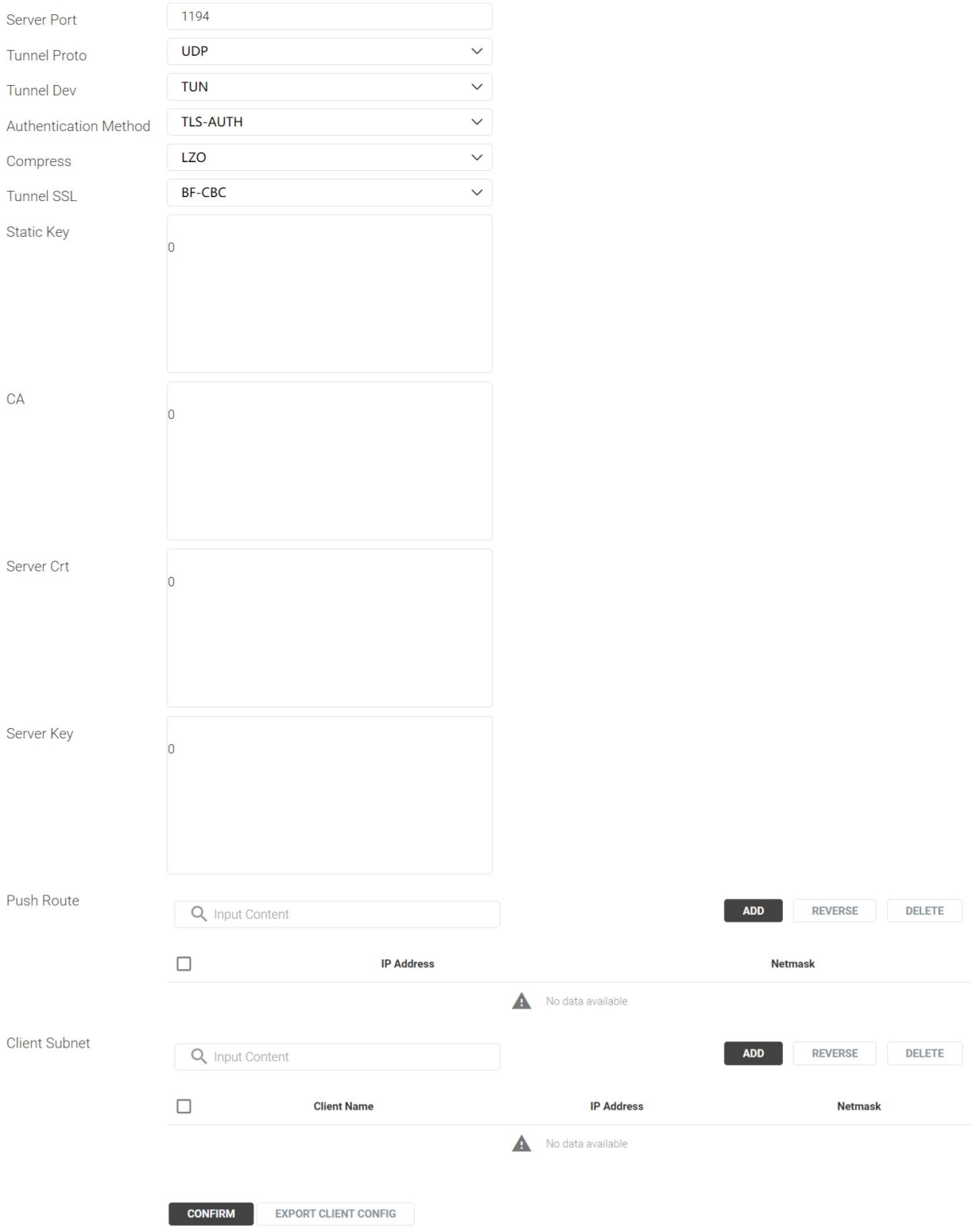
8.3. OpenVPN Service

Choose the menu **VPN Server > OpenVPN Service** to load the following page.



Parameter	Describe
OpenVPN Server	Enable or disable this rule.
IP Pool	IP pool assigned for VPN clients.
Netmask	Specify IP subnet range.

Then click on the **advanced** button to load the following page.



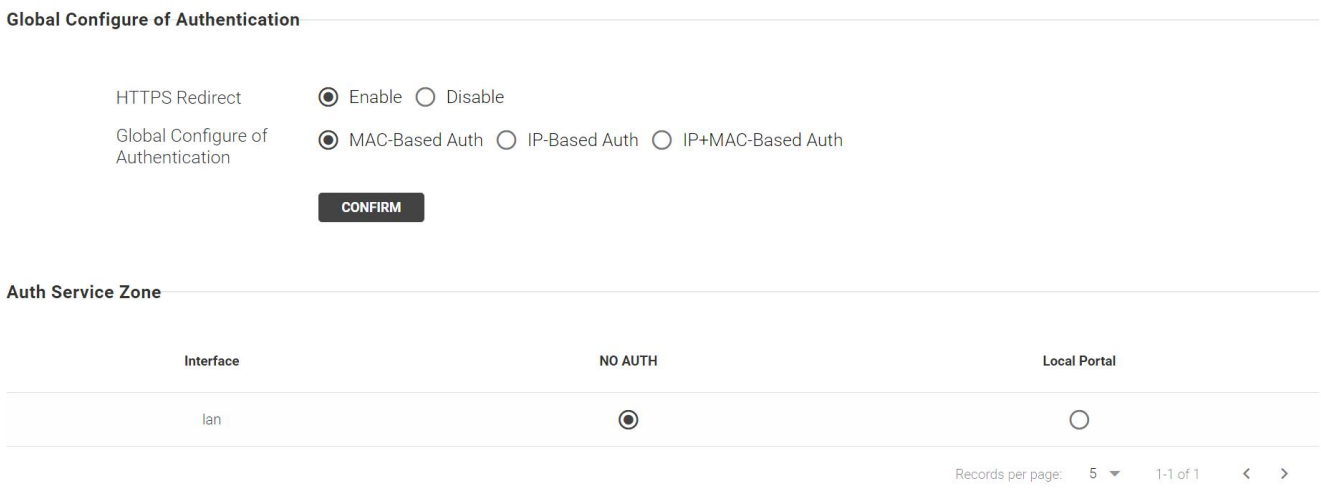
Parameter	Describe
Server Port	Specify UDP port number.
Tunnel Proto	Specify Tunnel protocol.
Tunnel Dev	Support TAP and TUN mode, TAP is similar to bridge mode, TUN is similar to routing mode, and the selection of client and server should be consistent.

Authentication Method	TLS_AUTH and TLA_CRYPY are supported. Make sure the server and client choose the same.
Compress	A data compression algorithm that supports LZO and LZ4 modes.Make sure the server and client choose the same.
Tunnel SSL	Specify the encryption algorithm type.Make sure the server and client choose the same.
Static Key	Gateway-generated or third-party certificate source. You can jump to the following page to generate a certificate **System**>**CA Configuration** Page
CA	
Server Crt	
Server Key	
Push Route	Allow the server-side to push routes to the client-side, enabling the client side subnet to access the service side subnet.
Client Subnet	Add a client-side subnet to the server-side, enabling server-side subnet access to the client-side subnet.
EXPORT CLIENT CONFIG	If the computer is running Open VPN software, download the configuration with one click and directly import the file, then achieve remote connection.

9. Hotspot

9.1. Service Zone

Choose the menu **HotSpot** > **Service Zone** to load the following page.



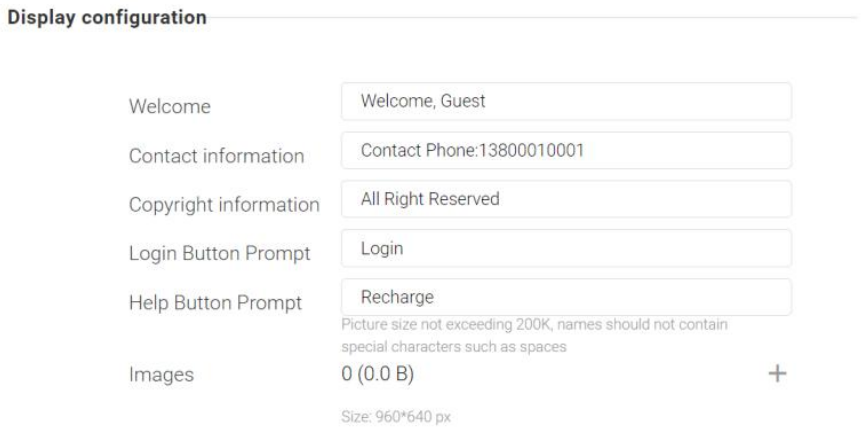
Parameter	Describe
HTTPS Redirect	Enable or disable HTTPS redirec.
Global Configure of Authentication	Select HTTPS redirect trigger condition.

In the **Auth Service Zone**, you will be able to select subnets that participate in authenticati on.

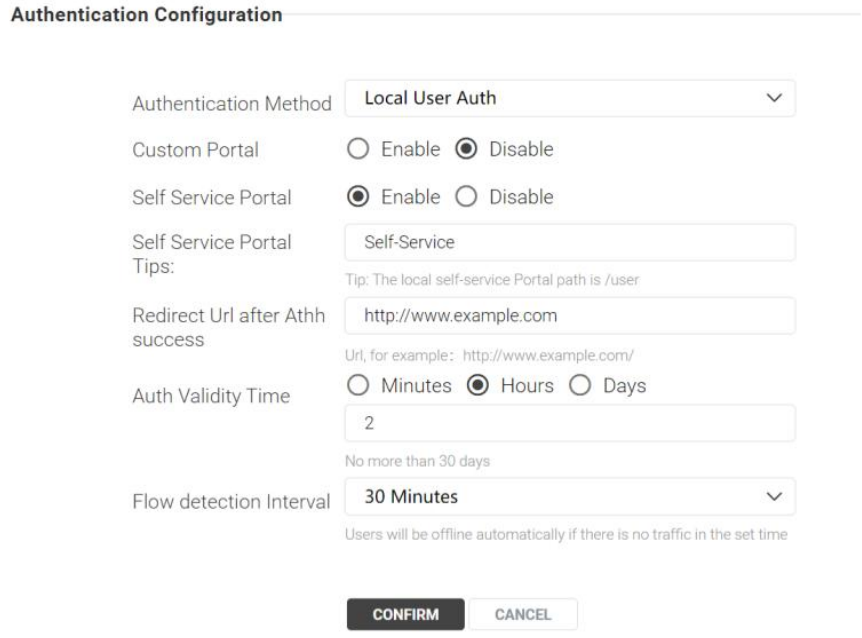
9.2. Local Portal

Choose the menu **HotSpot > Local Portal** to load the following page.

In the **Display configuration** area, follow the prompts to set the text and image for the log in page.



In the **Authentication Configuration** area, you will be able to set the authentication type.

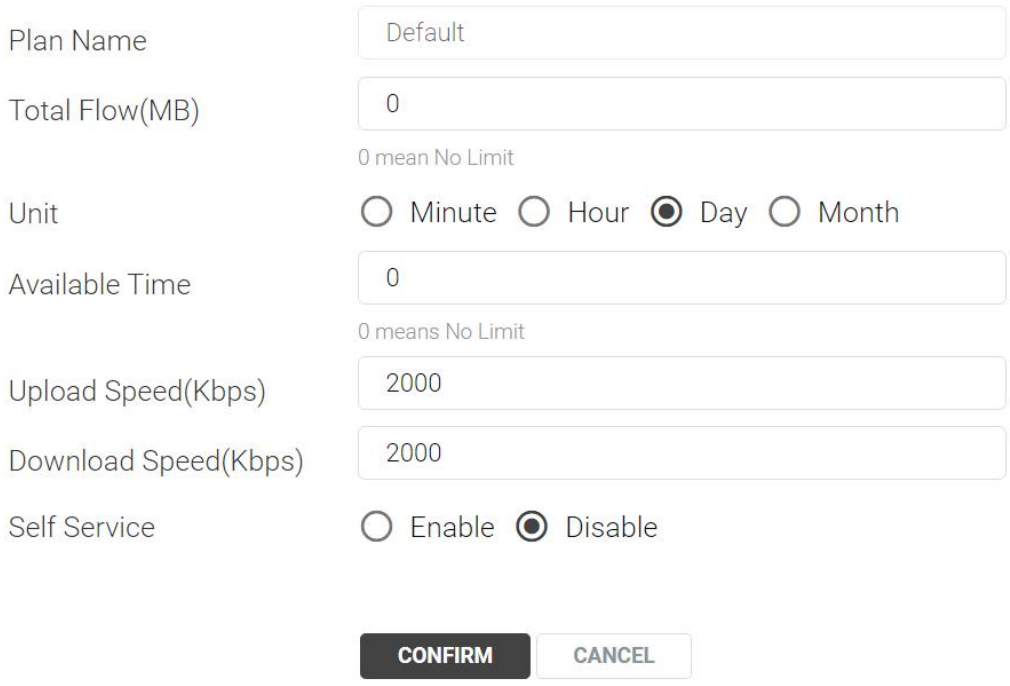


Parameter	Describe
Authentication Method	Select the authentication type from the dropdown option.
Custom Portal	Upload the designed login page file.
Self Service Portal	Enable it and the recharge button will appear on the login page.
Self Service Portal Tips	Enter a prompt and it will display the self-service login page.
Redirect Url after Athh success	Redirected address after successful authentication.
Auth Validity Time	Authentication is required after the preset time.
Flow detection Interval	Users will be offline automatically if there is no traffic in the set tim

9.3. Biling Plan

The billing plan prepares for user authentication and implements batch restrictions on the tr affic of locally authenticated users.

Choose the menu **HotSpot** > **Billing Plan** and click **ADD** to load the following page.

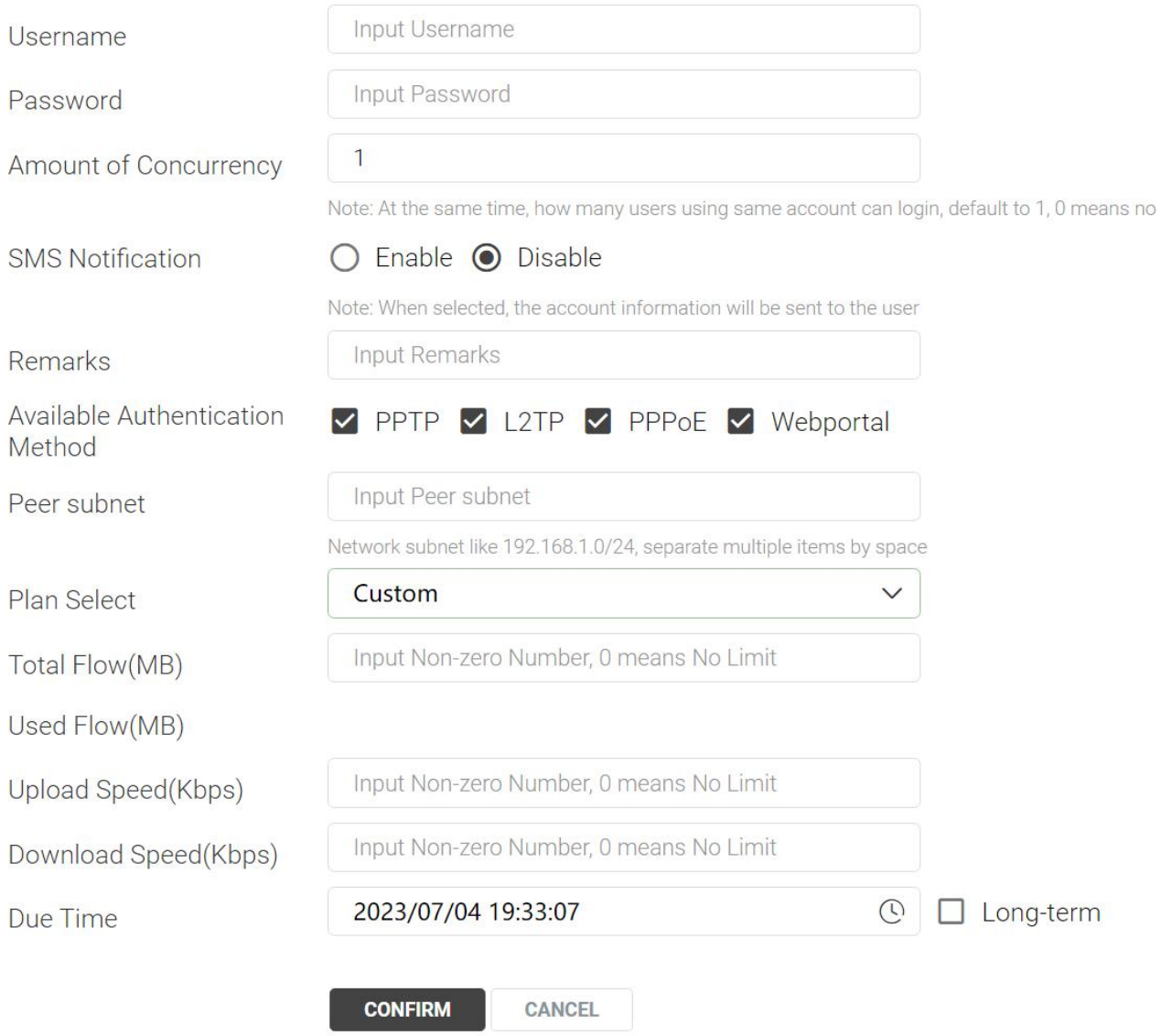


Parameter	Describe
Plan Name	Specify a name for easy identification.
Total Flow(MB)	Specify the total traffic of the plan. If used up within the designated time, authenticated users will be taken offline.
Unit	Limit the usage time of traffic for this plan.
Available Time	Enter time value.
Upload Speed(Kbps)	Specify upload speed for this plan.
Download Speed(Kbps)	Specify the download speed for this plan.
Self Service	Used in conjunction with the Self Service Portal function, users can choose a billing plan on the page.

9.4. Local Users

You can create users and passwords in advance to provide user and password services for local authentication.

Choose the menu **HotSpot** > **Local Users** and click **ADD** to load the following page.



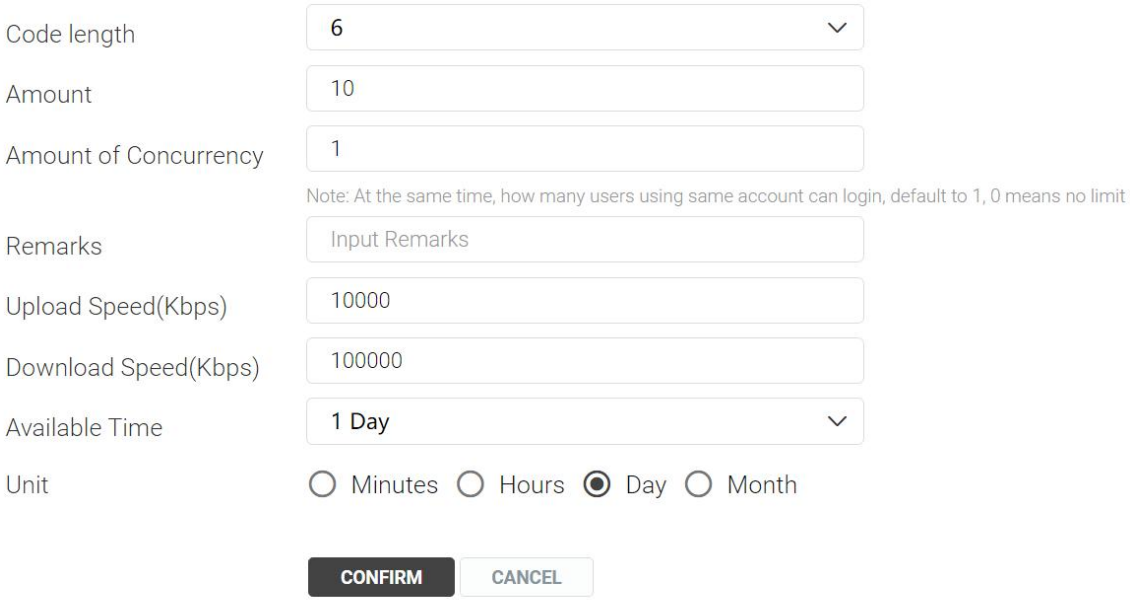
Parameter	Describe
Username	Specify a user name.
Password	Specify password for user name.
Amount of Concurrency	Limit the number of times an account can be used.
SMS Notification	After docking with the SMS authentication service, enable it to accept SMS verification codes.
Remarks	Enter a name for easy identification.
Available Authentication Method	Specify the type of authentication.
Peer subnet	Combined with VPN authentication, input the remote intranet IP or subnet.

Plan Select	Select an account to create a billing plan.
Total Flow(MB)	Specify the total traffic of the account.
Used Flow(MB）	The amount of traffic used by the account.
Upload Speed(Kbps)	Specify upload speed for the account.
Download Speed(Kbps)	Specify download speed for the account.
Due Time	Specify the validity period of the account

9.5. Vouchers

With Voucher configured, you can distribute the vouchers automatically generated by the AC to the clients. Clients can use the vouchers to access the network.

Choose the menu **HotSpot > Vouchers** and click **BATCHADD** to load the following page.

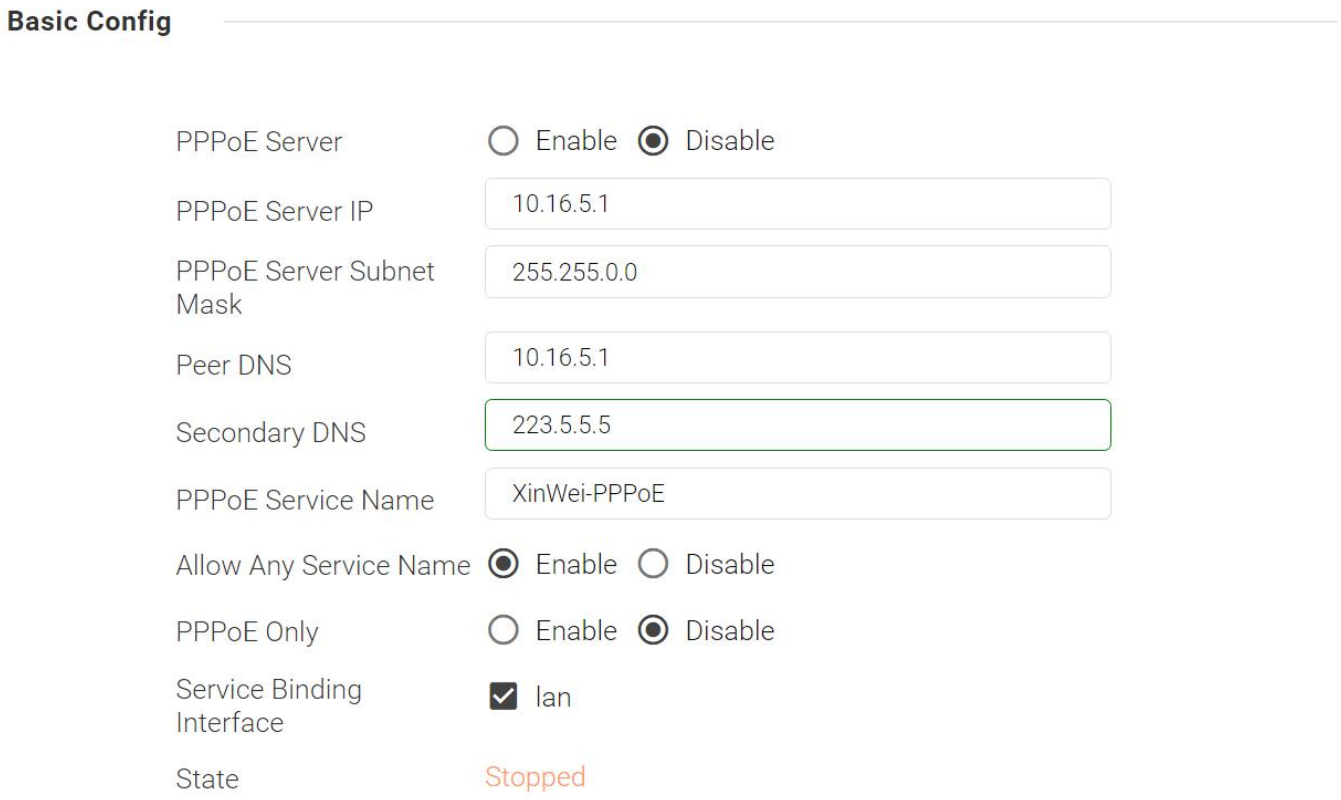


Parameter	Describe
Code length	Select Code Length.
Amount	Enter the number of Vouchers.
Amount of Concurrency	Enter the number of concurrent users using Vouchers.

Remarks	Specify a name for easy identification.
Upload Speed(Kbps)	Specify upload speed for the vouchers.
Download Speed(Kbps)	Specify download speed for the vouchers.
Available Time	Specify the validity period of the vouchers.
Unit	Valid Unit of time for Vouchers.

9.6. PPPoE Server

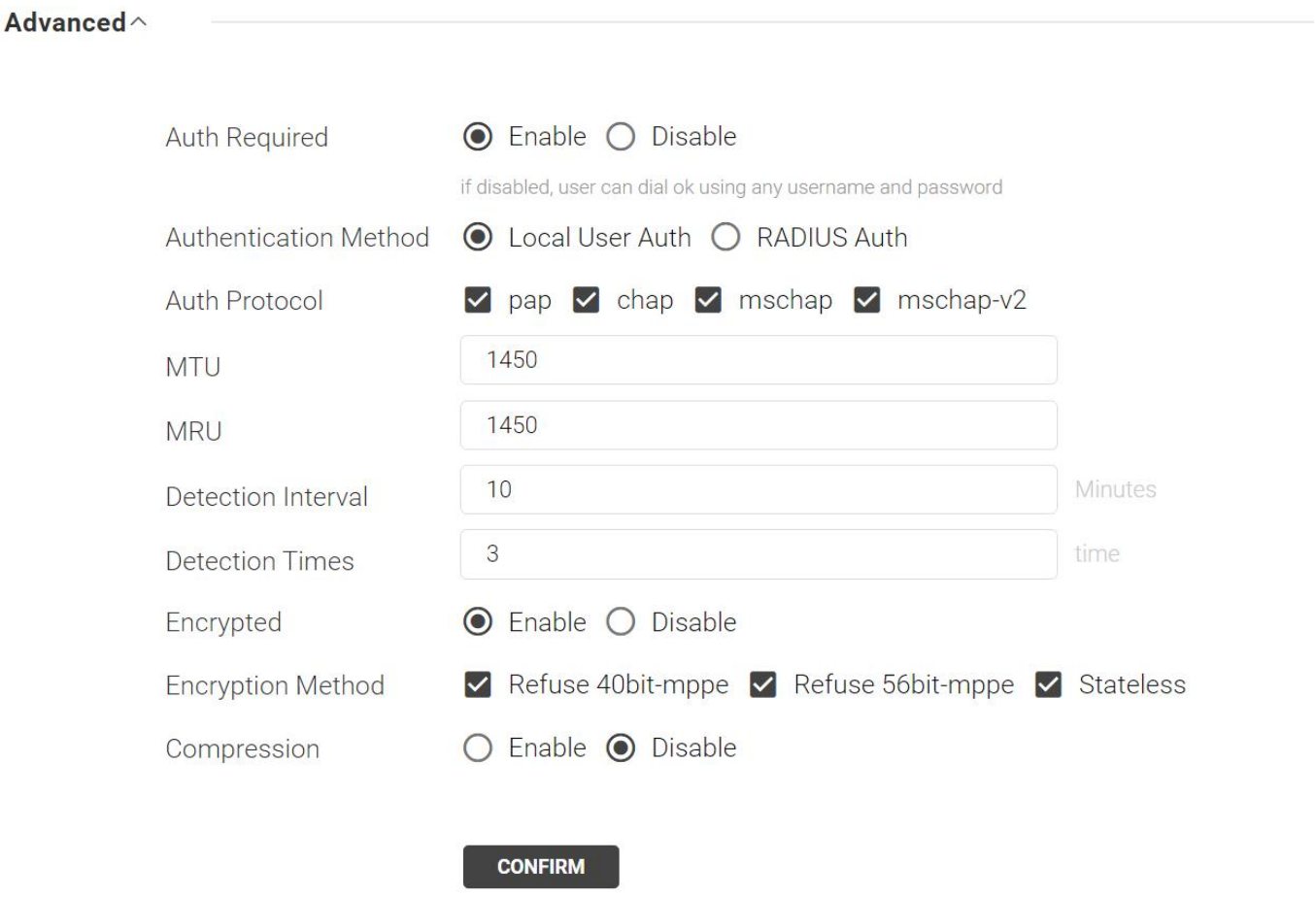
Choose the menu **HotSpot** > **PPPoE Server** and click BATCHADD to load the following page.



Parameter	Describe
PPPoE Server	Enable or disable PPPoE Server.
PPPoE Server IP	Specify the IP address for the PPPoE server.
PPPoE Server Subnet Mask	Specify subnet mask for PPPoE Server.

Peer DNS	Specify Peer DNS for PPPoE Server.
Secondary DNS	Specify Secondary DNS for PPPoE Server.
PPPoE Service Name	Customize the name for the PPPoE server.Run multiple PPPoE servers in the internal network and distinguish different PPPoE servers by name.
Allow Any Service Name	If you select Enable, do not check the PPPoE server name for the PPPoE client identification.
PPPoE Only	This subnet can only be used for PPPoE servers.
Service Binding Interface	Specify the line on which the PPPoE server runs.

Then click on the **advanced** button to load the following page.

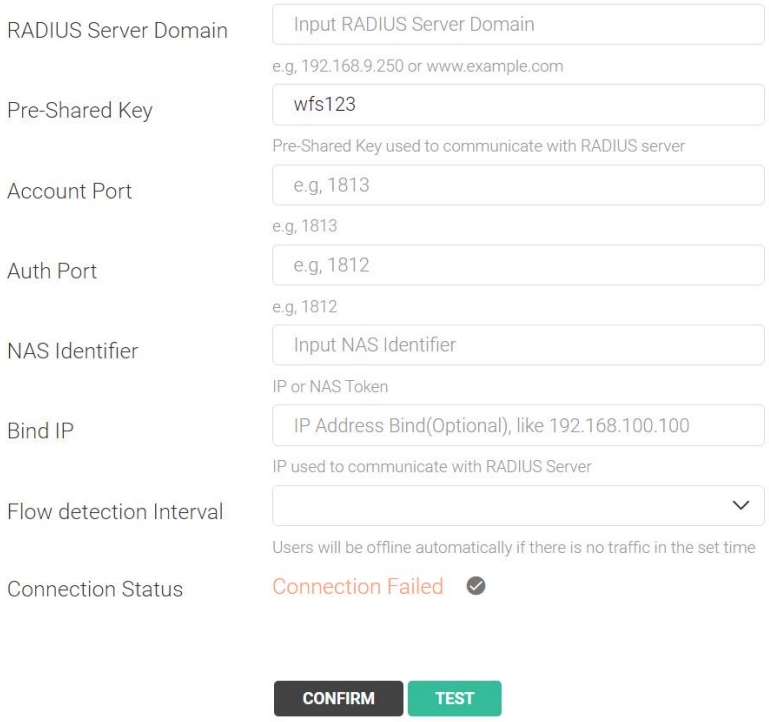


Parameter	Describe
Auth Required	if disabled, user can dial ok using any username and password.
Authentication	Local User Auth: Create an account locally.

Method	RADIUS Auth: Create an account on radius.
Auth Protocol	Specify authentication protocol.
MTU	Maximum Transmission Unit.You can keep the default value for this setting.
MRU	Maximum Receive Unit.You can keep the default value for this setting.
Detection Interval	Detect PPP link “heartbeat ”time interval.The default value is 600 seconds.
Detection Times	Detect PPP link “heartbeat ”count. The default value is 3.
Encrypted	Provide encryption for PPP link.The default is enabled.
Encryption Method	Specify tunnel encryption type.
Compression	Provide compression types for data.
Compression Method	Specify compression method.

9.7. RADIUS Server

Choose the menu **HotSpot > RADIUS Server** to load the following page.

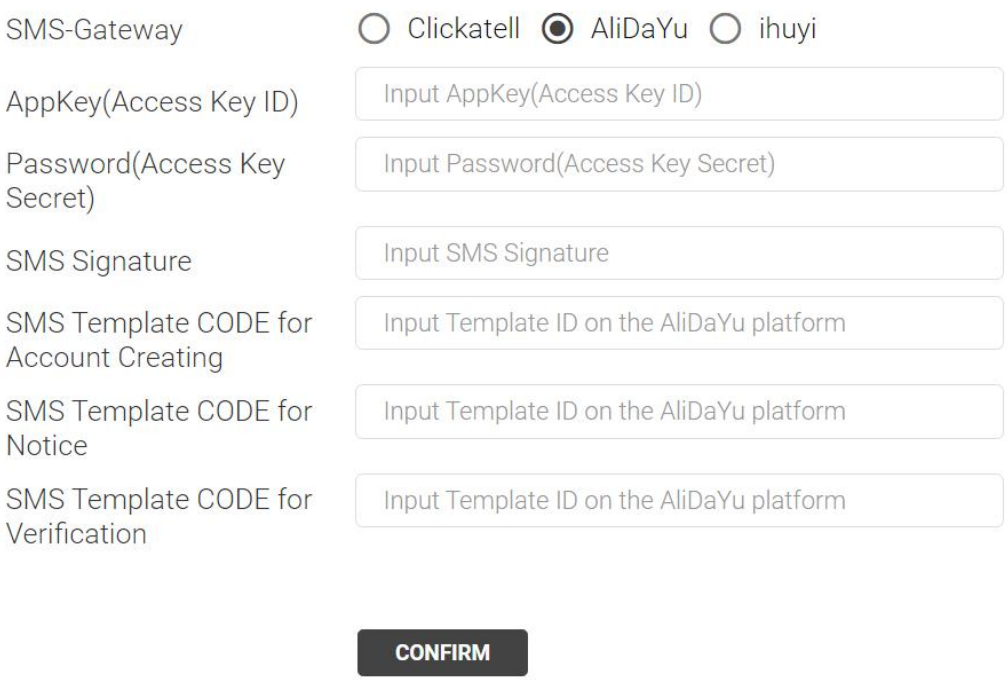


Parameter	Describe
RADIUS Server Domain	Enter the domain name or IP address of the RADIUS server.
Pre-Shared Key	Enter the password you have set on the RADIUS server.
Account Port	Enter the port number you have set on the RADIUS server.
Auth Port	Enter the port number of the accounting server. The default port number is 1812.
NAS Identifier	Enter NAS Identifier. (IP or NAS Token)
Bind IP	Enter Bind IP (optional) * IP used to communicate with RADIUS Server.
Connection Status	Show connection status.

9.8. SMS Gateway

Clients can get verification codes using their mobile phones and enter the received codes to pass the authentication

Choose the menu **HotSpot > PPPoE Server** to load the following page.

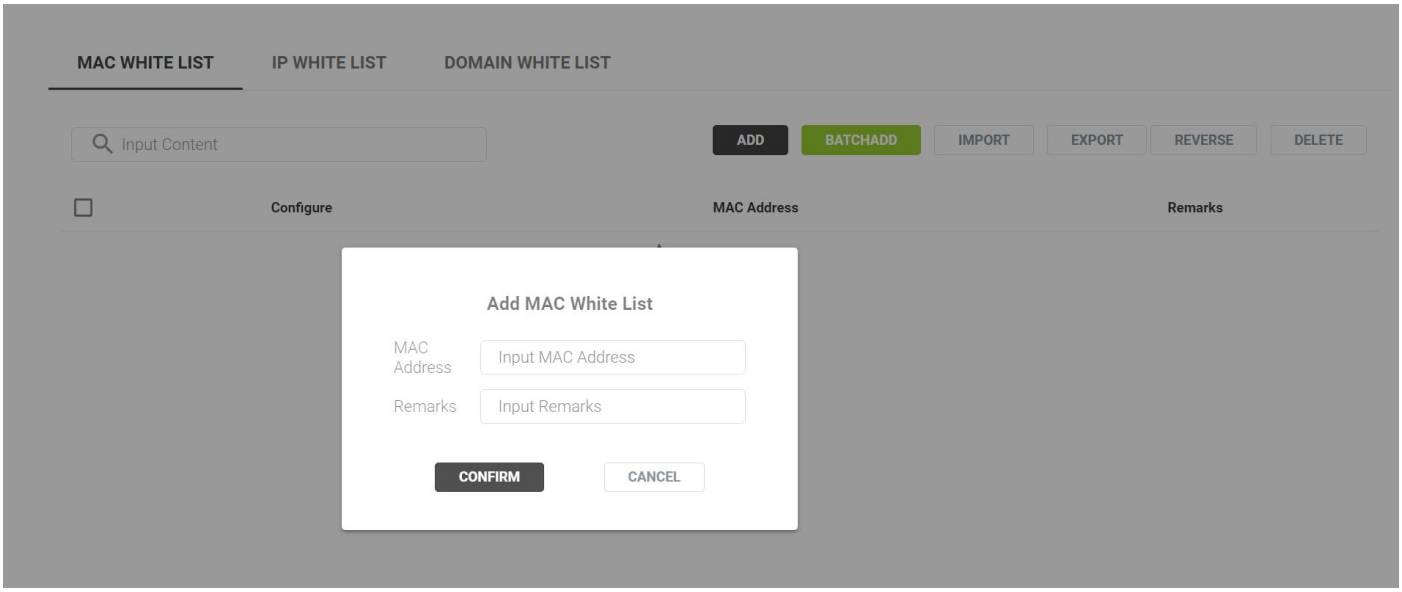


Parameter	Describe
SMS -Gateway	Select the specified SMS gateway.
App Key	The specified Access Key ID obtained from the SMS gateway.
Password	Get the specified password from the SMS gateway.
SMS Signature	Input SMS Signature.
SMS Template CODE for Account Creating	Input SMS Template C0DE for Account Creating.
SMS Template CODE for Notice	Input SMS Template CODE for Notice.
SMS Template CODE for Verification	Input SMS Template CODE for Verification.

9.9. White List

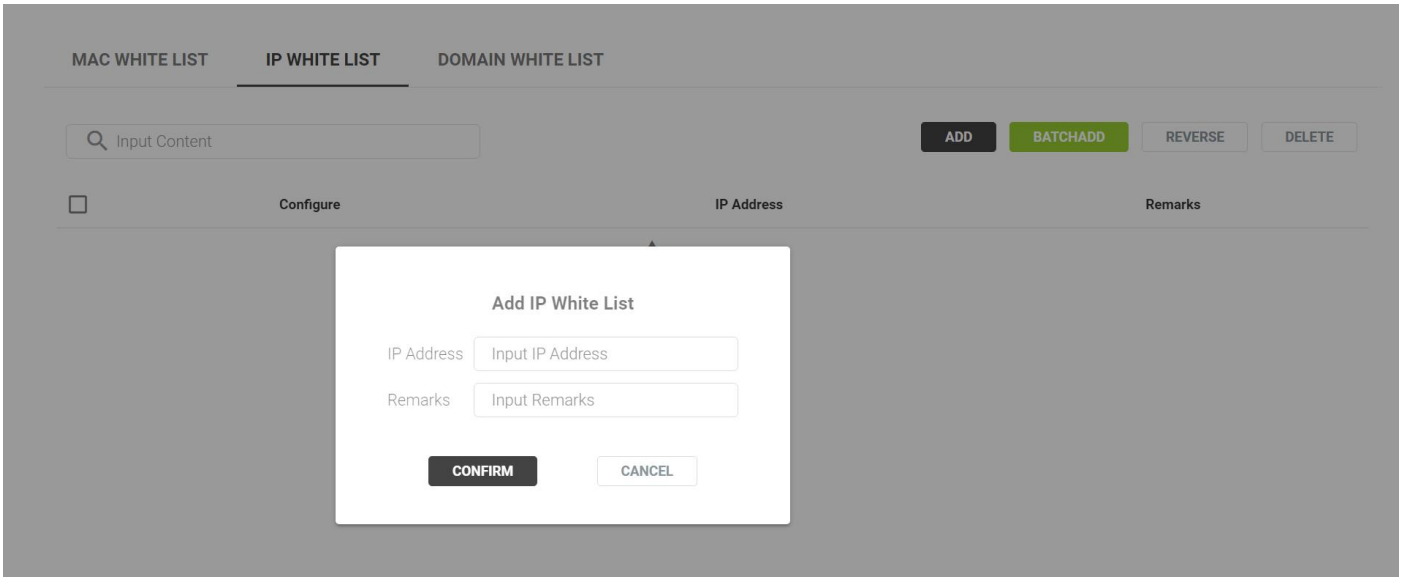
MAC whitelist allows only MAC in the list to access the network.

Choose the menu **HotSpot** > **White List** > **MAC WHITE LIST** and click **ADD** to load the following page.



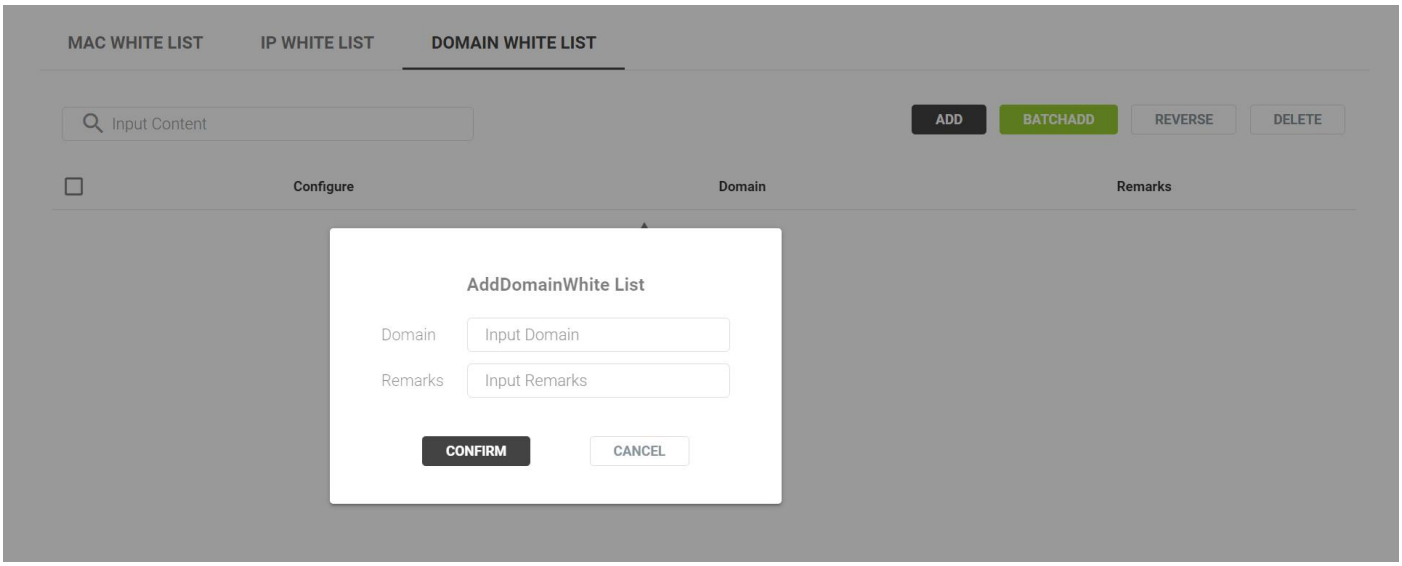
IP whitelist allows only IP in the list to access the network.

Choose the menu **HotSpot** > **White List** > **IP WHITE LIST** and click ADD to load the foll owing page.



Domain whitelist Only allow access to domain names within the list.

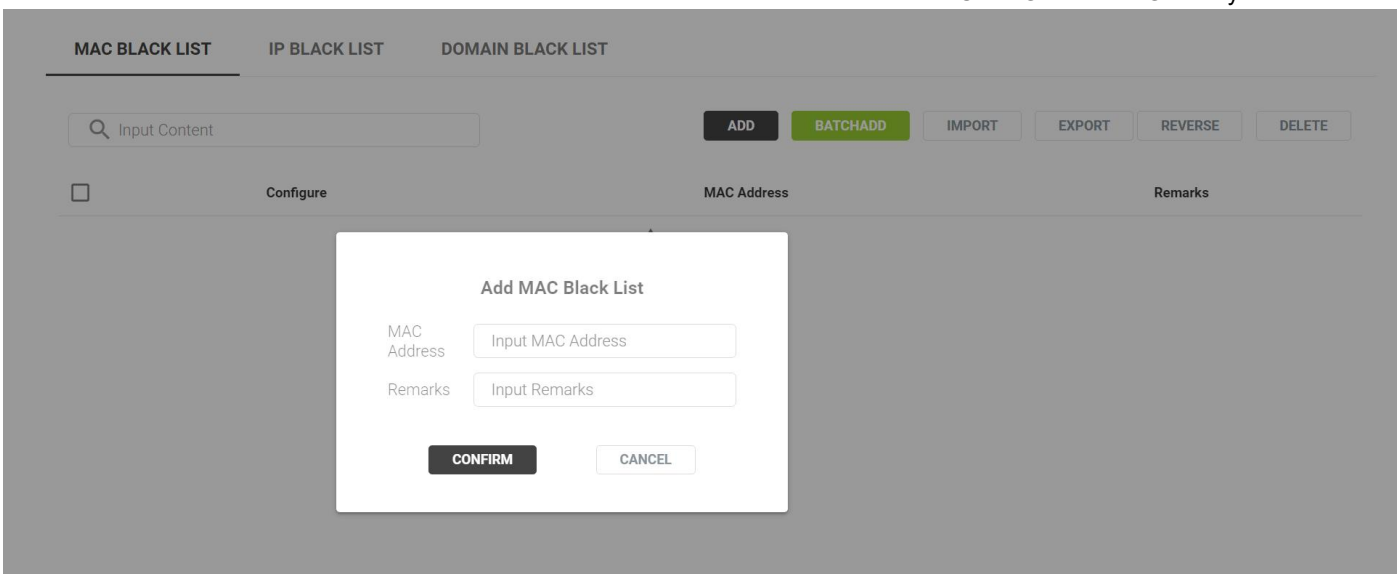
Choose the menu **HotSpot > White List > DAMAIN WHITE LIST** and click **ADD** to load t he following page.



9.10. Black List

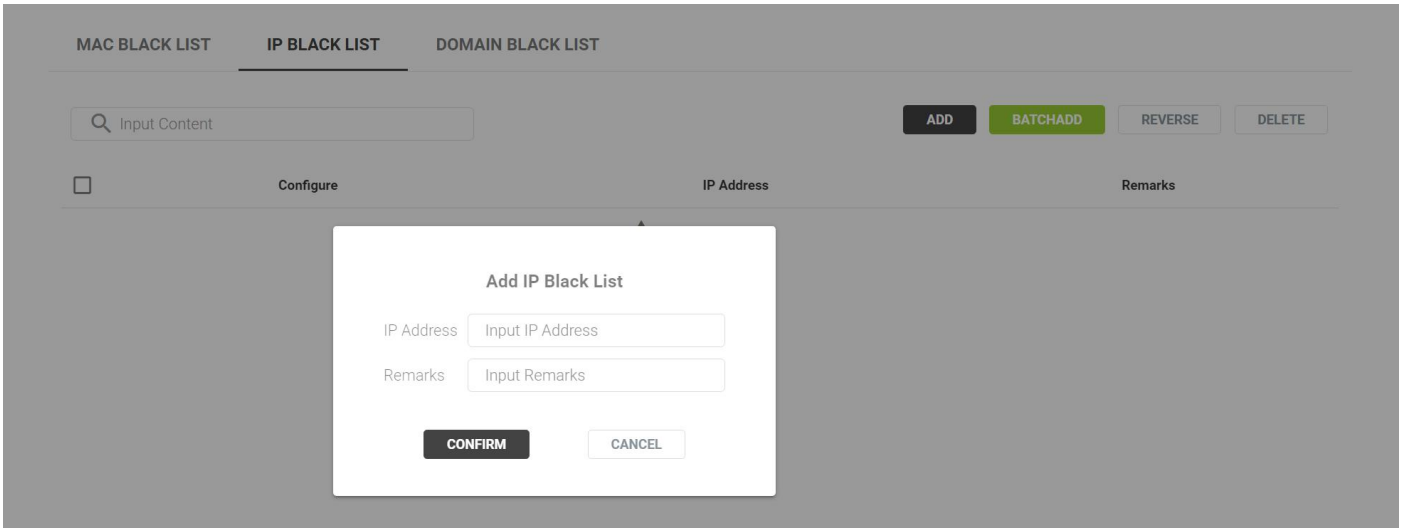
Based on the MAC blacklist, except for the MAC addresses in the list, other MAC addresse s can access the network.

Choose the menu **HotSpot > Black LIst > MAC BLACK LIST** and click **ADD** to load the following page.



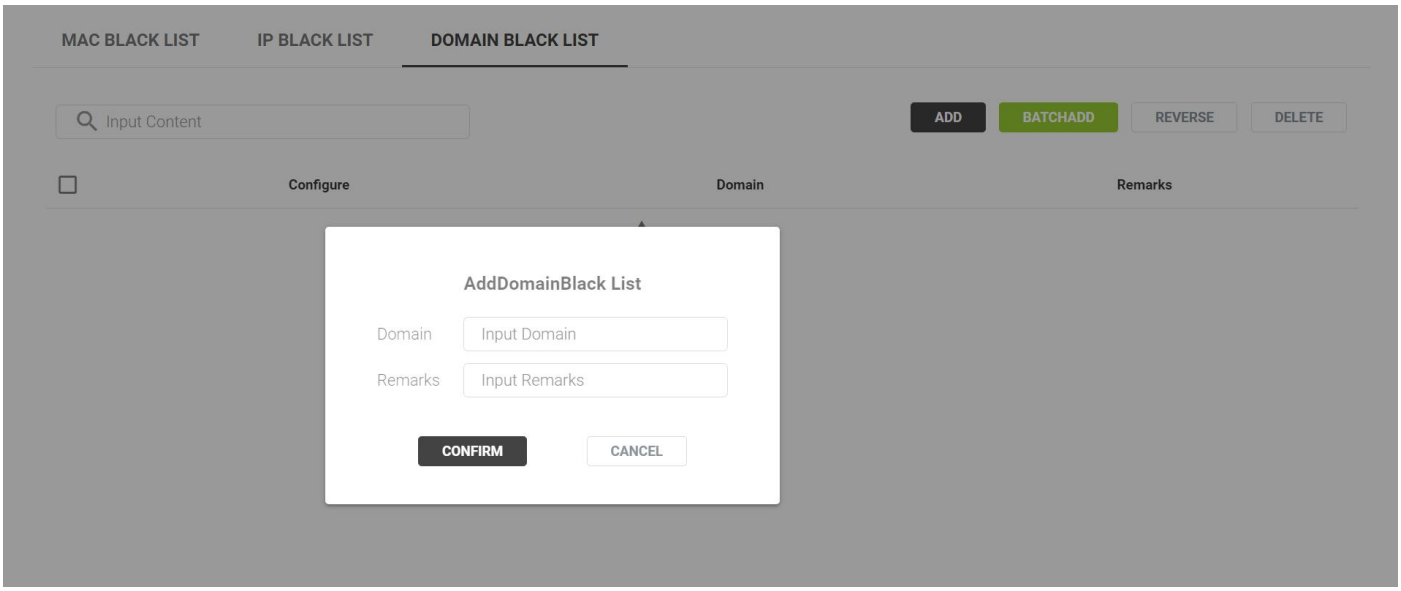
Based on the IP blacklist, except for the IP addresses in the list, other IP addresses can a ccess the network.

Choose the menu **HotSpot > Black LIst > IP BLACK LIST** and click **ADD** to load the foll owing page.



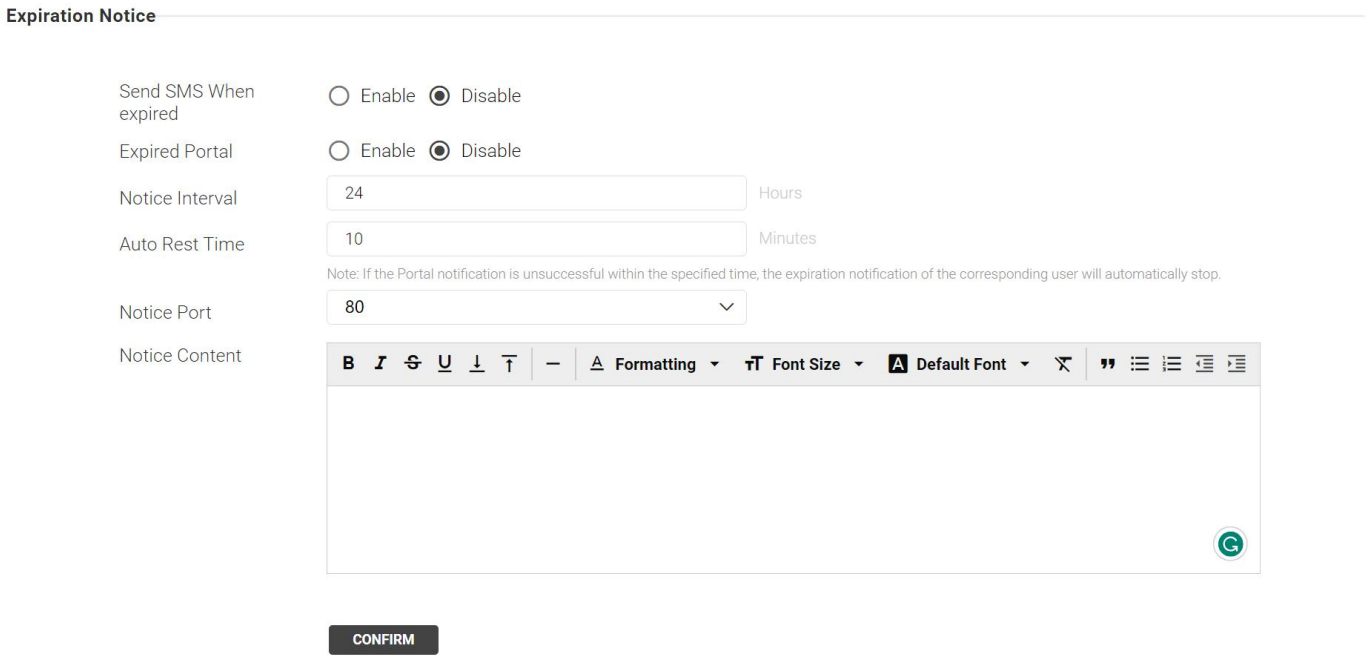
Block intranet devices from accessing domain names in the list.

Choose the menu **HotSpot > Black LIst > DOMAIN BLACK LIST** and click **ADD** to load the following page.



9.11. Expiration Notice

If you enable the PPPoE server on the gateway and enable this feature, a web page notification will be sent when the PPPoE account is about to expire.



Parameter	Describe
Sen SMS When expired	Used in conjunction with SMS services to notify via SMS.
Expired Portal	Enable or disable expired portal feature.
Notice Interval	Notify every 24 hours.You can modify the time.

Auto Rest Time	If the Portal notification is unsuccessful within the specified time, the expiration notification of the corresponding user will automatically stop.
Notice Port	Specify the port number for this service.
Notice Content	Specify oneself to edit the notification content.

9.12. Local Notice

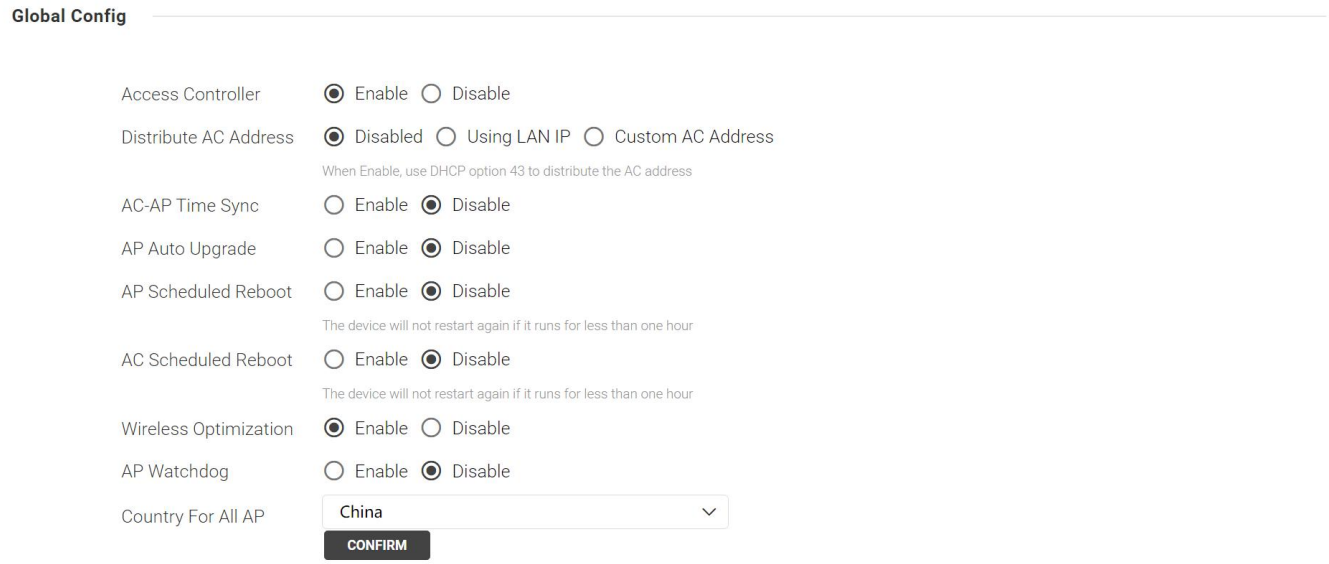
When the computer dials up and connects to the PPPoE server, the user opens a browser to access the internet, and a notification page will pop up. If the user does not take any action to access the browser, there will be no pop-up notification when accessing the brows er after 10 minutes. The reset time can be manually set.

Parameter	Describe
Local Announcement	Enable or disable this feature.
Enabled Interface	Choose which subnet to apply notifications to.
Announcement Content	Edit announcement text.

10. Wireless

10.1. Overview

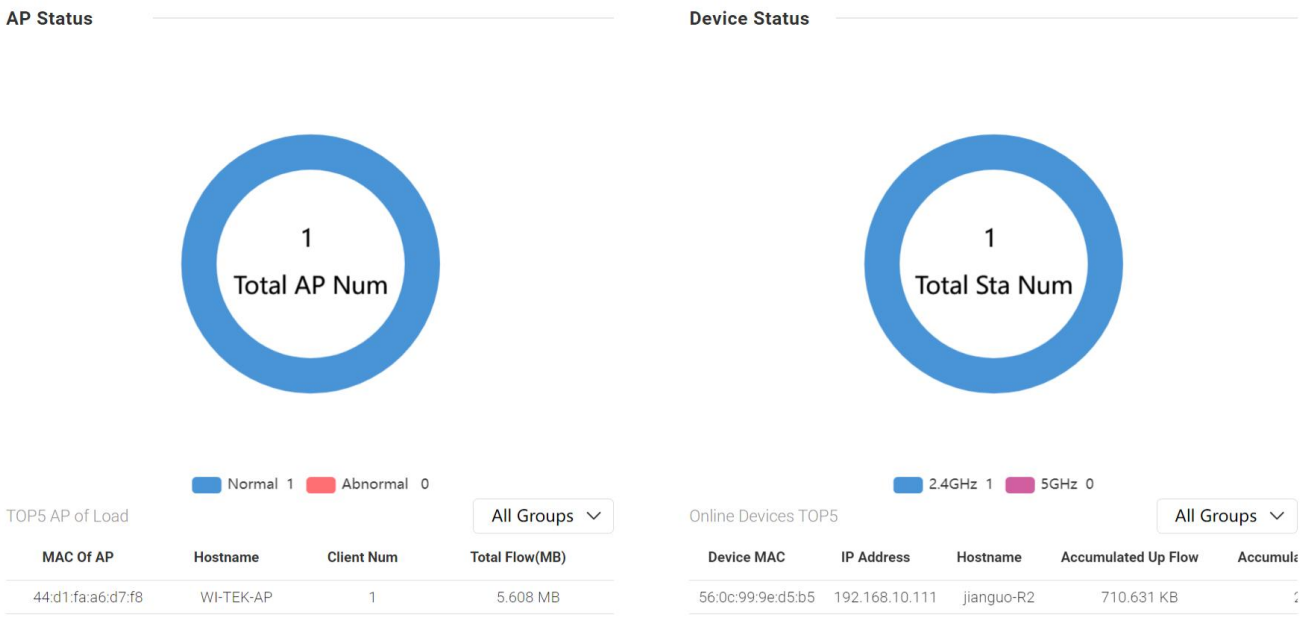
Choose the menu **Wireless** > **Overview** to load the following page.



Parameter	Describe
Access Controller	Enabled by default,If this option is disabled, the Access Controller function will be turned off.
AC-AP Time Sync	Select time type.
AP Scheduled Reboot	Disabled by default,If this option is enabled, you can periodically reboot all APs in the network as needed.
AC Scheduled Reboot	Disabled by default, If this option is enabled, you can periodically reboot AC in the network as needed.
Wireless Optimization	Disabled by default,If this option is disabled, the wireless Optimization function will be turned off. Note: Using this function, when all the channels of the AP are set to be automatic, when there is no client connected to the AP, the AC will automatically optimize the channel.
AP Watchdog	Disabled by default, If this option is enabled, when the Address Do not Alive, AP will Open Rescue Network Automatically (SSID: RESCUE_99_XXXX, Password: 99999999)

Country For All AP	Select the corresponding country from the drop-down menu.

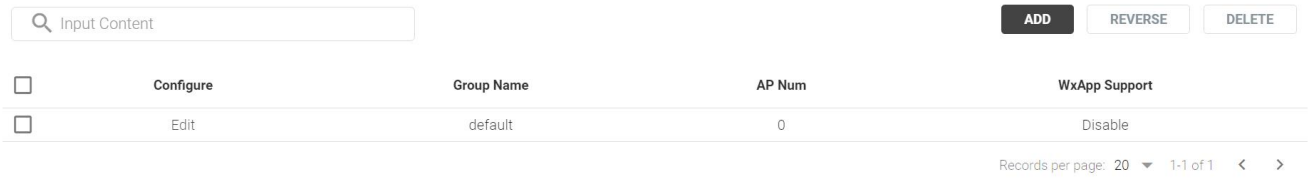
You can view the current AP status and device status.



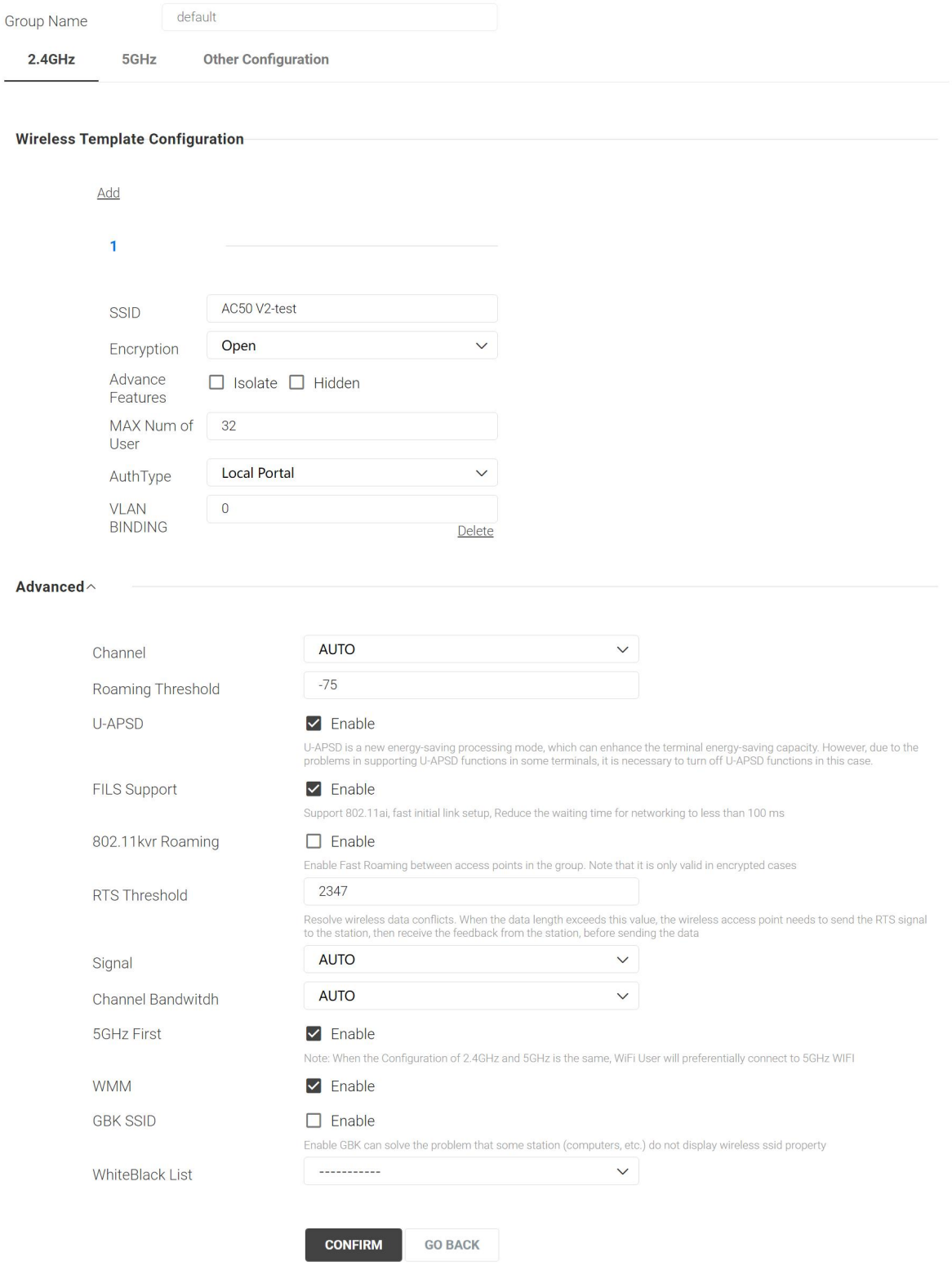
10.2. AP Group

The wireless parameters of APs can be synchronized in batches through AP groups.an ap can belong to one ap group at a time.

Choose the menu **Wireless > AP Group** to load the following page.



Click **Add** an ap group and click the **Edit** button in the Wireless > AP Group table to display this page.



Parameter	Describe
Group Name	Specify a name for the group.
SSID	Enter an SSID name contains up to 32 characters.

	Note: A maximum of 8 SSID profiles can be created in each AP group.
Encryption	Select the security mode of the wireless network WPA-Enterprise / WPA2-Enterprise
KEY	Enter the password for the SSID.
Advance Features	**Isolate:**Check this option box, wireless clients connected to the same SSID cannot access each other. **Hidden:**Check this option box, the AP will not broadcast the SSID and wireless clients will not be able to scan and search for the SSID.
MAX Num of User	Number of users connected to this SSID.
AuthType	It is associated with authentication. The default is none.
VLAN BINDING	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN.
delete	Delete wireless parameter profile.

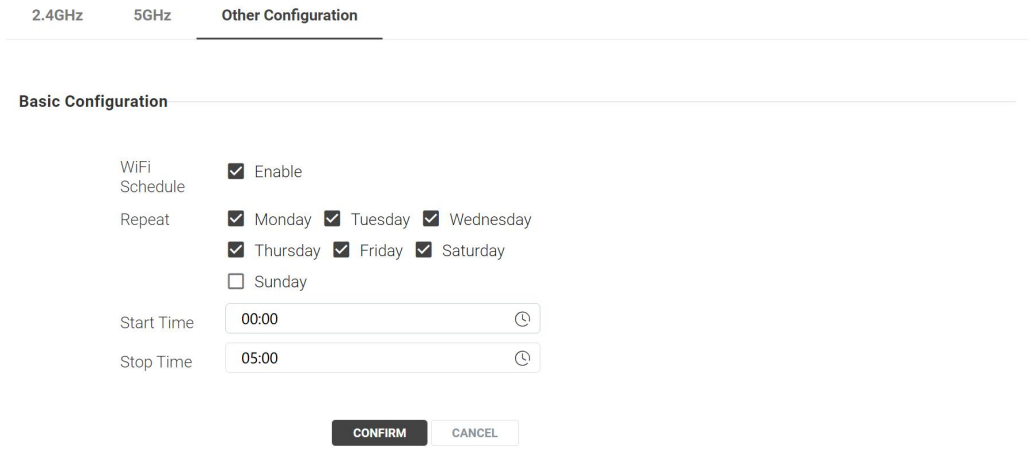
Advanced

Channel	Automatic by default,you can manually specify the channel. The range of available channels is determined by the radio mode and the country setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where the least amount of traffic is detected.
Roaming Threshold	minimum signal level required for a client to remain connected.
U-APSD	Enabled by default, U-APSD is a new energy-saving processing mode, which can enhance the terminal energy-saving capacity. However, due to the problems in supporting U-APSD functions in some terminals, it is necessary to turn off U-APSD functions in this case.
FILS Support	Enabled by default, supports 802.11ai, fast initial link setup, Reduce the waiting time for networking to less than 100 ms
802.11kvr Roaming	Enable Fast Roaming between access points in the group. Note that it is only valid in encrypted cases.

RTS Threshold	Resolve wireless data conflicts. When the data length exceeds this value, the wireless access point needs to send the RTS signal to the station, then receive the feedback from the station, before sending the data
Signal	Select the corresponding value according to the actual transmit power of the AP.
Channel Bandwidth	Select the wireless channel bandwidth.
5GHz First	Enabled by default, when the Configuration of 2.4GHz and 5GHz is the same, Wi-Fi User will preferentially connect to 5GHz Wi-Fi.
WMM	Enabled by default,the AP maintains the priority of audio and video packets for better media performance.
GBK SSID	Enable GBK can solve the problem that some station (computers, etc.) do not display wireless ssid property
WhiteBlack List	Select the created black/white list from the drop-down menu.

You can set the radio in the AP group to run at a specified time.

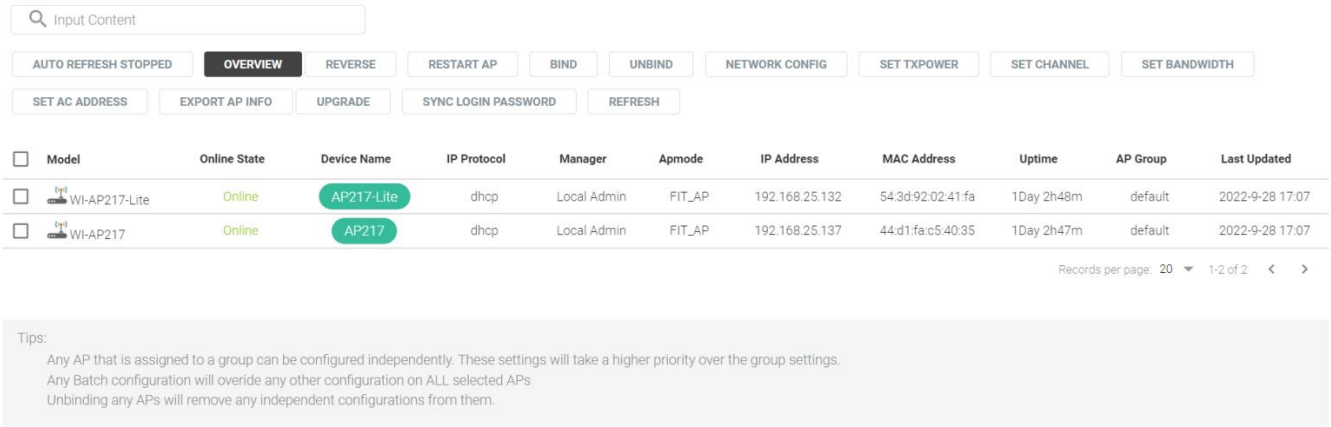
Choose the menu **Wireless > AP Group > Other Configuration** to load the following page.



10.3. AP List

Display Cloud AP from AC discovery to Wi Tek here.

Choose the menu **Wireless > AP List** to load the following page.By default, devices are di splayed in a spread out form OVERVIEW.



Parameter	Describe
AUTO REFRESHING	Click to automatically refresh the AP list.
REVERSE	Select all APs and click REVERSE to quickly deselect AP.
RESTART AP	Select an AP and click it to restart the AP.
BIND	Select the AP and bind it to the specified AP group.
UNBIND	Select the AP to unbind it from the AP group.
NETWORK CONFIG	Select AP to set IP address
SET TXPOWER	Select AP to set TX power.
SET CHANNEL	Select AP to set bandwidth.
SET BANDWIDTH	Select AP to set bandwidth.
SET AC ADDRESS	Select AP to manually set AC address for AP.
EXPORT AP INFO	Select AP to export AP information
UPGRADE	Select AP to upgrade the firmware. * It needs to be matched with 6.6 Firmware
SYNC LOGIN PASSWORD	Select AP and click it to synchronize the same password as AC
REFRESH	Click it to refresh the AP list.

OVERVIEW: Display the most basic parameters of AP.

Model	Online State	Device Name	IP Protocol	Manager	Apmode	IP Address	MAC Address	Uptime	AP Group	Last Updated
WI-AP317	Offline	AP317	dhcp	Local Admin	FIT_AP	192.168.25.184	44:d1:fa:a3:7d:c9	1Day 1h17m	-	2022-9-29 11:30
WI-AP217-Lite	Online	AP217-Lite	dhcp	Local Admin	FIT_AP	192.168.25.132	54:3d:92:02:41:fa	0Day 2h16m	-	2022-9-29 11:30
WI-AP217	Online	AP217	dhcp	Local Admin	FIT_AP	192.168.25.137	44:d1:fa:c5:40:35	0Day 2h17m	default	2022-9-29 11:30

Records per page: 20 1-3 of 3

WiFI VIEW: Display parameters related to wireless.

Model	Online State	AP Group	WiFi User	Channel	Txpower	Upload Flow	Download Flow	Device Name	MAC Address
WI-AP317	Offline	-	0/ 1	9/ 56	26/ 26	33.851 MB	290.285 MB	AP317	44:d1:fa:a3:7d:c9
WI-AP217-Lite	Online	-	0/ 1	1/ 44	23/ 26	885.517 MB	2.138 GB	AP217-Lite	54:3d:92:02:41:fa
WI-AP217	Online	default	0/ 0	2/ 40	24/ 23	874.167 KB	10.092 MB	AP217	44:d1:fa:c5:40:35

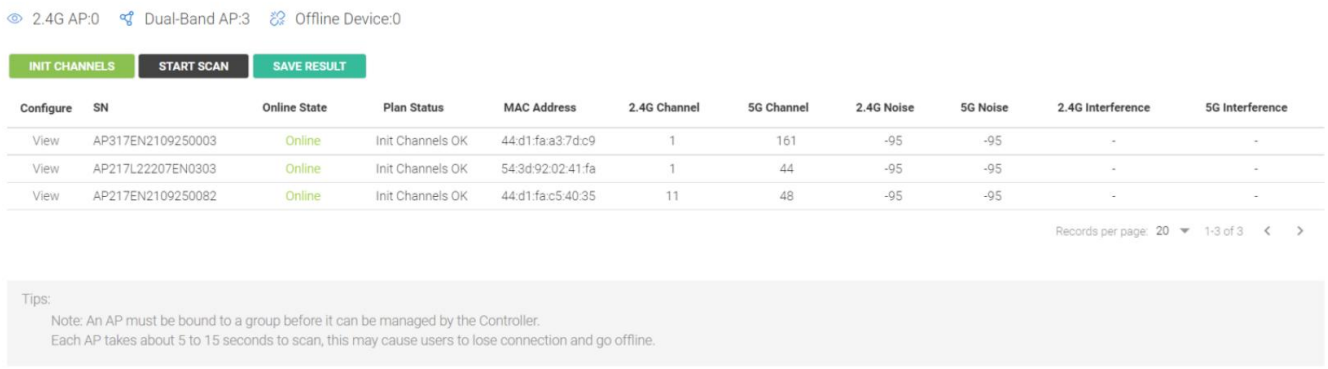
Records per page: 20 1-3 of 3

DETAILS VIEW: Display the most comprehensive parameters of AP.

Model	Online State	Device Name	SN	IP Protocol	IP Address	MAC Address	Uptime	AP Group	WiFi User	CPU Usage	Channel	Txpower	Upload Flow
WI-AP317	Offline	AP317	AP317EN2109250003	dhcp	192.168.25.184	44:d1:fa:a3:7d:c9	1Day 1h17m	-	0/ 1	7%	9/ 56	26/ 26	33.851 M
WI-AP217-Lite	Online	AP217-Lite	AP217L22207EN0303	dhcp	192.168.25.132	54:3d:92:02:41:fa	0Day 2h16m	-	0/ 1	7%	1/ 44	23/ 26	885.517 M
WI-AP217	Online	AP217	AP217EN2109250082	dhcp	192.168.25.137	44:d1:fa:c5:40:35	0Day 2h17m	default	0/ 0	7%	2/ 40	24/ 23	874.167 K

10.4. RF Planning

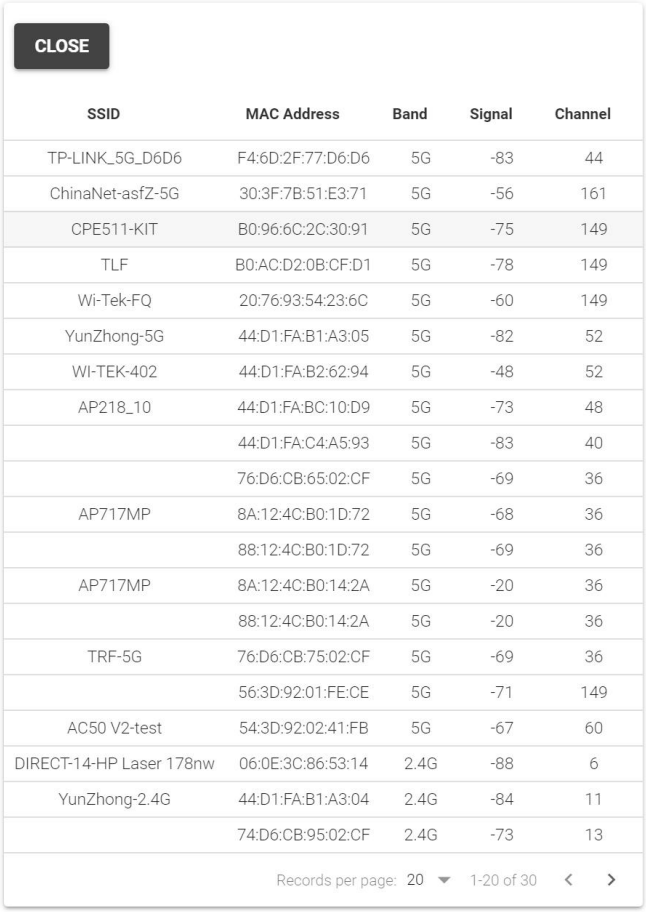
The purpose of this function is to assist in the rapid optimization of the wireless channel. Analyze and calculate the busyness of the channel according to the scanning situation, and choose the lower one first.Choose the menu **Wireless > RF Planning** to load the follo wing page.



Parameter	Describe
INIT CHANNELS	Click it to assign channels based on APs within the group.
START SCAN	Click it to automatically scan the Wi-Fi interference sources around the AP.

SAVE RESULT	After scanning, you need to click it to save the result.

Click **View** to view the surrounding Wi-Fi signals.



Note:

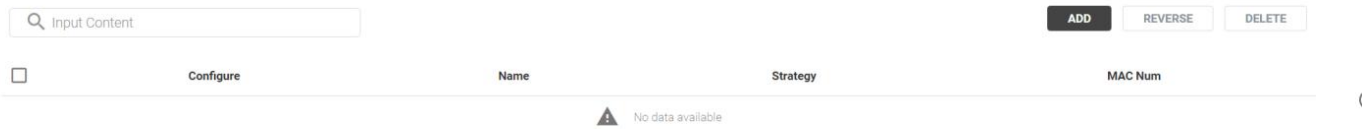
- An AP must be bound to a group before it can be managed by the Controller.
- Each AP takes about 5 to 15 seconds to scan, this may cause users to lose connection and go offline.

10.5. WhiteBlack LIst

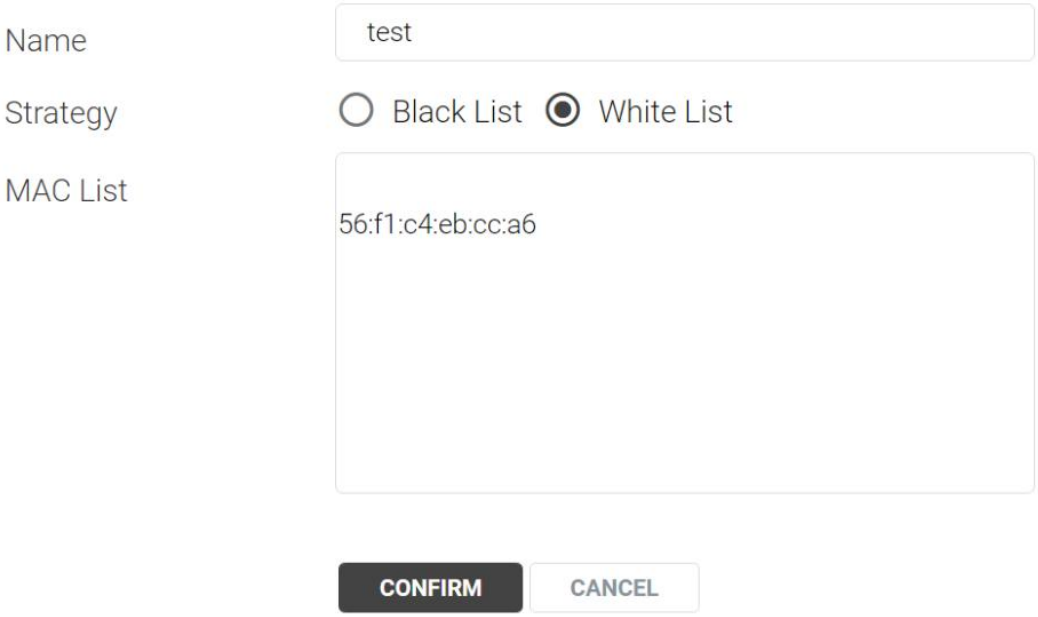
White/Black List can be used to allow or block the listed clients to access the network. The reby it can effectively control the client's access to the wireless network.

Whitelist: Only allow wireless clients in the list to connect to Wi-Fi. **Blacklist**: Except for the wireless clients in the blacklist, other wireless clients can connect to Wi-Fi.

Choose **Wireless > White Black List** to load the following page.



Choose **ADD** to load the following page.

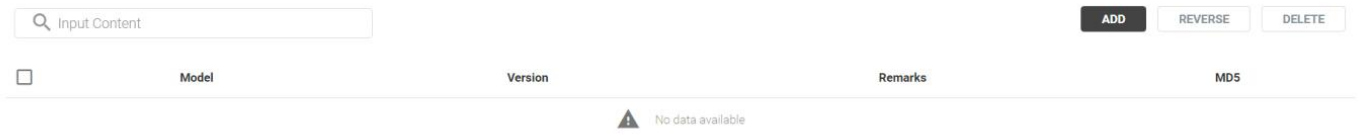


Parameter	Describe
Name	Enter any name for easy recognition.
Strategy	Specify policy type for wireless clients.
MAC List	Specify the MAC address of the wireless client.

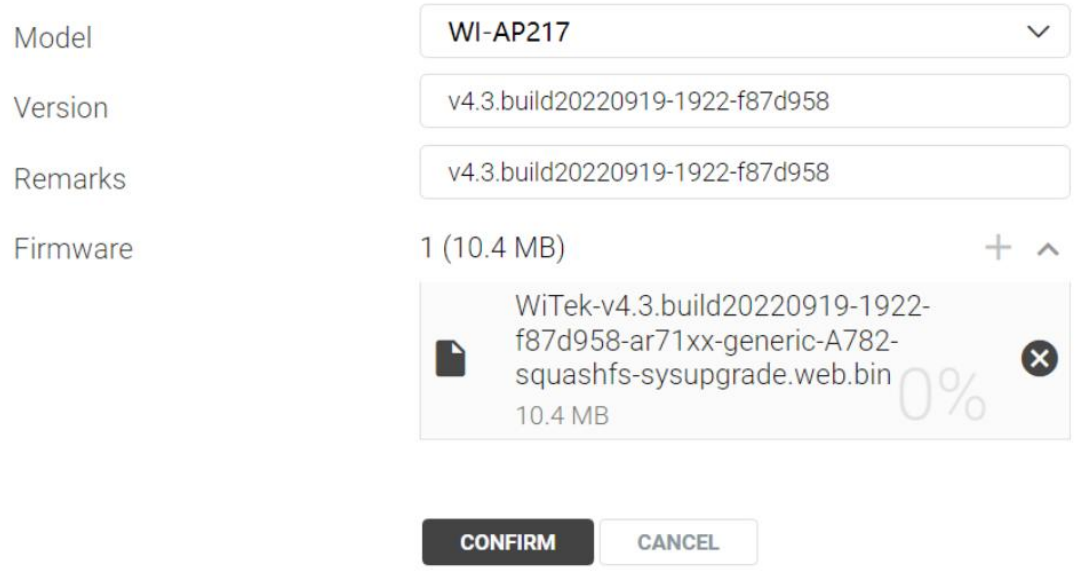
10.6. Firmware

If AC manages multiple APs, you can use this function when you want to upgrade the APs in batches.

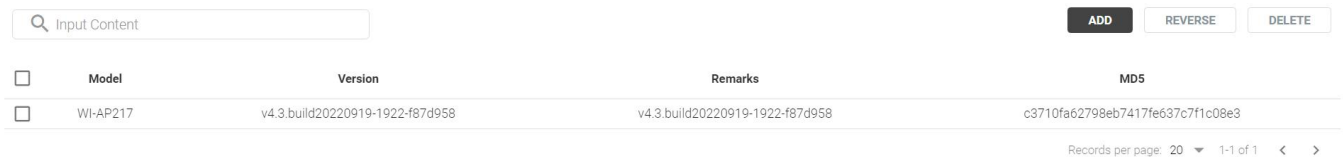
Click **Wireless > Firmware** to load the following page.



Click **ADD** button to upload the firmware file from a local disk.



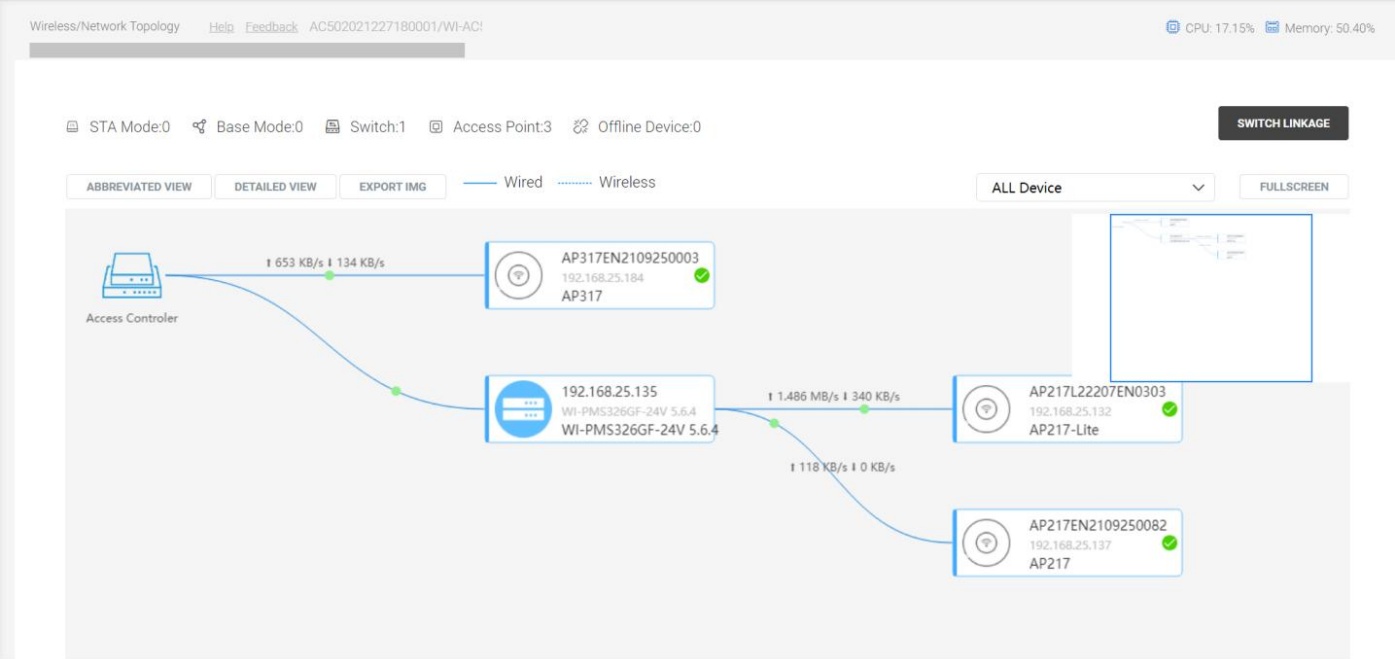
Upload succeeded.



Then go back to the **AP group** option, select the check box to access the point group fro m the list, and click Upgrade.

10.7. Network Topology

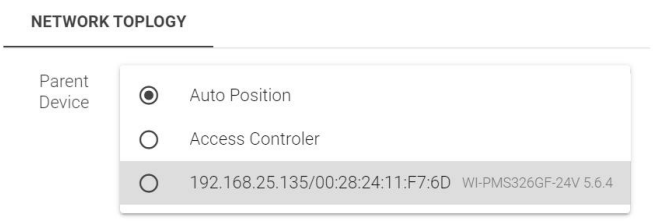
With this feature, if you have AP and Switch deployed in your network, you will be able to see a visual view of the topology of all supported devices in the network. Click **Wireless > Network Topology** to load the following page..



Parameter	Describe
ABBREVIATED VIEW	Click it to display only the devices managed by AC.
DETAILED VIEW	Click it to display which AP is connected to the wireless client
EXPORT IMG	Click it to export the topology map as an image

Note: Only supports simple topology display.

If you click the AP on the topology diagram, the following interface will pop up, and manual ly adjust the uplink device of the AP.

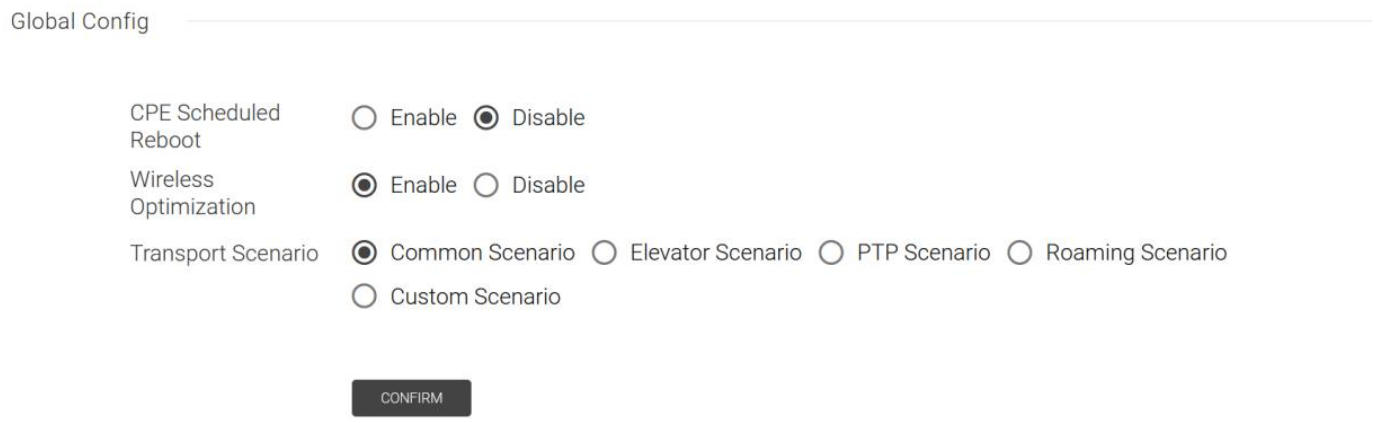


11. CPE Management

11.1. CPE Global Configuration

Using this function, once the wireless CPE is managed by AC50, the following configuration information will be automatically synchronized.

Click **CPE Management > CPE Global Configuration** to load the following page.



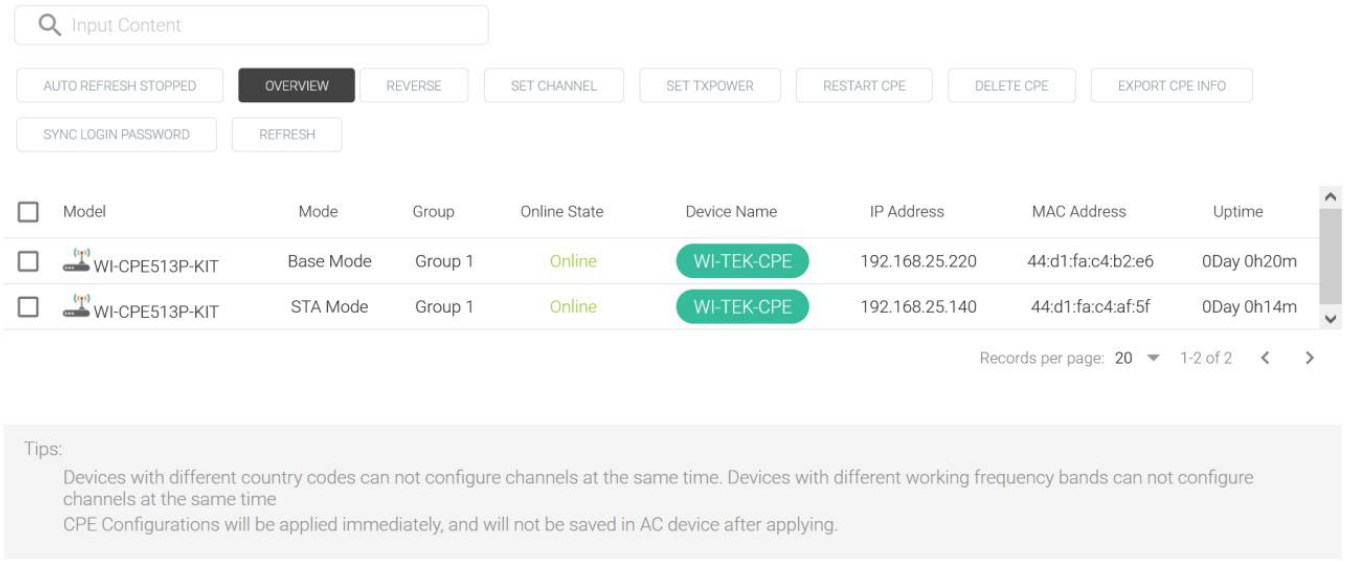
Select Roaming Scenario option, and the following content pops up.

Parameter	Describe
CPE Scheduled Reboot	Disabled by default,If this option is enabled, you can periodically reboot all CPE in the network as needed.
Wireless Optimization	Enable by default, it automatically optimize wireless CPE.
Transport Scenario	Select the scenario according to the actual application. You can choose to have 4 built-in Scenarios or customize parameters.
RTS/CTS Threshold	Keep the default value: 2347.
Ms Sta Signal(dBm)	Number of minimum received and transmitted signals between CPEs.
Distance(KM)	Select the corresponding value according to the actual transmission distance of the CPE.

11.2. CPE List

Using this function, multiple groups of CPEs in the network can be centralized.

For the explanation of CPE List parameters, refer to 6.3 AP List.Click **CPE Management > CPE List** to load the following page.



Note:

- Only available for CPE that supports cloud management.
- Devices with different country codes can not configure channels at the same time.
- Devices with different working frequency bands can not configure channels at the same time.
- CPE Configurations will be applied immediately, and will not be saved in AC device after applying.

11.3. Unified Cloud

You can bind your device to the cloud platform.

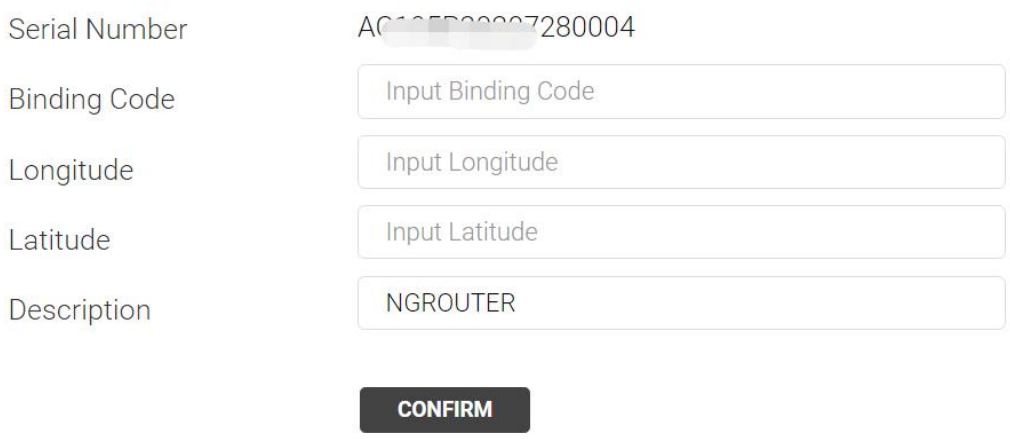
For Cloud1.0: http://cloud.wireless-tek.com/

Login the Unified Cloud Control Platform -> Obtain the Binding Code -> Input the Binding Code and Note Name On Device -> Save and complete the binding;

For Cloud2.0: http://cloud2.wireless-tek.com (Recommend)

Login the Unified Cloud Control Platform -> Add Group -> Add NetWork --> Add Device -> Input the Serial Number -> Save and complete the binding;

Click **Unified Cloud** to load the following page.



Parameter	Describe
Serial Number	Applicable to CLoud2.0, copying projects created on cloud platforms with SN added.
Binding Code	Applicable to Cloud1.0, fill in the binding code of the cloud platform account.
Longitude/Latitude	Suitable for Cloud1.0, synchronizing longitude and latitude to the cloud platform.
Description	Enter any name for easy recognition.

11.4. SD-LAN

SD-LAN is a practical application of SDN (Software Defined Network) technology. Wi-Tek launched the SD-LAN intelligent networking scheme, which can quickly establish a dedicated virtual LAN on the Internet, so as to realize one-key interconnection and data interchange between different branch nodes.

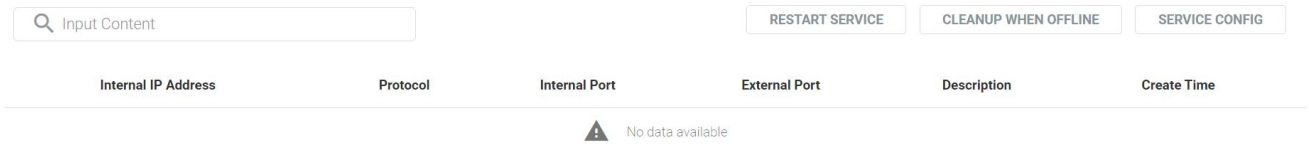
For example, the gateways of the headquarters and branch offices are bound to the same cloud account, and remote access to the internal network is achieved through SD-LAN networking.

Click **Unified Cloud > SD-LAN** to load the following page.You can check the SD-LAN link status and latency.

12. Application

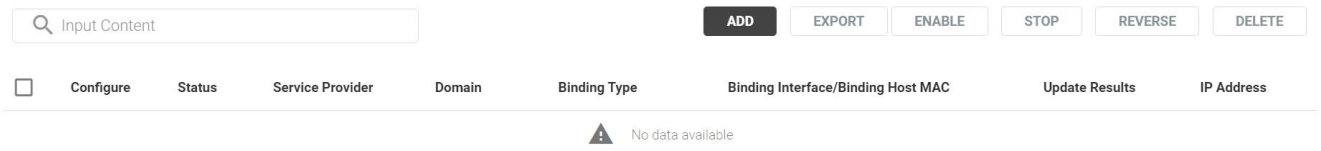
12.1. UPnP Server

With the development of networking and advanced computing techniques, great numbers of devices feature in networks. UPnP is designed to solve the problem of communication betw een these network devices. UPnP function allows devices dynamically discover and commun icate with each other without additional configurations. For example, allows the download of P2P software without opening ports.Click **Application > UPNP Server** to load the following page.

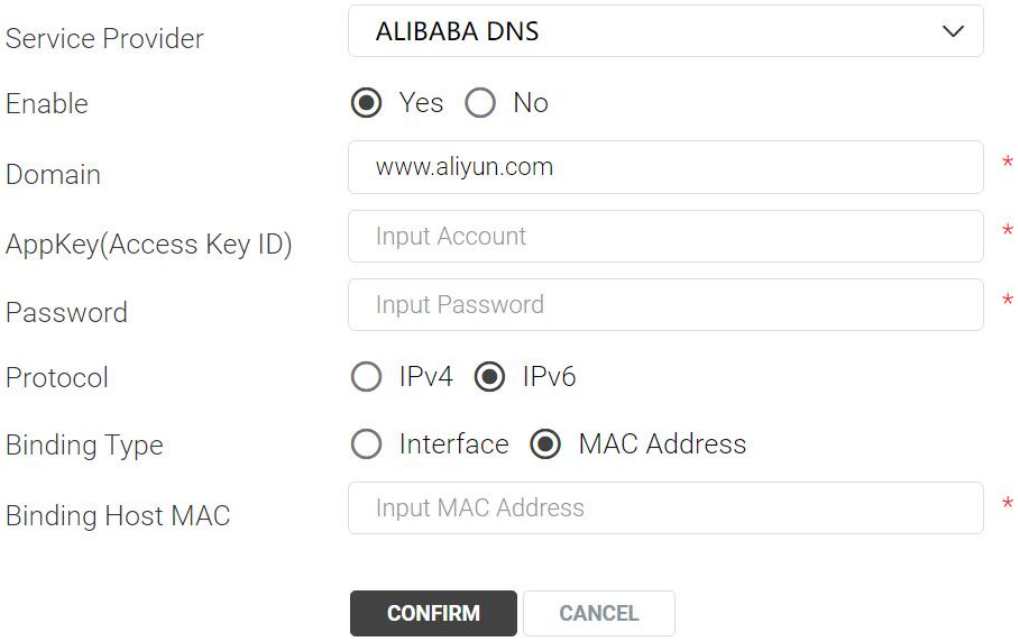


12.2. DDNS

Nowadays, network protocols such as PPPoE and DHCP are widely employed by ISPs to assign public IP addresses to users. The use of these protocols can cause the user's publi caddress to change dynamically. DDNS is an internet service that ensures a fixed domain name can be used to access a network with a varying public IP address. This means the user's network can be more easily accessed by internet hosts.Click **Application > DDNS** to load the following page.



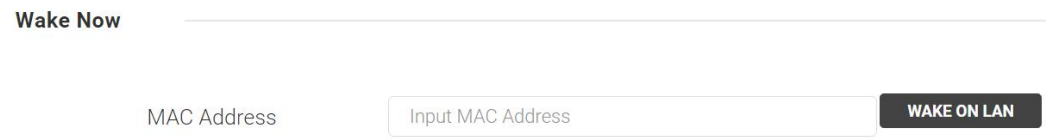
Click the **ADD** button to fill in the DDNS entry.



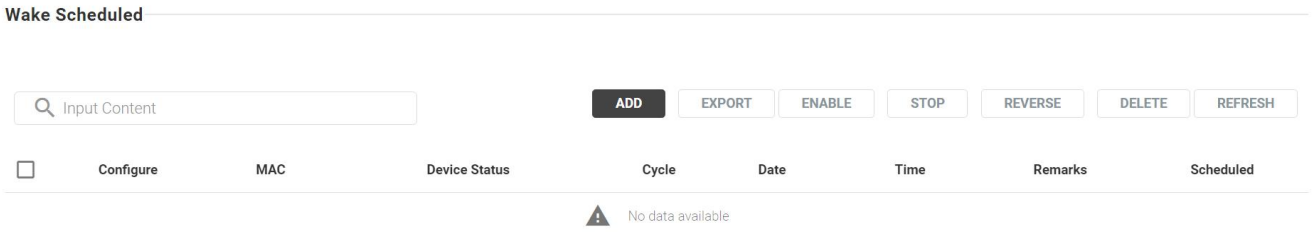
Parameter	Describe
Service Provider	Select the service providers, including Alibaba DNS, dynv6.com, dyndns org, Oray. net, 3322.org.
Enable	Enable or disable DNS entries.
Domain	Input Domain
AppKey	Get the secret key from the service provider.
Password	Enter the password from the service provider.
Protocol	Select IPV4 or IPv6.
Binding Type	Select interface or MAC.
Binding Host MAC	Enter the MAC mapping the intranet device.
Binding Interface	Enter the MAC mapping the intranet interface.

12.3. Wake on LAN

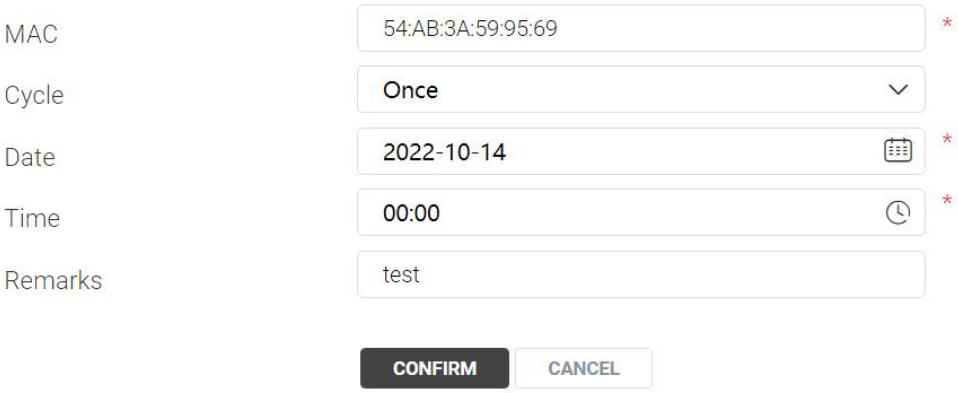
Wake-on-LAN (WoL) is an Ethernet or Token ring computer networking standard that allows a computer to be turned on or awakened by a network message. The message is usuallysent by a program executed on another computer on the same local area network. It is also possible to initiate the message from another network by using subnet directed broadcasts or a WOL gateway service. Click **Application > Wake on LAN** to load the following page.



Parameter	Describe
MAC Address	Enter the MAC address, such as 54: AB: 3A: 59:95:69.
WAKE ON LAN	After entering the MAC address, tap it to wake up immediately.



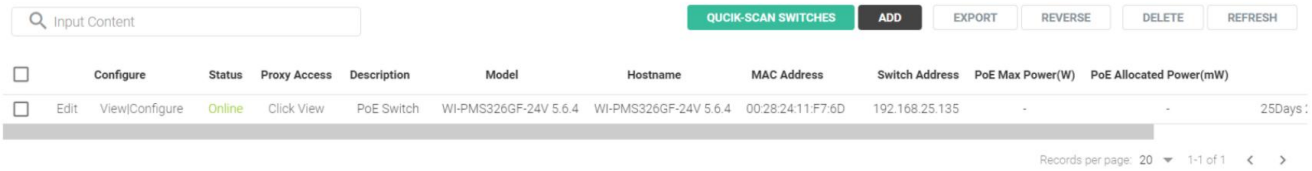
Click the **ADD** button to add an entry.



Parameter	Describe
MAC	Specify MAC Address
Cycle	Specify cycle (Once / Daily / Weekly / Monthly).
Date	Specify date.
Time	Specify time range.
Remarks	Specify input comments.

12.4. Switch Linkage

Use this function to manage switches that support the SNMP protocol through the AC, and only support reading simple port information.Click **Application > Switch Linkage** to load the following page.



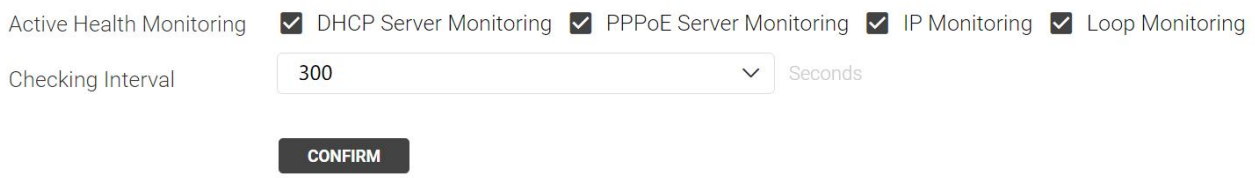
12.5. Smart device

With this feature, the gateway can automatically discover devices with Onvif in the same subnet, such as IP cameras. After the gateway is bound to the cloud 2.0 platform, use the EWEB function to remotely access the web interface.Click **Application > Smart device** to l oad the following page.

13. Security

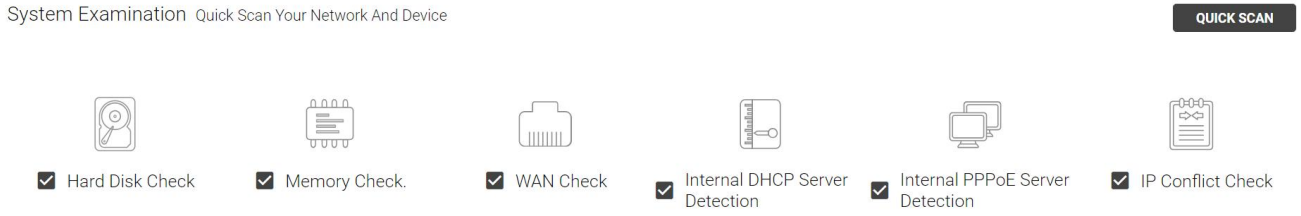
13.1. Health Monitoring

This section is used in conjunction with the Examination function to set the detection cycle. Click **System > Health Monitoring** to load the following page.



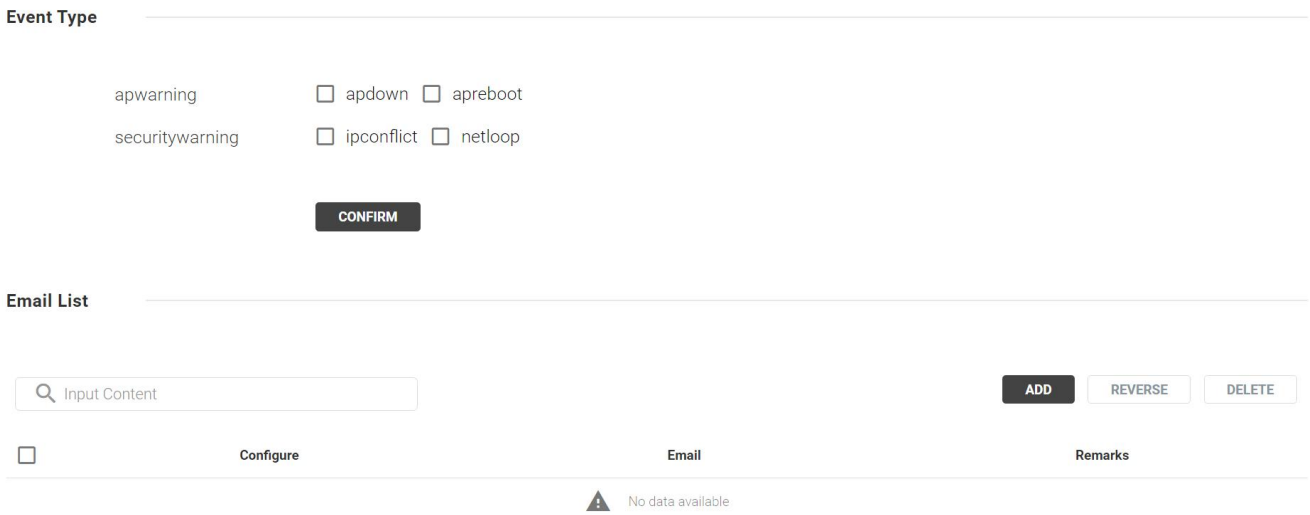
13.2. Examination

This part can locate simple network failures in the intranet.Click **System > Examination** to load the following page.



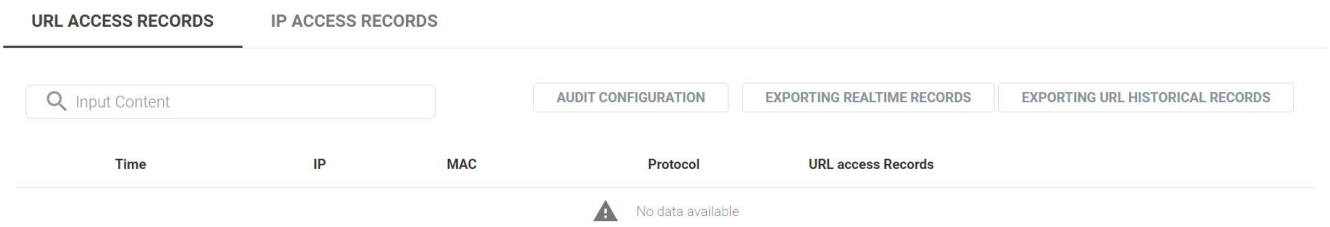
13.3. Email Notice

With this function, when the device has the following 4 states, send an alarm email through the bound mailbox.Click **System > Email Notice** to load the following page.

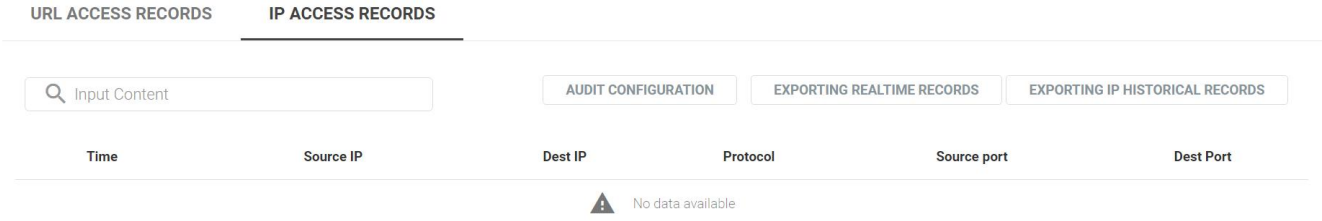


13.4. Audit

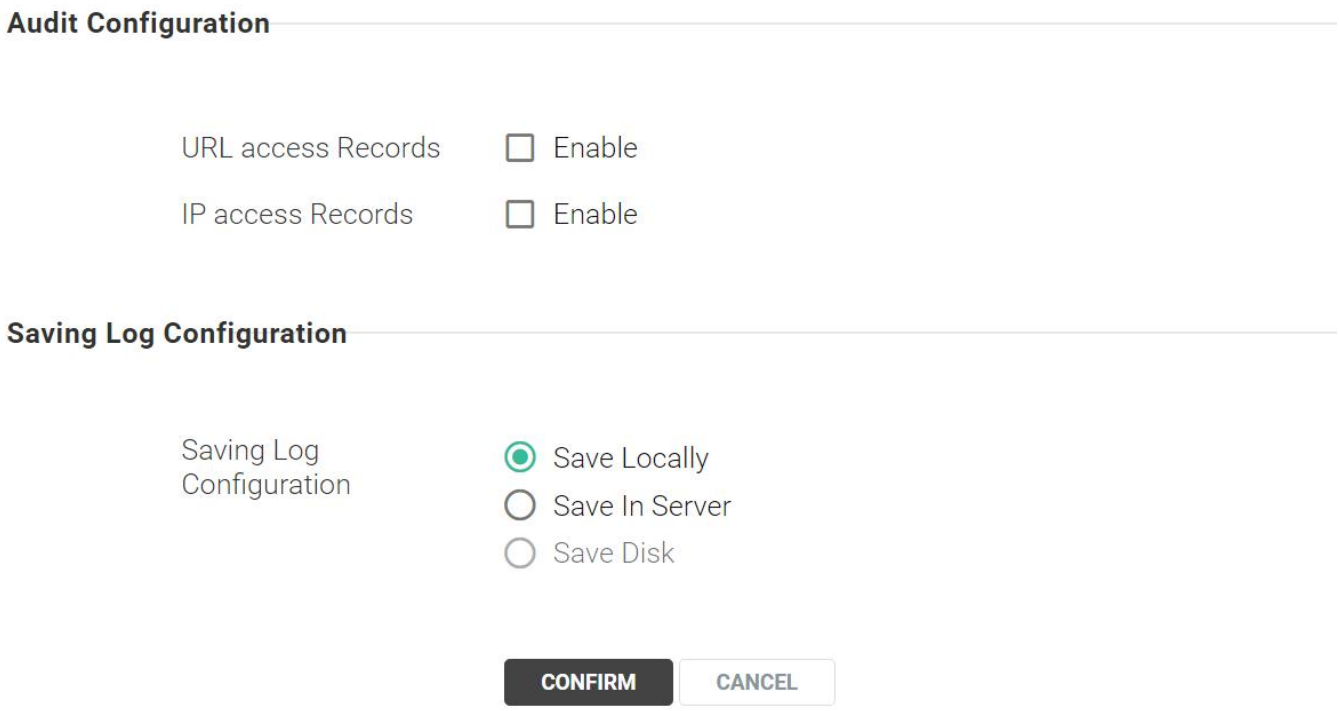
This part is the URL and IP behavior records for LAN clients to access the Internet. Click **Security > Audit > URL ACCESS RECORDS** to load the following page.



Click **Security > Audit > IP ACCESS RECORDS** to load the following page.



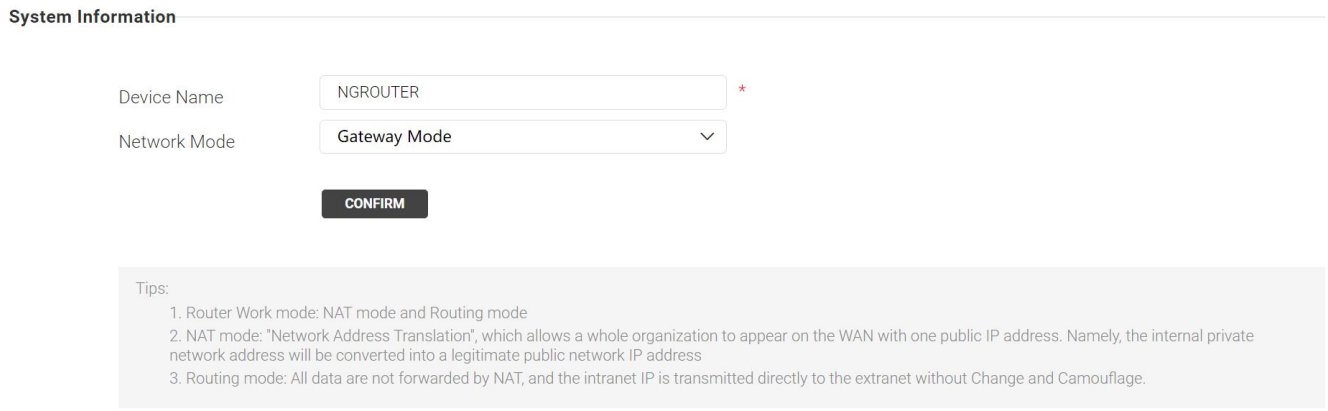
You can enable URL or IP access records and set the storage of log records.Click **AUDIT CONFIGURATION** to load the following page.



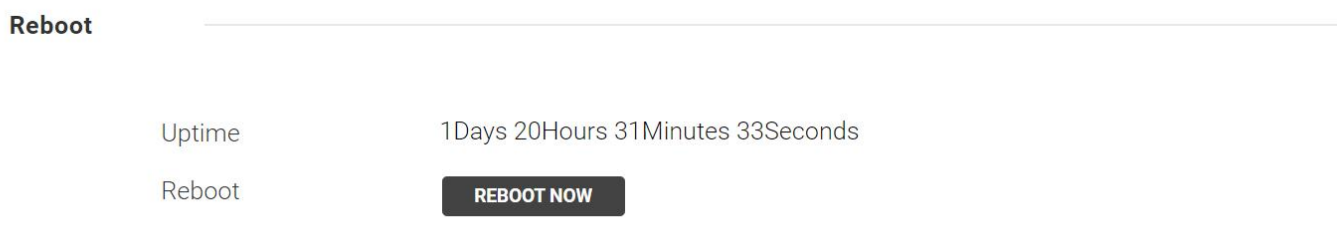
14. System

14.1. System Maintenance

Click **System > System Maintenance** to load the following page.

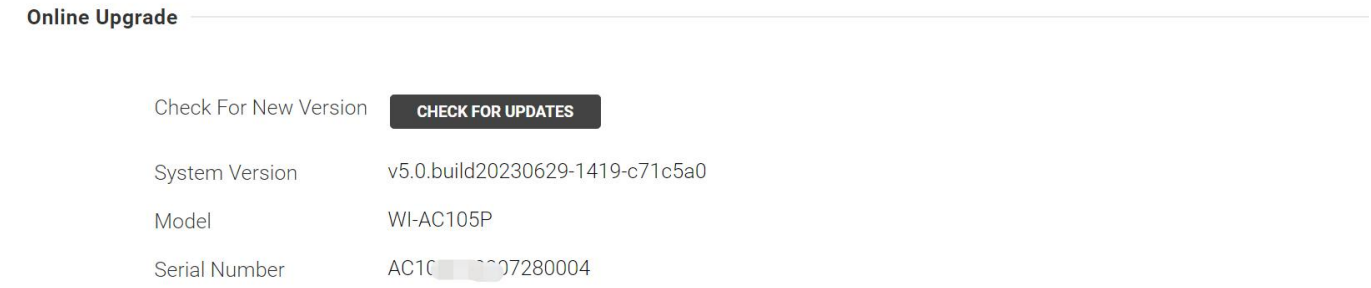


Parameter	Describe
Device Name	Specify a name for gateway.
Network Mode	Network mode: **Gateway mode** and **Router mode.** **Gateway mode**: "Network Address Translation", which allows a whole organization to appear on the WAN with one public IP address. Namely, the internal private network address will be converted into a legitimate public network IP address. **Router mode**: All data are not forwarded by NAT, and the intranet IP is transmitted directly to the extranet without Change and Camouflage.

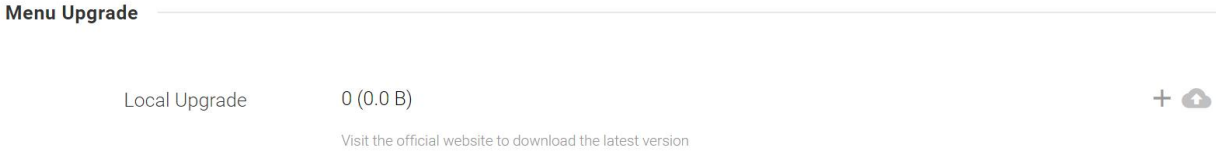


Parameter	Describe

Uptime	Display device running time.
Reboot	Click it to reboot the device.



Parameter	Describe
System Version	Display the firmware version of the device.
Model	Display device model.
Serial Number	Display the SN of the device.

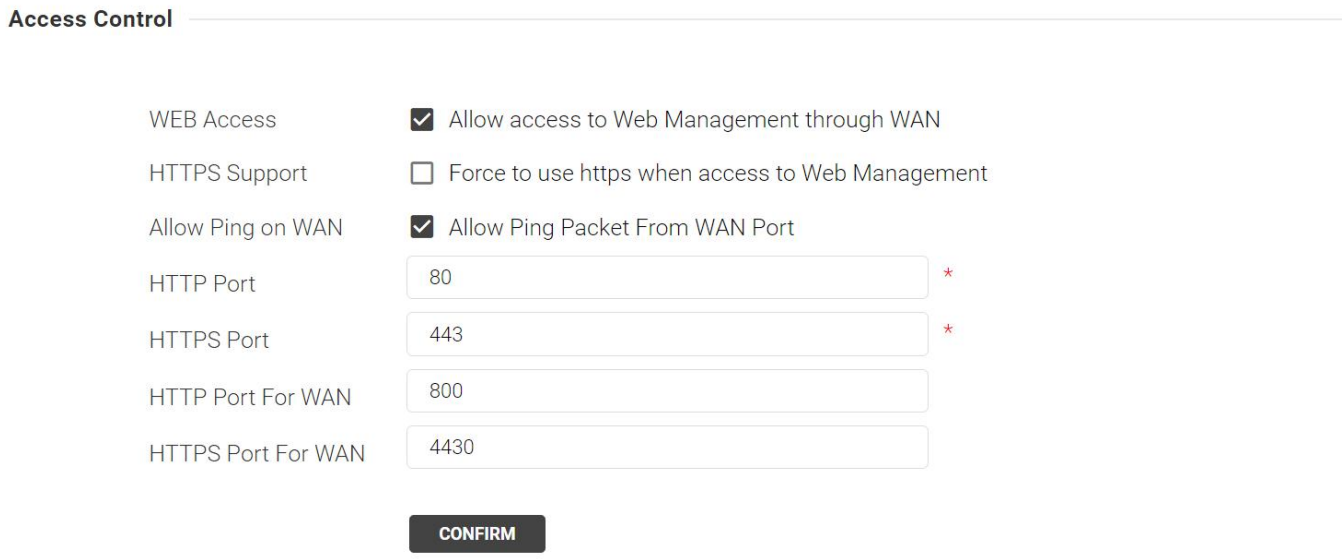


Parameter	Describe
Local Upgrade	Display the name of the uploaded firmware.
+	Click on it to upload firmware.
	Click on it to upgrade the firmware.

Parameter	Describe
Last Backup Time	Display Last Backup Time.
+	Click on it to upload backup files.
	Click on it to upgrade backup files.

14.2. Remote Access

Click **System > Remote Access** to load the following page.



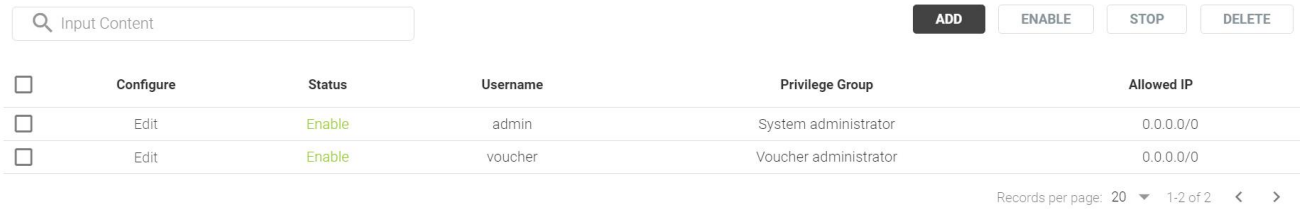
Parameter	Describe
WEB Access	Tick box allow access to Web Management through WAN.
HTTPS Support	Tick box force to use https when access to Web Management.
Allow Ping on WAN	Tick box allow Ping packet from WAN port.
HTTP Port	Specify the HTTP port for accessing the web interface through LAN.
HTTPS Port	Specify the HTTPS port for accessing the web interface through LAN.
HTTP Port For WAN	Specify the HTTP port for accessing the web interface through

	the WAN.
HTTPS Port For WAN	Specify the HTTPS port for accessing the web interface through the WAN.

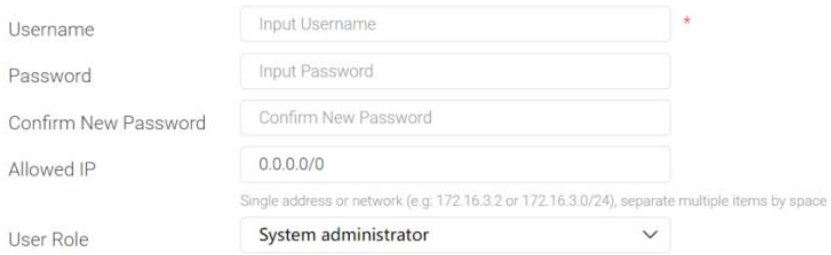
With a third-party log server, device log records can be synchronized to the log server.

14.3. User Management

You can use different user account to log in to the AC50. The administration authority varies among different roles.Click **System > User Management** to load the following page.



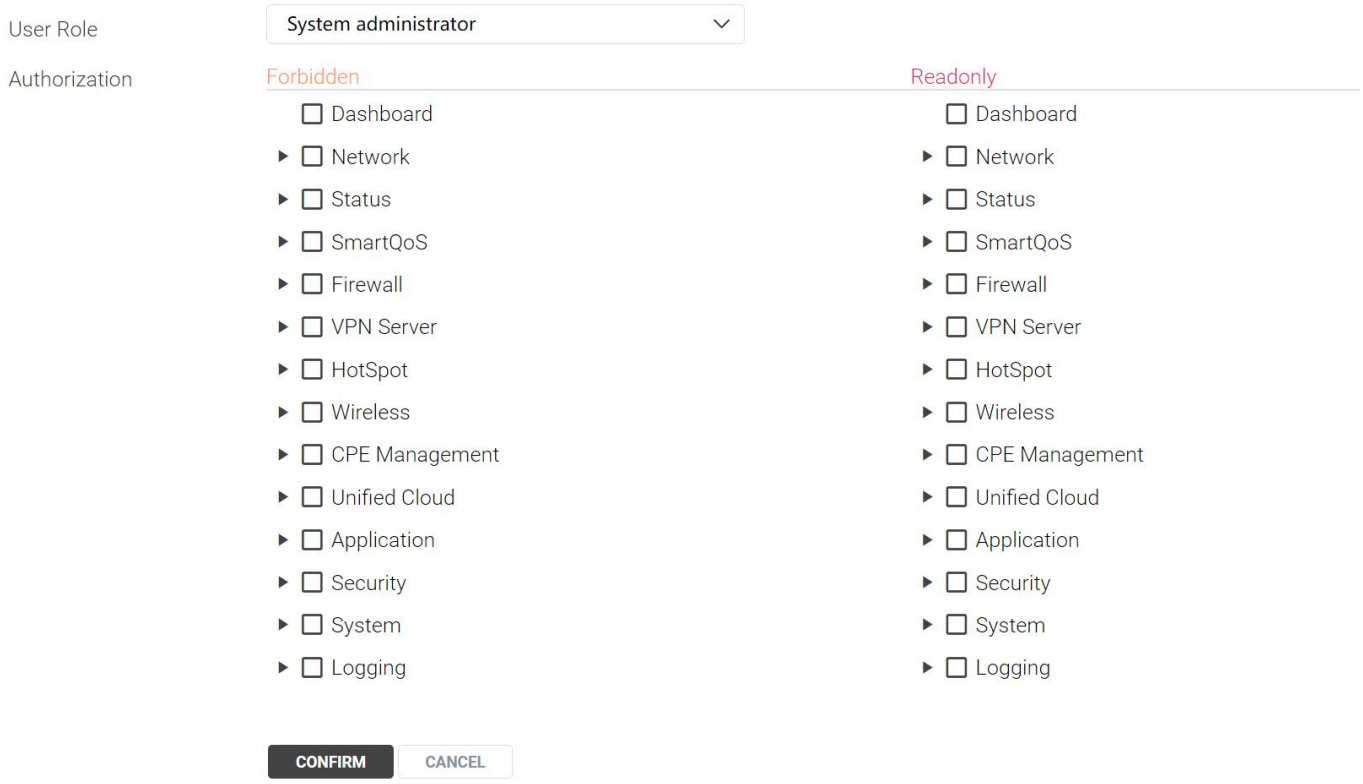
Then click **ADD** to load the following page.



Parameter	Describe

Username	Specify account name.
Password	Assign a password for the account.
Confirm New Password	Confirm password again
Allowed IP	Restrict allowed access to IP addresses
User Role	Select the role type: Voucher administrator and System administrator.

Select the role of **System administrator**, you will be able to select the access rights of functional modules.



14.4. Diagnosis

Ping and traceroute are both used to test the connectivity between two devices in the netw ork. In addition, ping can show the roundtrip time between the two devices directly and trac eroute can show the IP address of routers along the route path.Click **System > Diagnosis** to load the following page.

PING

IP or Domain: Input IP or Domain,e.g. 192.168.1.1 *

Protocol: IPV4

Interface: ANY

PING Count: 4 time

Result

START TESTING

Tracert

IP or Domain: Input IP or Domain,e.g. 192.168.1.1 *

Protocol: IPV4

Interface: ANY

Result

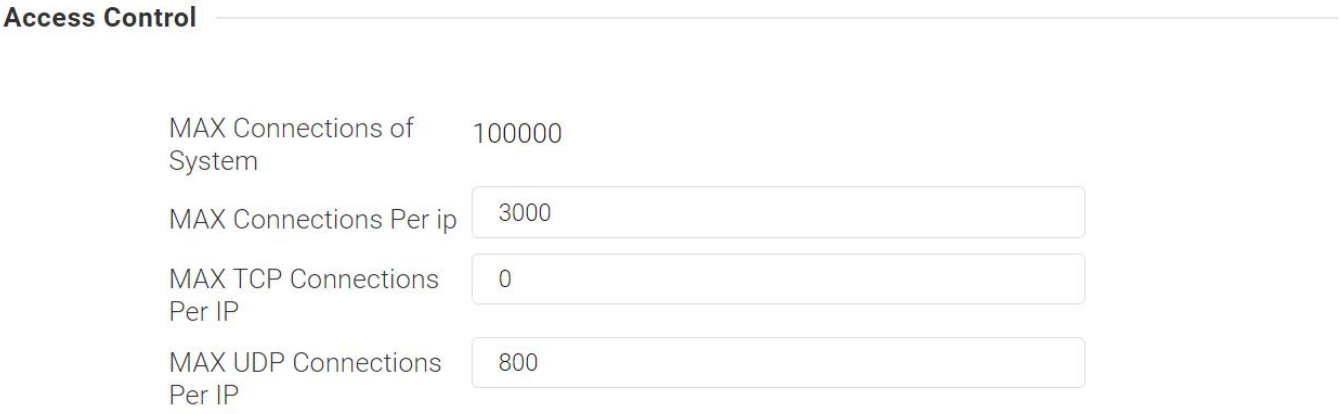
START TESTING

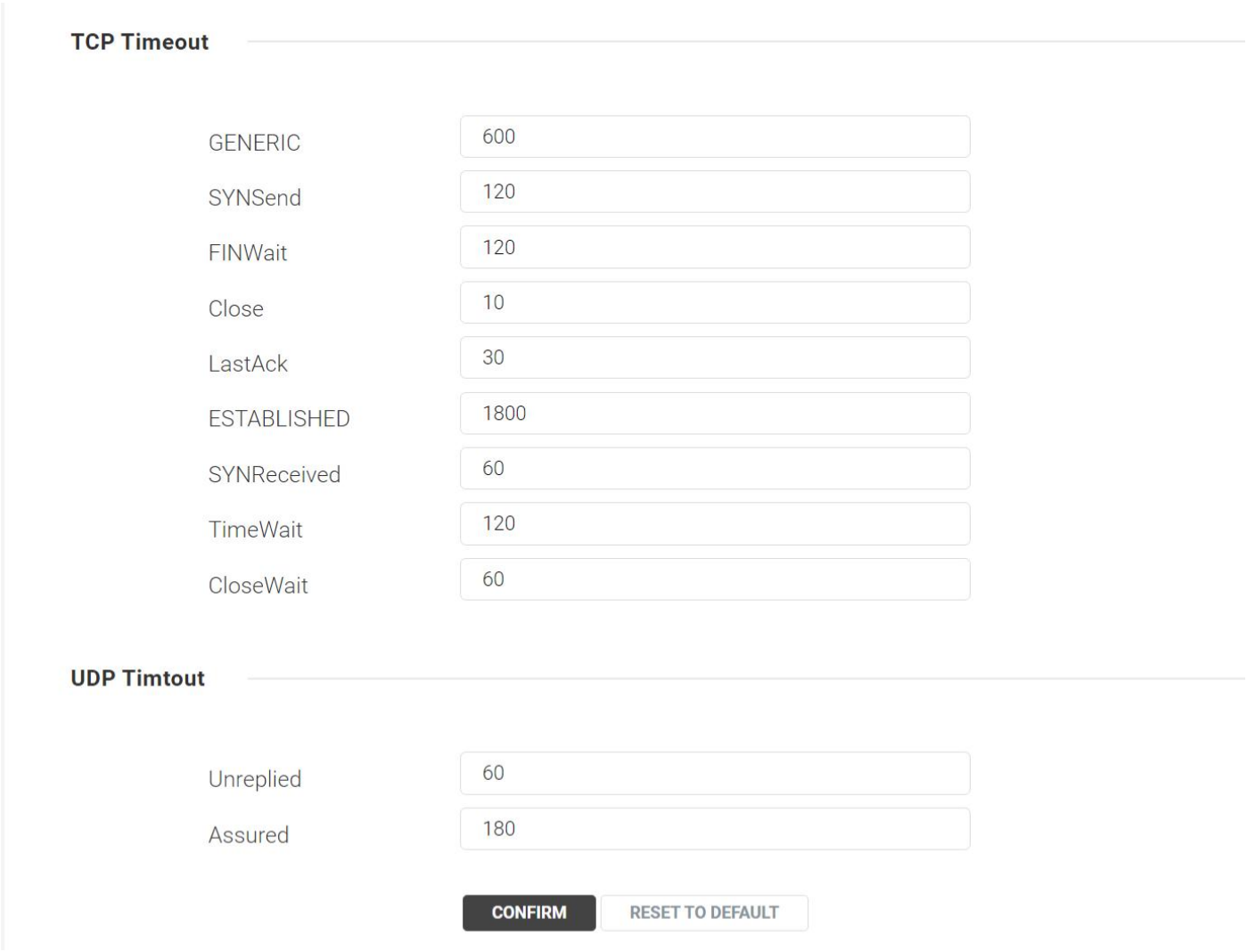
14.5. Network Tools

The gateway is equipped with a built-in Telnet tool, making it convenient for administrators t o log in remotely.Click **System > Network Tools** to load the following page.

14.6. Network Parameters

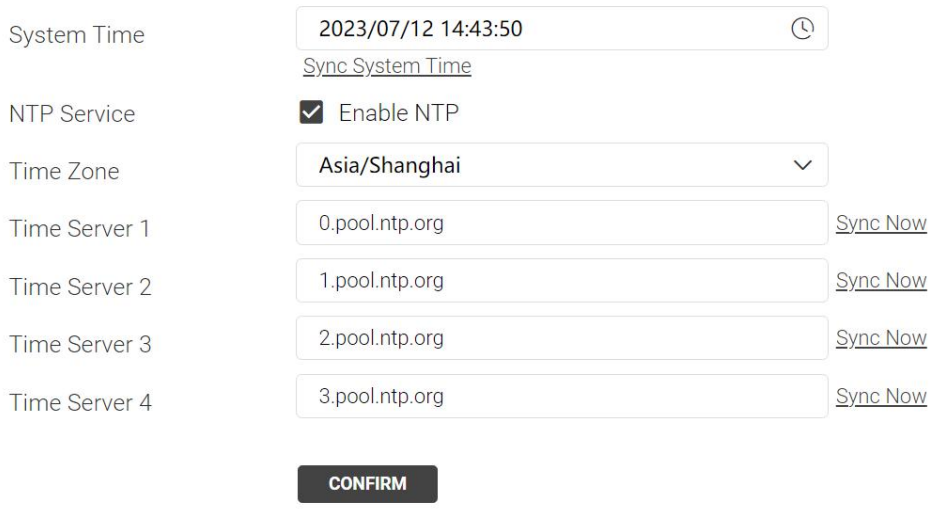
This displays the settings for TCP and UDP session parameters. If there are no special req uirements, please keep the default parameters.Click **System > Network Parameters** to load the following page.





14.7. System Time

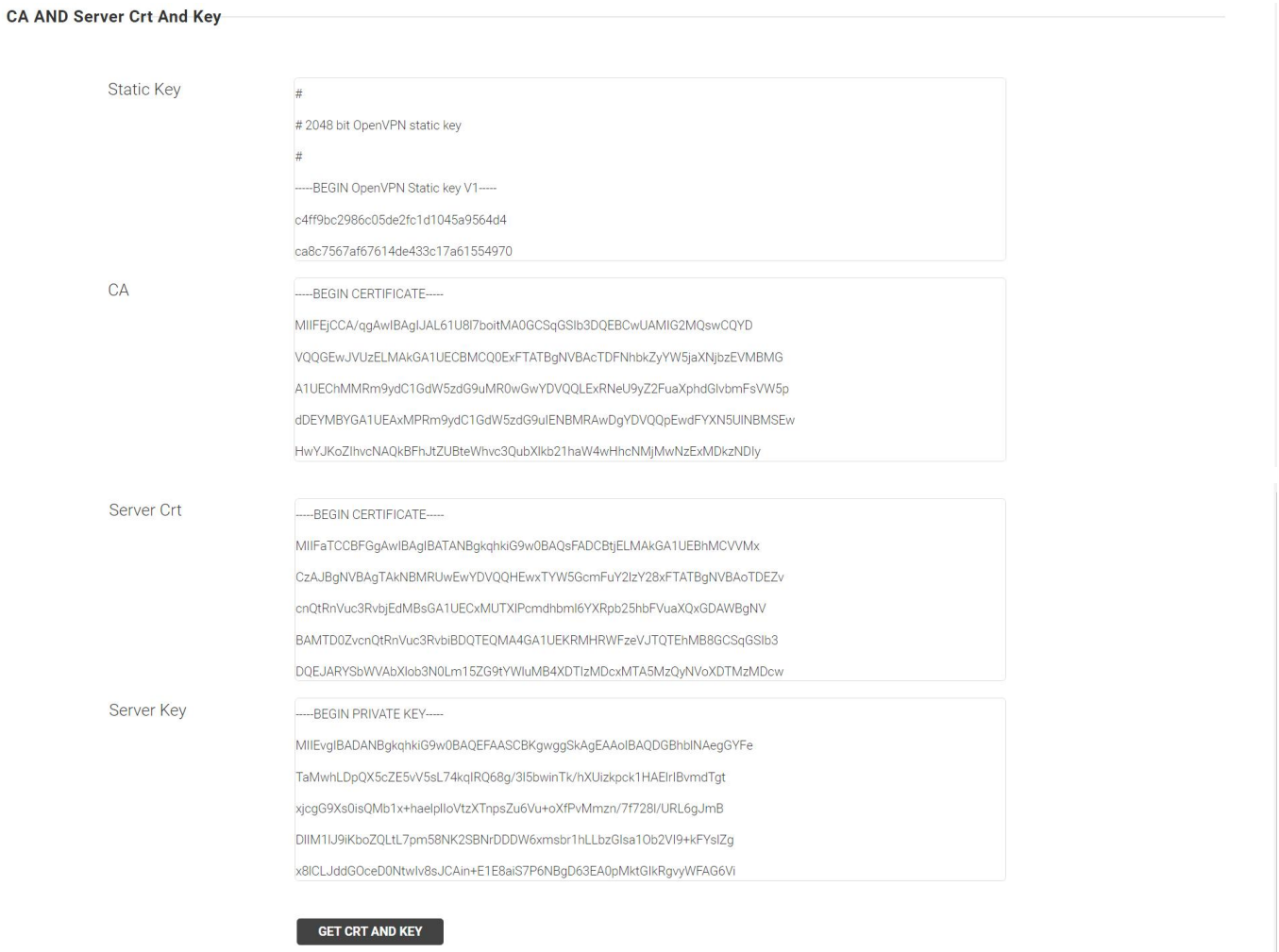
This displays the settings for system time parameters.Click **System > System Time** to load the following page.



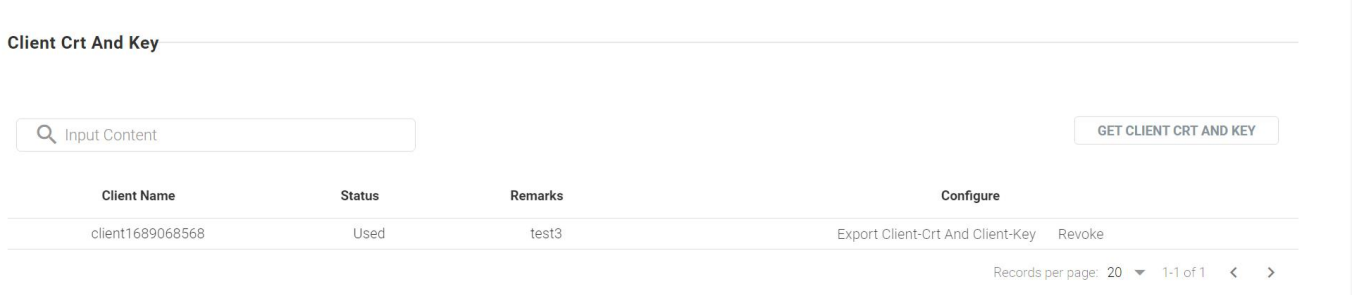
14.8. CA Configuration

Provide certificates and keys for OpenVPN.Click **System > CA Configuration** to load the fo llowing page.

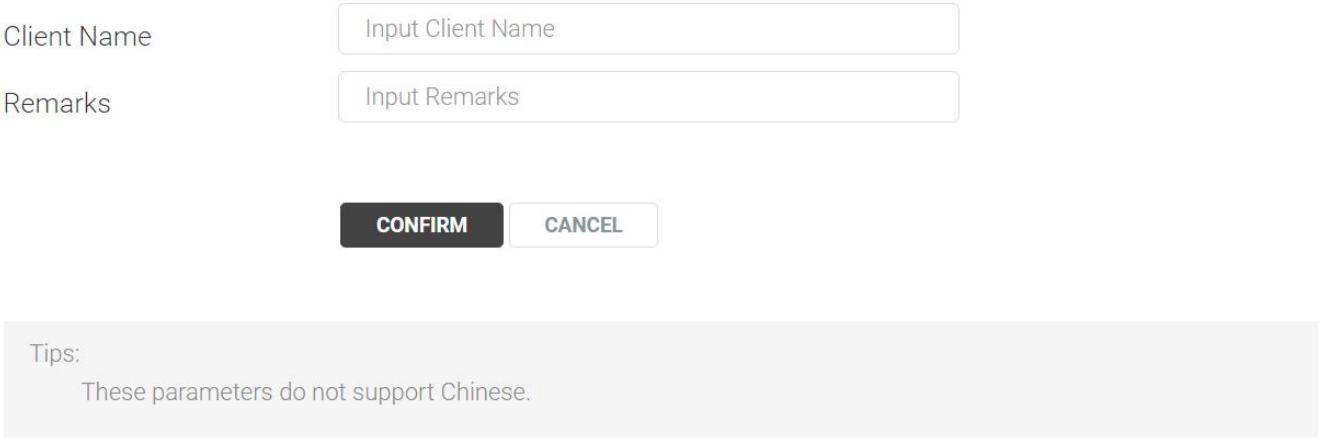
Click the **GET CERT AND KEY** button, and the certificate and key will be automatically ge nerated, and then automatically synchronized to the OpenVPN server.



If there is an OpenVPN client connected to the OpenVPN server, it will appear in the follow ing list.



If you need to create a certificate and secret key for the OpenVPN client, Click on the **GE P CLIENT CRT AND KEY** button to load the following page.


Client Name
Input Client Name
Remarks
Input Remarks
CONFIRM
CANCEL
Tips:
These parameters do not support Chinese.