Ruijie Reyee RG-EG Series Routers

Web-Based Configuration Guide

Copyright Statement

Exemption Statement

Preface

Thank you for using our products.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

1 Overview

eWeb is a Web-based network management system that manages or configures devices. You can access eWeb via browsers such as Google Chrome.

Web-based management involves a Web server and a Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

1.1 Conventions

In this document, texts in bold are names of buttons (for example, **OK**) or other graphical user interface (GUI) elements (for example, **DHCP Security**).

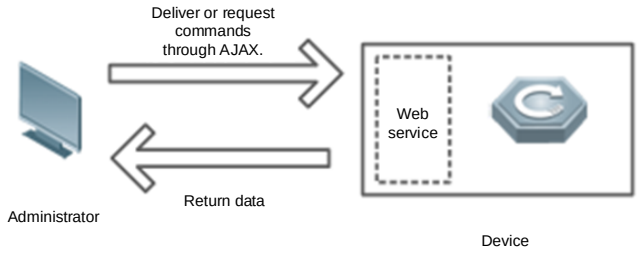
2 Configuration Guide

2.1 Preparation

Scenario

As shown in the figure below, an administrator can access the device from a browser and configure the device through the eWeb management system.

Figure 2-1 Data Exchange Principle



Remarks	The eWeb management system combines various device commands and then delivers them to the device through AJAX requests. The device then returns data based on the commands. A Web service is available on the device to process basic HTTP protocol requests.

Deployment

Configuration Environment Requirements

Client requirements:

- An administrator can log into the eWeb management system from a Web browser to manage devices. The client refers to a PC or some other mobile endpoints such as laptops or tablets.
- Google Chrome, Firefox, IE10.0 and later versions, and some Chromium-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned and the GUI is less artistic, or other exceptions may occur.
- The client IP address is set in the same LAN network as the device IP address, such as 192.168.110.X. The subnet mask is 255.255.255.0. The default management address is 192.168.110.1. Alternatively, you can set the IP assignment mode to **Obtain an IP address automatically**.

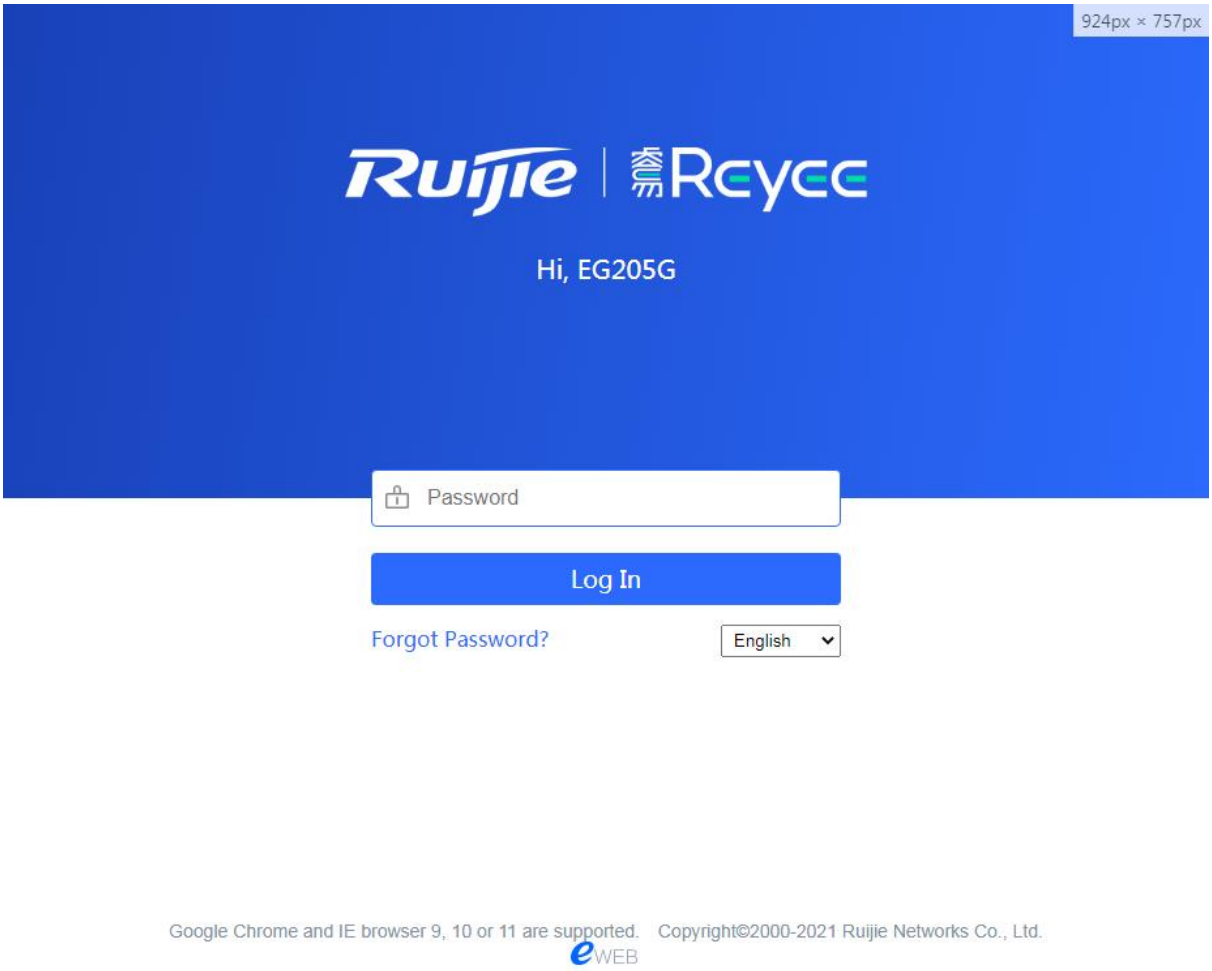
Server requirements:

- You can log into the eWeb management system through a LAN port or from Ruijie Cloud on an external network.
- The device is enabled with Web service (enabled by default).

- The device is enabled with login authentication (enabled by default).
- The default IP address of an EG device is 192.168.110.1. The default IP address of an AP is 10.44.77.254.

To log into the eWeb management system of an EG device, open the Google Chrome browser, and enter 192.168.110.1 into the address bar, and press **Enter**.

Figure 2-2 Login Page



Enter the password and click **Login**.

2.2 Network Setup

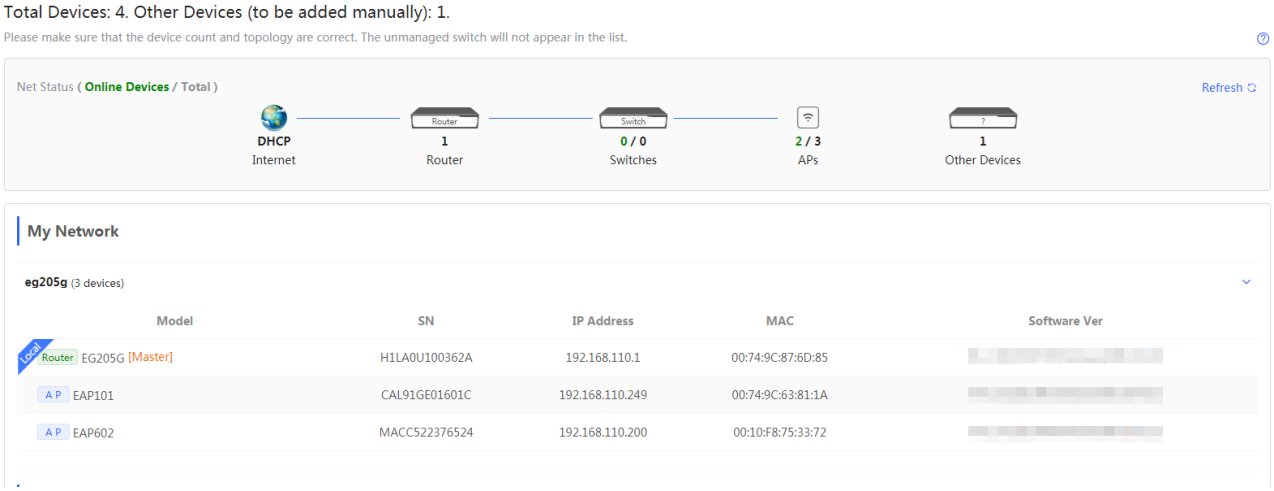
You will enter the **Network Setup** page without login at initial setup.

2.2.1 Discover Device

The page displays online device count and network status.

You can add the device to **My Network** before configuring the network. If the device works in the standalone mode, this feature is not supported.

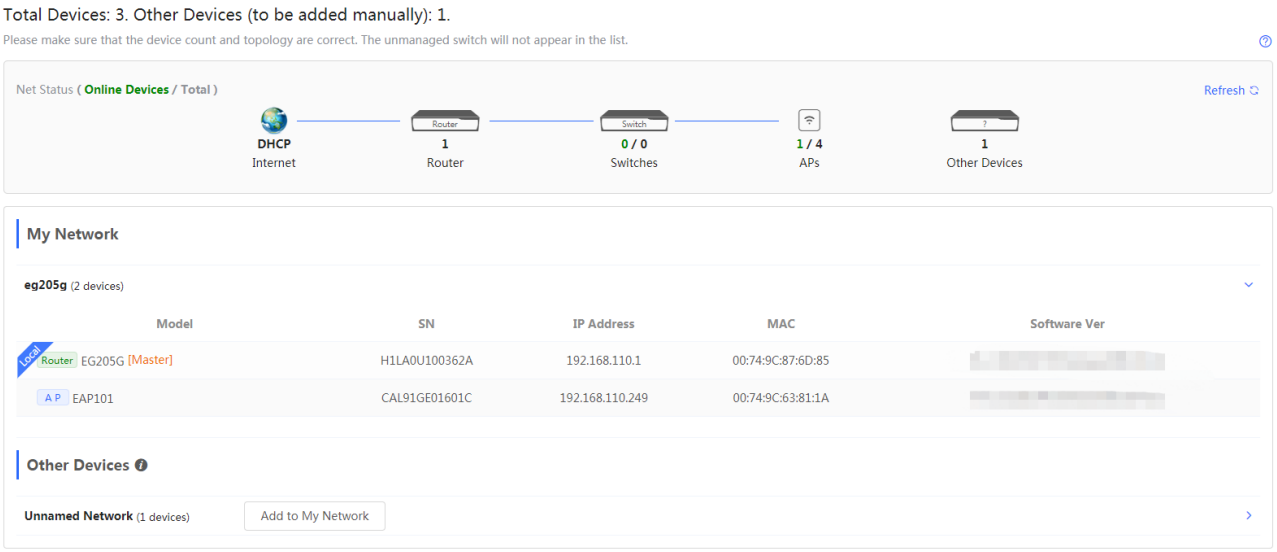
Figure 2-3 Discover Device



2.2.2 Add to My Network

Select the target device and click **Add to My Network**. If the target device is not configured yet, you can add the device directly without a password.

Figure 2-4 Add Device to My Network

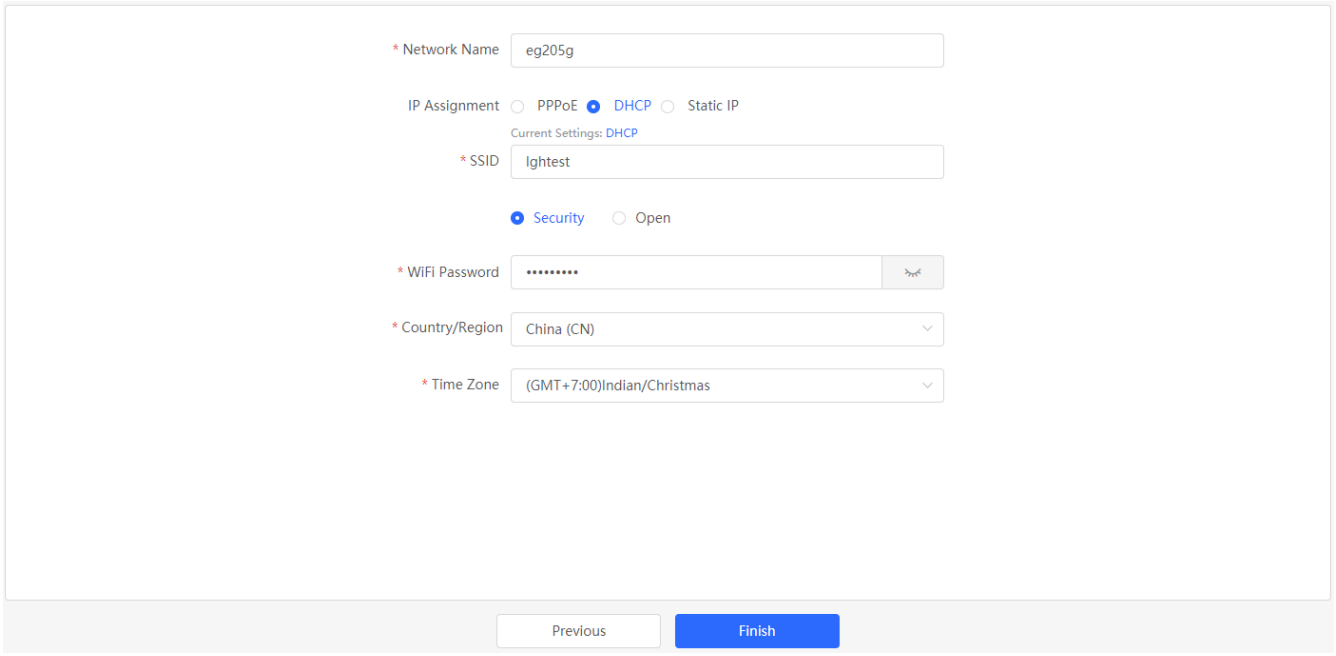


2.2.3 Create Network & Connect

If the device is configured for the first time, the network name, management password and SSID are required. If the device is already configured, the management password will not be displayed here. You can navigate to **Network** > **Password** to change the management password.

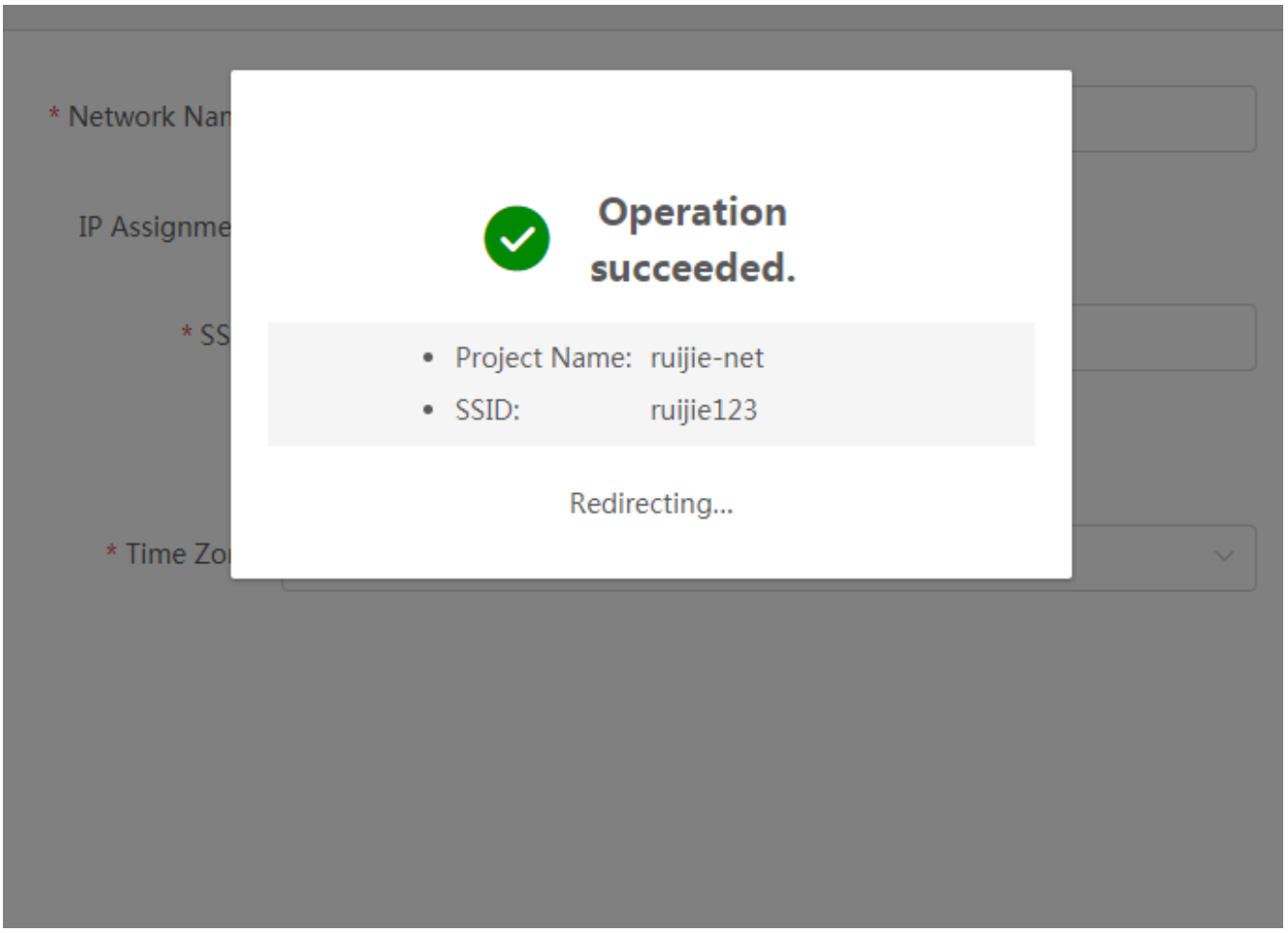
If the device is detected disconnected to Ruijie Cloud, the Ruijie Cloud page will be embedded for you to bind your account after the device accesses the Internet successfully. If the device is already connected to Ruijie Cloud, the eWeb homepage will be displayed after this step.

Figure 2-5 Create Network



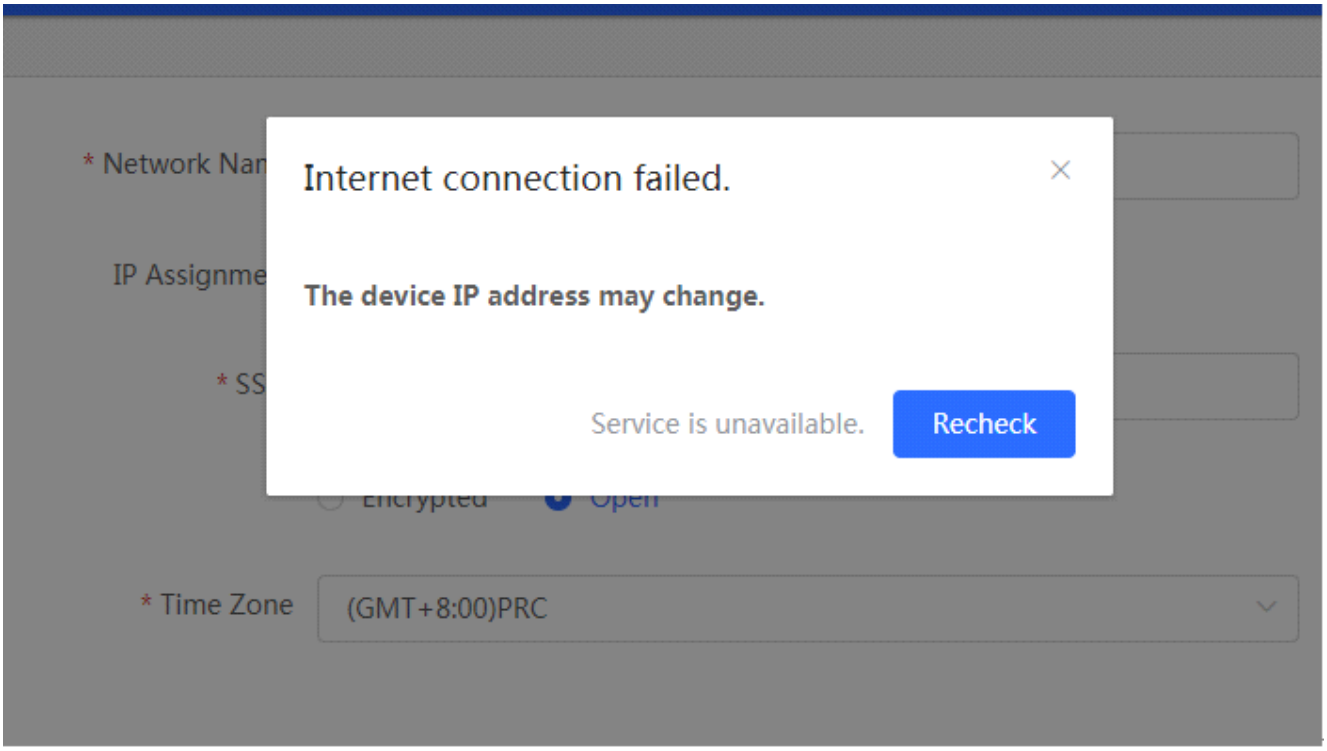
Click **Create Network & Connect**, and it takes about 60 seconds to deliver and activate settings. The following message will appear after Internet connection is set up.

Figure 2-6 Connect to Internet



If the Internet connection failed, please follow the instruction in the prompt message.

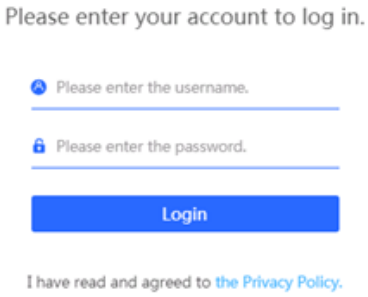
Figure 2-7 Failed Connection



2.2.4 Cloud Service

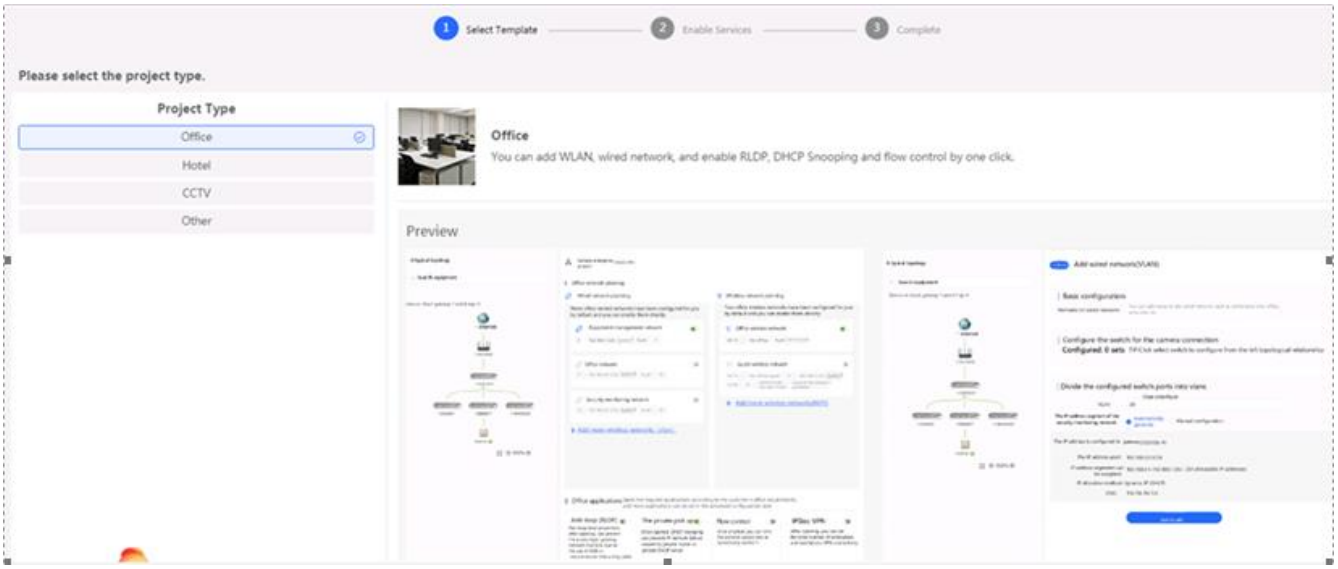
The **Network Setup** module requires a Ruijie Cloud account. If you are a new user, please register an account first at the Ruijie Cloud website.

Figure 2-8 Log In with Ruijie Cloud Account



If the device works in the standalone mode, log in and the account will be binded with Ruijie Cloud automatically. If the device works in the self-organizing network mode, the following page will appear.

Figure 2-9 Select Template



It takes about 3 minutes to discover devices and generate a topology. The following confirmation box will appear:

Figure 2-10 Confirm Device Status

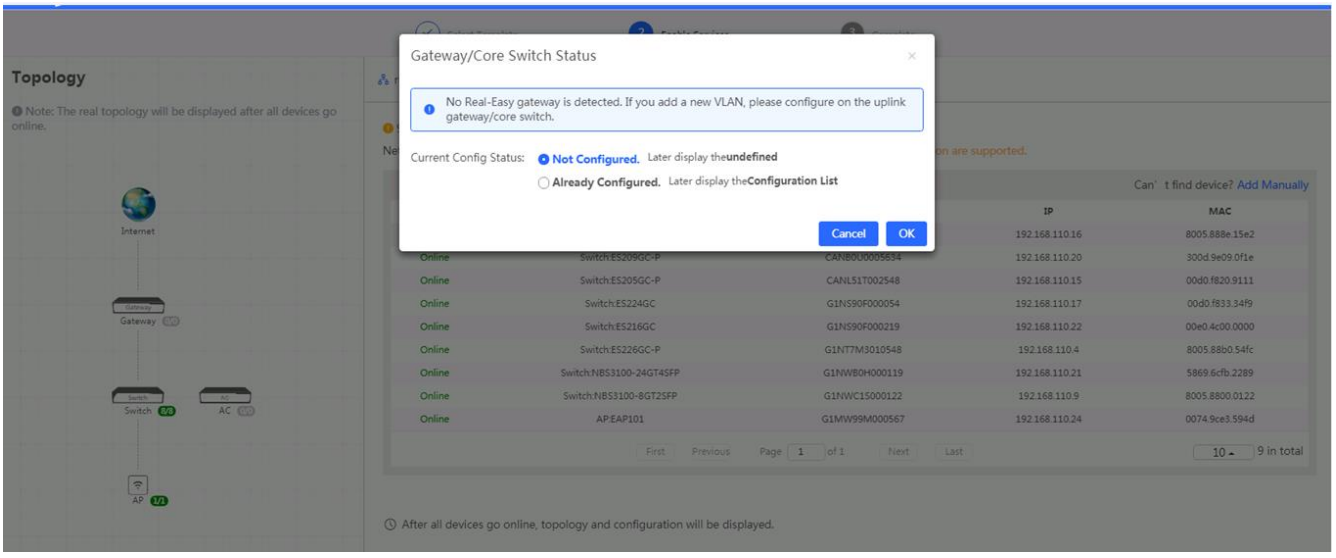
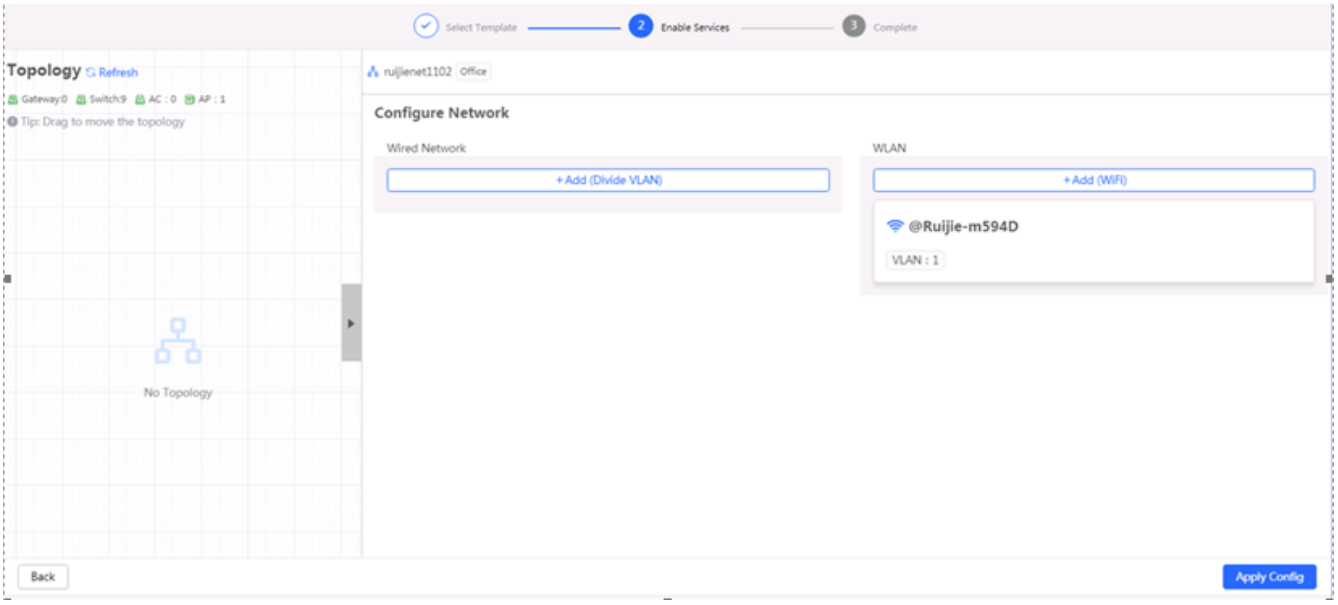
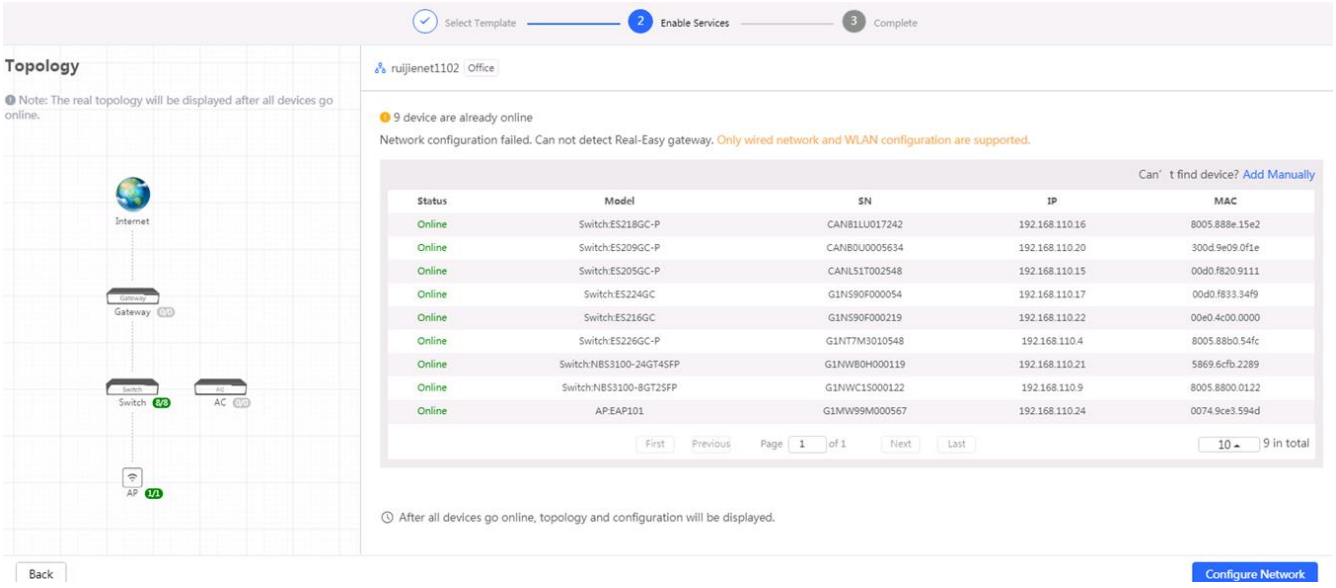


Figure 2-11 Enable Services



Click **Apply Config**. The following page will appear after configuration is delivered successfully.

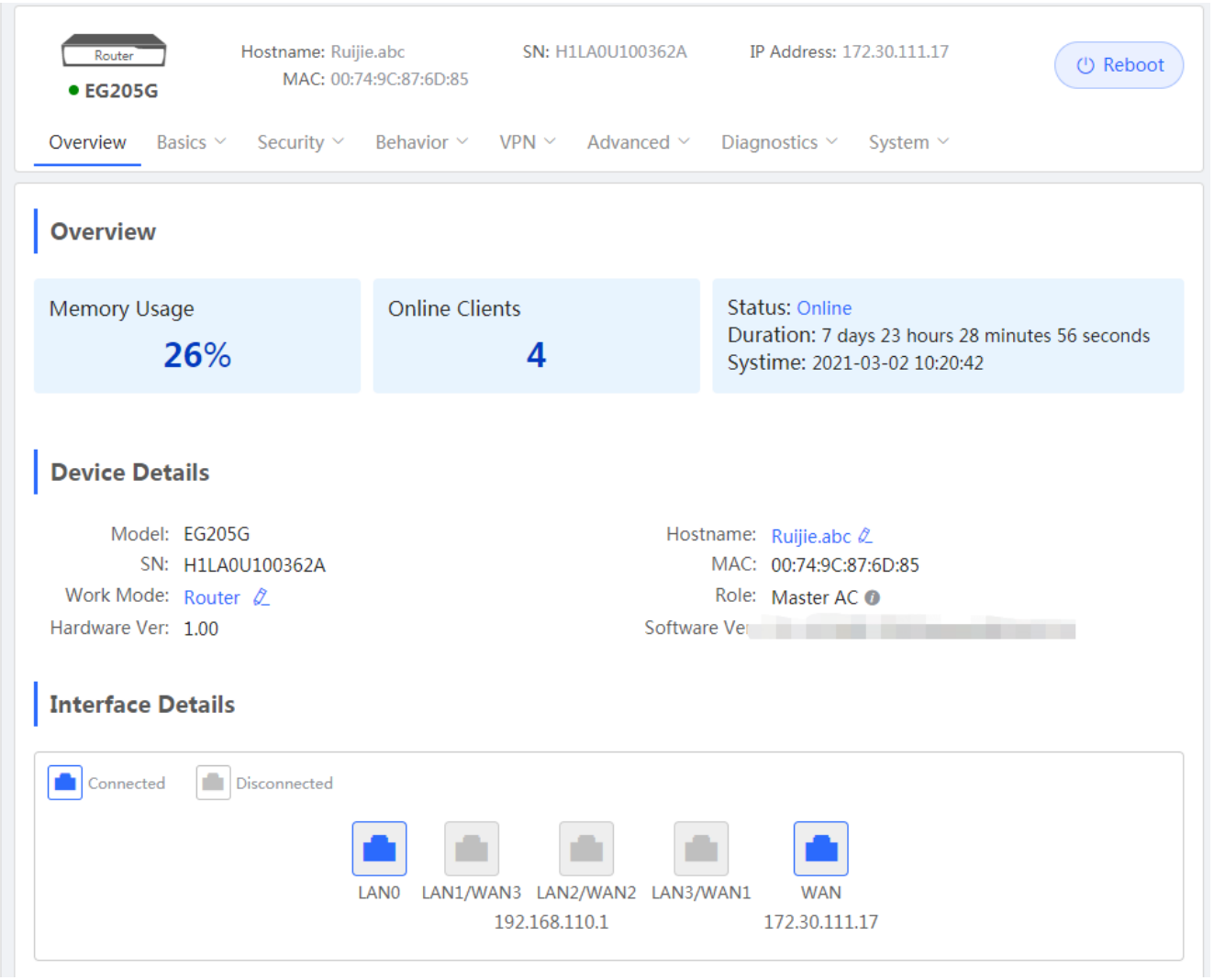
Figure 2-12 Complete



2.3 Work Mode

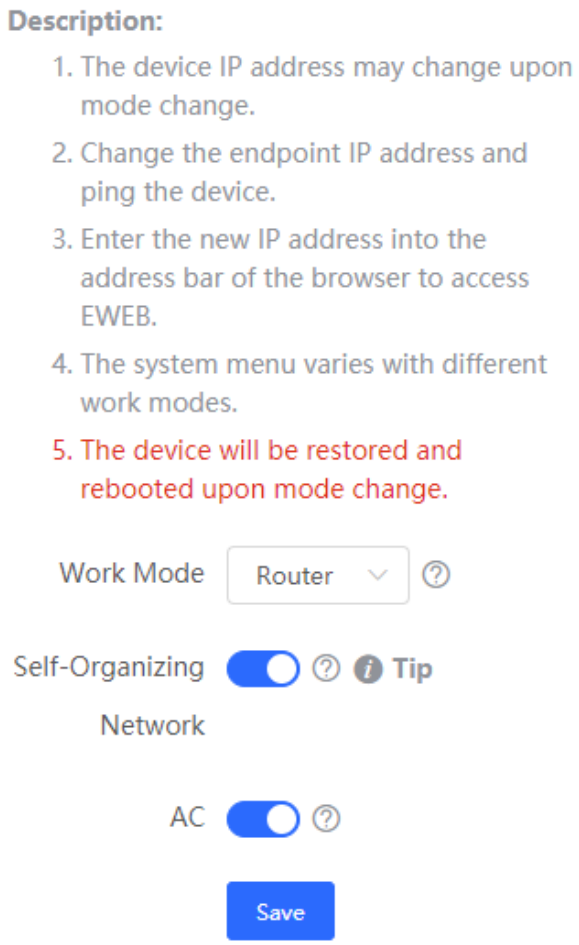
The eWeb menu varies with different work modes. The EG device works in the **Router** mode and the EAP device works in the **AP** mode by default. The work mode is displayed on the **Route > Overview** page.

Figure 2-13 Device Overview



Click the current work mode, and the following page will appear. You can switch over the work mode here.

Figure 2-14 Work Mode



2.3.1 Router Mode

The **Router** mode indicates NAT forwarding.

The EG device in the **Router** mode contains networking, network setup and gateway features including VPN and behavior management.

The AP in the **Router** mode contains networking, network setup and some radio features.

2.3.2 AC/AP Mode

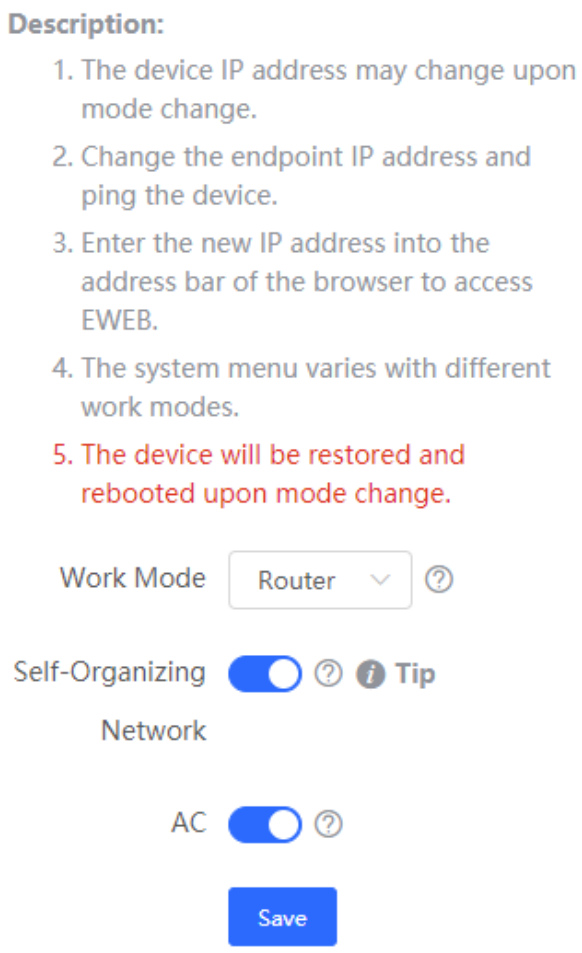
The device in the **AC** mode supports router-on-a-stick.

The **AP** mode refers to fit AP mode. All WAN ports are enabled with DHCP by default. You can configure a WAN port with a static IP address or enable PPPoE manually.

2.4 Self-Organizing Network

Click the current work mode, and the following page will appear. You can enable or disable self-organizing network here.

Figure 2-15 Self-Organizing Network

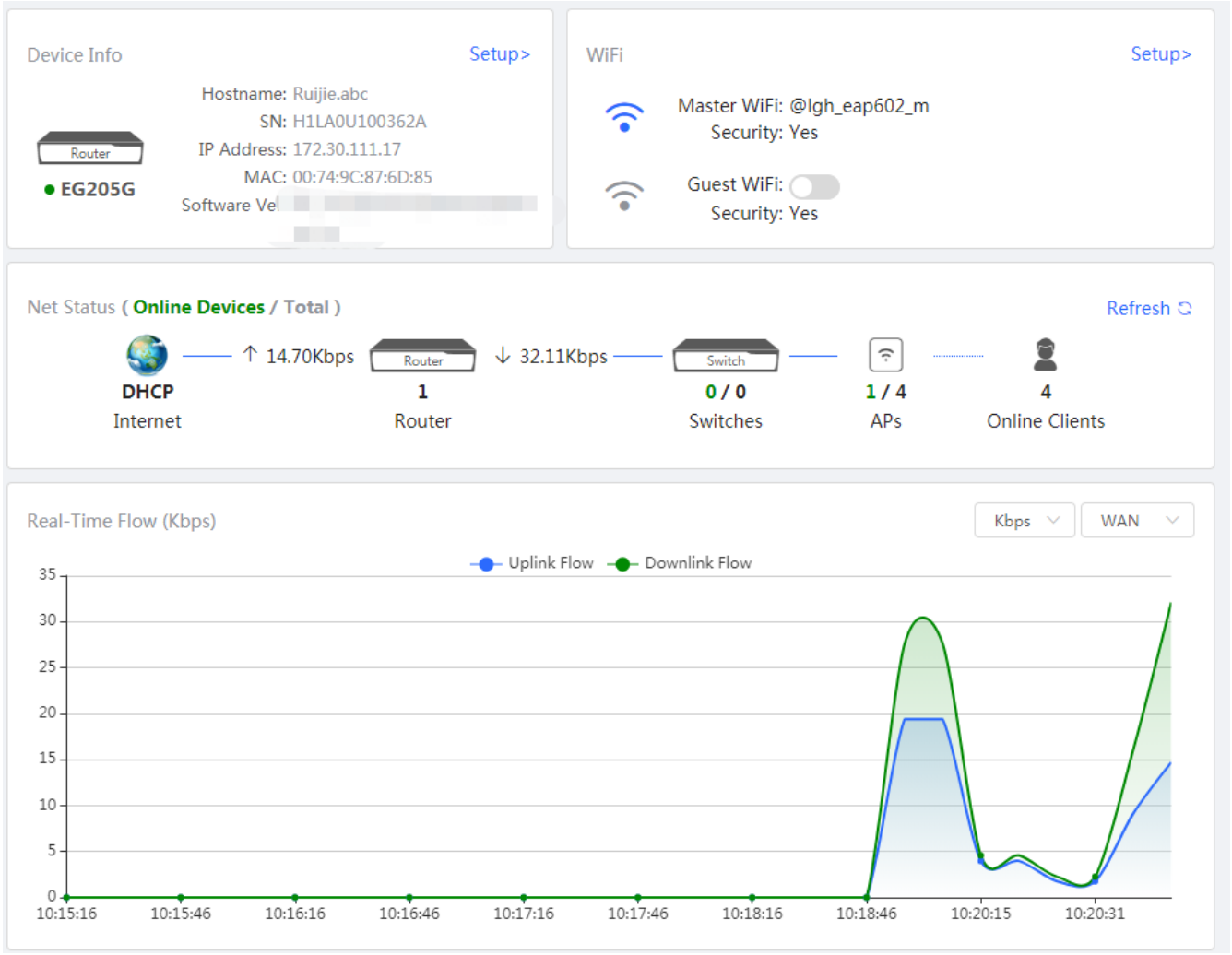


2.4.1 Enable

If self-organizing network is enabled, the device in the network will be discovered and discover other devices. These devices will form a network and be synchronized with network settings.

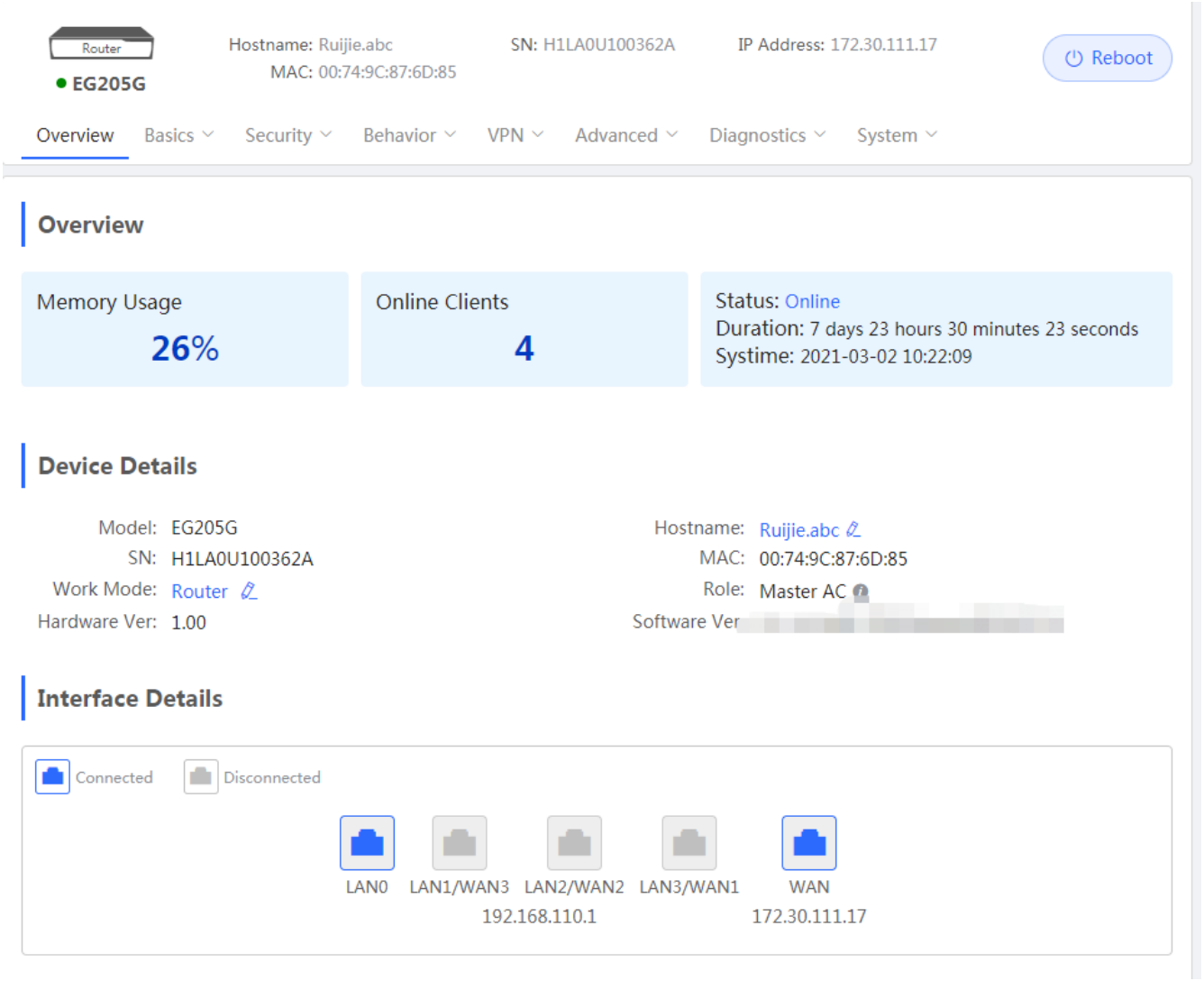
The menu on the left contains all network settings, including wireless management, switch management and system management.

Figure 2-16 Enable Self-Organizing Network



If there is a wireless router enabled with self-organizing network in the network, the **Router** module will appear in the menu on the left. Click **Router**_Gateway, and a horizontal menu will be displayed.

Figure 2-17 Router Menu

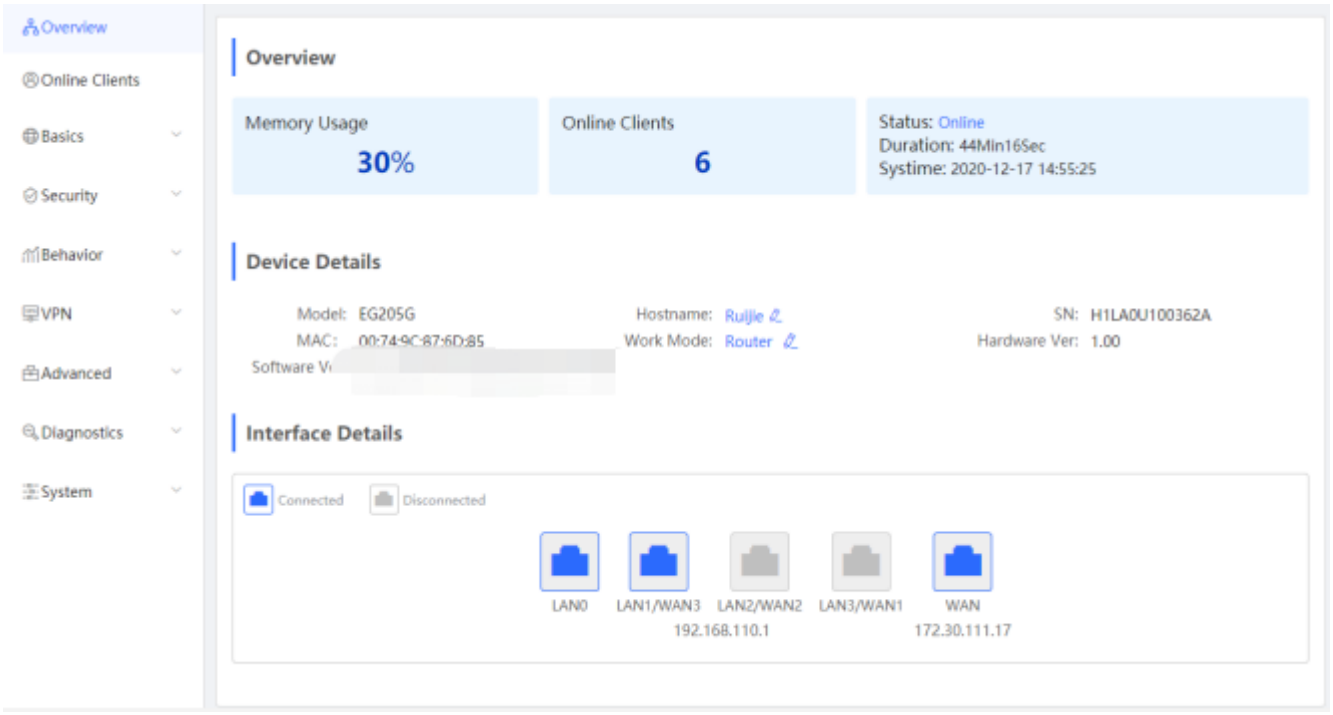


2.4.2 Disable

If self-organizing network is disabled, the device will work in the standalone mode.

After self-organizing network is disabled, a horizontal menu will be displayed vertically on the left.

Figure 2-18 Disable Self-Organizing Network

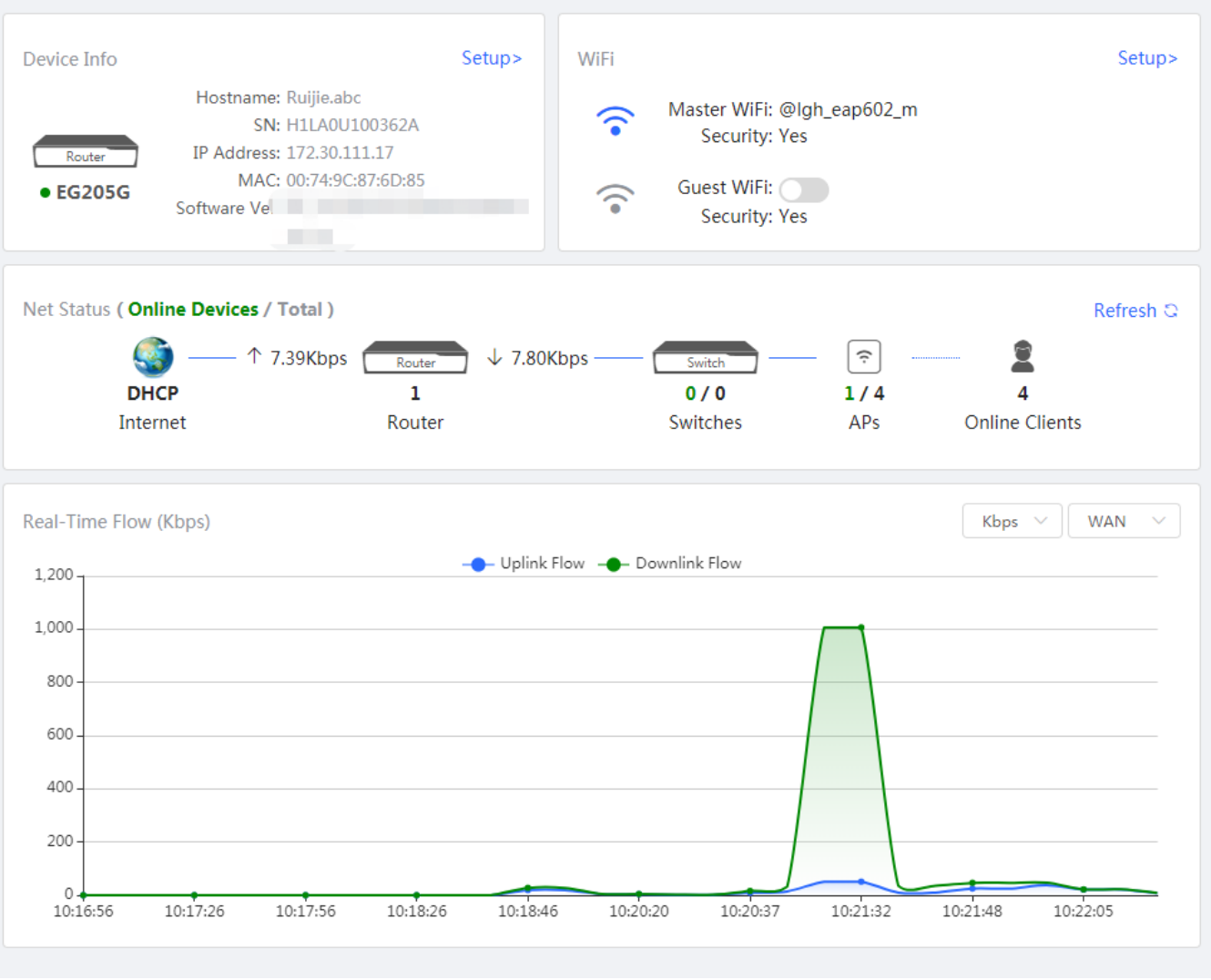

Overview
Online Clients
Basics
Security
Behavior
VPN
Advanced
Diagnostics
System
Overview
Memory Usage
30%
Online Clients
6
Status: Online
Duration: 44Min16Sec
Systime: 2020-12-17 14:55:25
Device Details
Model: EG205G
MAC: 00:74:9C:87:6D:85
Software V
Hostname: Ruijie
Work Mode: Router
SN: H1LA0U100362A
Hardware Ver: 1.00
Interface Details
Connected
Disconnected
LAN0
LAN1/WAN3
LAN2/WAN2
LAN3/WAN1
WAN
192.168.110.1
172.30.111.17

3 eWeb Configuration

3.1 Overview

The **Overview** page displays login device, wireless information, network status and real-time flow.

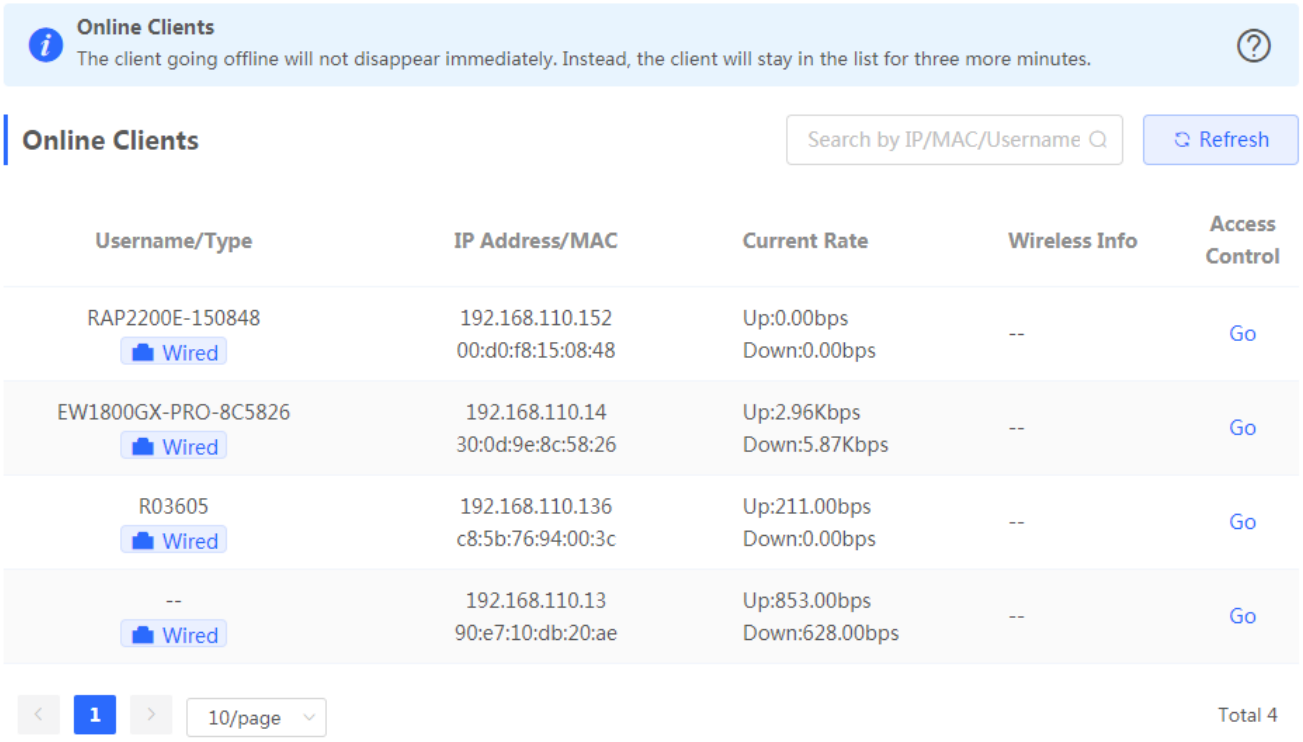
Figure 3-1 Overview



3.2 Online Clients

The **Online Clients** module is supported by the **Router** mode of the EG device.

Figure 3-2 Online Clients



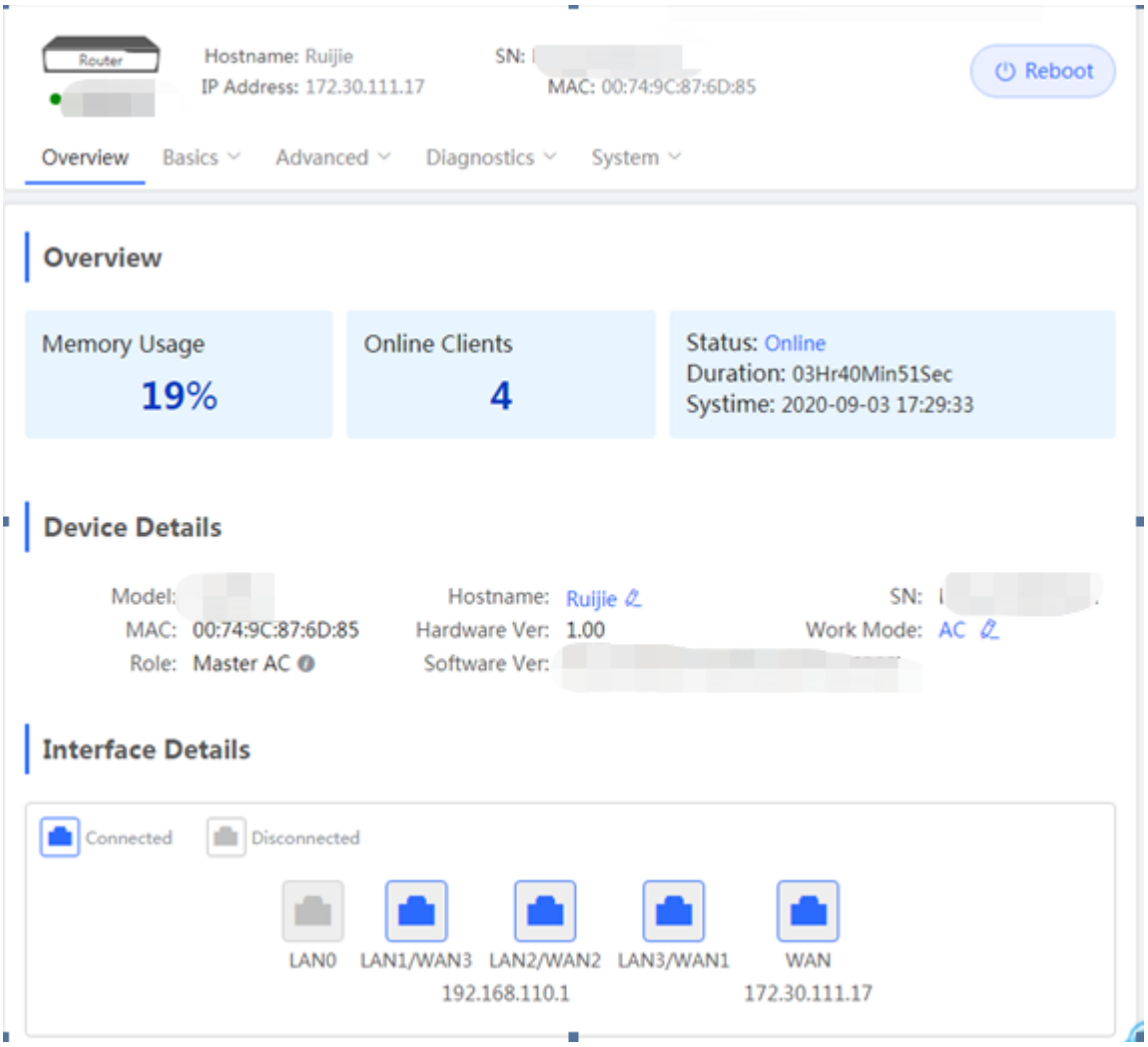
3.3 Router

If there is a wireless router enabled with self-organizing network in the network, the **Gateway** module will appear in the menu on the left. Click **Router**, and a horizontal menu will be displayed.

3.3.1 Overview

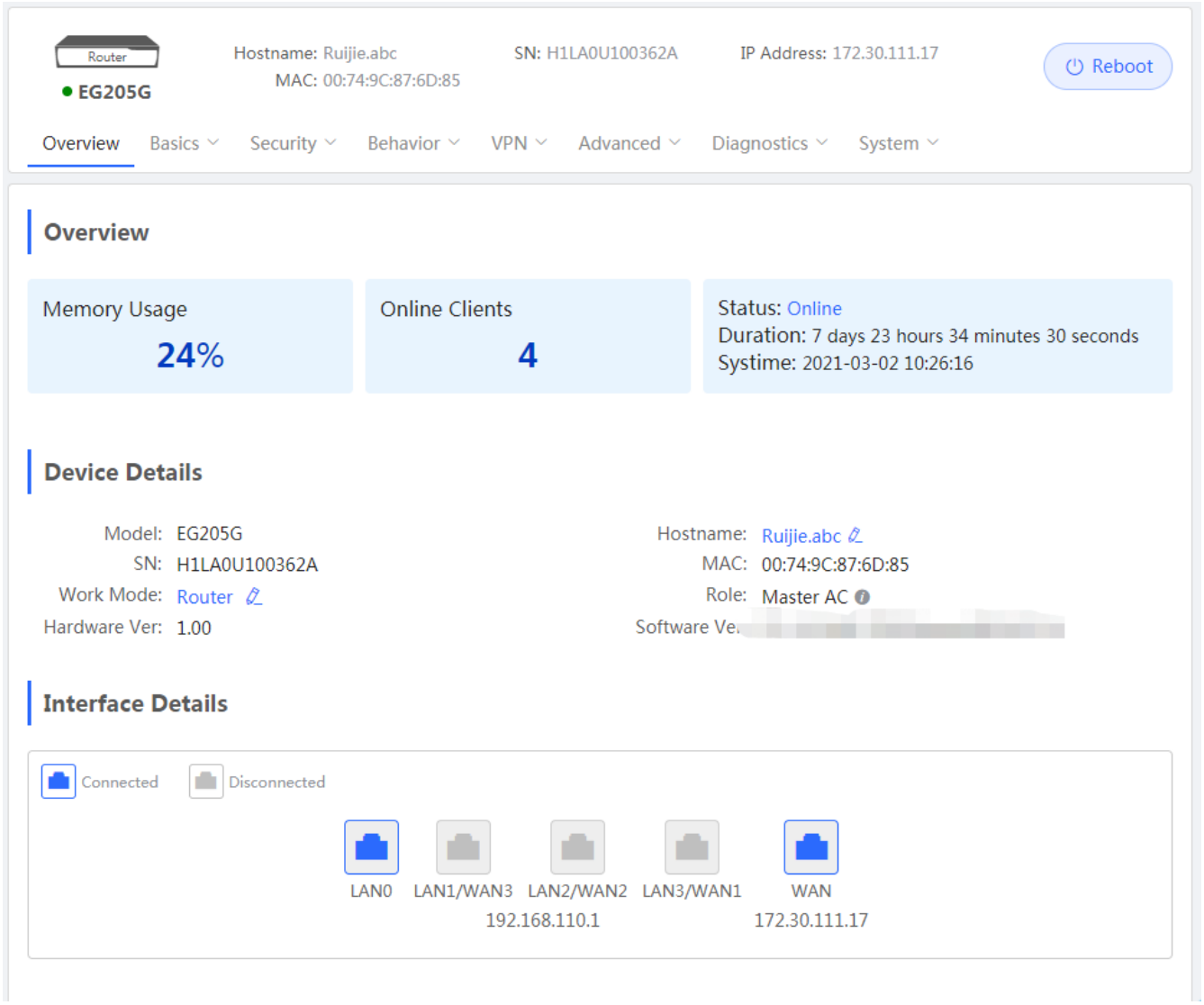
If the EG device works in the **AC** mode, the **Router** module does not contain **Security**, **Behavior** and **VPN**.

Figure 3-3 Overview



This chapter describes the Web configuration process of an EG device in the **Router** mode.

Figure 3-4 Router Mode



3.3.2 Basics

3.3.2.1 WAN

The **WAN** module allows you to configure WAN settings. There are three Internet types available: **Static IP Address**, **DHCP** and **PPPoE**. WAN settings support multiple lines (some models support only dual-line). If you select more than one line, you can configure each specific line, e.g., WAN and WAN1, and ISP/load settings.

Figure 3-5 WAN Settings

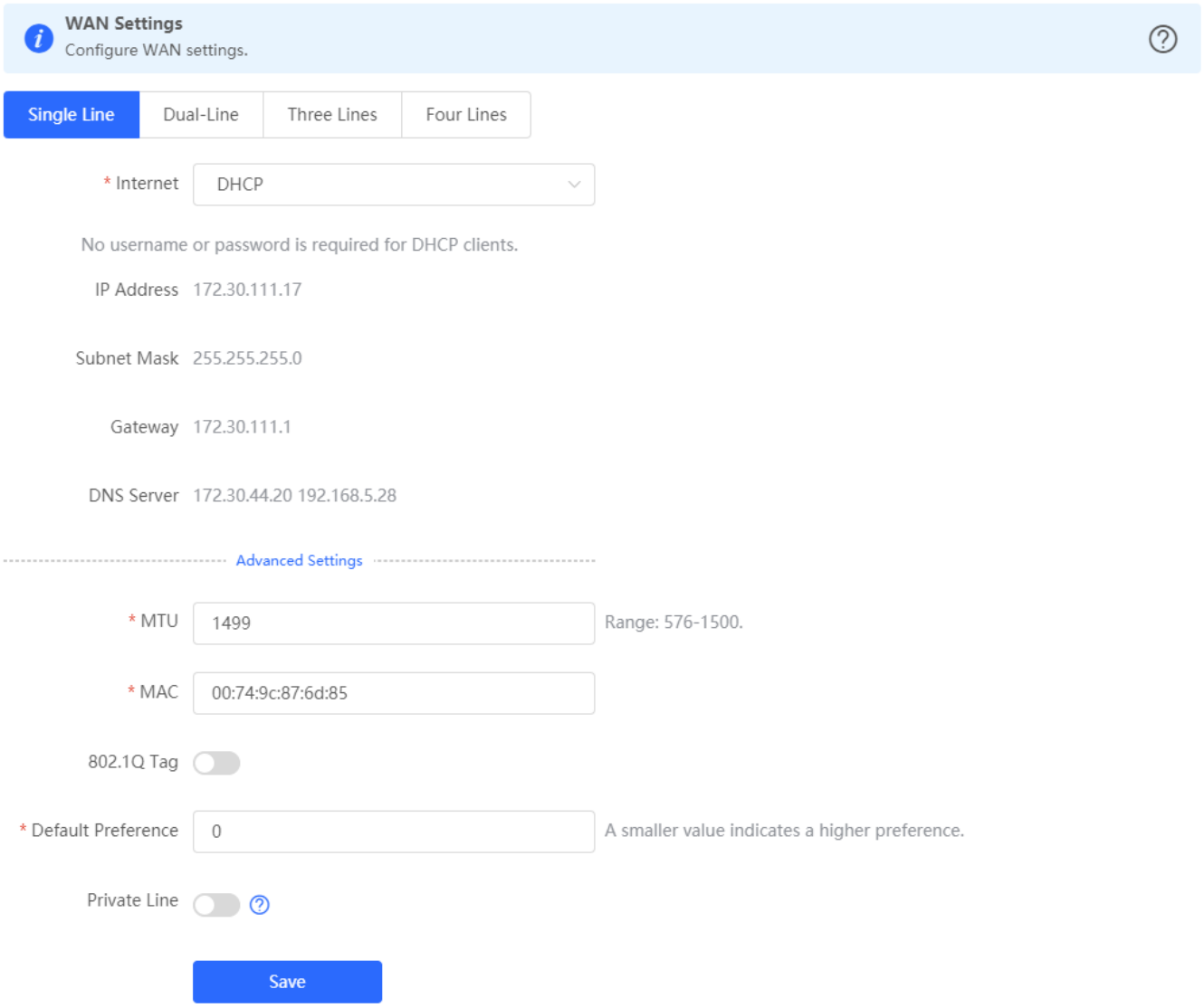
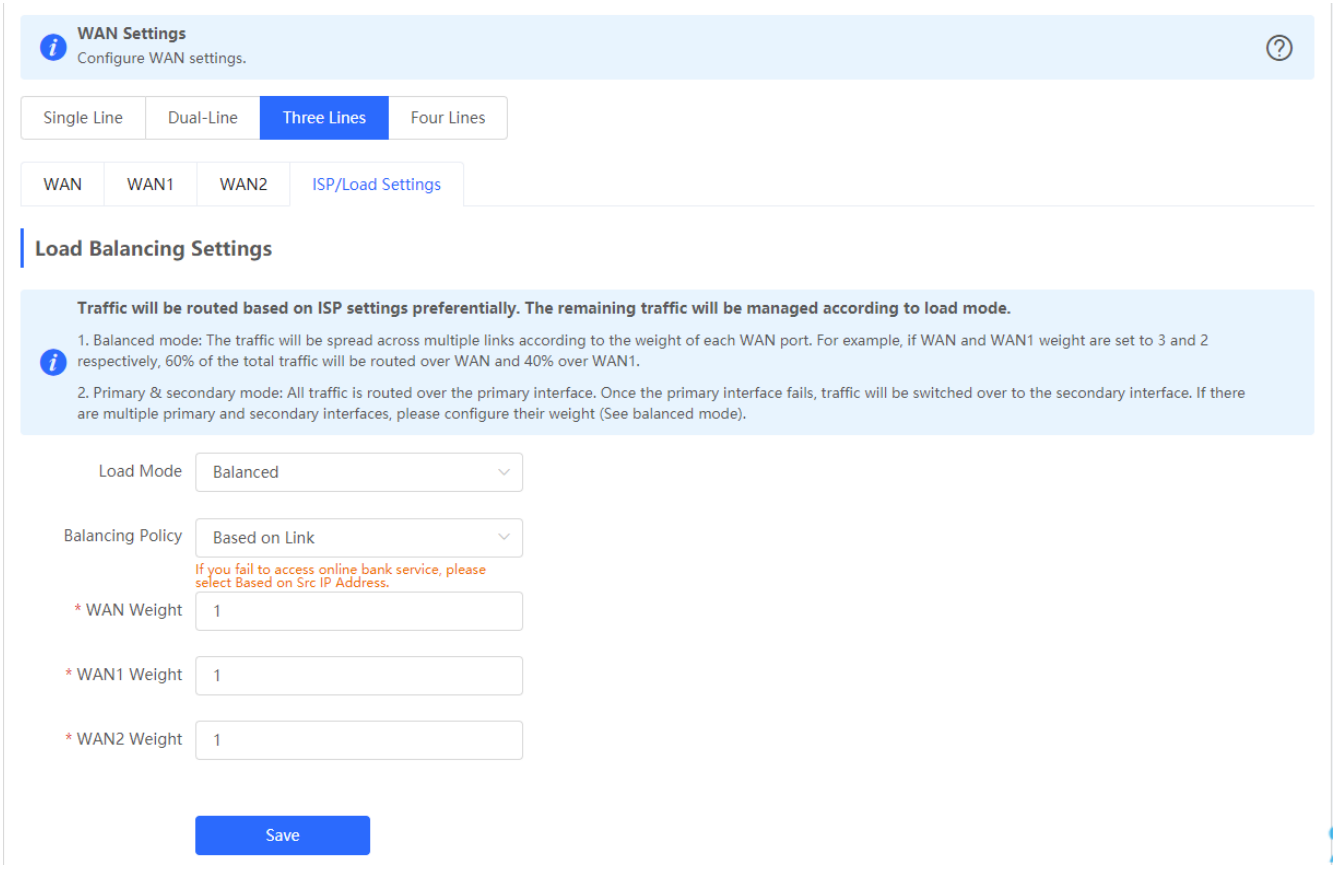


Figure 3-6 ISP/Load Settings



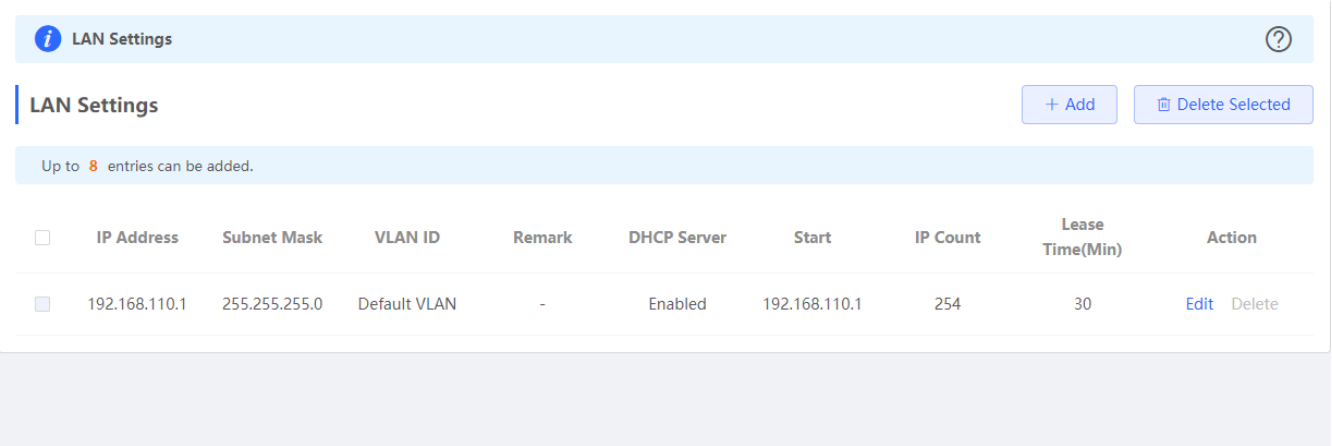
3.3.2.2 LAN

The **LAN** module contains **LAN Settings**, **Port VLAN**, **DHCP Clients**, **Static IP Addresses**, **DHCP Option** and **DNS Proxy**.

3.3.2.2.1 LAN Settings

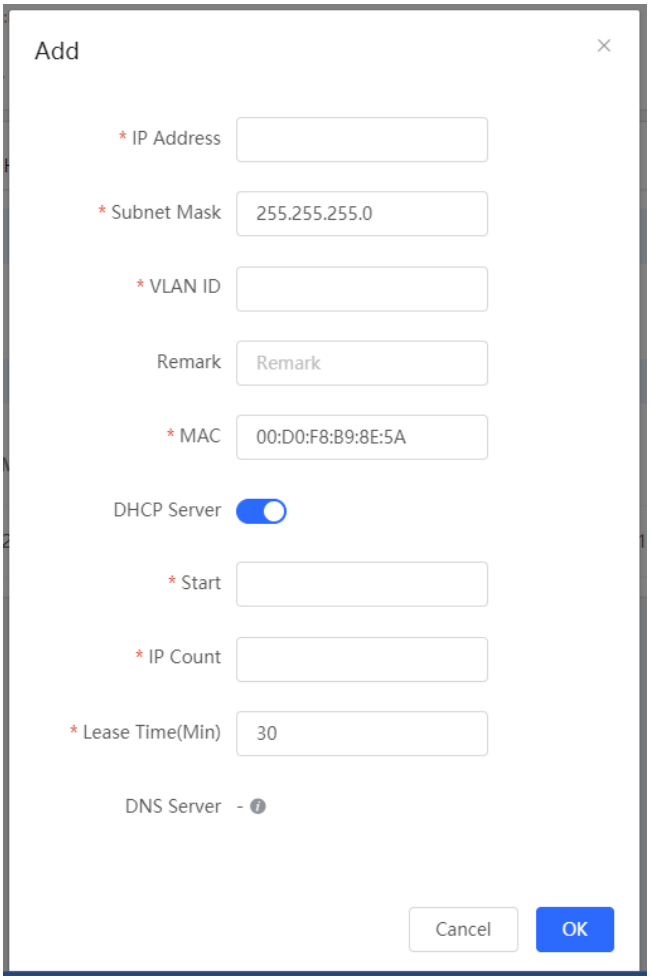
The **LAN** module allows you to set the IP address of the LAN port and DHCP status.

Figure 3-7 LAN Settings



Click **Add** to add a VLAN. In the displayed dialog box, configure settings and click **OK**.

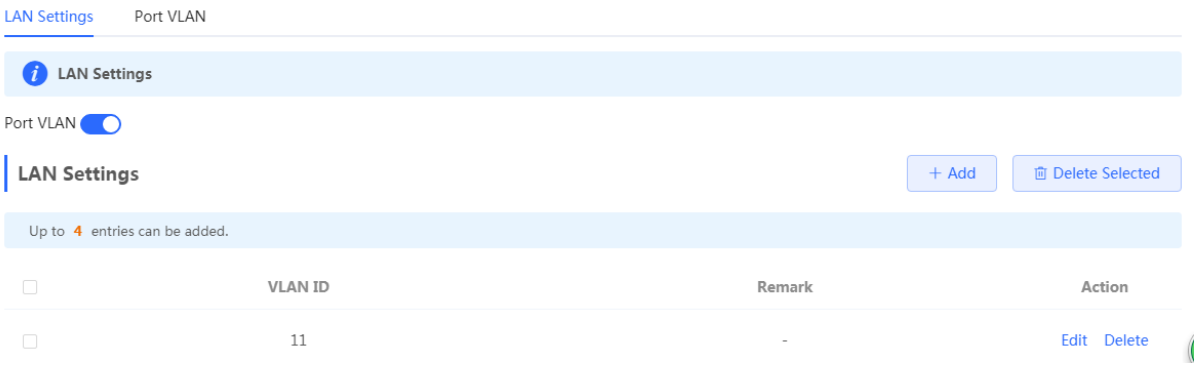
Figure 3-8 Add IP Address



You can click in the upper right corner to see description about each configuration item.

If an EAP device working in the AP mode supports port VLAN, there will be a port VLAN toggle displayed here.

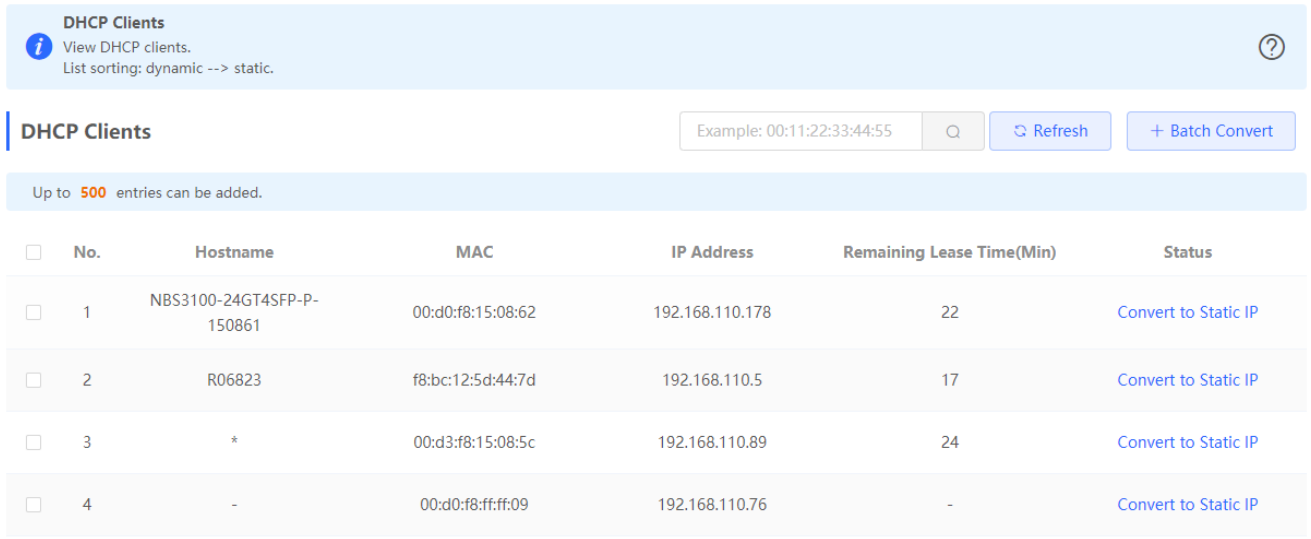
Figure 3-9 Port VLAN



3.3.2.2.2 DHCP Clients

The **DHCP Clients** page displays DHCP clients.

Figure 3-10 DHCP Clients

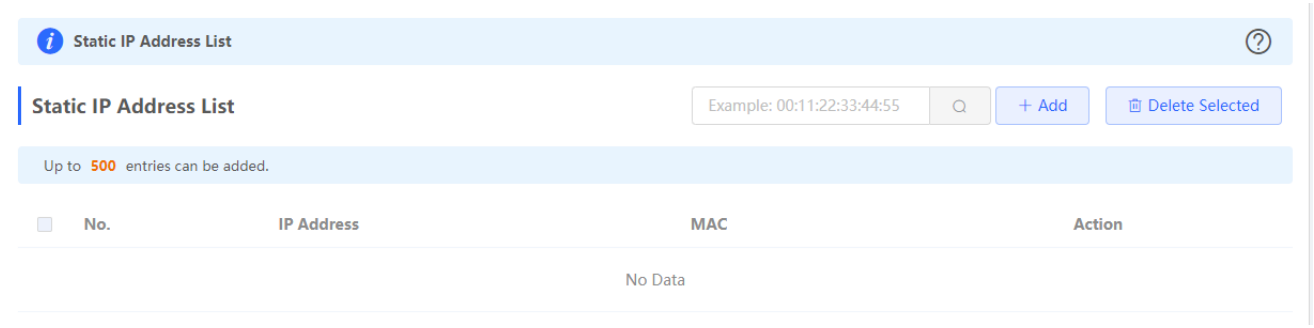


Click **Convert to Static IP** in the **Action** column to convert a DHCP-assigned IP address to a static IP address. Alternatively, select DHCP-assigned IP addresses and click **Batch Convert** to convert more than one IP address.

3.3.2.2.3 Static IP Addresses

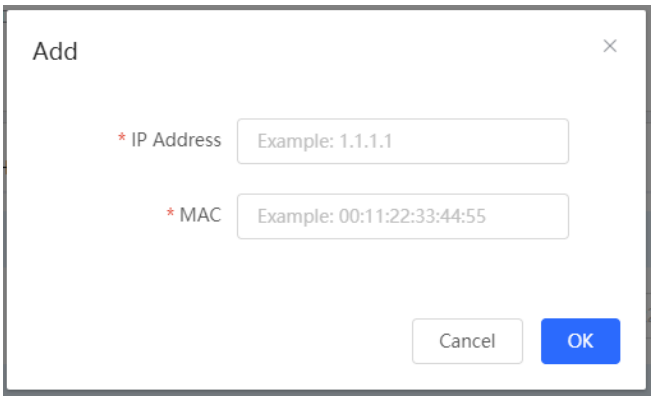
The **Static IP Addresses** module allows you to add, delete and edit static IP addresses.

Figure 3-11 Static IP Addresses



Click **Add** to add a static IP address manually. In the displayed dialog box, configure settings and click **OK**.

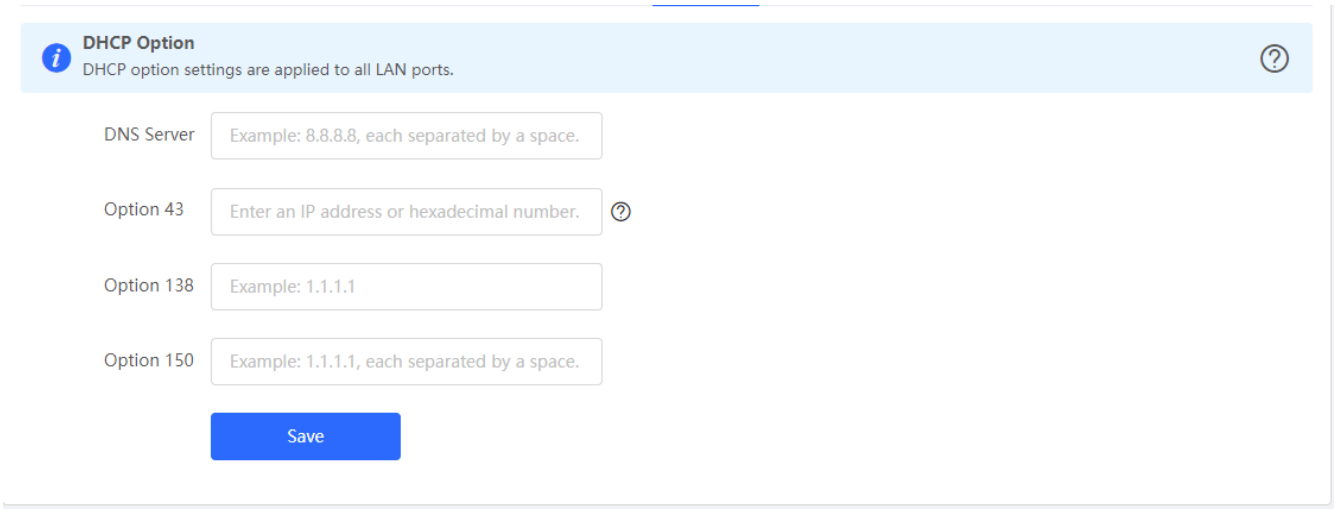
Figure 3-12 Add Static IP Address



3.3.2.2.4 DHCP Option

The **DHCP Option** module allows you to configure DHCP option settings.

Figure 3-13 DHCP Option



3.3.2.2.5 DNS Proxy

The **DNS Proxy** module allows you to configure DNS proxy settings.

Figure 3-14 DNS Proxy

3.3.2.3 IPv6 Address

After you enable **IPv6 Address**, the IPv6 tab pages of all WAN ports will be diplayed in **WAN Settings**.

Figure 3-15 WAN Settings

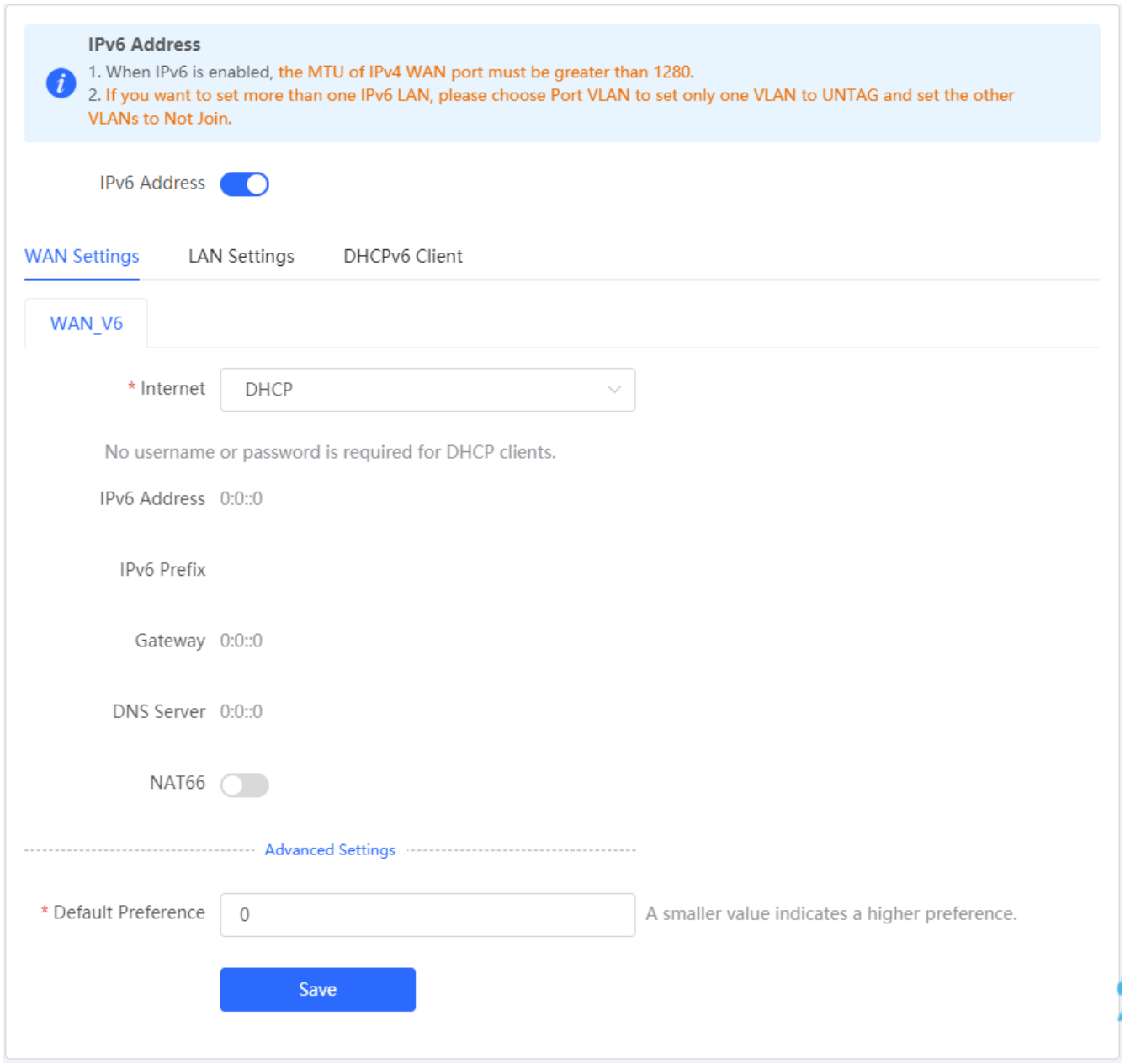


Figure 3-16 LAN Settings

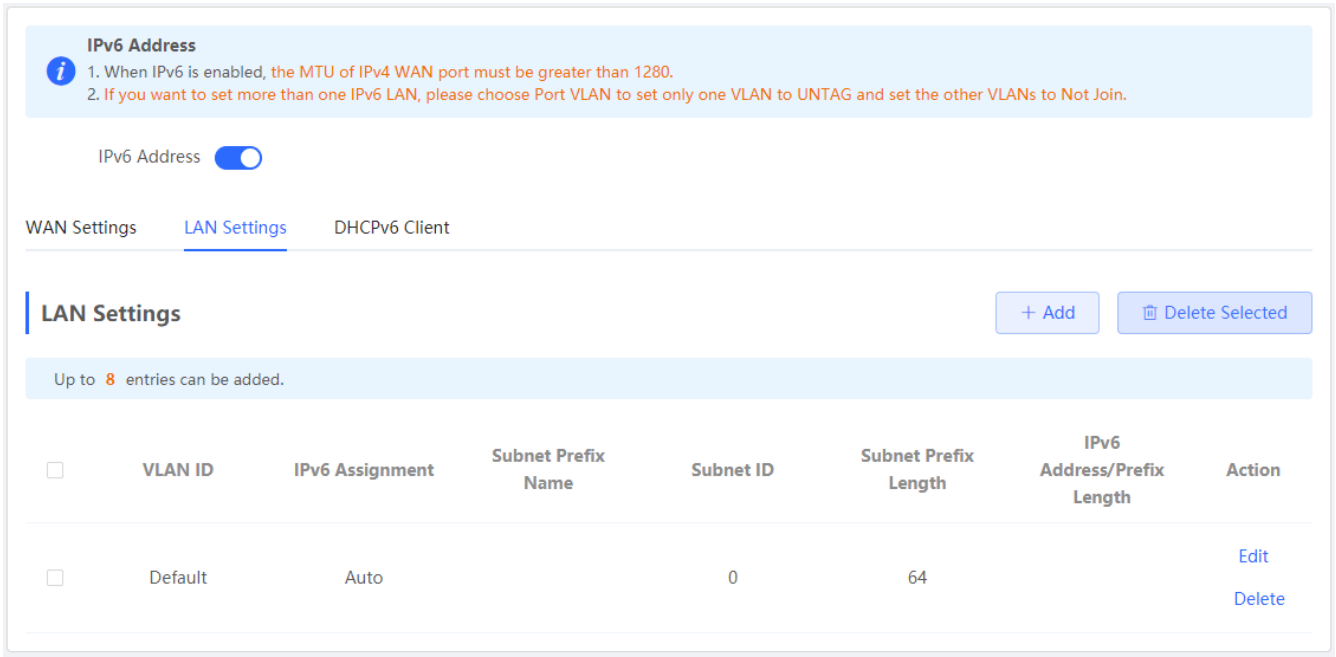


Figure 3-17 Add LAN

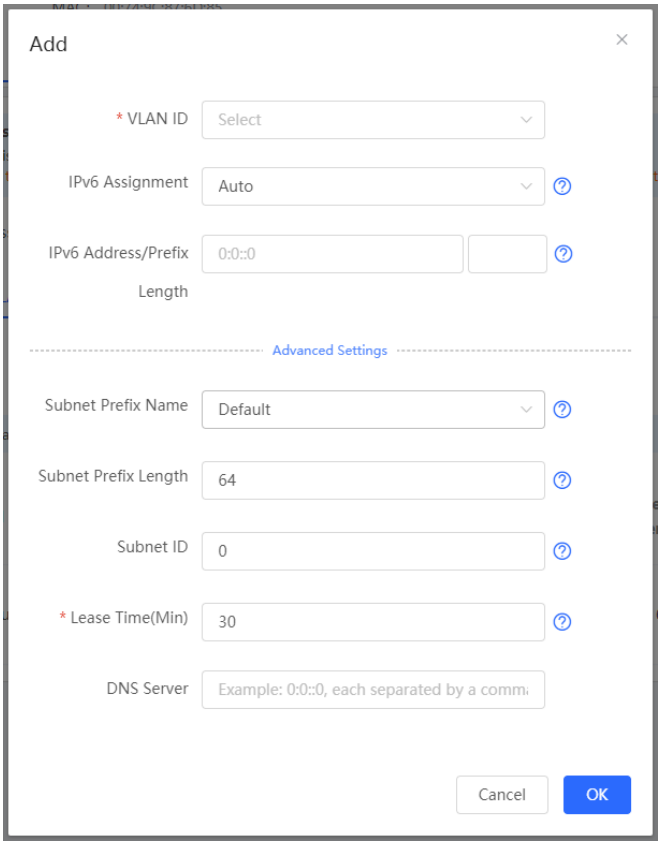
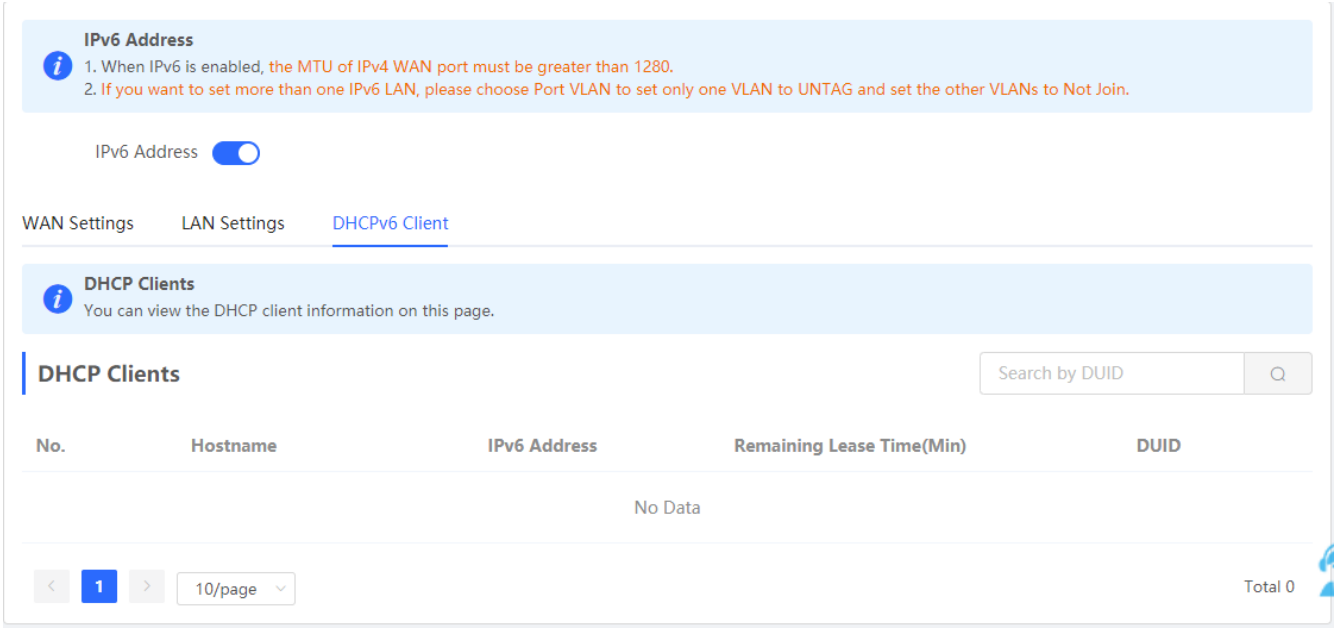


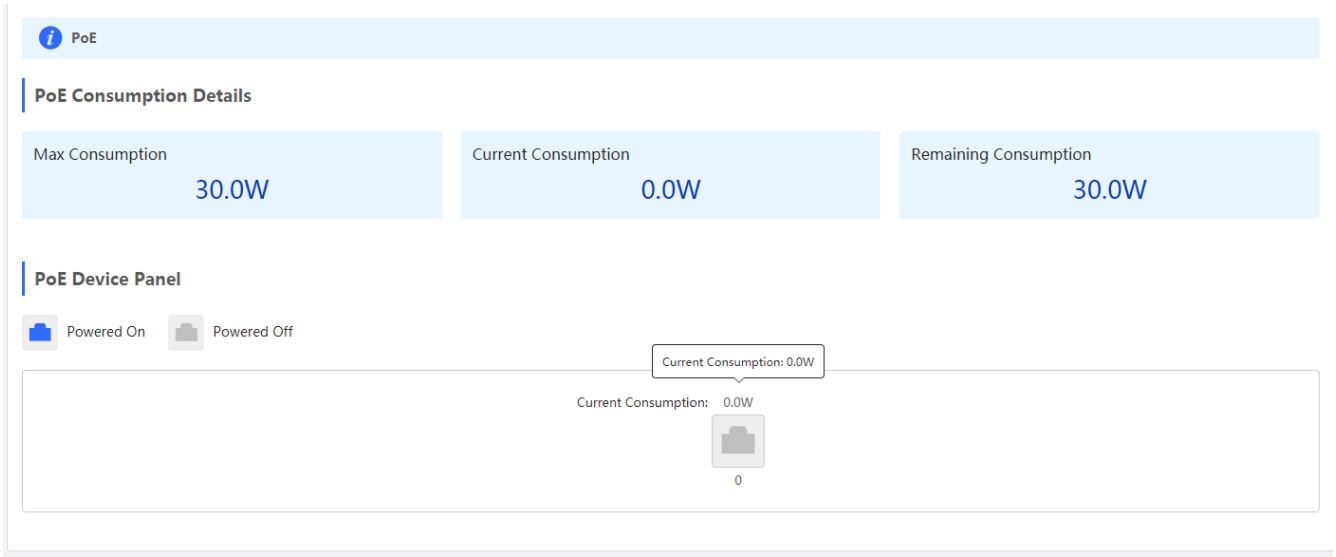
Figure 3-18 DHCPv6 Client



3.3.2.4 PoE

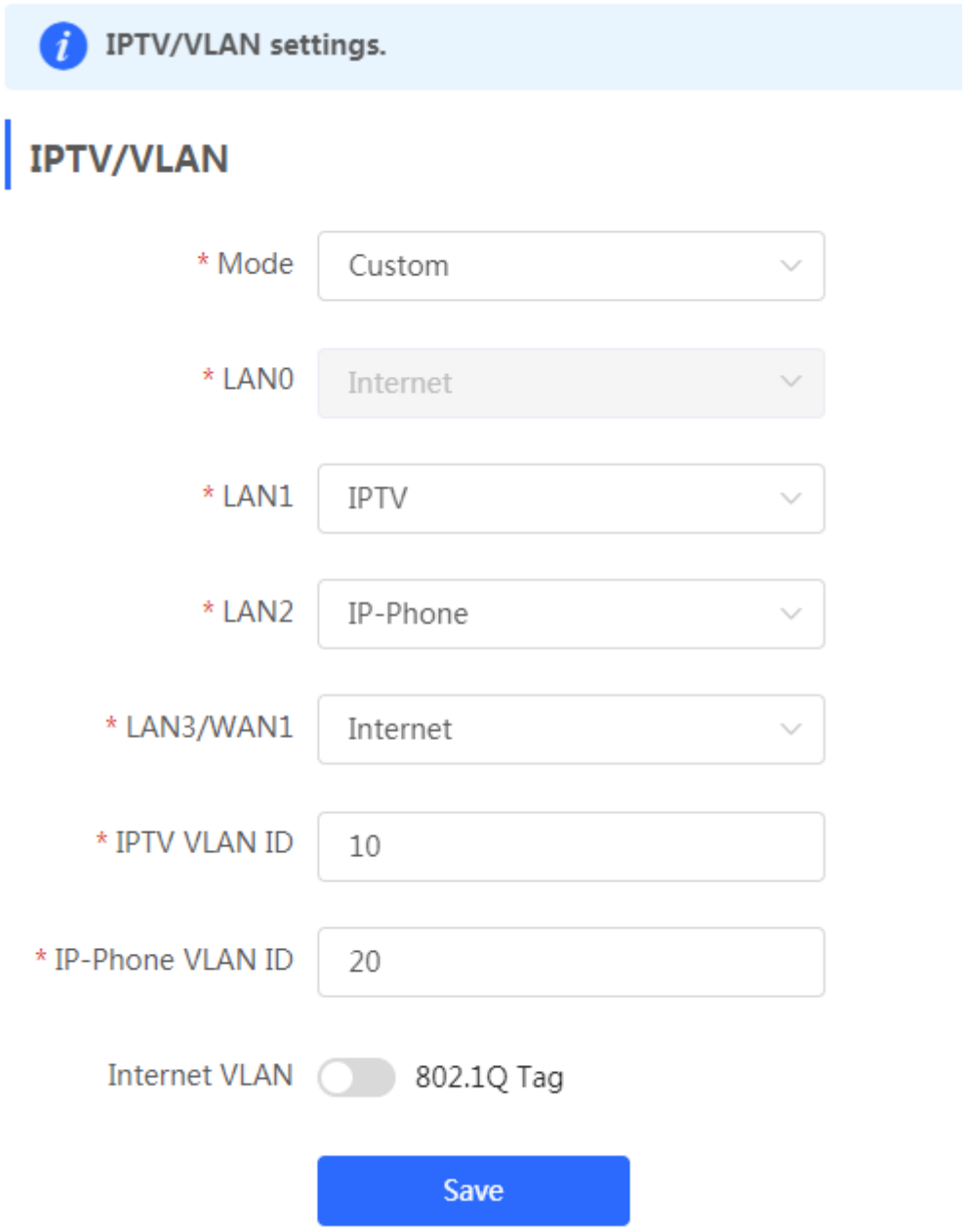
The **PoE** page displays PoE status and power consumption. Only the models ending with -P, e.g., EG105G-P and EG210G-P, support this feature.

Figure 3-19 PoE



3.3.2.5 IPTV/VLAN

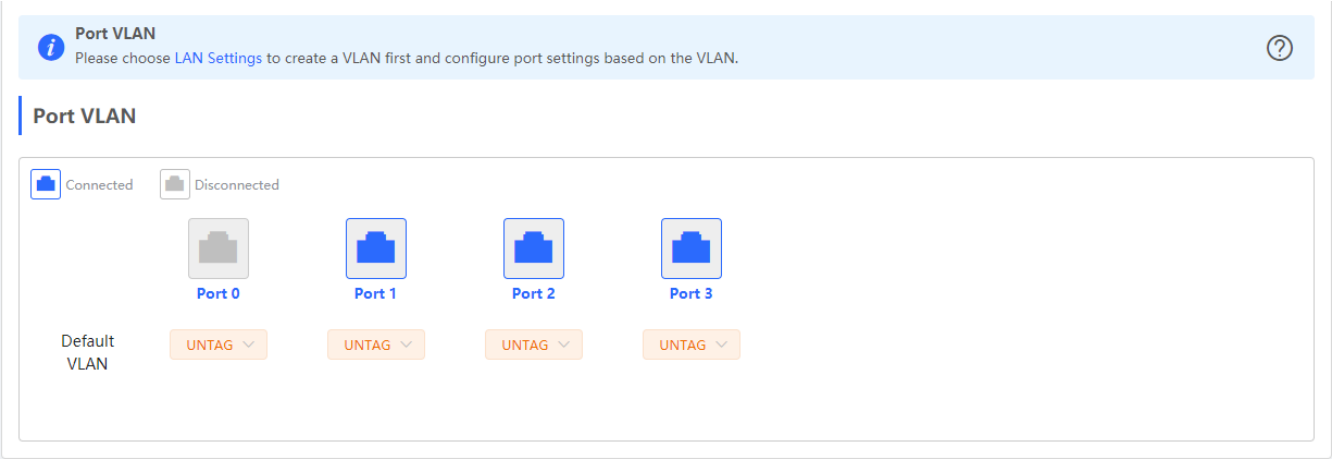
Figure 3-20 IPTV/VLAN



3.3.2.6 Port VLAN

The **Port VLAN** page displays VLAN information.

Figure 3-21 Port VLAN



3.3.3 Security

3.3.3.1 ARP List

The **ARP List** page displays ARP entries.

Figure 3-22 ARP List

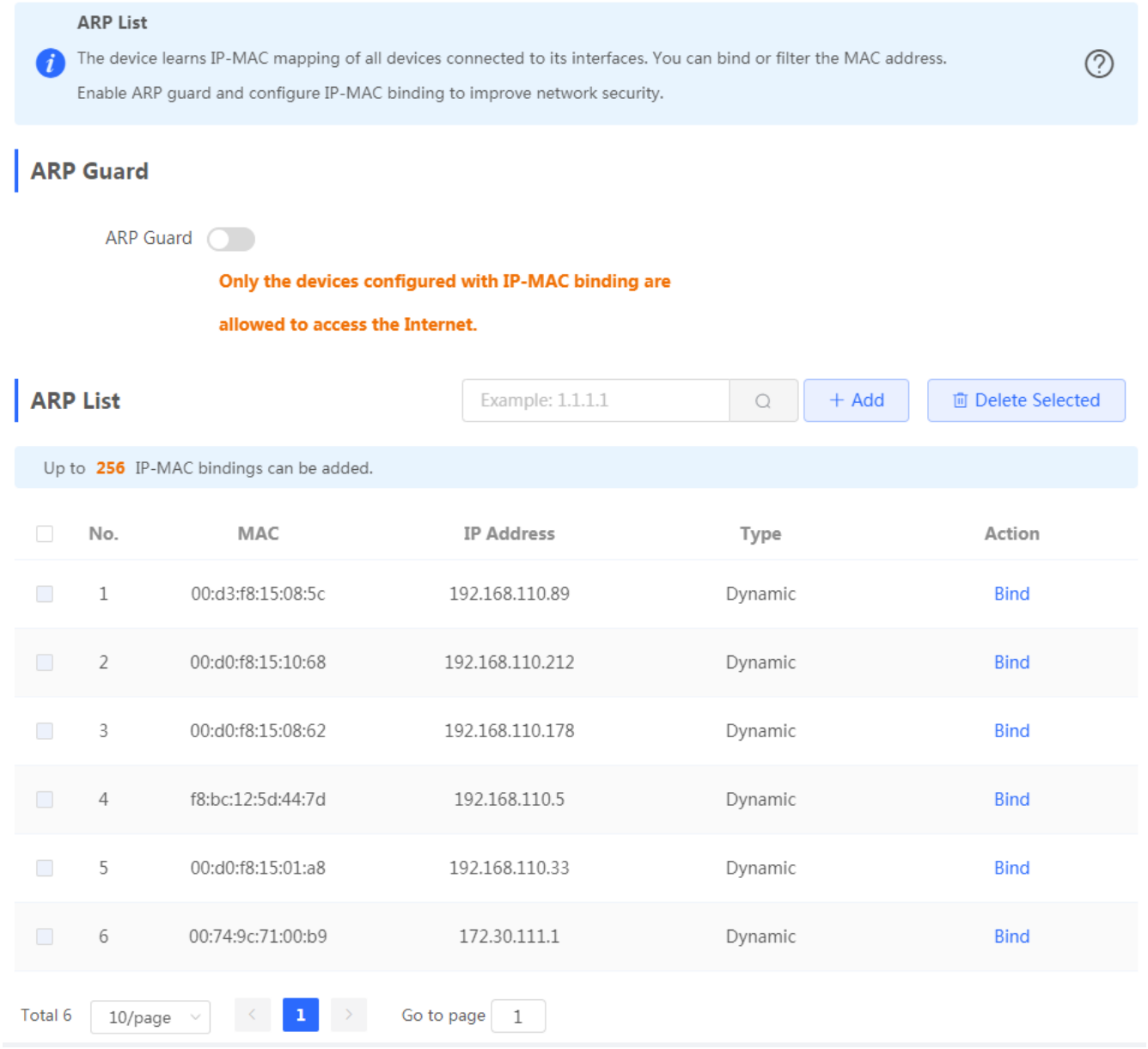
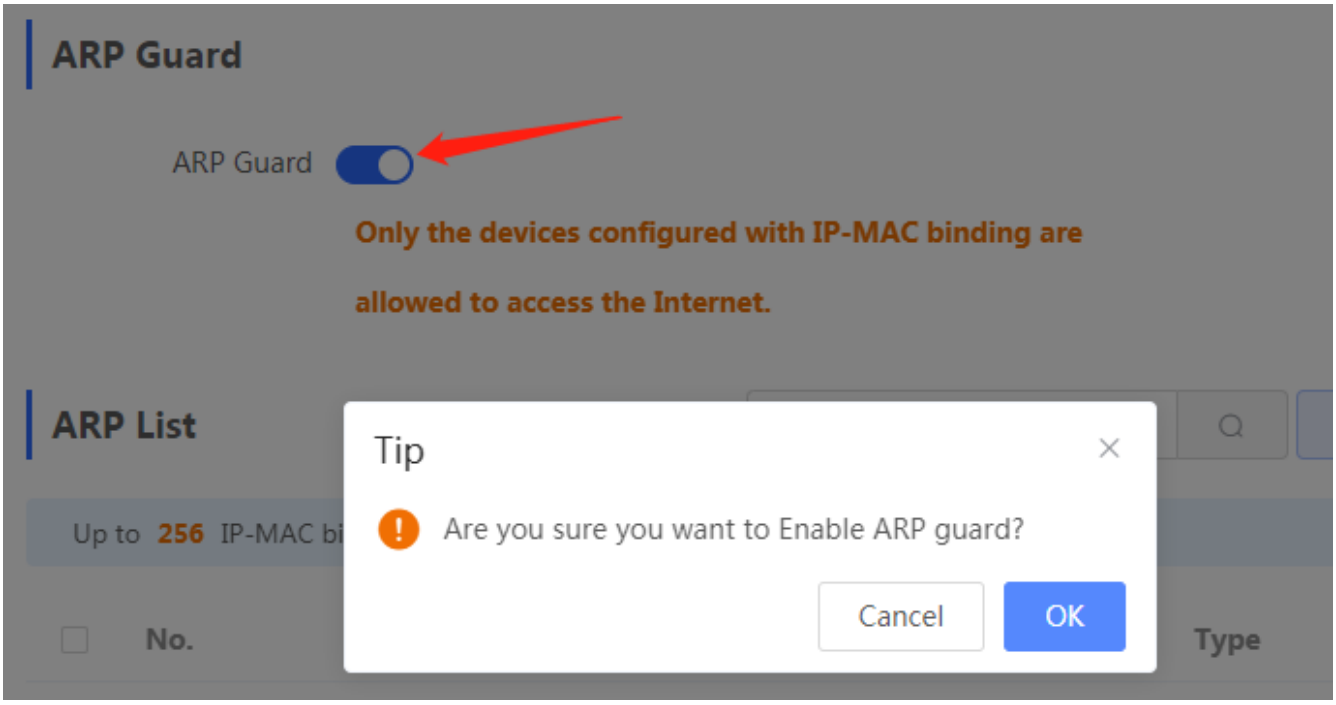
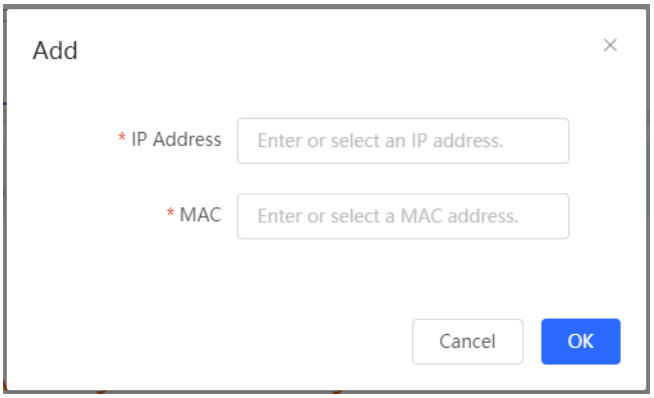


Figure 3-23 ARP Guard



Click **Add** to add an IP-MAC binding. In the displayed dialog box, enter or select an IP address and a MAC address and click **OK**.

Figure 3-24 Add IP-MAC Binding

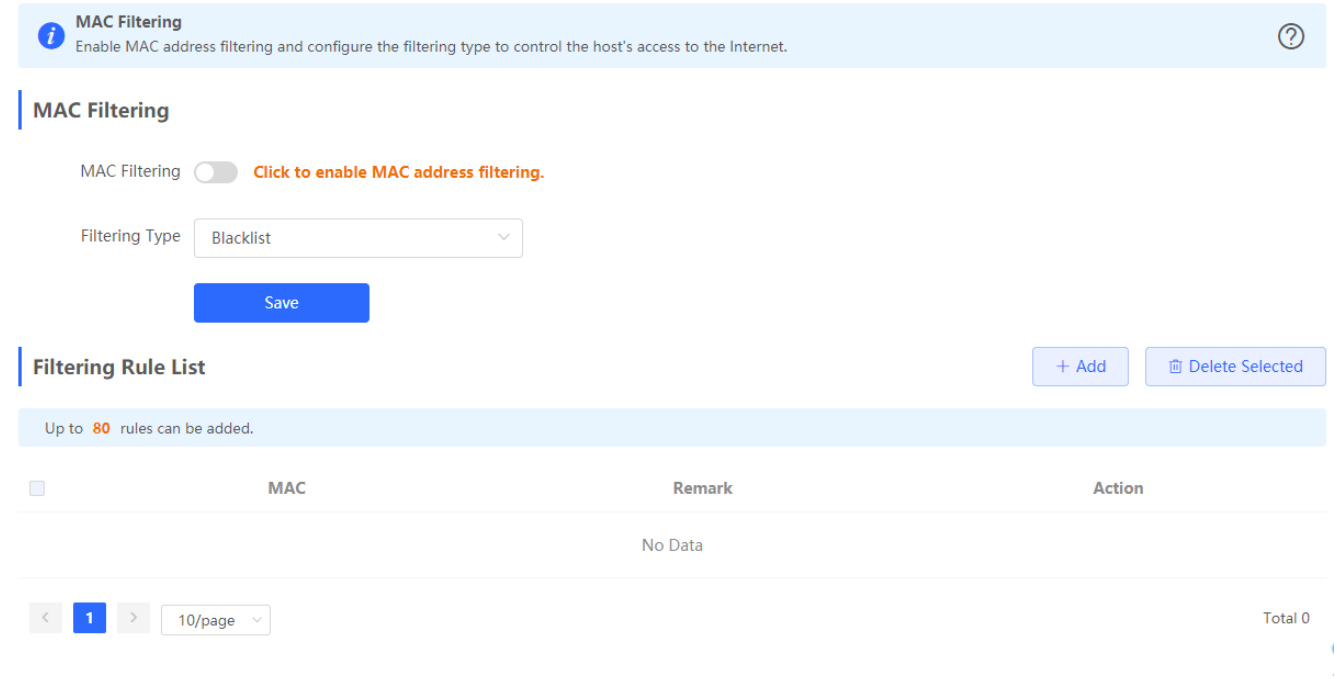


Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

3.3.3.2 MAC Filtering

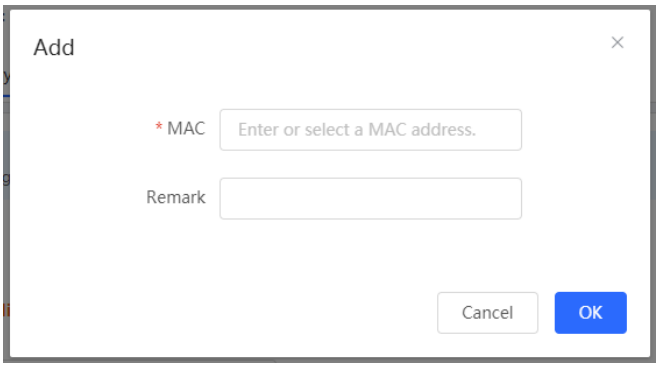
The **MAC Filtering** module allows you to add, delete and edit MAC filtering entries.

Figure 3-25 MAC Filtering



Click **Add** to add a filtered MAC address. In the displayed dialog box, enter or select a MAC address and click **OK**.

Figure 3-26 Add Filtered MAC Address



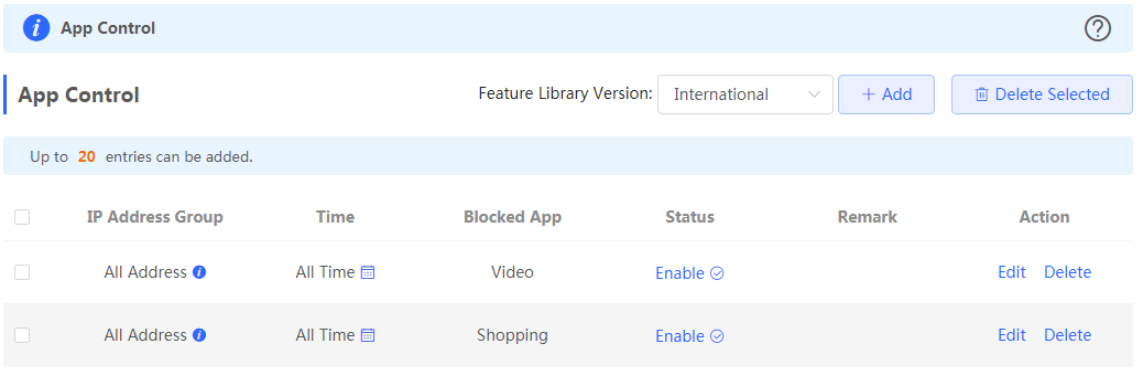
Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

3.3.4 Behavior

3.3.4.1 App Control

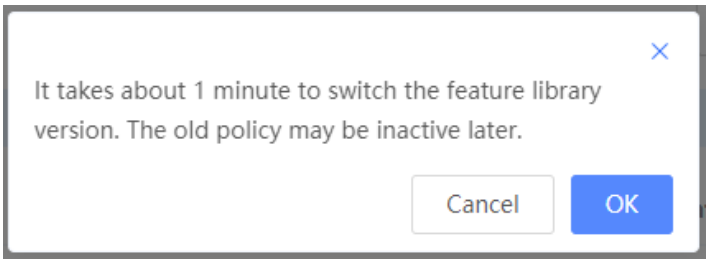
The **App Control** module allows you to add, delete and edit application control policies.

Figure 3-27 App Control



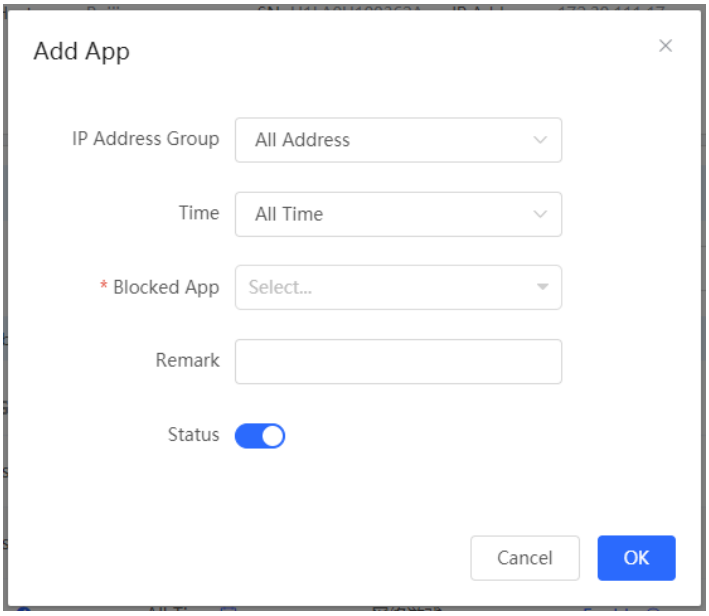
Select a feature library version from the dropdown list. In the displayed dialog box, click **OK** to confirm switchover.

Figure 3-28 Switch Feature Library Version



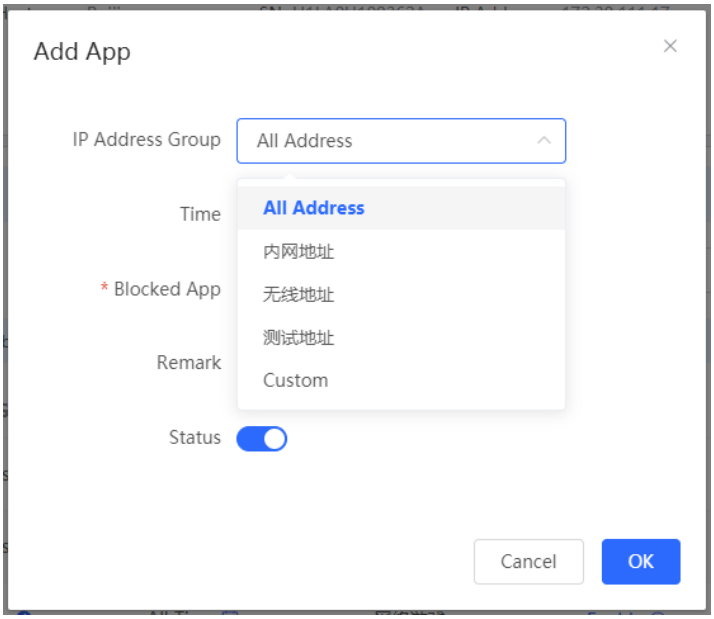
Click **Add** to add an application control policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-29 Add Application Control Policy



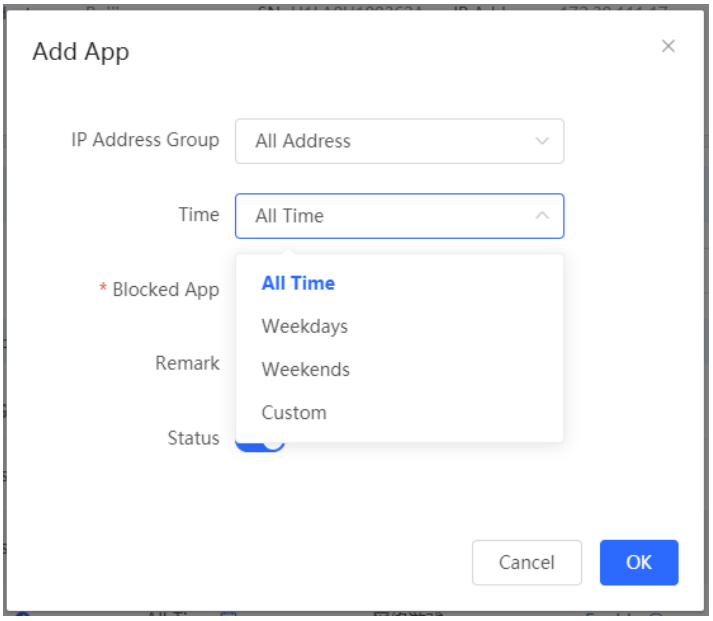
Define IP address groups on the **Address Management** page and you can select IP address groups here.

Figure 3-30 Select IP Address Group



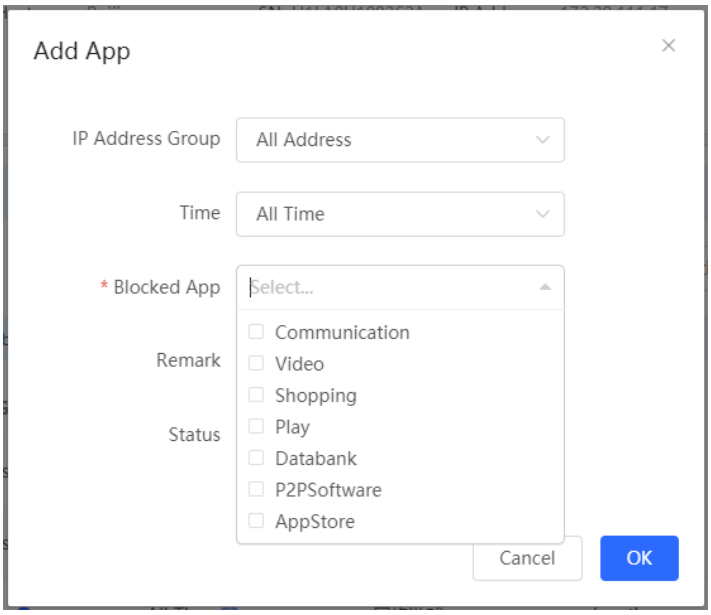
Define time objects on the **Time Management** page and you can select time objects here.

Figure 3-31 Select Time



Select the target application from the **Blocked App** dropdown list and click **OK**.

Figure 3-32 Select Blocked App

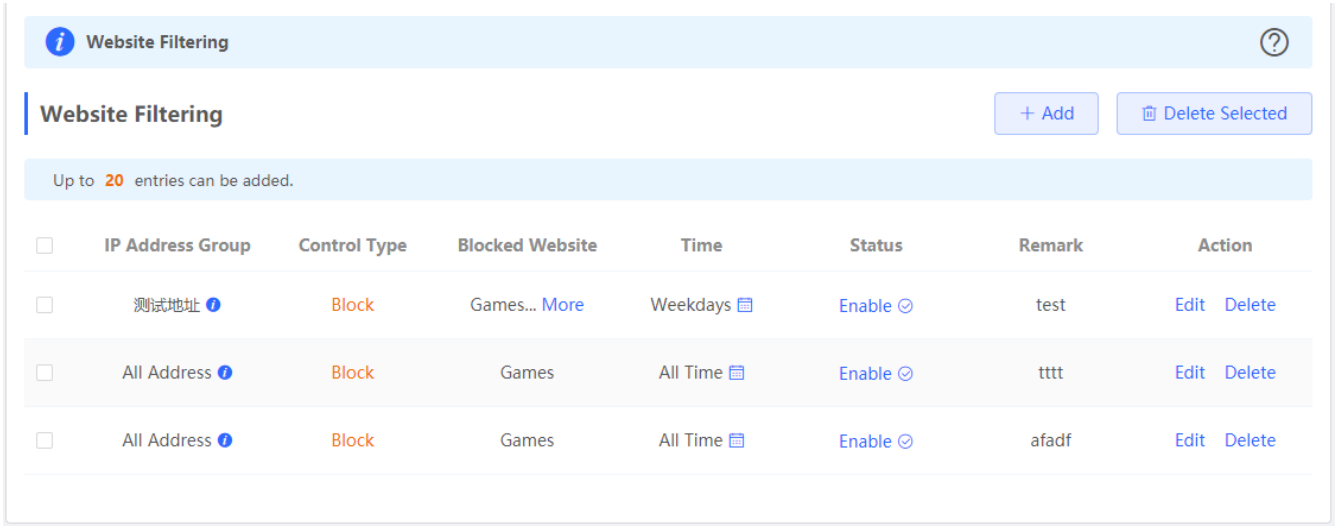


3.3.4.2 Website Management

3.3.4.2.1 Website Filtering

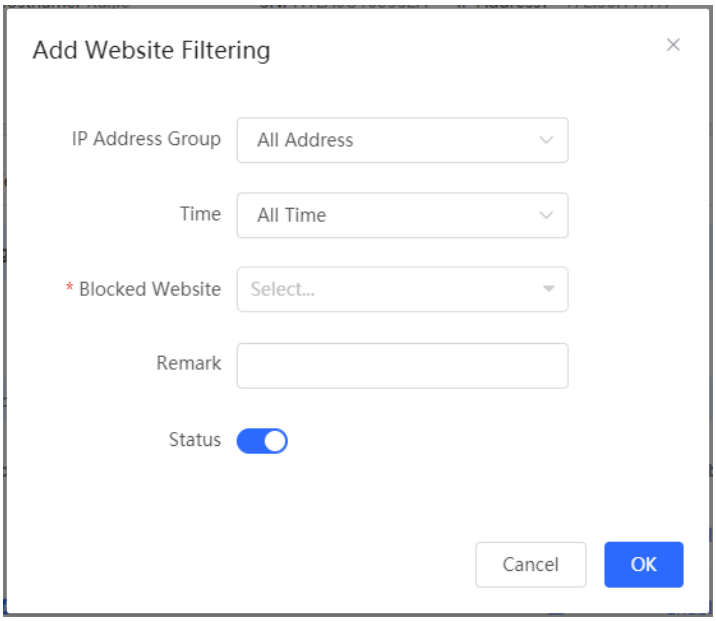
The **Website Filtering** module allows you to add, delete and edit website filtering policies.

Figure 3-33 Website Filtering



Click **Add** to add a website filtering policy. In the displayed dialog box, configure settings and click **OK**.

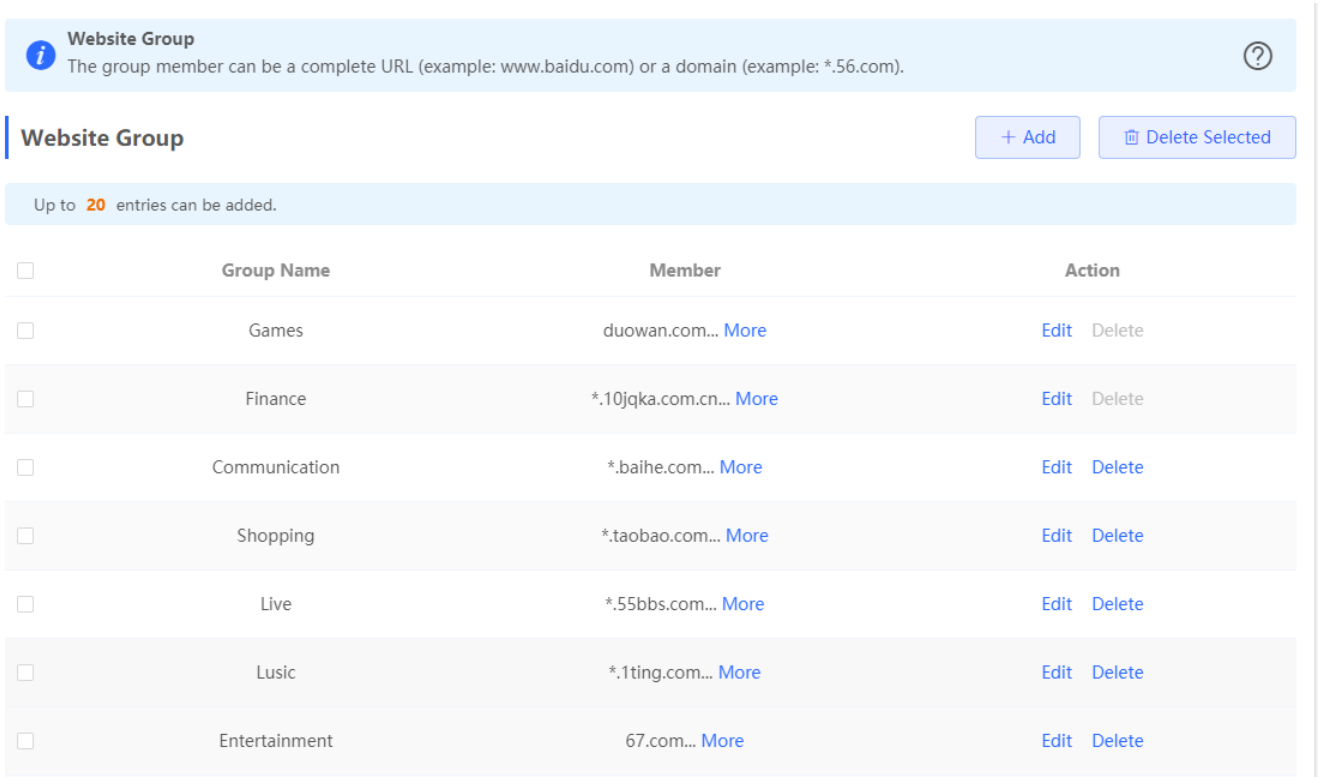
Figure 3-34 Add Website Filtering Policy



3.3.4.2.2 Website Group

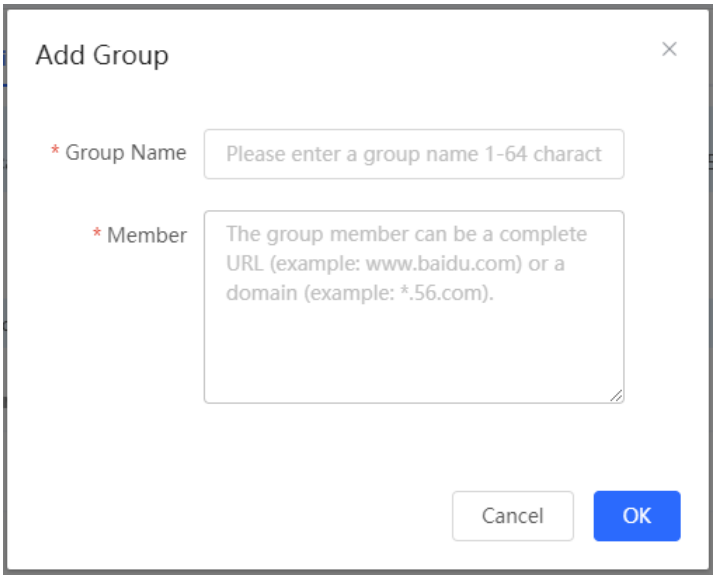
The **Website Group** module allows you to add, delete and edit website grouping policies.

Figure 3-35 Website Group



Click **Add** to add a website filtering policy. In the displayed dialog box, configure settings and click **OK**.

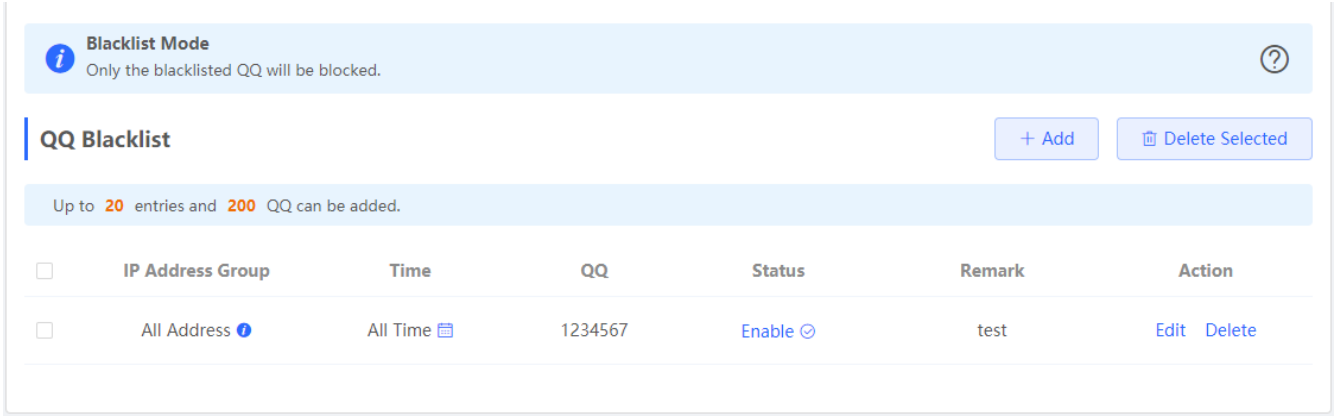
Figure 3-36 Add Website Grouping Policy



3.3.4.3 QQ Management

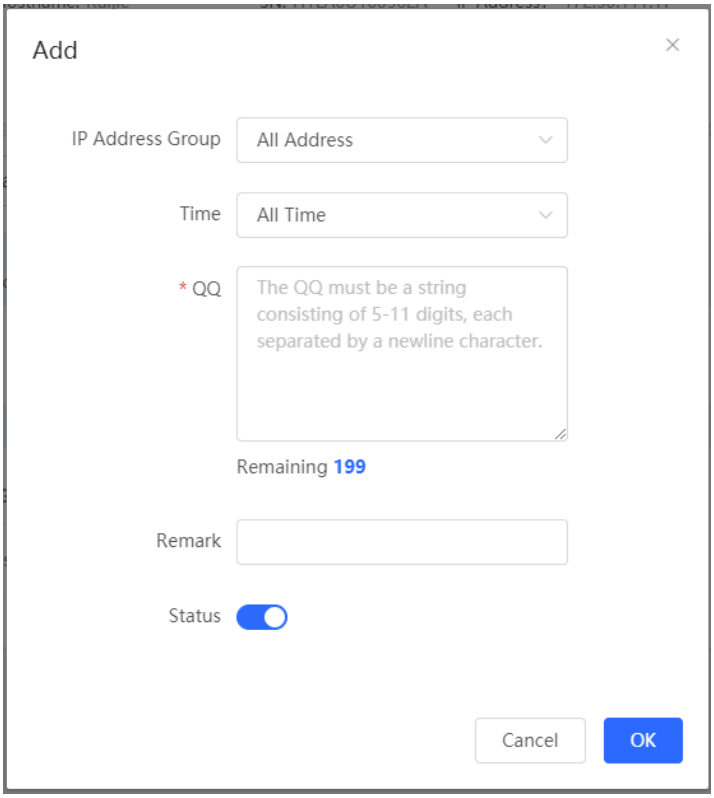
The **QQ Management** module allows you to add, delete and edit QQ management policies.

Figure 3-37 QQ Management



Click **Add** to add a QQ management policy. In the displayed dialog box, configure settings and click **OK**.

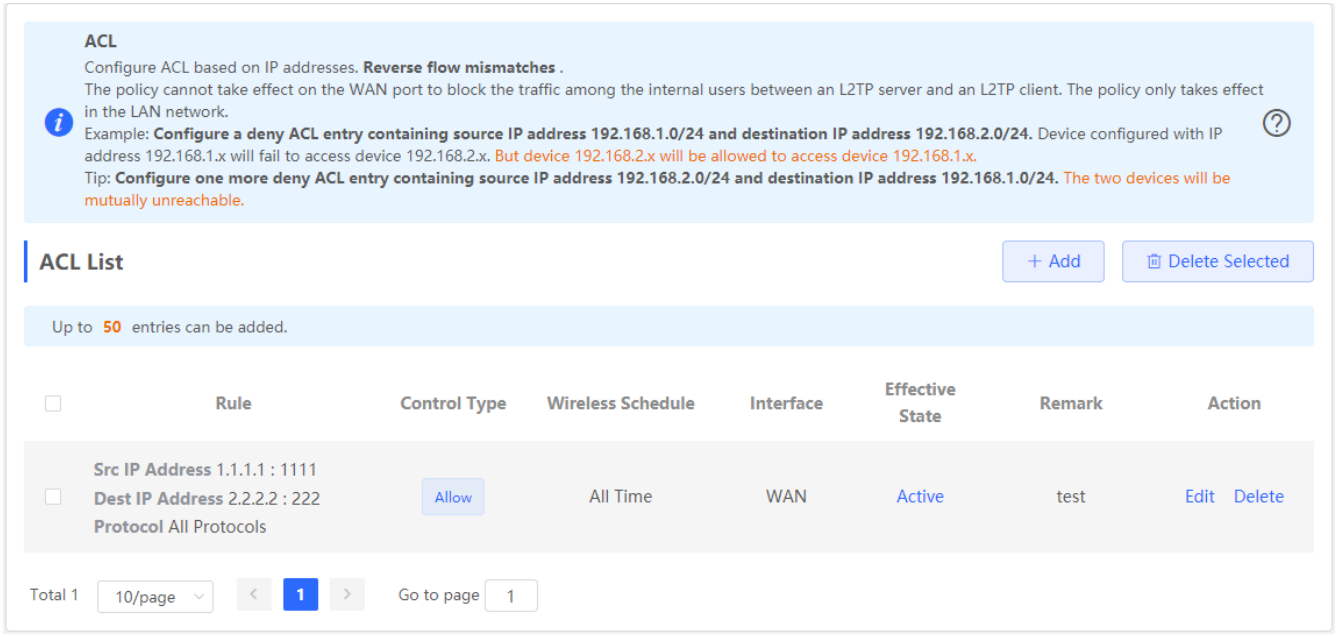
Figure 3-38 Add QQ Management Policy



3.3.4.4 Access Control

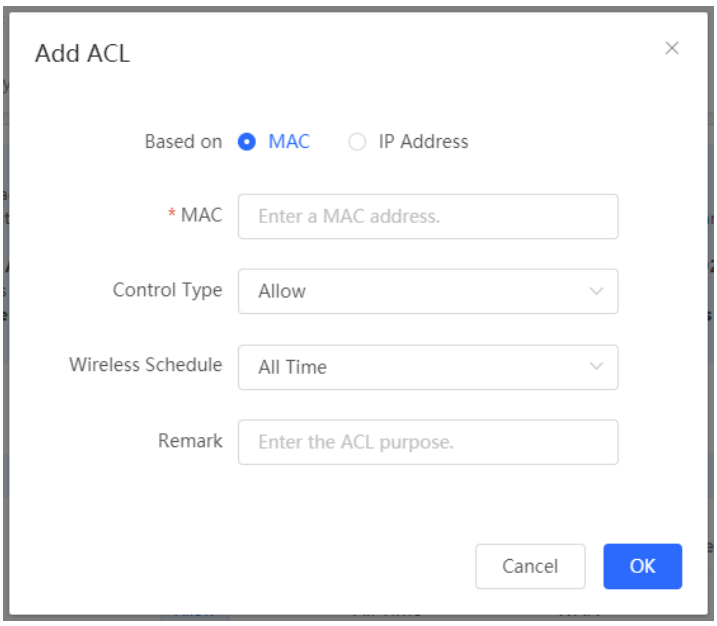
The **Access Control** module allows you to add, delete and edit access control policies.

Figure 3-39 Access Control



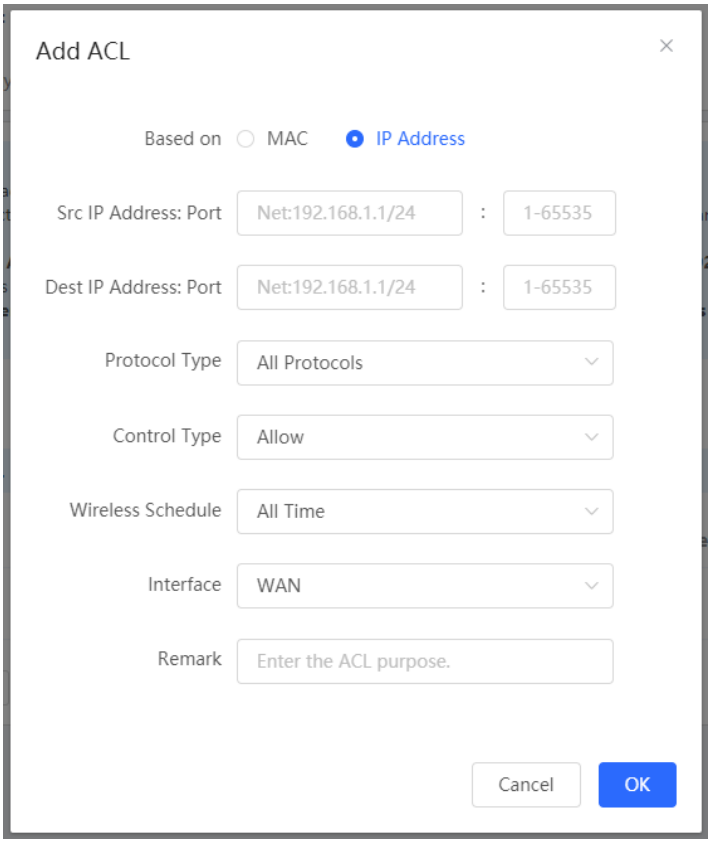
Click **Add** to add a MAC-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-40 Add MAC-Based ACL



Click **Add** to add an IP address-based policy. In the displayed dialog box, configure settings and click **OK**.

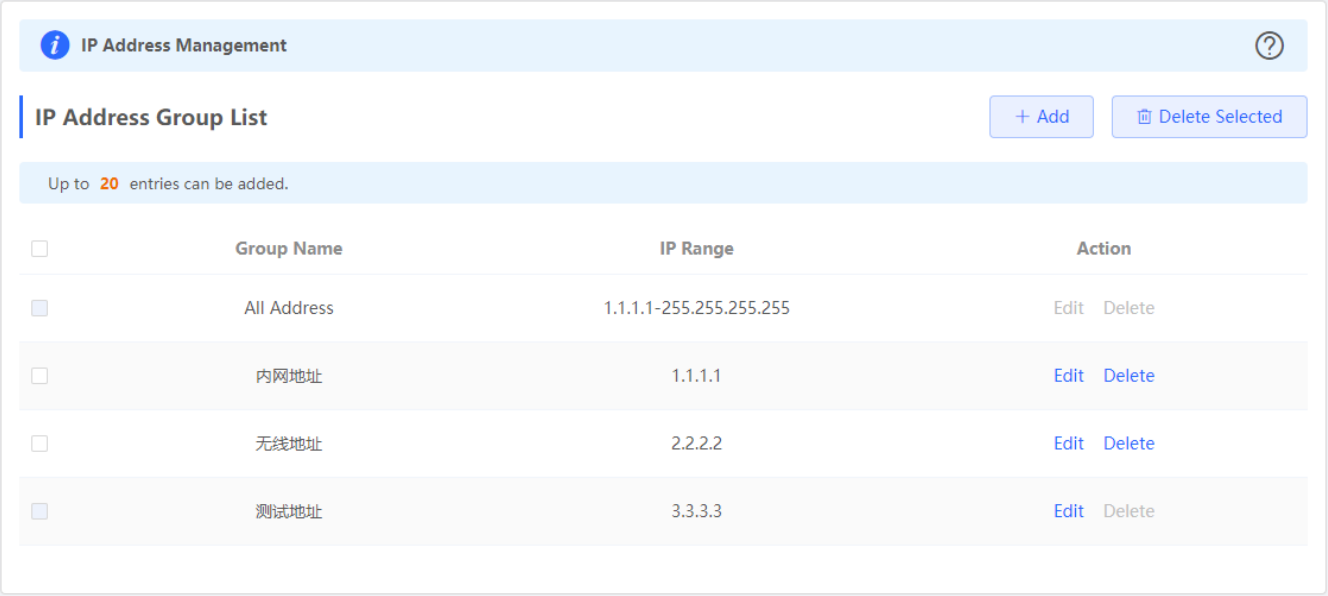
Figure 3-41 Add IP Address-Based ACL



3.3.4.5 Address Management

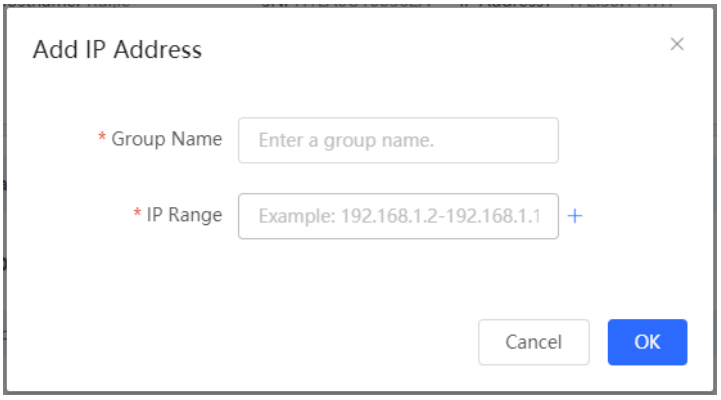
The **Address Management** module allows you to add, delete and edit IP address groups.

Figure 3-42 IP Address Management



Click **Add** to add an IP address group. In the displayed dialog box, configure settings and click **OK**.

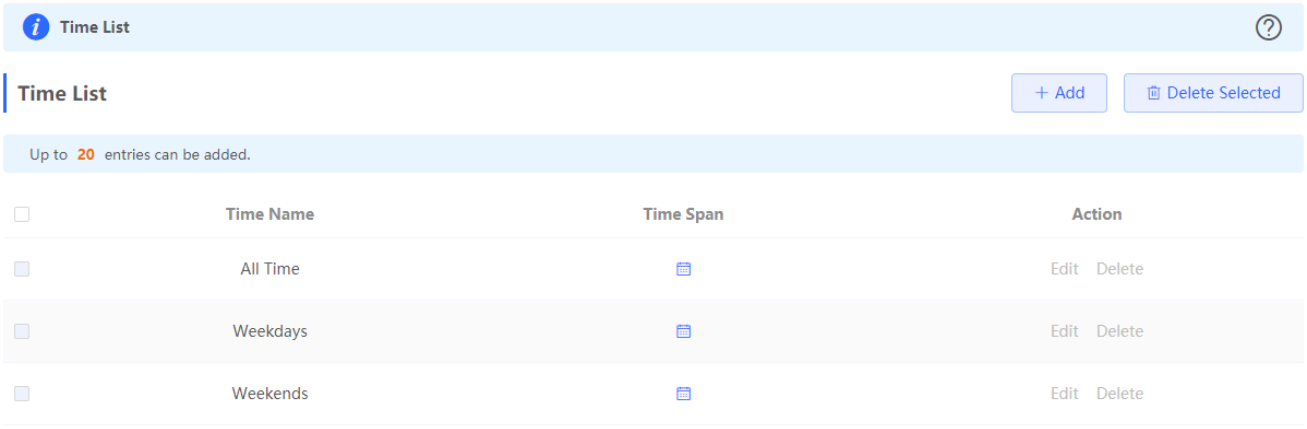
Figure 3-43 Add IP Address Group



3.3.4.6 Time Management

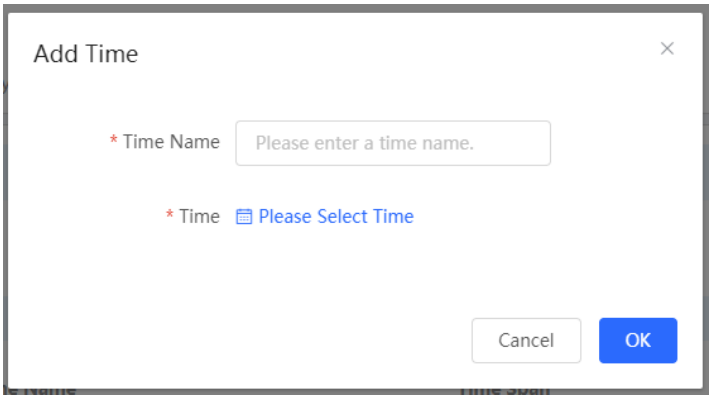
The **Time Management** module allows you to add, delete and edit time objects.

Figure 3-3-41 Time List



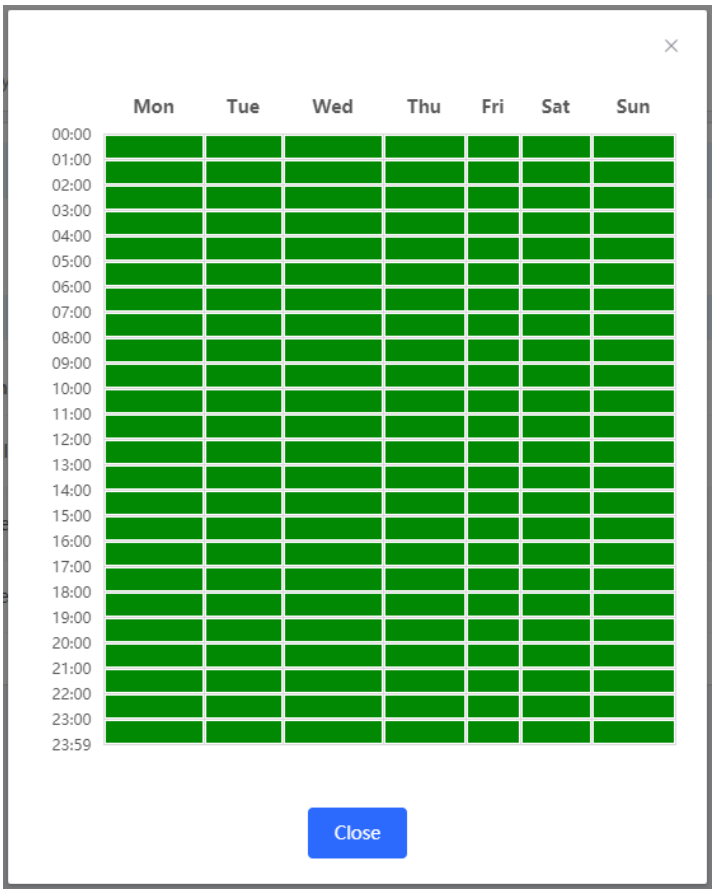
Click **Add** to add a time object. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-42 Add Time Object



Click  in the time list or in the **Add Time** box, and a time management page will appear.

Figure 3-3-43 Select Time



Select the time and click **OK**.

3.3.5 VPN

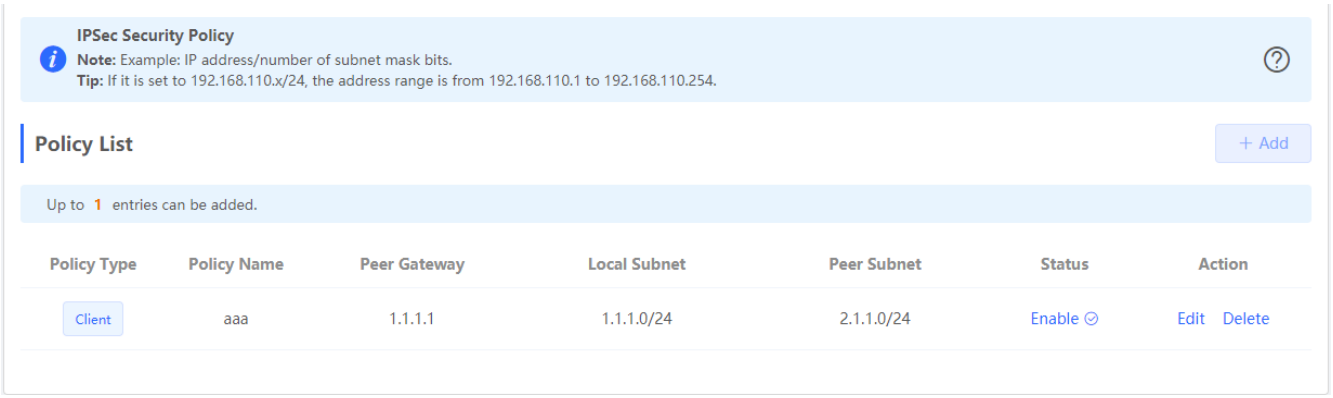
3.3.5.1 IPSec

The **IPSec** module contains **IPSec Security Policy** and **IPSec Connection Status**.

3.3.5.1.1 IPSec Security Policy

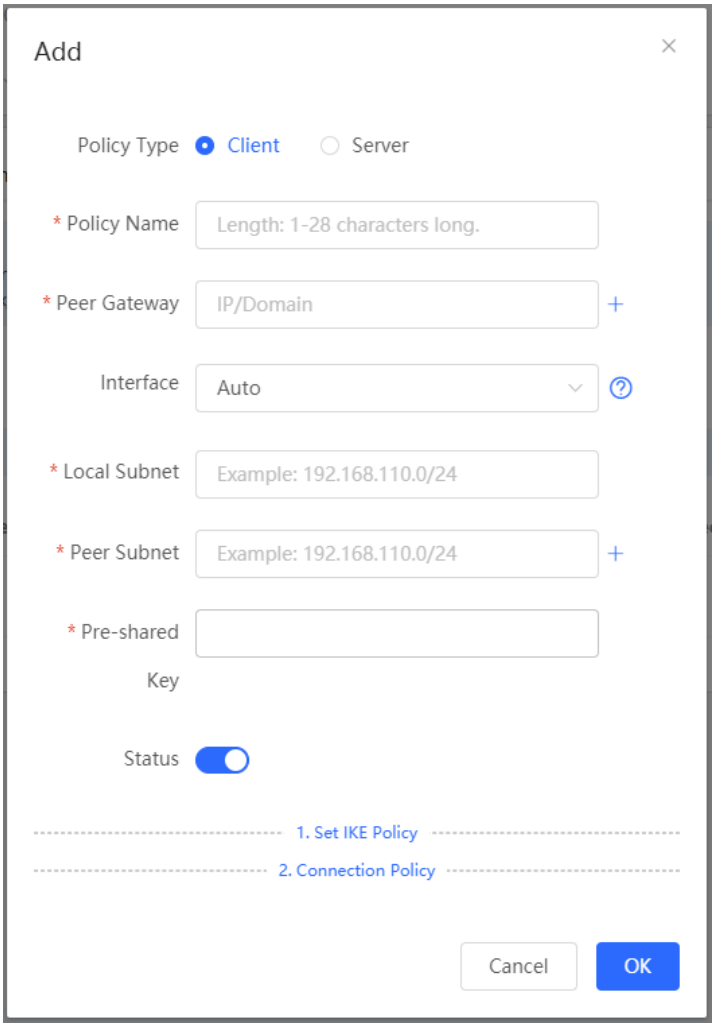
The **IPSec Security Policy** module allows you to add, delete and edit IPSec security policies.

Figure 3-3-44 IPSec Security Policy



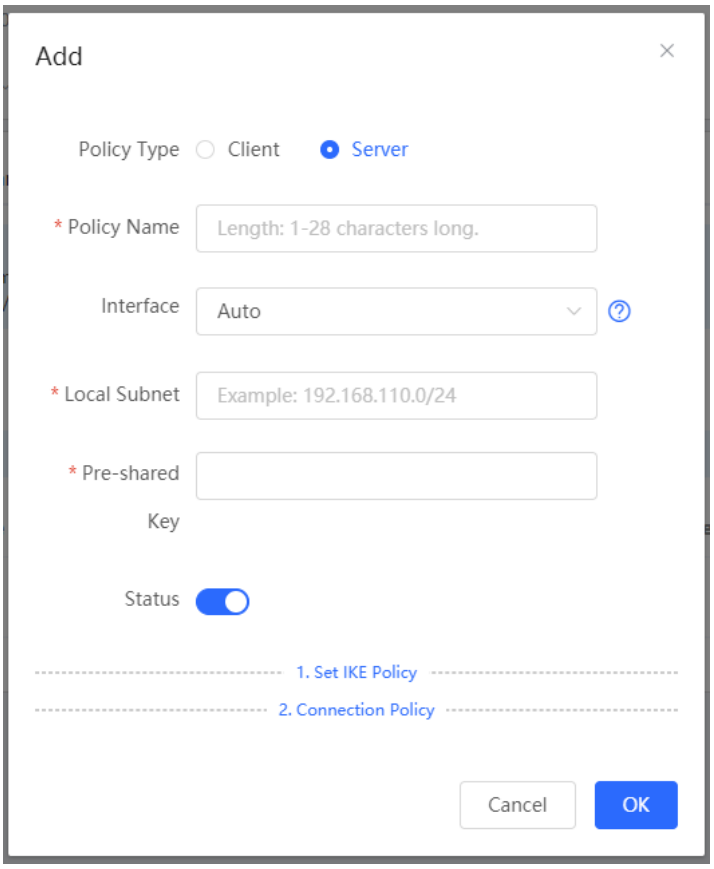
Click **Add** to add a client-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-45 Add Client-Based Policy



Click **Add** to add a server-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-46 Add Server-Based Policy

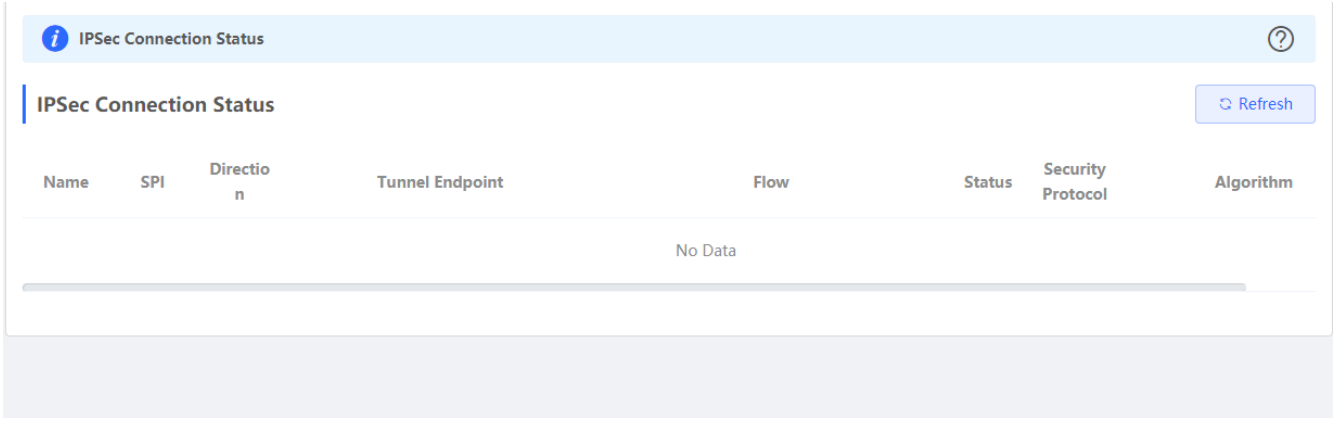


Only one policy can be added currently.

3.3.5.1.2 IPSec Connection Status

The **IPSec Connection Status** page displays IPSec connections.

Figure 3-3-47 IPSec Connection Status



3.3.5.2 L2TP

3.3.5.2.1 L2TP Settings

Layer 2 Tunneling Protocol (L2TP) is a computer networking protocol used by Internet service providers (ISPs) to enable virtual private network (VPN) operations. Because it does not provide any security for data such as encryption and confidentiality, an encryption protocol such as Internet Protocol security (IPsec) is often used with L2TP, namely, L2TP/IPsec.

Figure 3-3-48 L2TP Server Settings

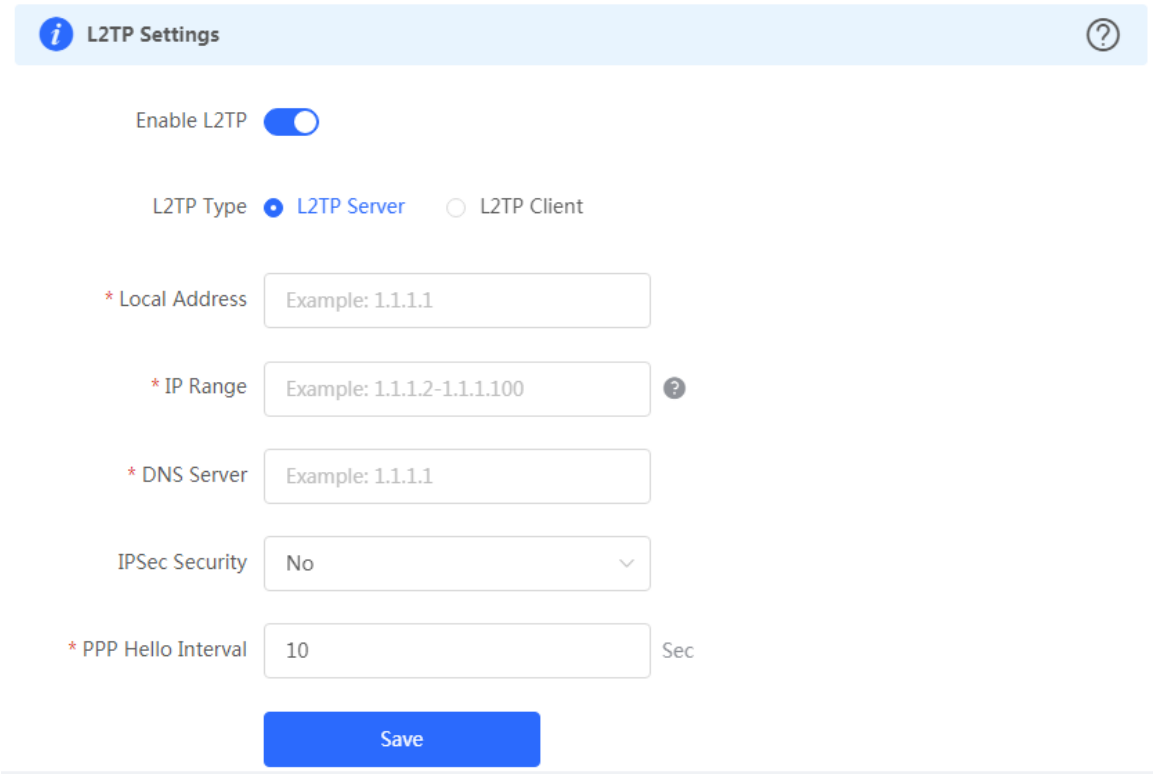
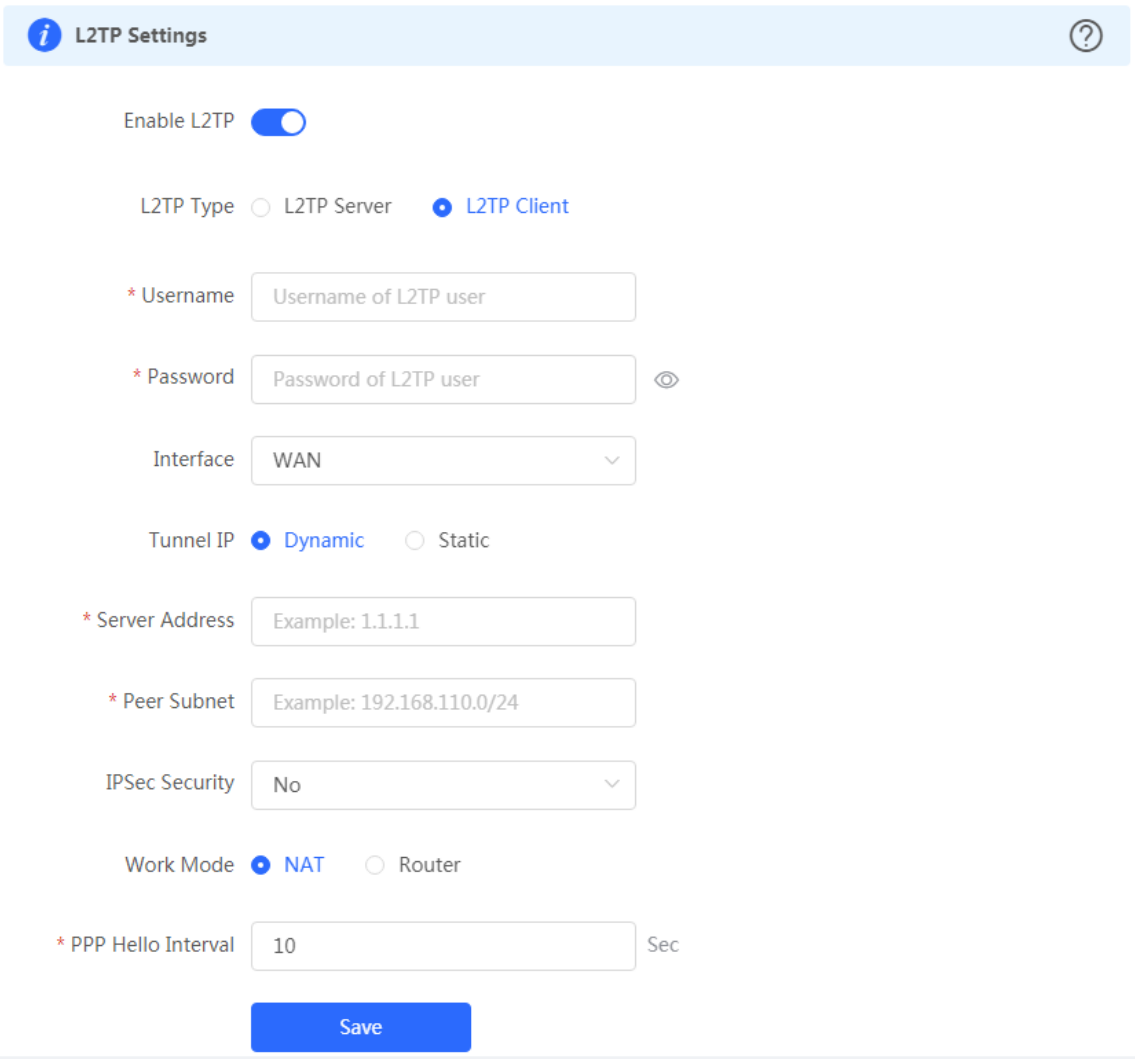
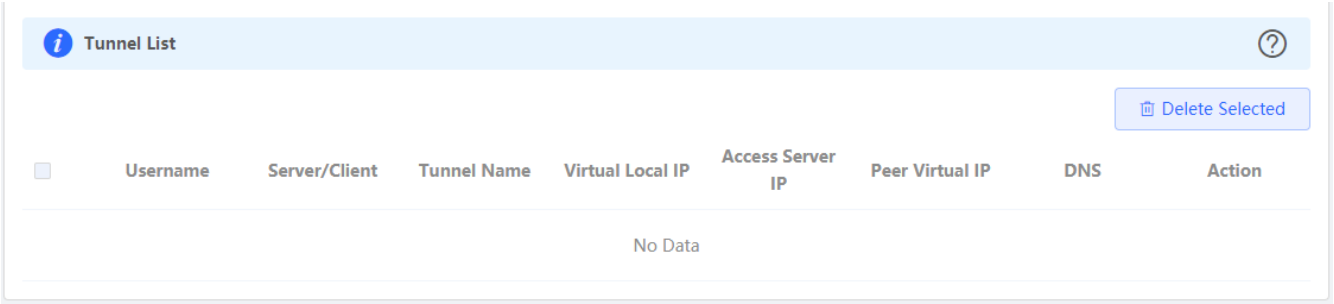


Figure 3-3-49 L2TP Client Settings



3.3.5.2.2 Tunnel List

Figure 3-3-50 L2TP Tunnel List



3.3.5.3 PPTP

Figure 3-3-51 PPTP Server Settings

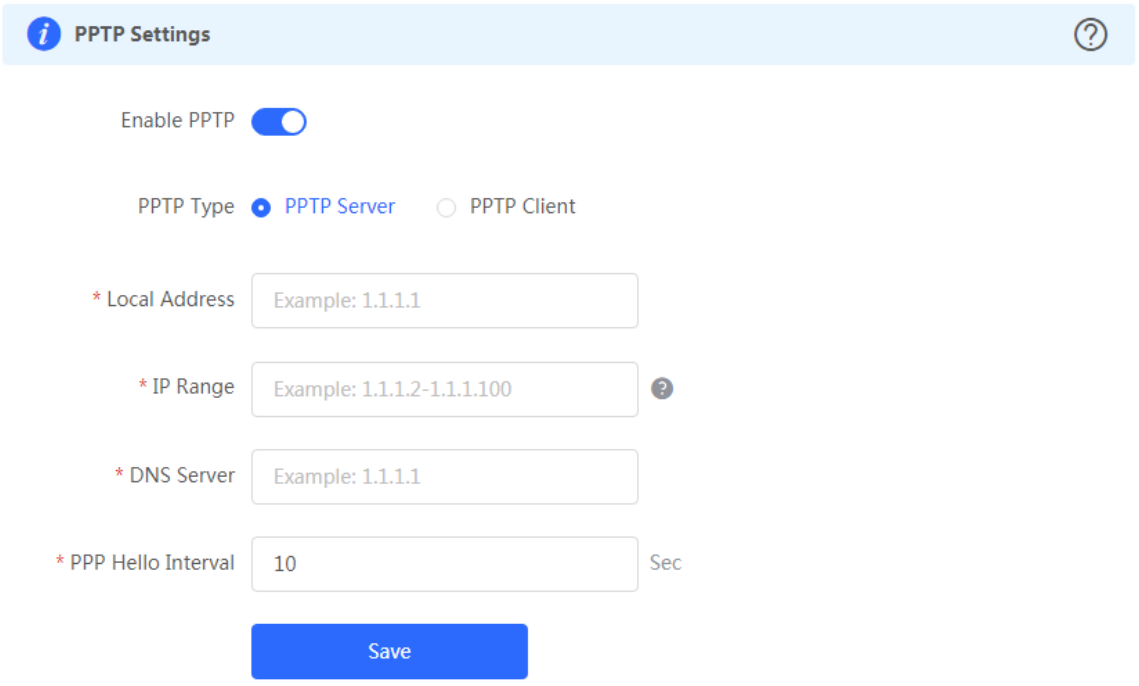


Figure 3-3-52 PPTP Client Settings

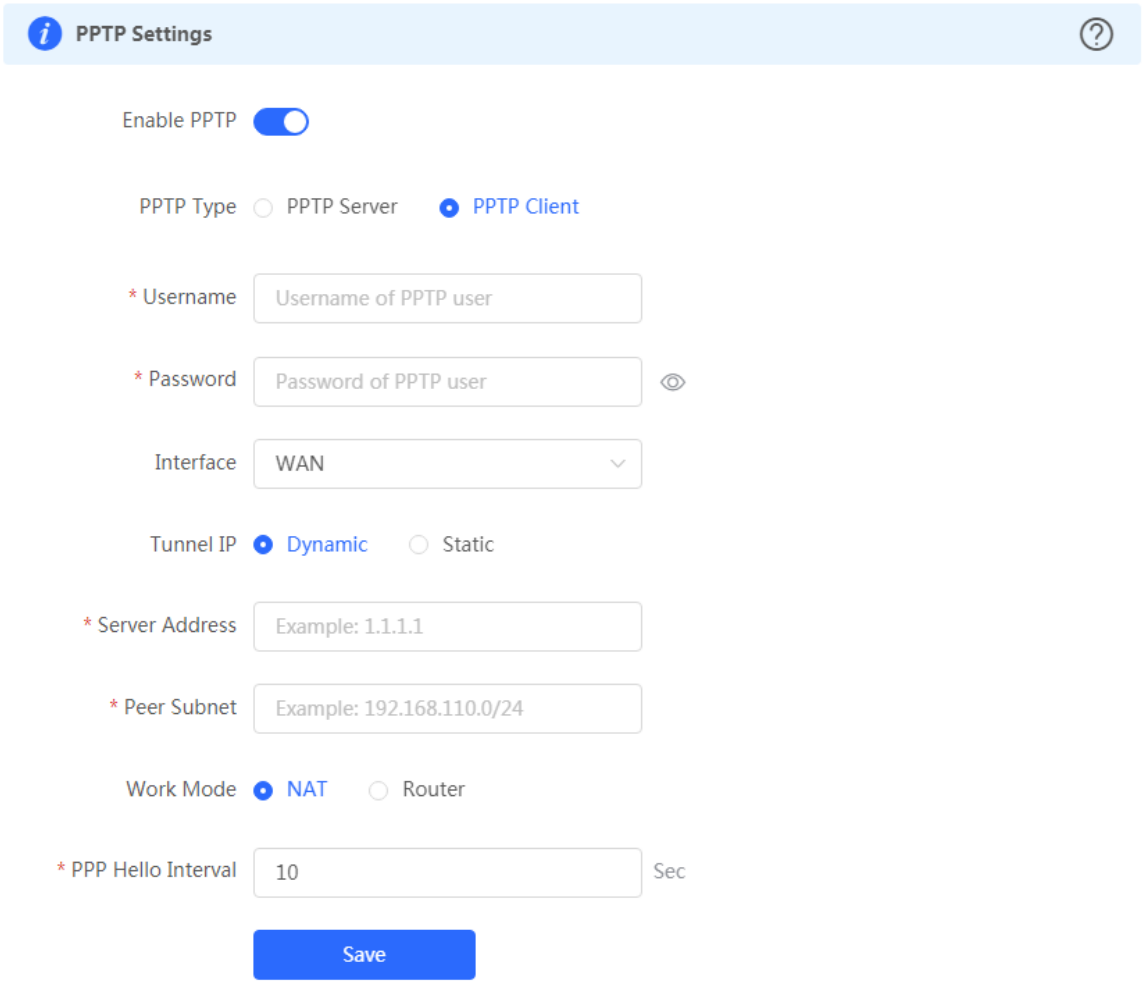
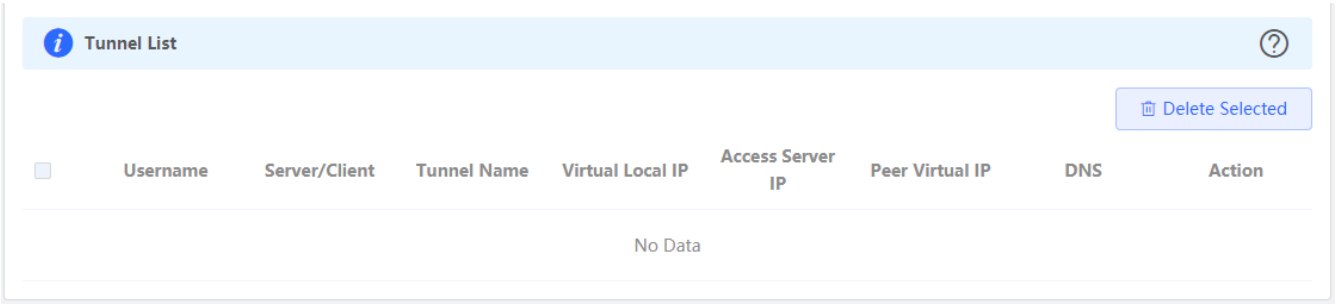


Figure 3-3-53 PPTP Tunnel List



3.3.5.4 OpenVPN

3.3.5.4.1 Overview

- Concepts

Virtual private tunnels are required between enterprises, individuals and companies due to security or cross-NAT concern. OpenVPN is an SSL/TLS based virtual private network solution. Compared with other VPNs, OpenVPN supports more flexible client authorization, including certificate and account authorization, and allows users to connect to the VPN's virtual interface through a firewall. OpenVPN runs on Linux, xBSD, Mac OS X and Windows2000/XP. The EG device supports VPN connection to PCs, Android/iOS-based mobile phones, routers and Linux-based devices, compatible with most OpenVPN devices on the market.

OpenVPN supports connections through most proxy servers and work well in NAT environments. The server can deliver certain configuration to the client, including IP address, routing and DNS configuration.

- Certificates

The advantage of OpenVPN lies in its own security, and OpenVPN security depends on certificate support.

The OpenVPN certificate system is as follows:

```
├──pki
│    ├── ca.crt    #CA Certificate
│    ├── dh.pem    #Authentication Algorithm
│--issued
│    │    ├── client.crt     #Client Certificate
│    │    └── server.crt    #Service Certificate
│    ├── private
│    │    ├── ca.key
│    │    ├── client.key     #Client Private Key
│    │    └── server.key     #Service Private Key
      ├── tls.key       #tlsTLS Authentication Key
```

The client certificate includes ca.CRT, ca.key, client.CRT, client.key, and the server-side certificate includes ca.CRT, ca.key, server.CRT, server.key.

3.3.5.4.2 Configuration Tasks

The device supports OpenVPN server or client. The following describes the configuration parameters of the server and client.

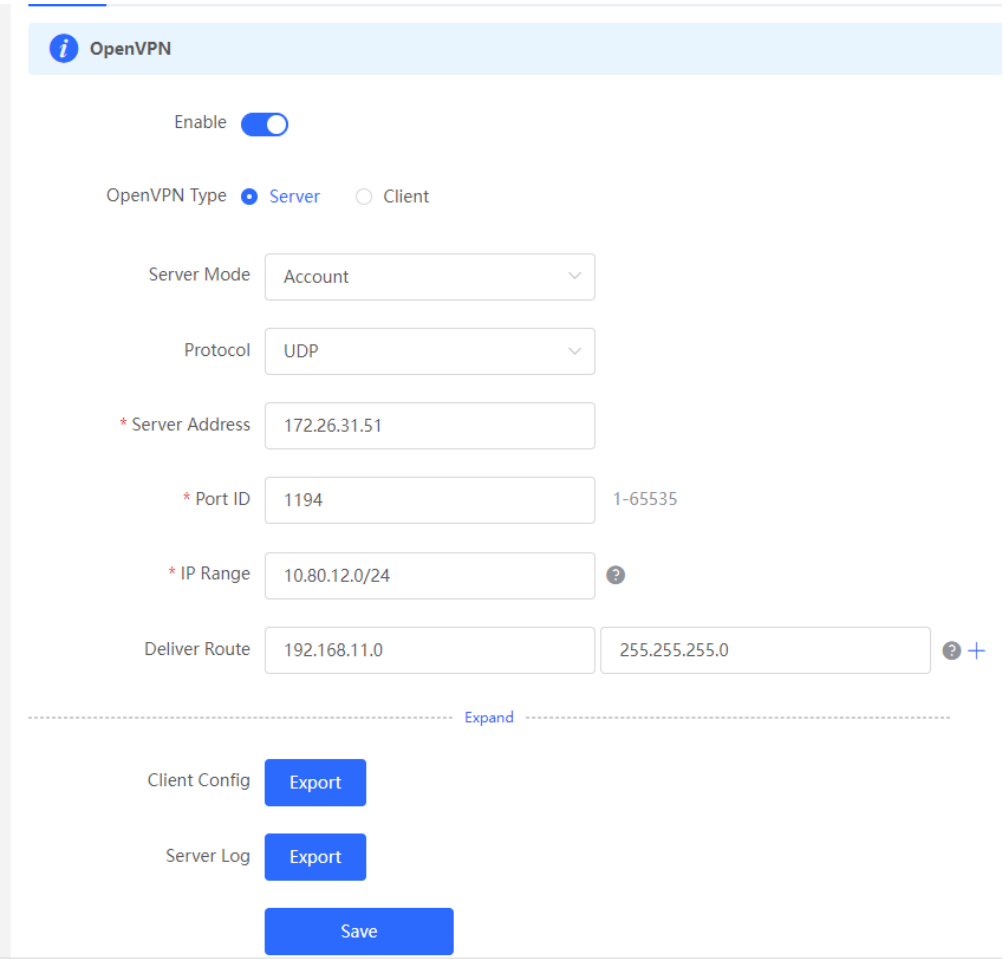
1. Server Mode
2. Client Mode

3.3.5.4.3 Server Mode

Basic Settings

Choose **Router** > **VPN** > **OpenVPN**.

Figure 3-3-54 OpenVPN



- Server Mode

The EG device supports three authentication modes: **Account**, **Certificate**, and **Account & Certificate**. In the **Account** mode, the client needs to enter the correct account, including the username and password, and import the CA certificate. In the **Certificate** mode, the client needs to use the CA certificate, client certificate, and private key to connect to the server. The **Account & Certificate** mode requires all configuration mentioned above, mainly applied in security-demanding scenarios.

- Protocol

All OpenVPN communication is based on a single IP port. The UDP protocol is used by default and TCP is also supported. When selecting a protocol, please pay attention to the network conditions about the encrypted tunnels. If there is a high delay or a lot of packet loss, please select the TCP protocol as the underlying protocol.

- Server Address

The server address can be either an IP address or a domain name.

- Port ID

The official IANA (Internet assigned numbers Authority) assigned port number is 1194. If the port is occupied or disabled on the local network, the server log will prompt that port binding fails and remind you to change the port ID.

- IP Range

The OpenVPN address pool, except for the first address reserved for the server, is assigned to the clients. For example, if you set 10.80.12.0/24, the virtual IP address of the OpenVPN server is 10.80.12.1.

- Deliver Route

The server informs clients to access the intranet by a VPN tunnel. This is the only way to inform clients of the access method.

- Client Config

Export a tar package containing client configuration.

1. If you select the **Account** mode, the package includes the configuration file (client.ovpn), CA certificate (ca.CRT), CA private key (ca.key).
2. If you select the **Certificate** mode, the package includes the configuration file (client.ovpn), CA certificate (ca.CRT), CA key (ca.key), client certificate (client.cart) and client key (client.key).
3. If TLS authentication is enabled, the package includes a TLS authentication key (tls.key) in addition to the files mentioned above.

- Server Log

Export the service log, including the server startup time and client dial-up logs.

- Save

When the basic settings are complete, you can view the server tunnel information in **Tunnel List**.

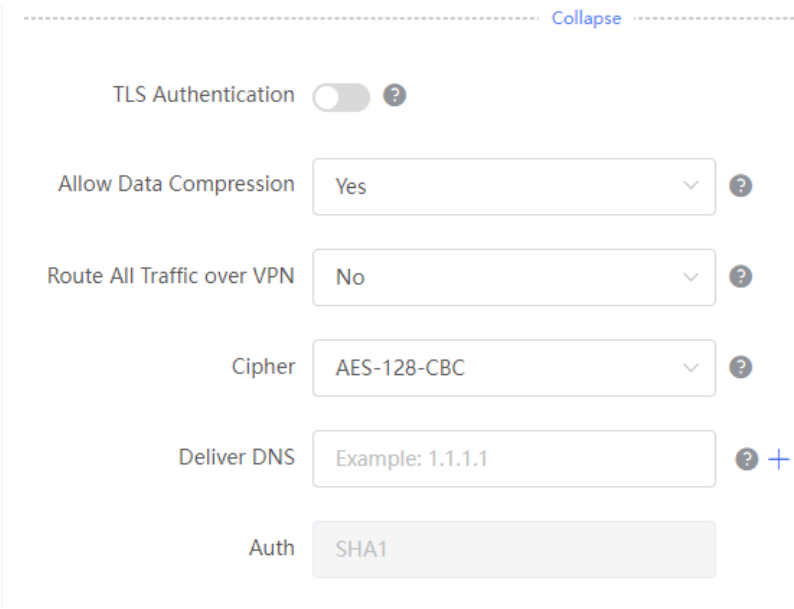
Advanced Settings

Click **Expand**.

Figure 3-3-55 Expand

The following advanced settings are available, and can be left as default if there are no special needs.

Figure 3-3-56 Advanced Settings



- TLS Authentication

The TLS key is used to enhance OpenVPN security by requiring both parties to have a shared key before the TLS handshake. After TLS authentication is enabled, the client must import a TLS key (The OpenVPN client version must be greater than 2.40).

- Allow Data Compression

This feature is be used to compress the transmitted data by the LZO algorithm, which saves bandwidth, but consumes CPU resources. The configuration on the client side and on the server side must be consistent. Otherwise, the connection will not be set up.

- Route all Traffic over VPN

This feature is used to router all traffic over the VPN tunnel. The VPN tunnel will be used as the default route.

- Cipher

Encrypting the data before transmission will ensure that the information cannot be read even if the data packet is intercepted during transmission. If the server is set to the **Auto** mode, the client can configure any encryption algorithm and will use the default algorithm (AES-256-GCM) automatically. If the server is set to a specific encryption algorithm, the client must have the same configuration as the server. Otherwise, the connection will not be set up.

- Deliver DNS

The server pushes DNS information to the client, only the windows-based client.

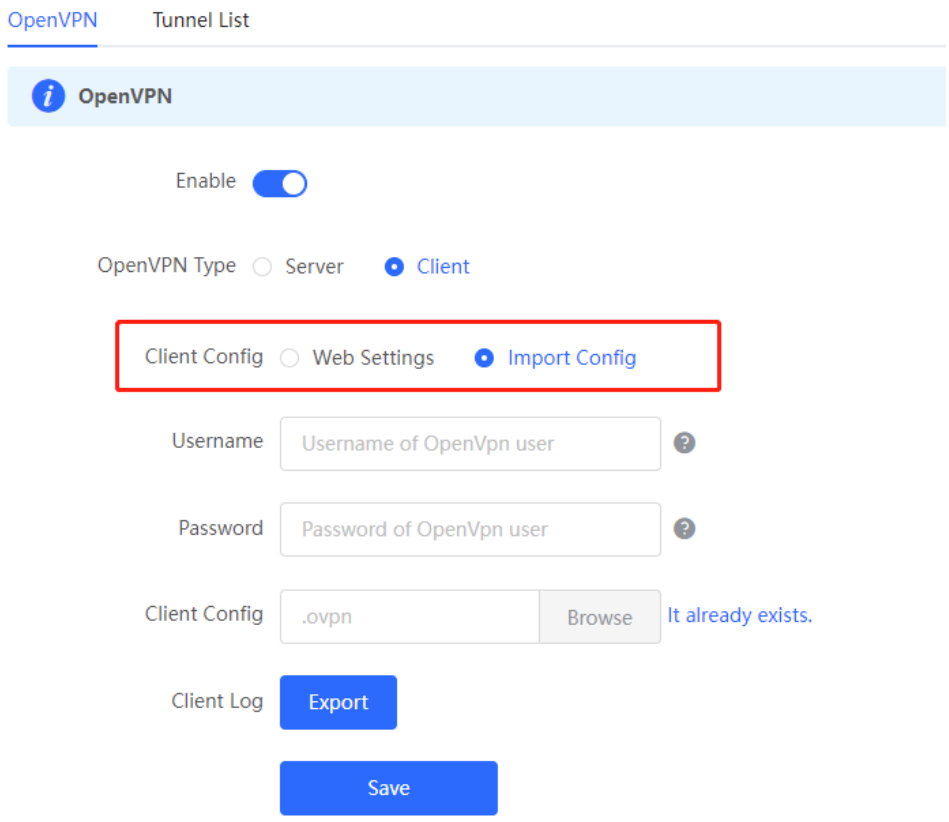
- Auth

The server informs the client to use the default digest algorithm SHA1.

3.3.5.4.4 Client Mode

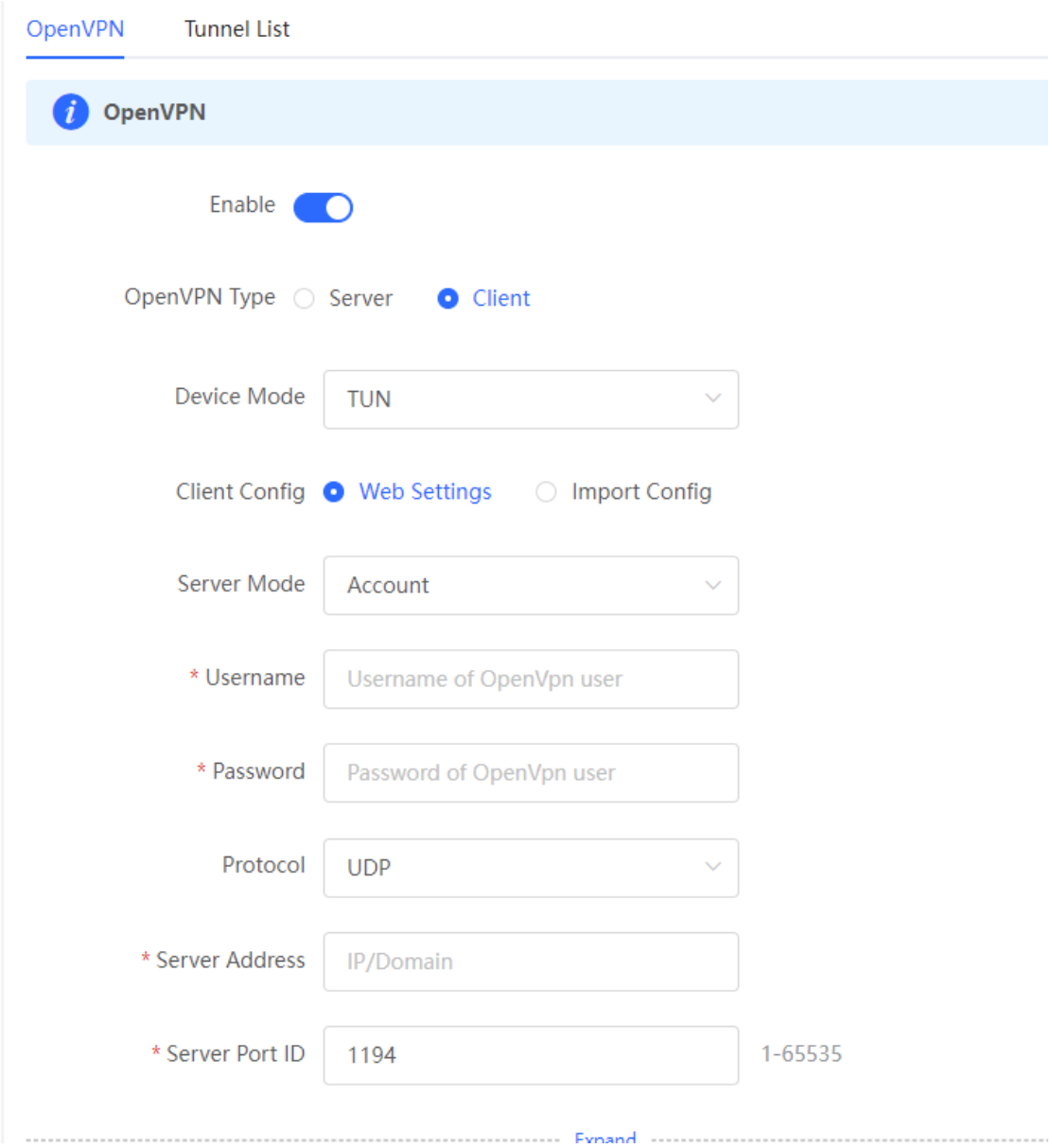
The EG device currently supports two client configuration modes: **Web Settings** and **Import Config**. **Web Settings** is typically used to connect to any server except the EG device. **Import Config** is mainly used to connect to an EG device because it working as a server supports exporting the client configuration file (client.ovpn).

Figure 3-3-57 Import Config



Basic Settings

Figure 3-3-58 Web Settings



- Device Mode

The EG device working as a client supports both the TUN and TAP modes. The configuration must be consistent with the server. The EG device working as a server supports the TUN mode only.

- Server Mode

The server supports three authentication modes: **Account**, **Certificate**, and **Account & Certificate**.

- Protocol

Both UDP and TCP are supported. The configuration must be consistent with the server side.

- Server Address

Enter the server IP address or domain name.

- Server Port ID

Enter the server port ID.

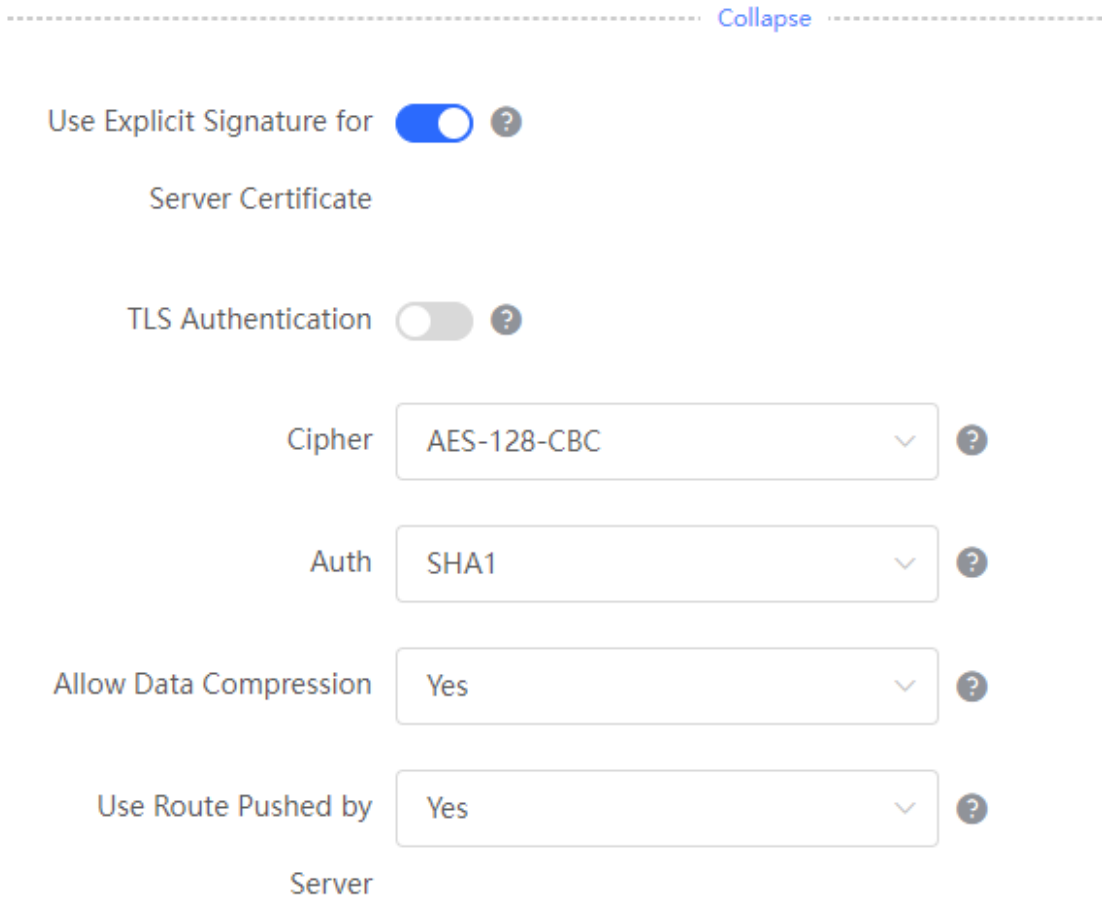
Advanced Settings

Click **Expand**.

Figure 3-3-59 Expand

The following advanced settings are available, and can be left as default if there are no special needs.

Figure 3-3-60 Advanced Settings



- Use Explicit Signature for Server Certificate

This feature is enabled by default. If you want to connect to a Mikrotik router, please disable this feature.

- TLS Authentication

Please upload a TLS certificate for TLS authentication.

- Cipher

The configuration must be consistent with the server side.

- Auth

The following digest algorithms are available: SHA1, MD5, SHA256 and NULL. The configuration must be consistent with the server side.

- Allow Data Compression

Data compression is allowed, and the configuration must be consistent with the server side.

- Use Route pushed by Server

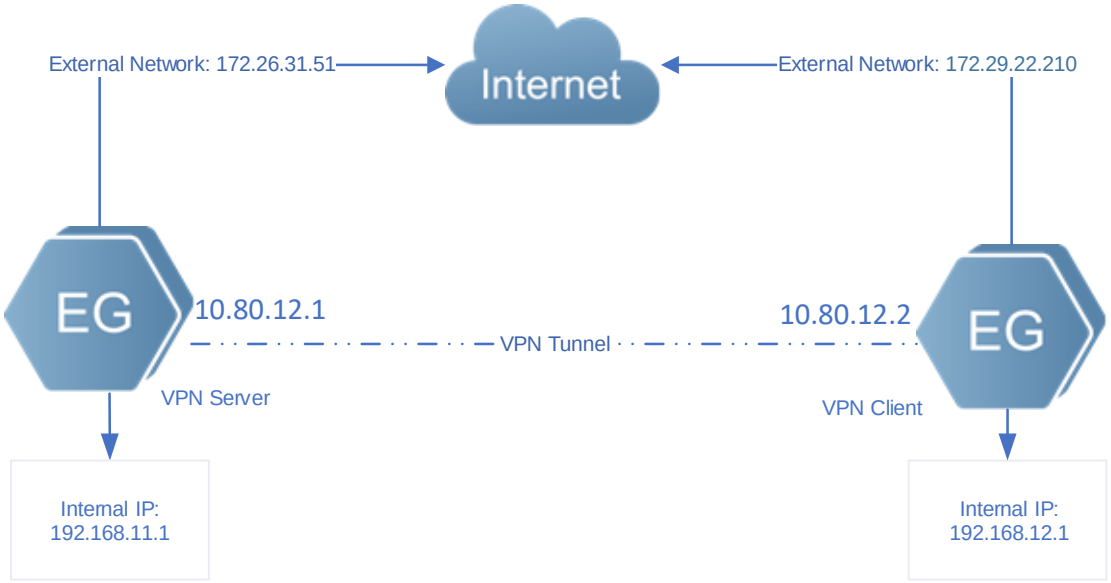
If this feature is disabled, the client will not receive the route delivered by the server. If you want to access the internal network of the server, please enable this feature.

3.3.5.4.5 Typical Applications

3.3.5.4.5.1 Networking Topology

Scenario 1. An EG device connects to another EG device.

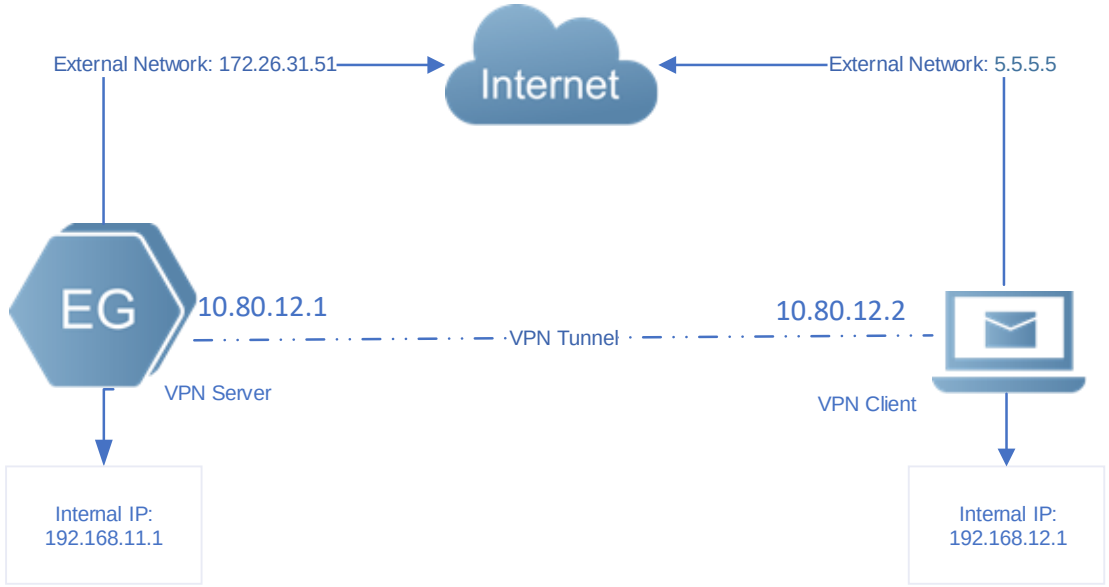
Figure 3-3-61 Scenario 1



The client (192.168.11.1) wants to connect to the server (192.168.12.1) by OpenVPN and achieve mutual access between the client network and the server network.

Scenario 2. An EG device connects to a PC.

Figure 3-3-62 Scenario 2



3.3.5.4.5.2 Notes

1. OpenVPN allows a PC to dial in to the VPN as a client, and supports connection between a router and another router.

⚠ The client address pool cannot overlap with the internal network of the EG device.

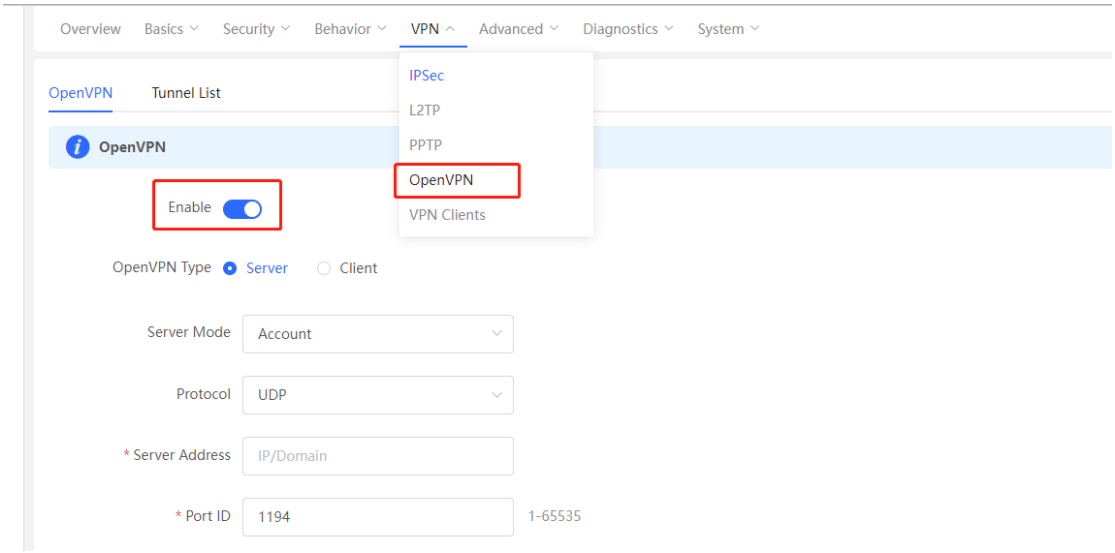
2. Enable **Deliver Router** on the server side and **Use Route Pushed by Server** on the client side. The client will be able to access the internal network of the server.
3. The external IP address of the EG device must be reachable from the client.
4. The configuration on the client side and the server side must be consistent.

3.3.5.4.5.3 Configuration Steps

Server

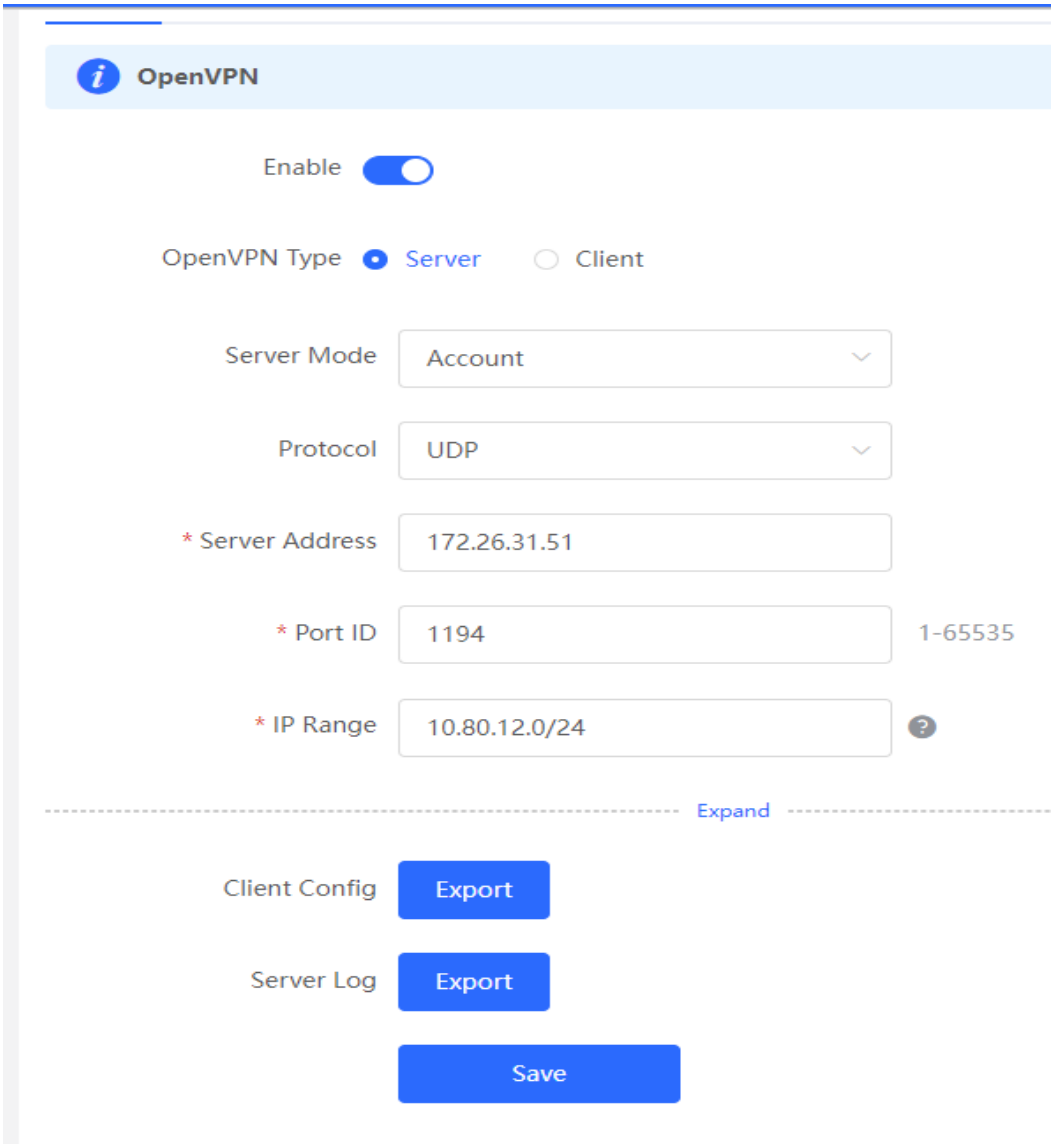
1. Log in to the web management system. Choose **Router** > **VPN** > **OpenVPN**.

Figure 3-3-63 OpenVPN



2. Set **OpenVPN Type** to **Server**. Select a server mode and a protocol, enter a port ID (default: 1194), a server address (local address, reachable from the client) and an IP address range. For example:

Figure 3-3-64 Server Settings



⚠ The local address and IP address range cannot overlap with the internal network.

⚠ The OpenVPN server assigns the IP address pool to the PC, and the server reserves the first address xx.xx.xx1 to itself. In the figure above, the virtual IP address of the OpenVPN server is 10.80.12.1.

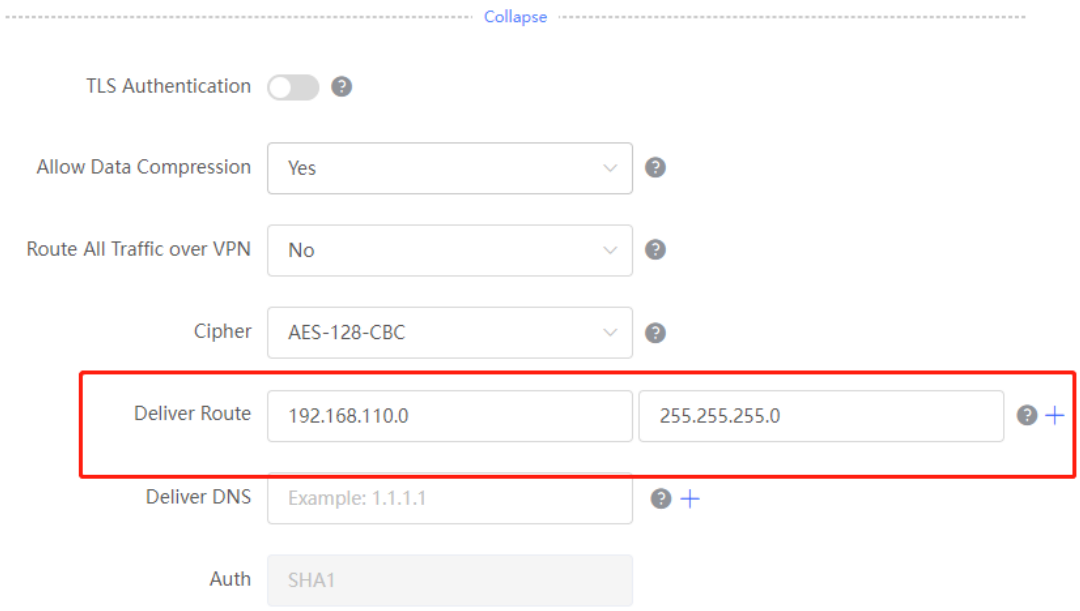
⚠ The port ID ranges from 1 to 65536 (Default: 1194). If the port is occupied, the connection will not be set up.

3. If the EG device connects to another EG device, it is recommended to use default configuration. If the EG device connects to a device from other vendors, please make sure that the configuration on the client side and the server side are consistent. If the client wants to access the internal network 192.168.110.x, please add the route.

Figure 3-3-65 Deliver Route

Enable **Deliver Router** on the server side and **Use Route Pushed by Server** on the client side. The client will be able to access the internal network of the server. Up to three routes can be added.

Figure 3-3-66 Deliver Route

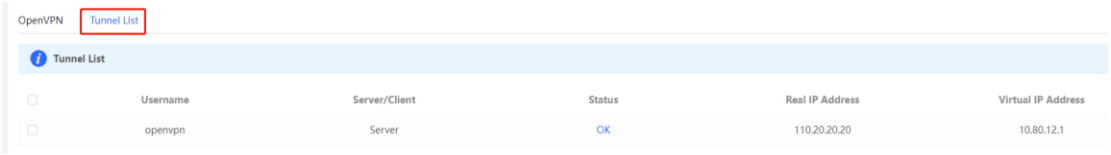


Remarks

- **Route all Traffic over VPN**: After this feature is enabled, all traffic will be routed over VPN.
- **Cipher**: If the server is set to the **Auto** mode, the client can configure any encryption algorithm and will use the default algorithm (AES-256-GCM) automatically. If the server is set to a specific encryption algorithm, the client must have the same configuration as the server. Otherwise, the connection will not be set up.
- **Allow Data Compression**, **Cipher** and **Auth** configuration must be consistent on the server side and the client side.

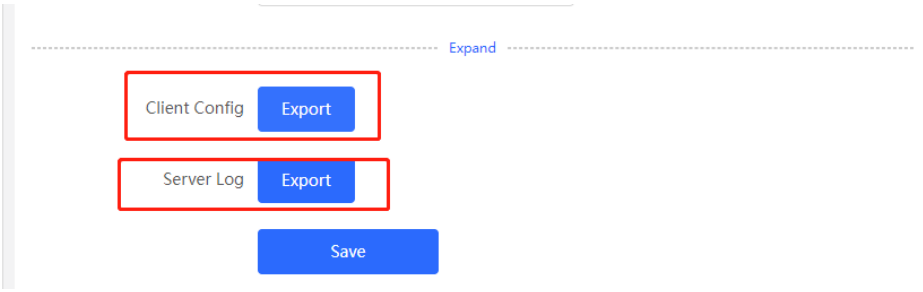
4. After the server is created successfully, you can view the server information in **Tunnel List**.

Figure 3-3-67 Tunnel List



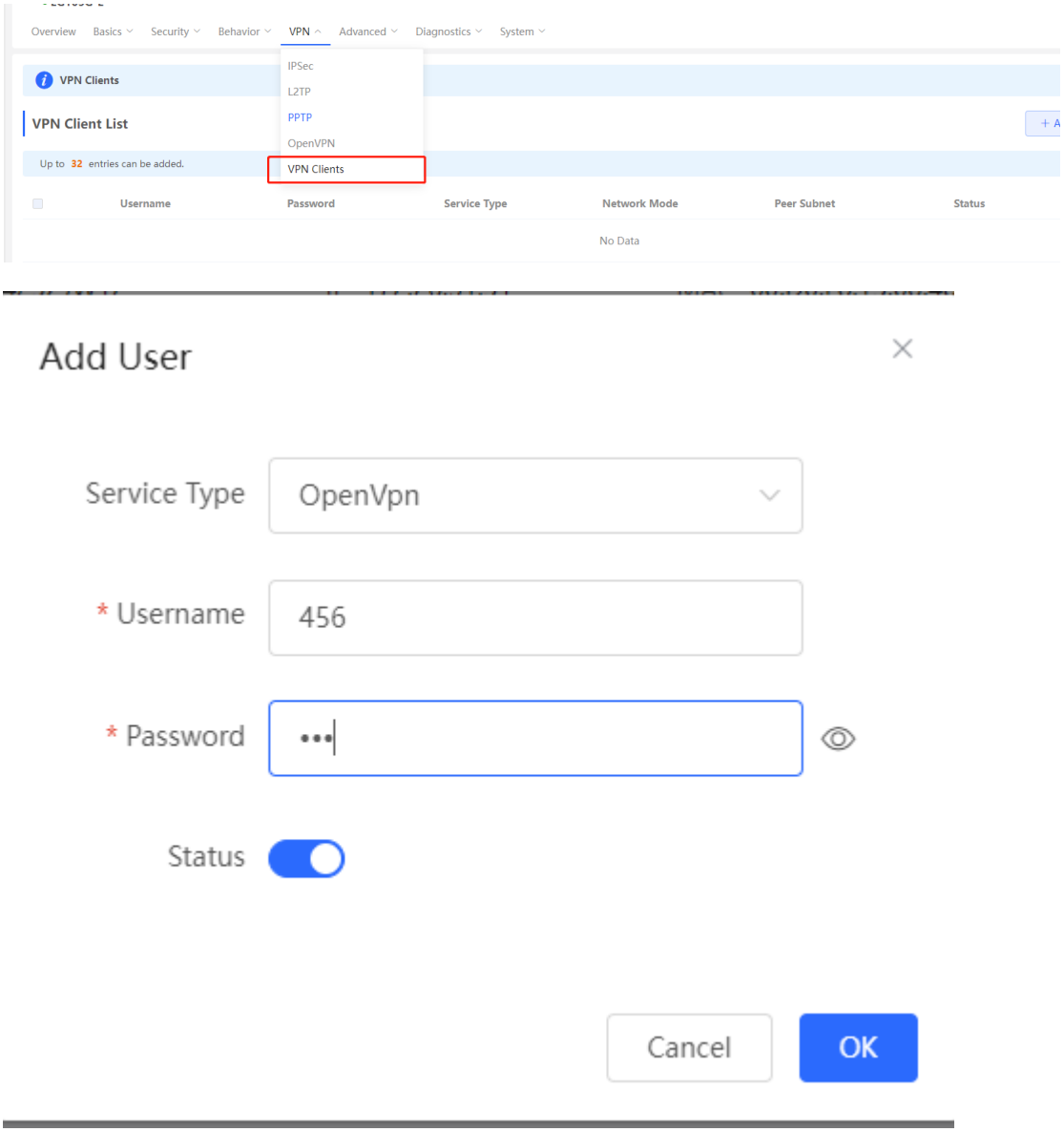
After the server is created successfully, you can export the configuration file of the client connected to the server. If you fail to create the server, please check log for failure prompt.

Figure 3-3-68 Export Config



5. Choose **VPN** > **VPN Clients** to create an account for OpenVPN.

Figure 3-3-69 OpenVPN Account

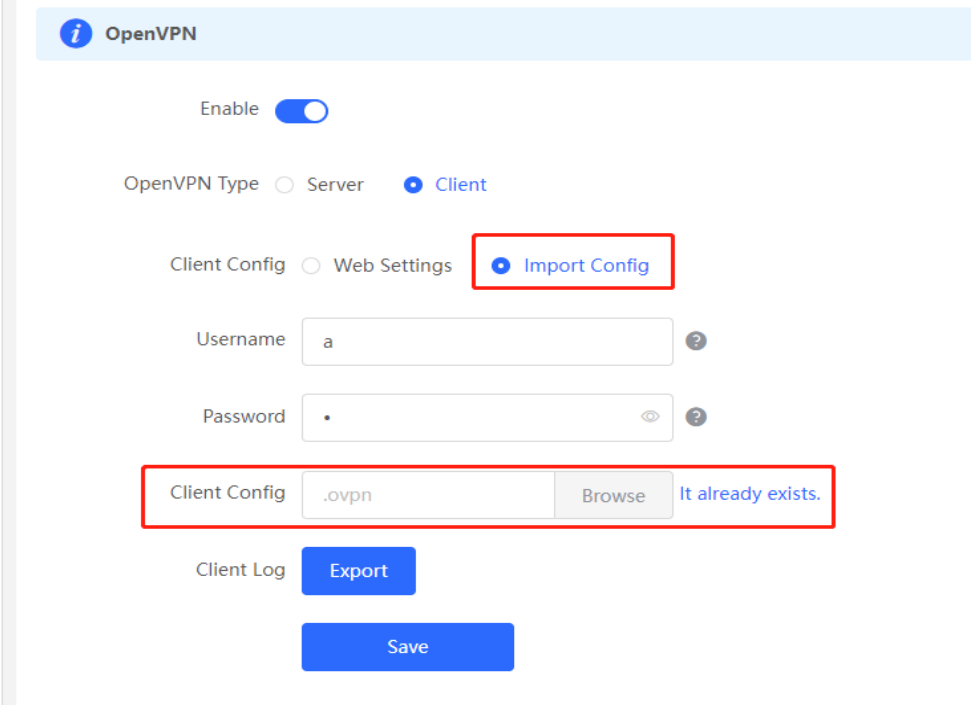


Select **OpenVPN** from the **Service Type** dropdown list.

Client

1. Set **OpenVPN Type** to **Client**. Select **Import Config**. If the server is configured with the **Account** mode, please enter the correct account, including the username and password.

Figure 3-3-70 Client Settings



2. View the tunnel information. If the client is created successfully, you can view the client information in **Tunnel List** on both the client side and the server side.

Figure 3-3-71 Tunnel List on Client Side

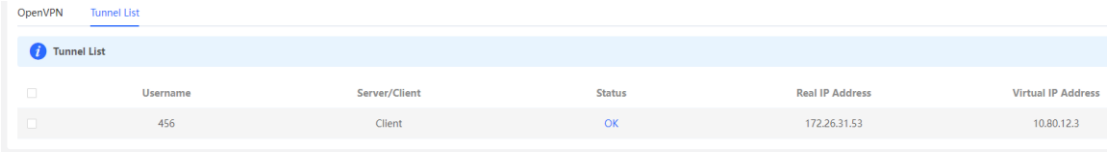
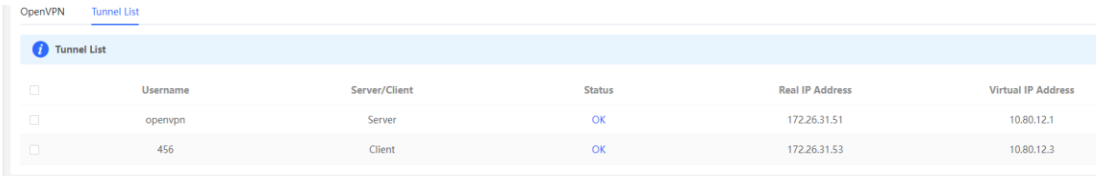
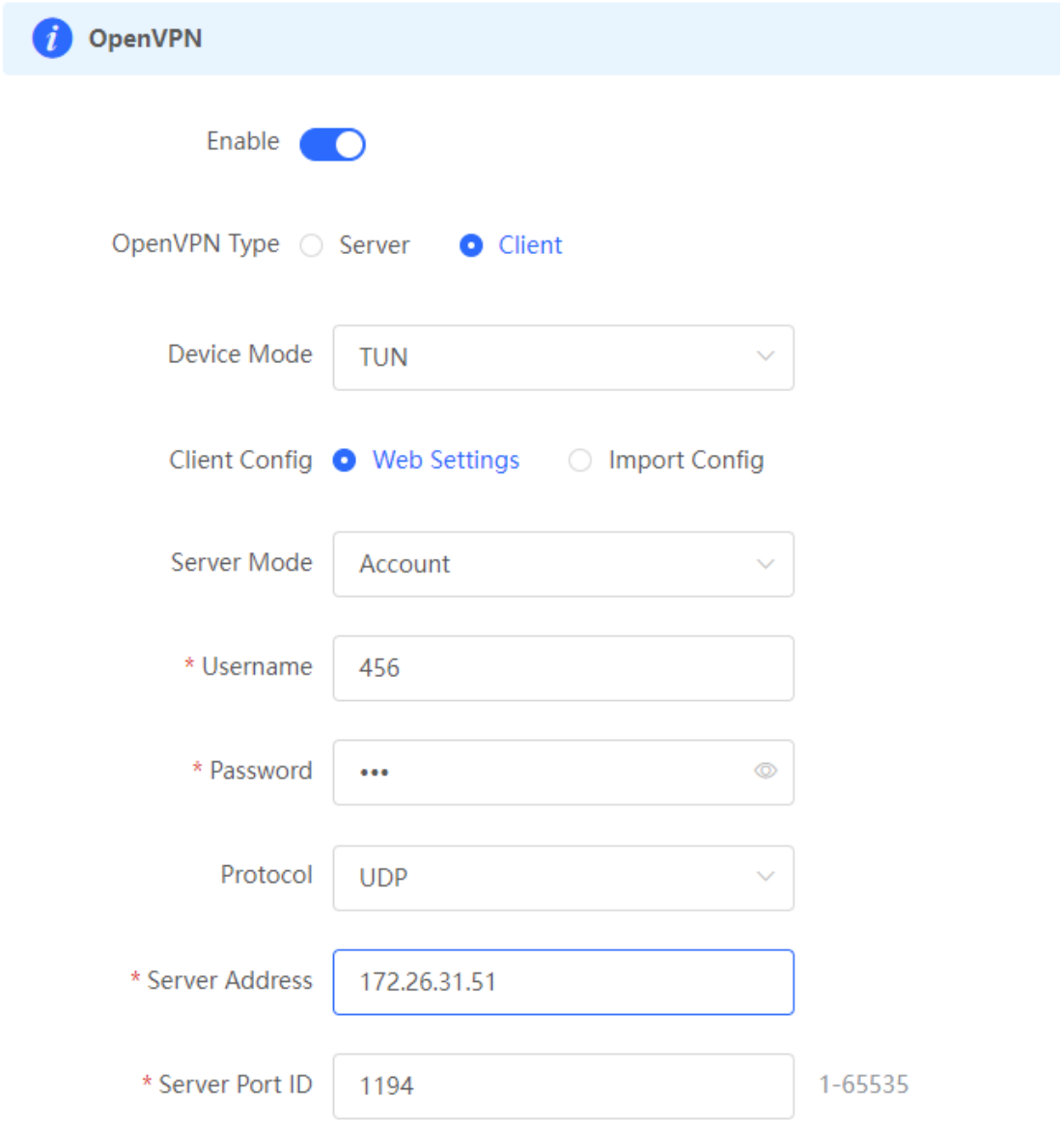


Figure 3-3-72 Tunnel List on Server Side



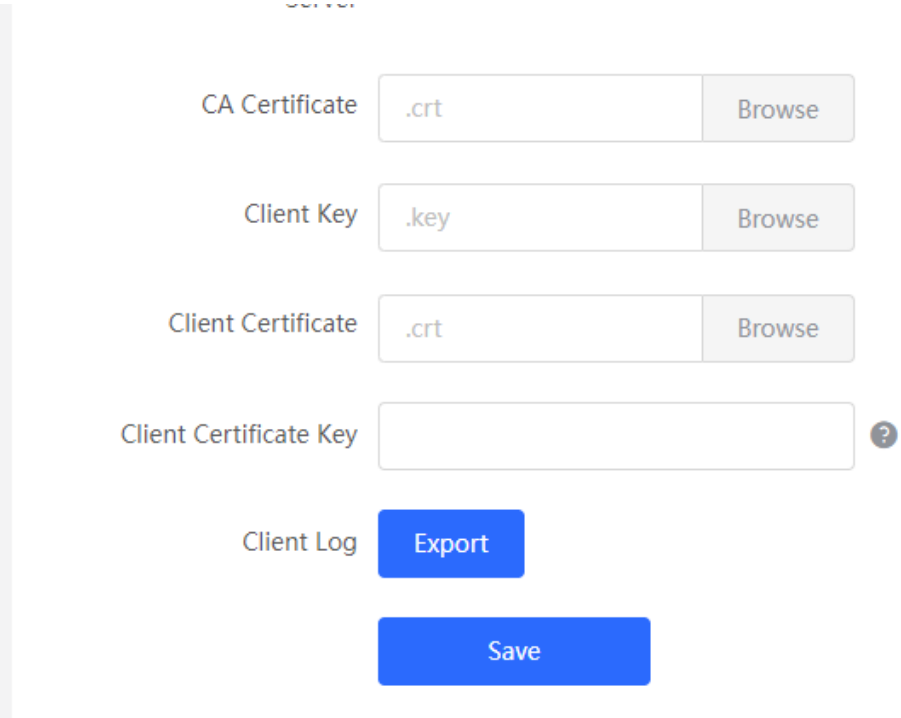
3. You can also set **Client Config** to **Web Settings**. Select a device mode, server mode and protocol. If the server mode is set to **Account**, please enter the correct account, including username and password. The server address and server port ID are also required.

Figure 3-3-73 Client Settings



The **Device Mode**, **Protocol** and **Server Mode** must be consistent on the server and the client. The server address must be reachable from the client.

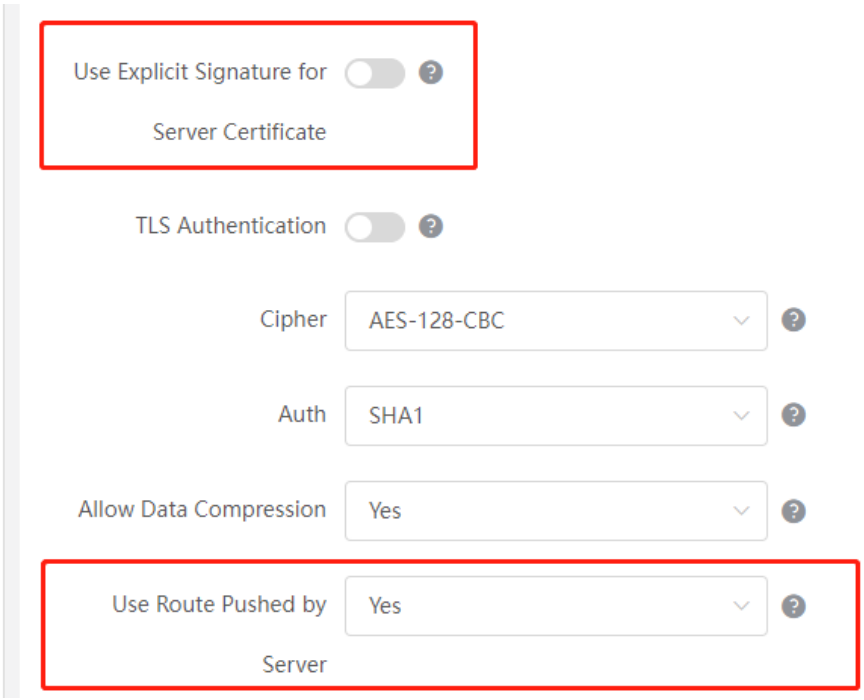
Figure 3-3-74 Client Settings



If you select the **Certificate** mode, please import the CA certificate, client certificate and private key. If you select the **Account** mode, please import the CA certificate.

4. If an EG device working as a client connects to another EG device as a server, please use the default configuration. If an EG device connects to any server except the EG device, e.g., Mikrotik device, please disable **Use Explicit Signature for Server Certificate** on the client.

Figure 3-3-75 Client Settings

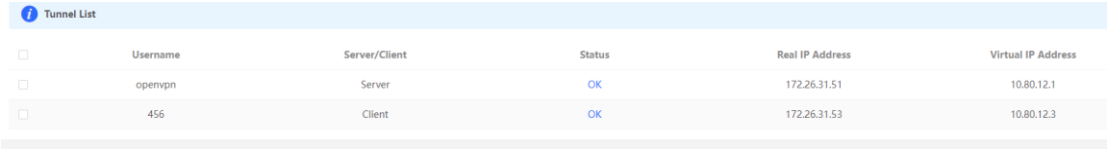


If the client wants to access the internal network of the server, please enable **Deliver Route** on the server and keep the other configuration consistent on the client and the server. Click **Save**, and you can view the created server and client in **Tunnel List**.

3.3.5.4.5.4Validation

1. The server and client information are available in **Tunnel List**.

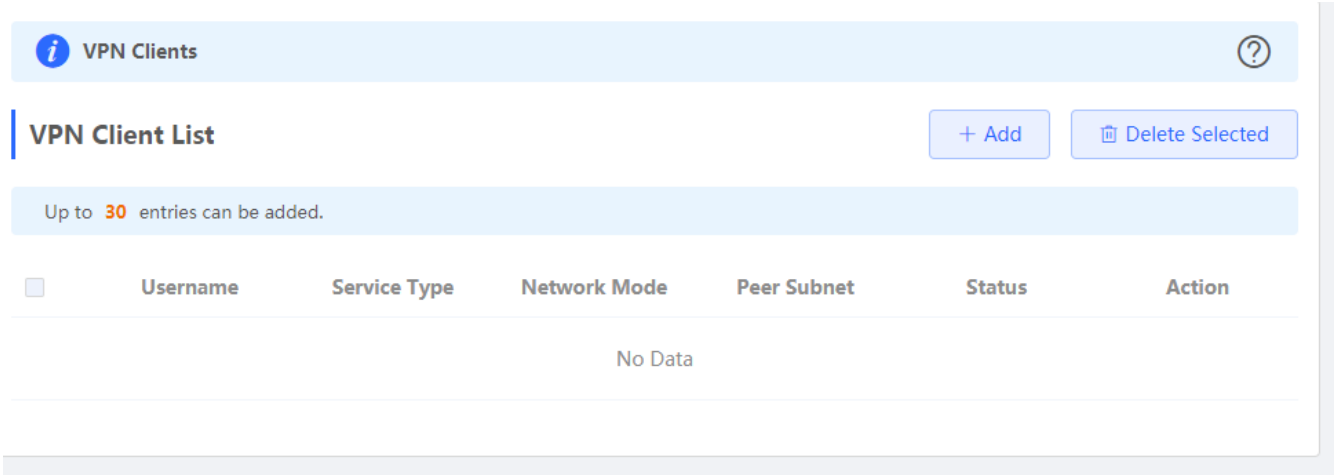
Figure 3-3-76 Tunnel List



2. Virtual addresses can ping each other and the client can access the internal network of the server.

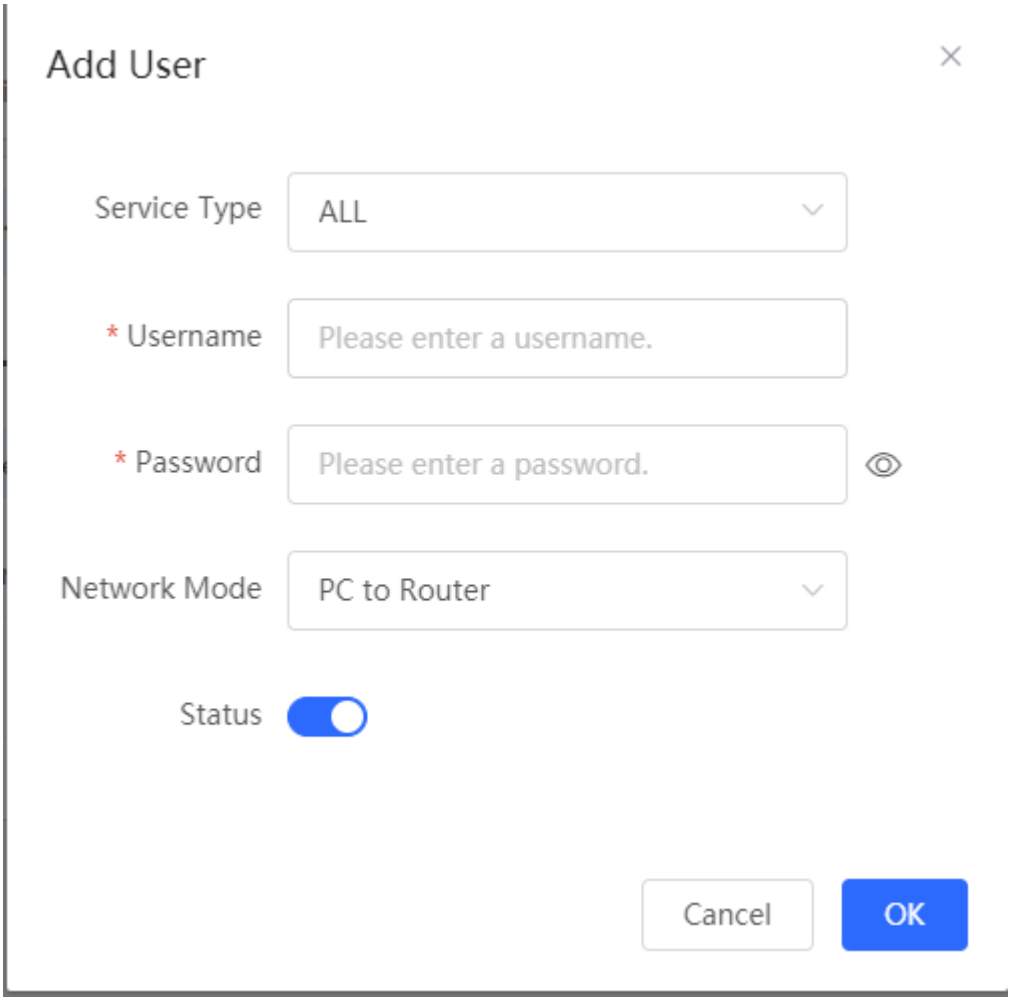
3.3.5.5 VPN Clients

Figure 3-3-77 VPN Clients



Click **Add** to add a vpn client. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-78 VPN Clients



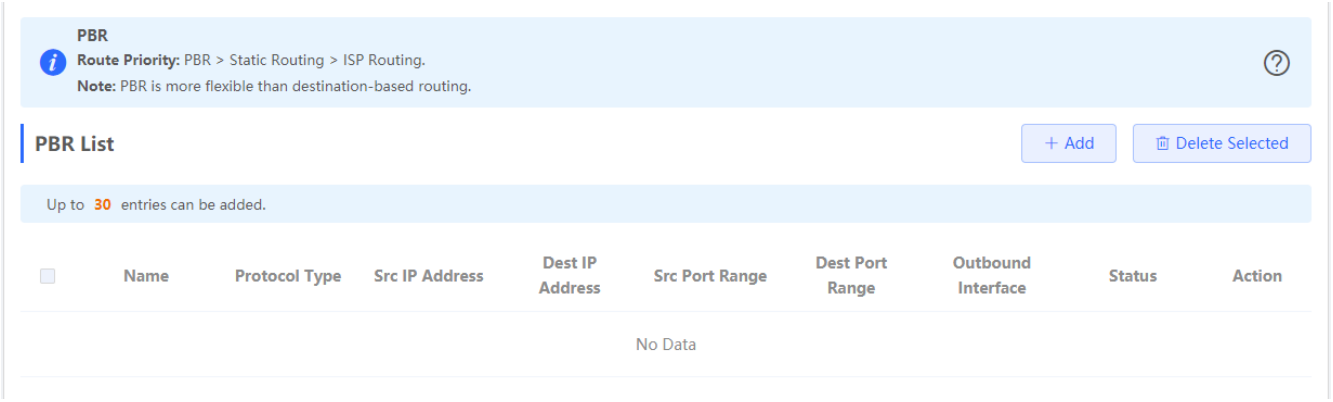
3.3.6 Advanced

3.3.6.1 Routing

3.3.6.1.1 PBR

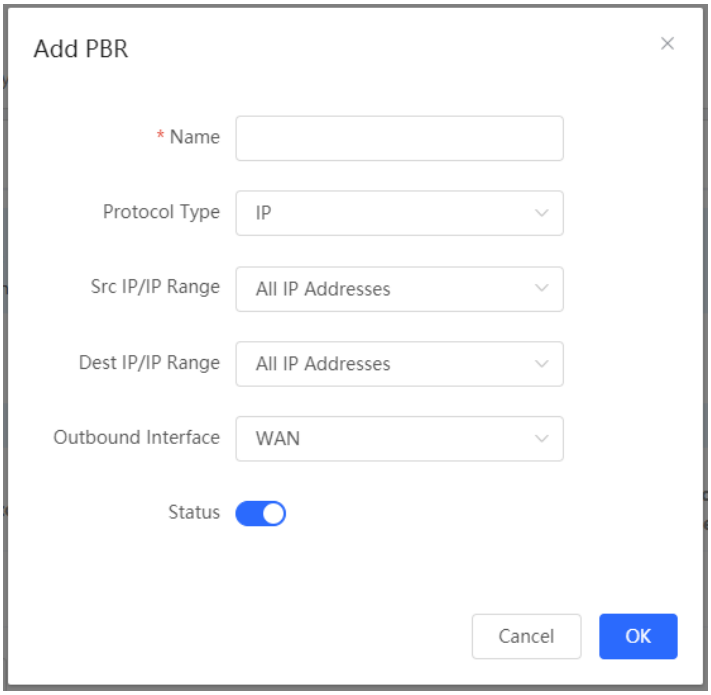
The **PBR** module allows you to add, delete and edit policy-based routes.

Figure 3-3-79 PBR List



Click **Add** to add a policy-based route. In the displayed dialog box, configure settings and click **OK**.

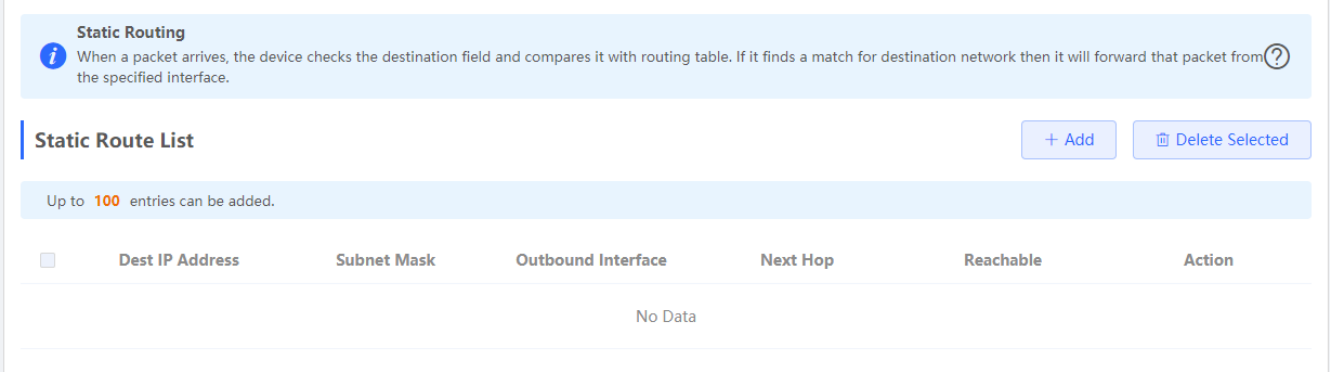
Figure 3-3-80 Add PBR



3.3.6.1.2 Static Routing

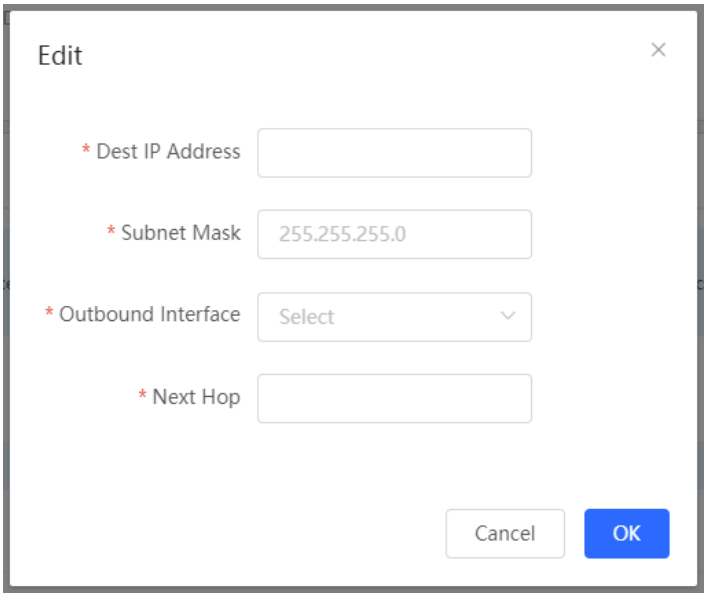
The **Static Routing** module allows you to add, delete and edit static routes.

Figure 3-3-81 Static Route List



Click **Add** to add a static route. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-82 Add Static Route



3.3.6.2 Flow Control

3.3.6.2.1 Smart Flow Control

The **Smart Flow Control** module allows you to configure smart flow control.

Figure 3-3-83 Smart Flow Control

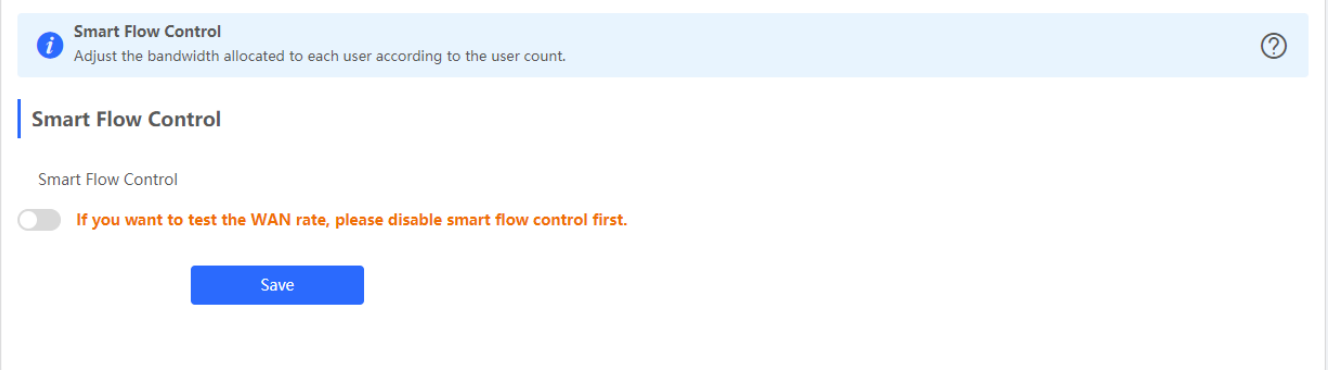
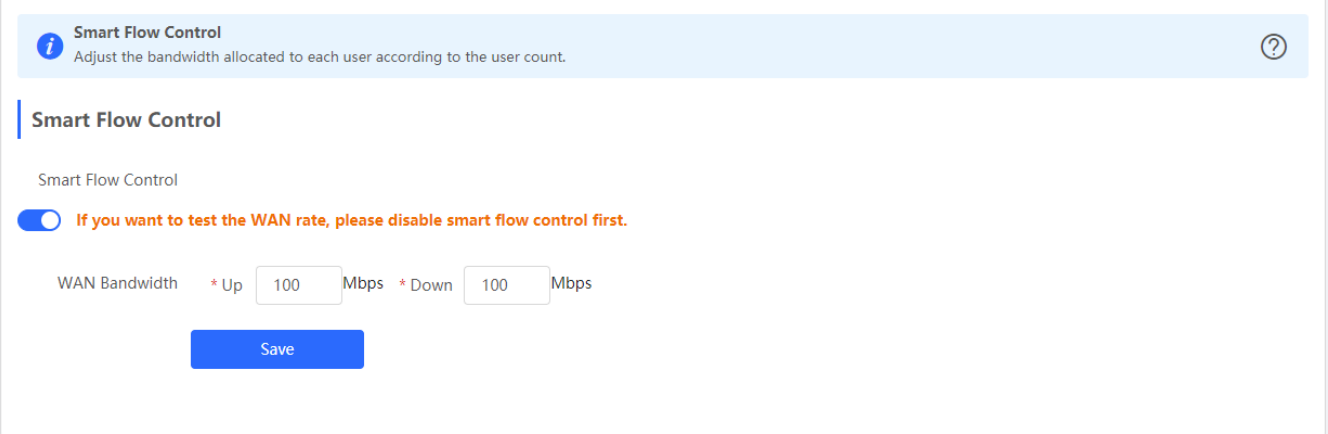


Figure 3-3-84 Enable Smart Flow Control

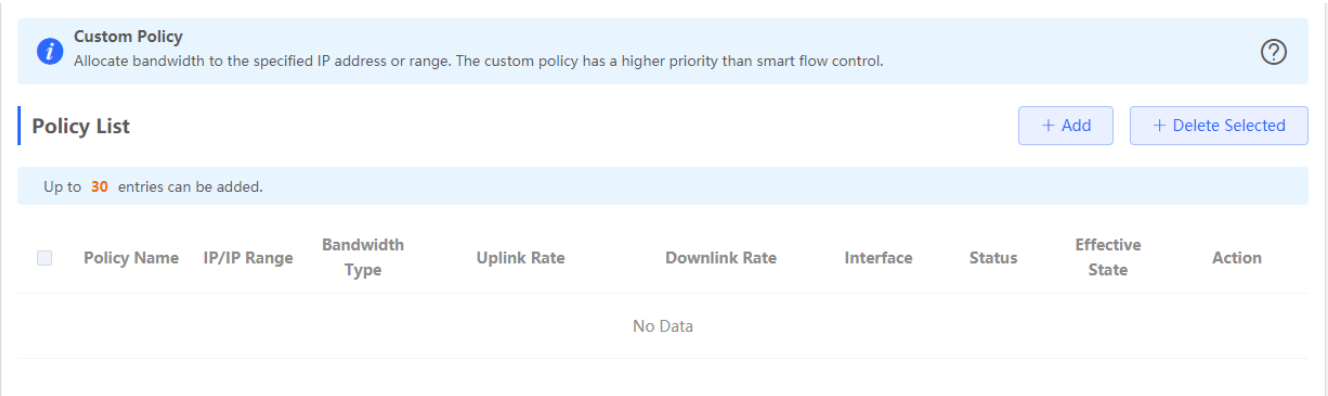


If there is more than one WAN port, **WAN Bandwidth** settings of each port will be displayed accordingly.

3.3.6.2.2 Custom Policy

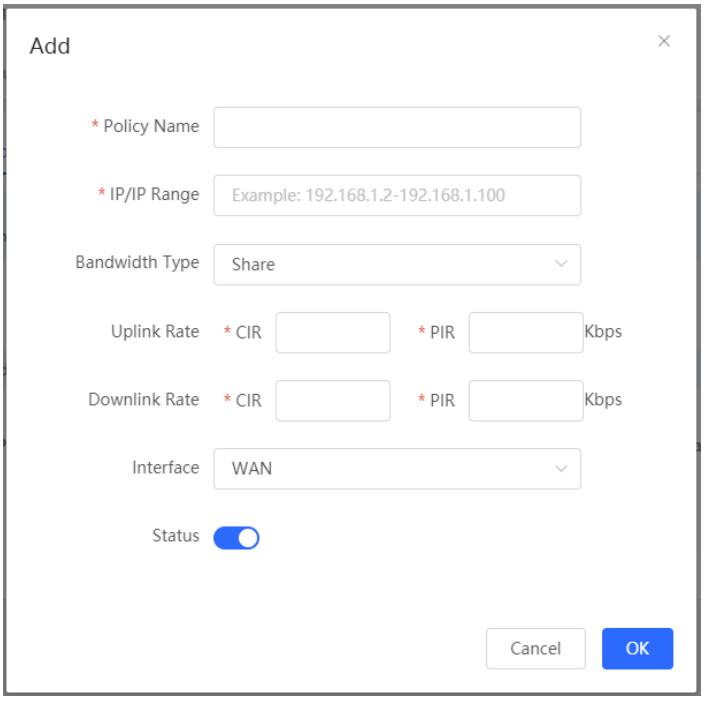
The **Custom Policy** module allows you to add, delete and edit custom flow control policies.

Figure 3-3-85 Custom Flow Control Policy



Click **Add** to add a custom flow control policy. In the displayed dialog box, configure settings and click **OK**.

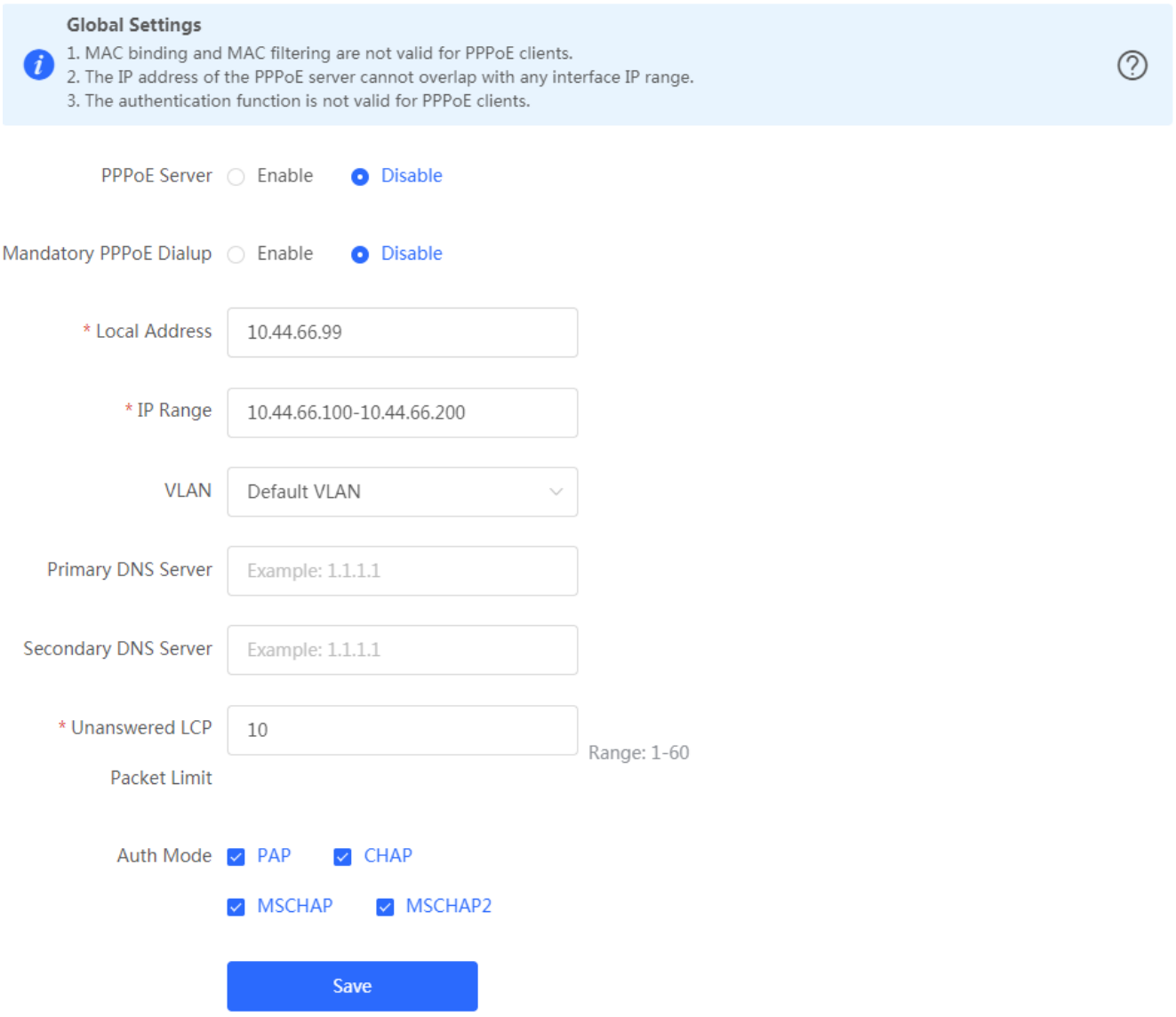
Figure 3-3-86 Add Flow Control Policy



3.3.6.3 PPPoE Server

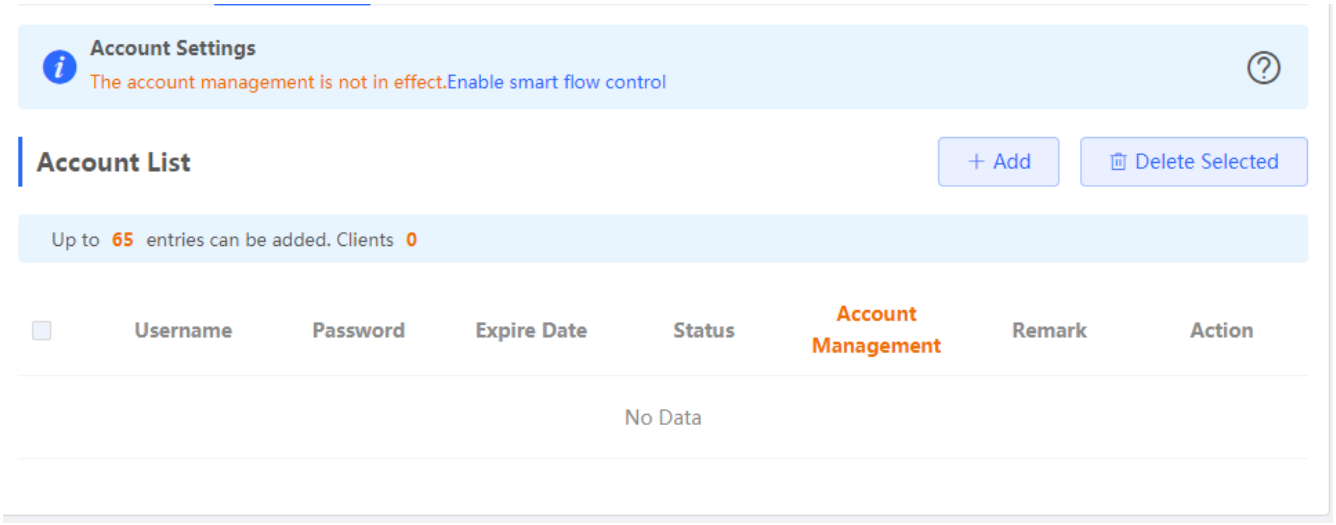
3.3.6.3.1 Global Settings

Figure 3-3-87 Global Settings



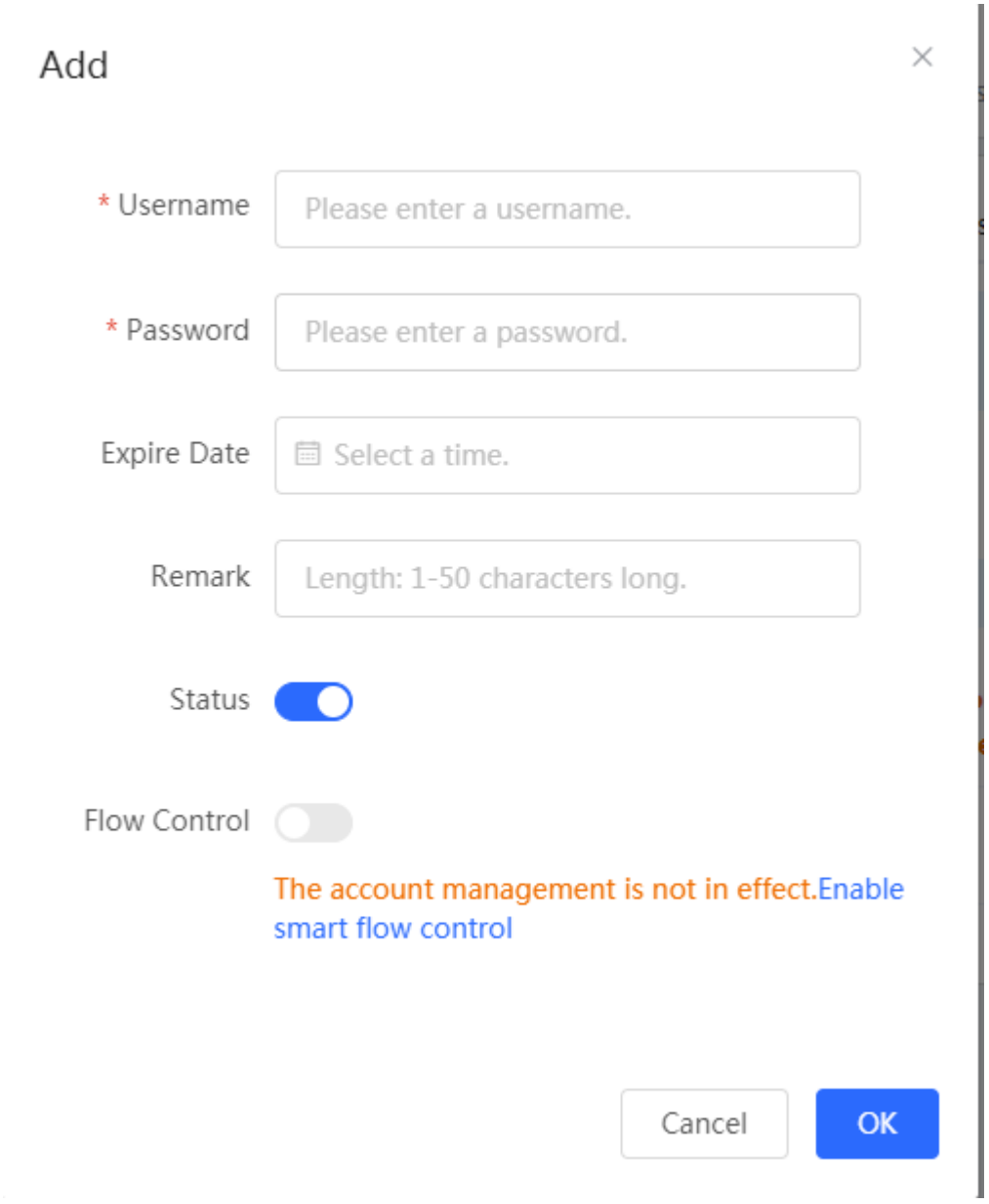
3.3.6.3.2 Account Settings

Figure 3-3-88 Account Settings



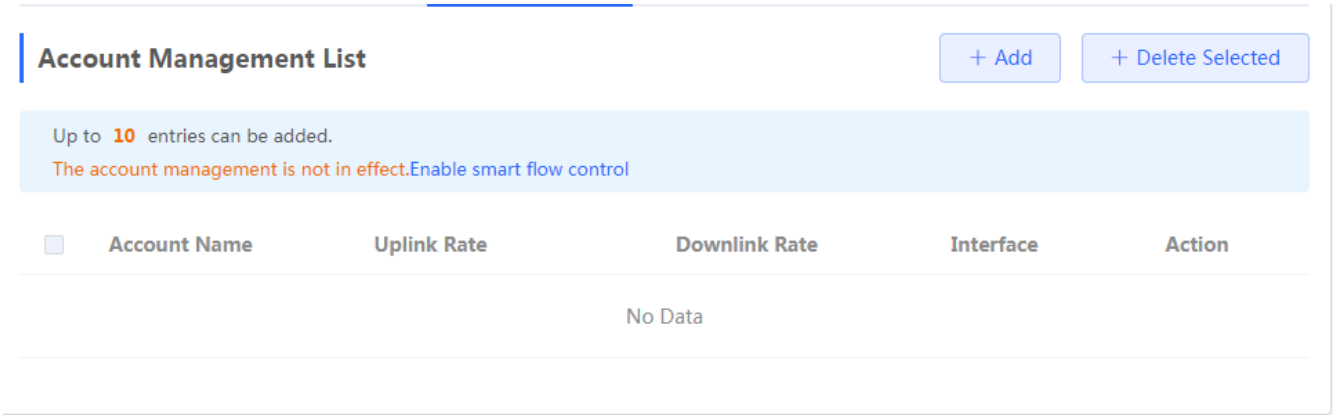
Click **Add** to add a account. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-89 Add Account Settings



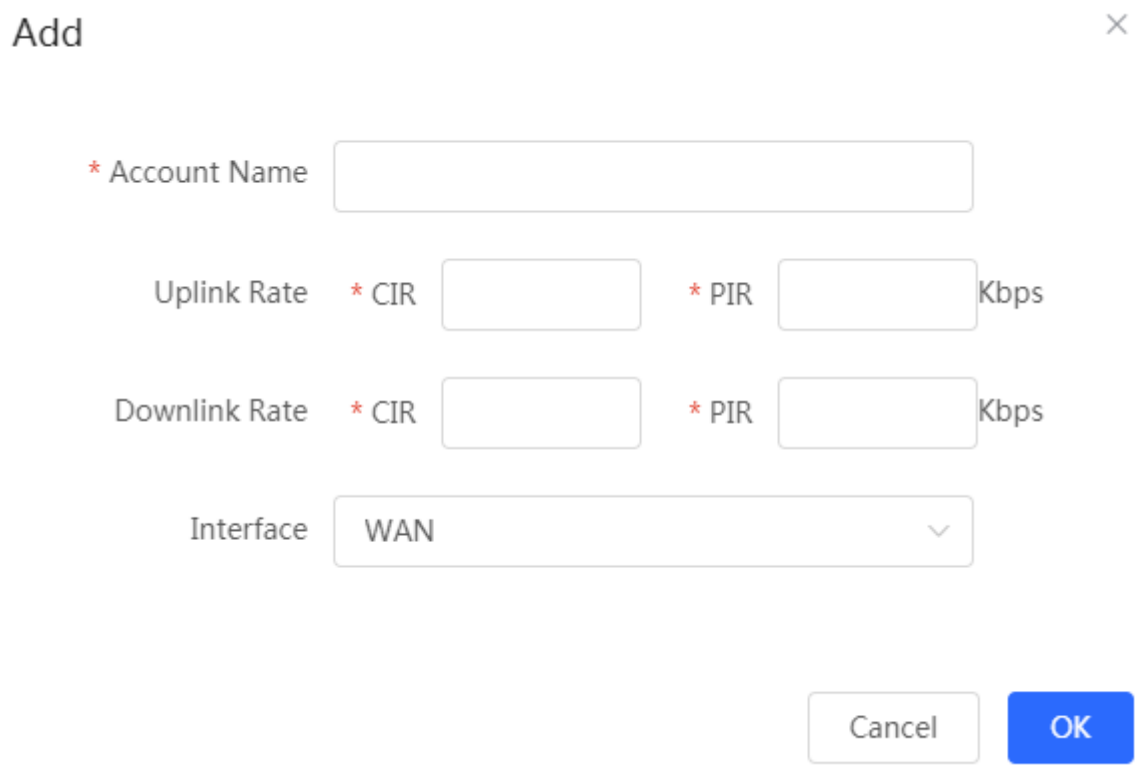
3.3.6.3.3 Account Management

Figure 3-3-90 Account Management



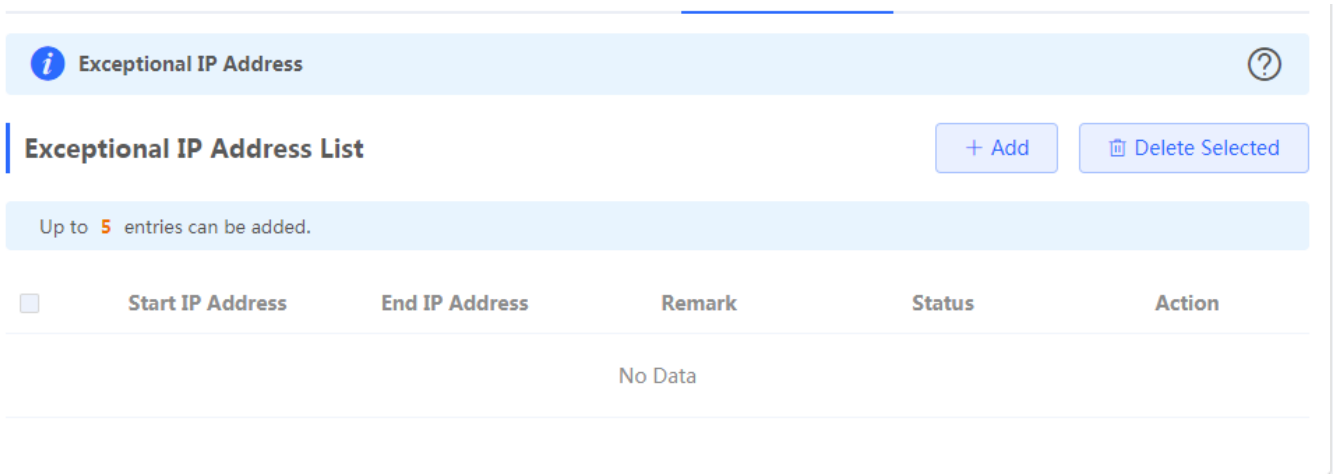
Click **Add** to add an IP address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-91 Add Account



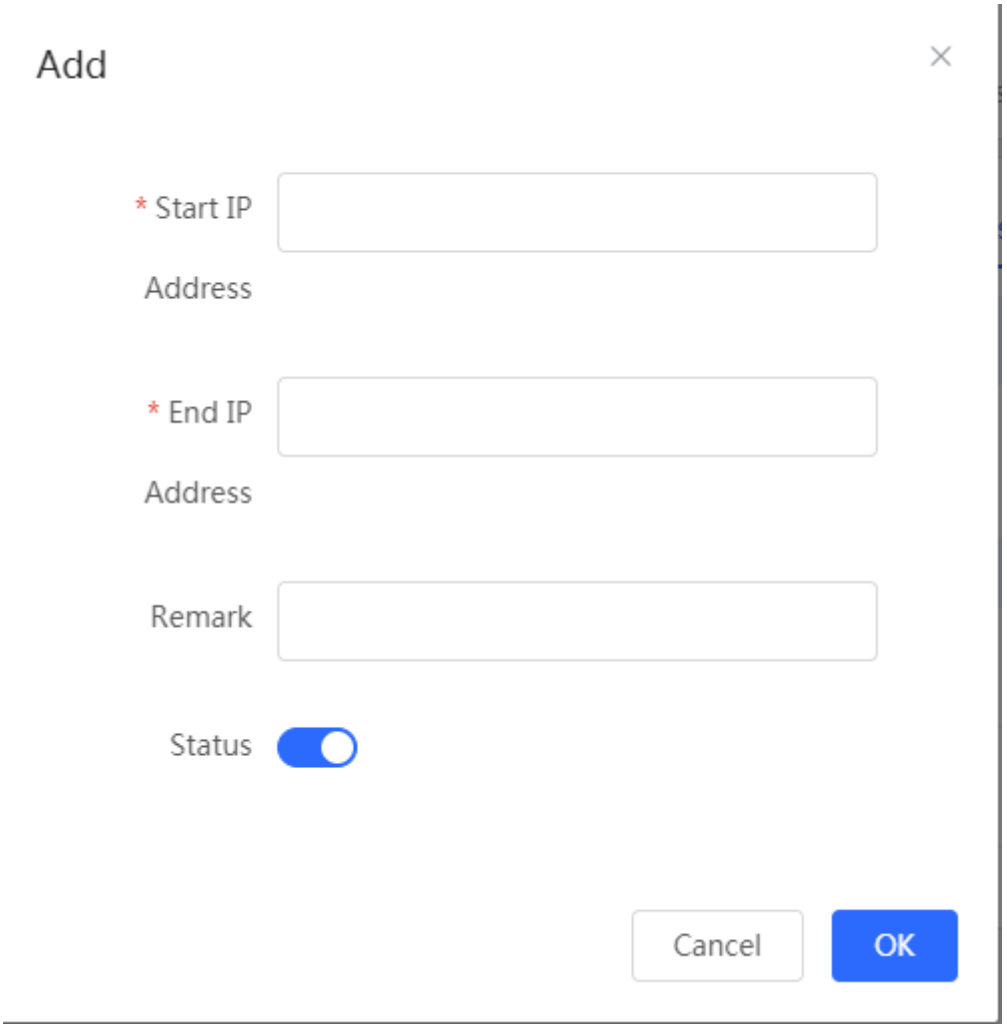
3.3.6.3.4 Exceptional IP Address

Figure 3-3-92 Exceptional IP Address



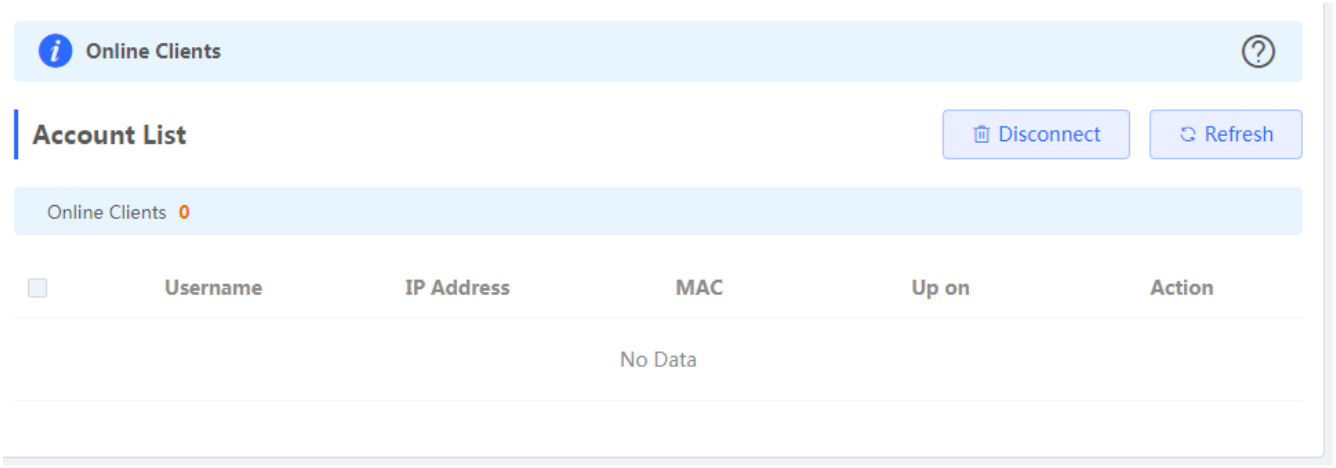
Click **Add** to add a IP In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-93 Add Exceptional IP Address



3.3.6.3.5 Online Clients

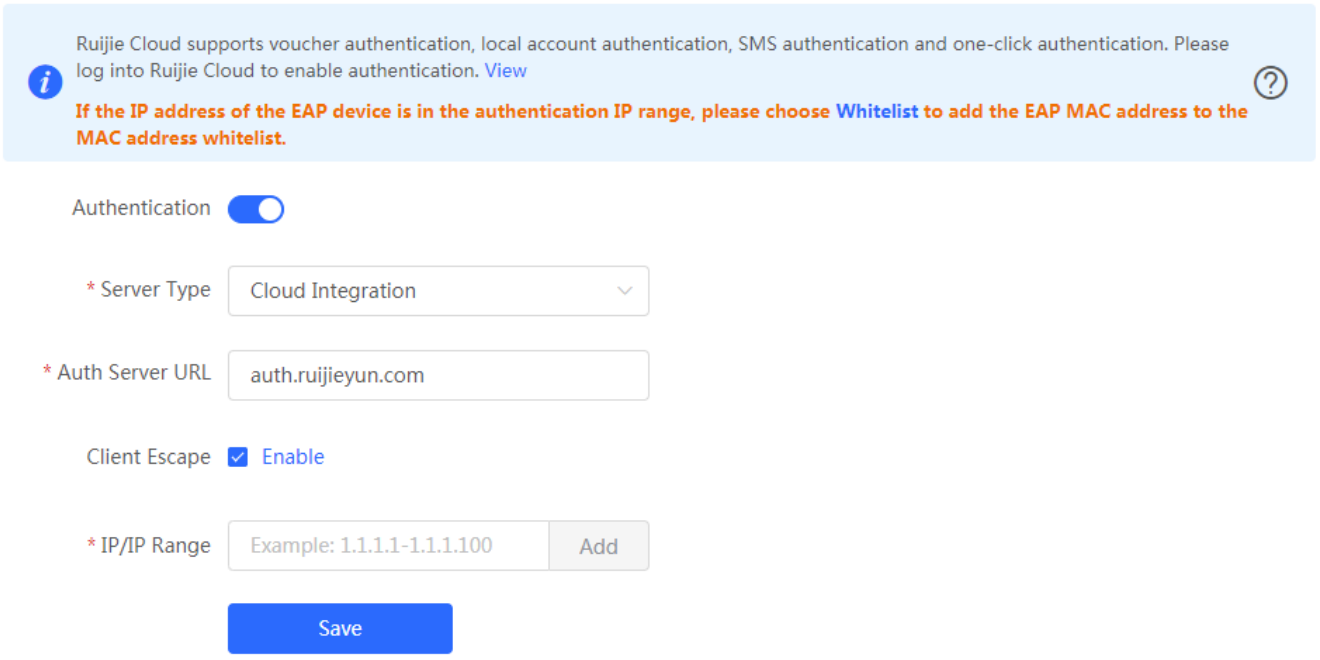
Figure 3-3-94 Online Clients



3.3.6.4 Authentication

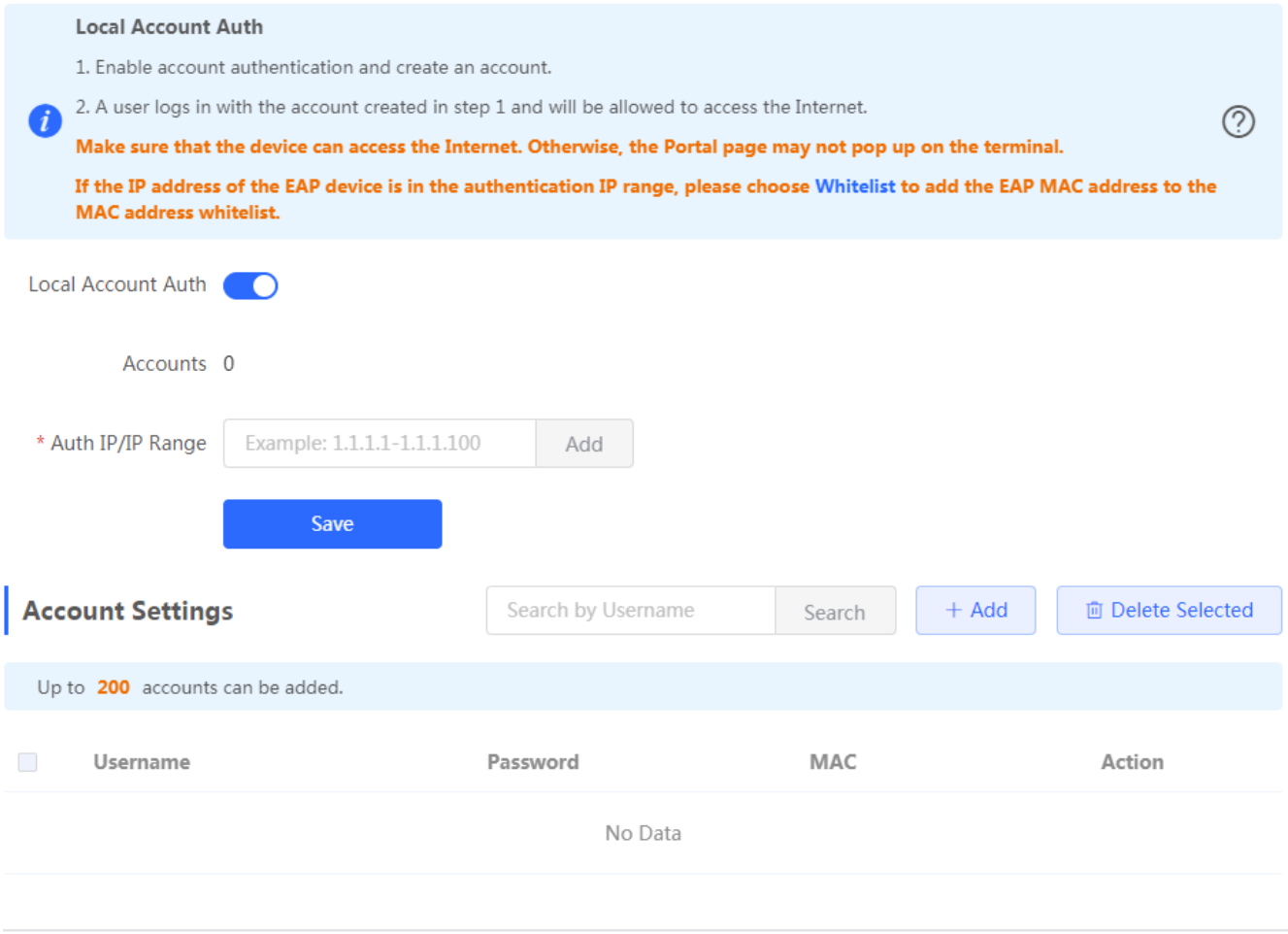
3.3.6.4.1 Cloud Auth

Figure 3-3-95 Cloud Auth



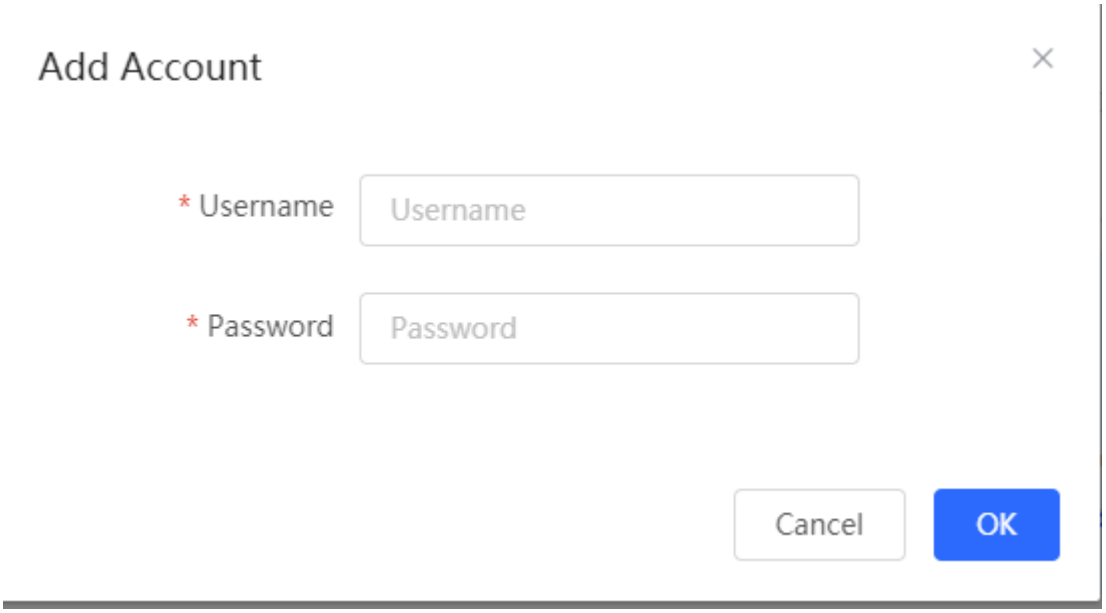
3.3.6.4.2 Local Account Auth

Figure 3-3-96 Cloud Auth



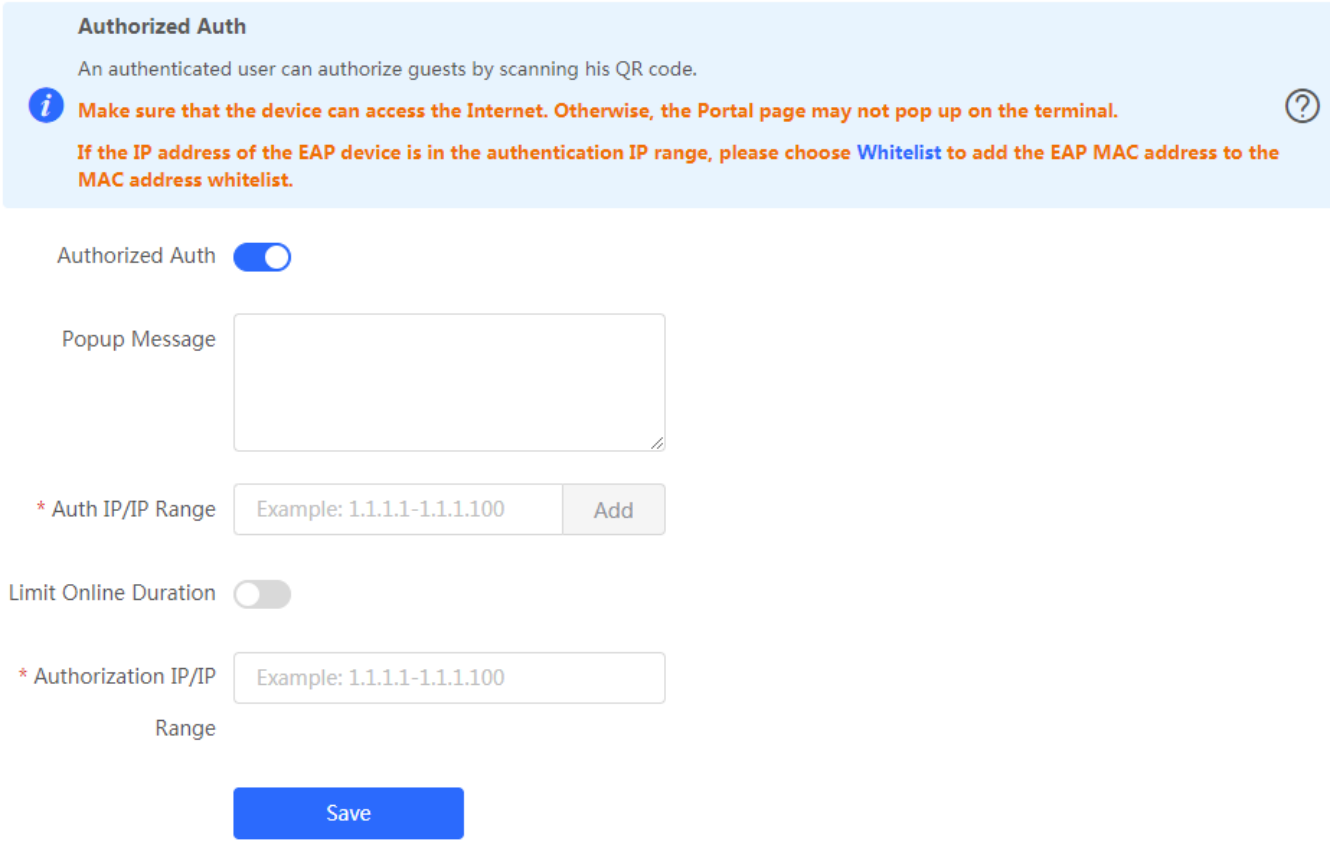
Click **Add** to add an account. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-97 Add Account



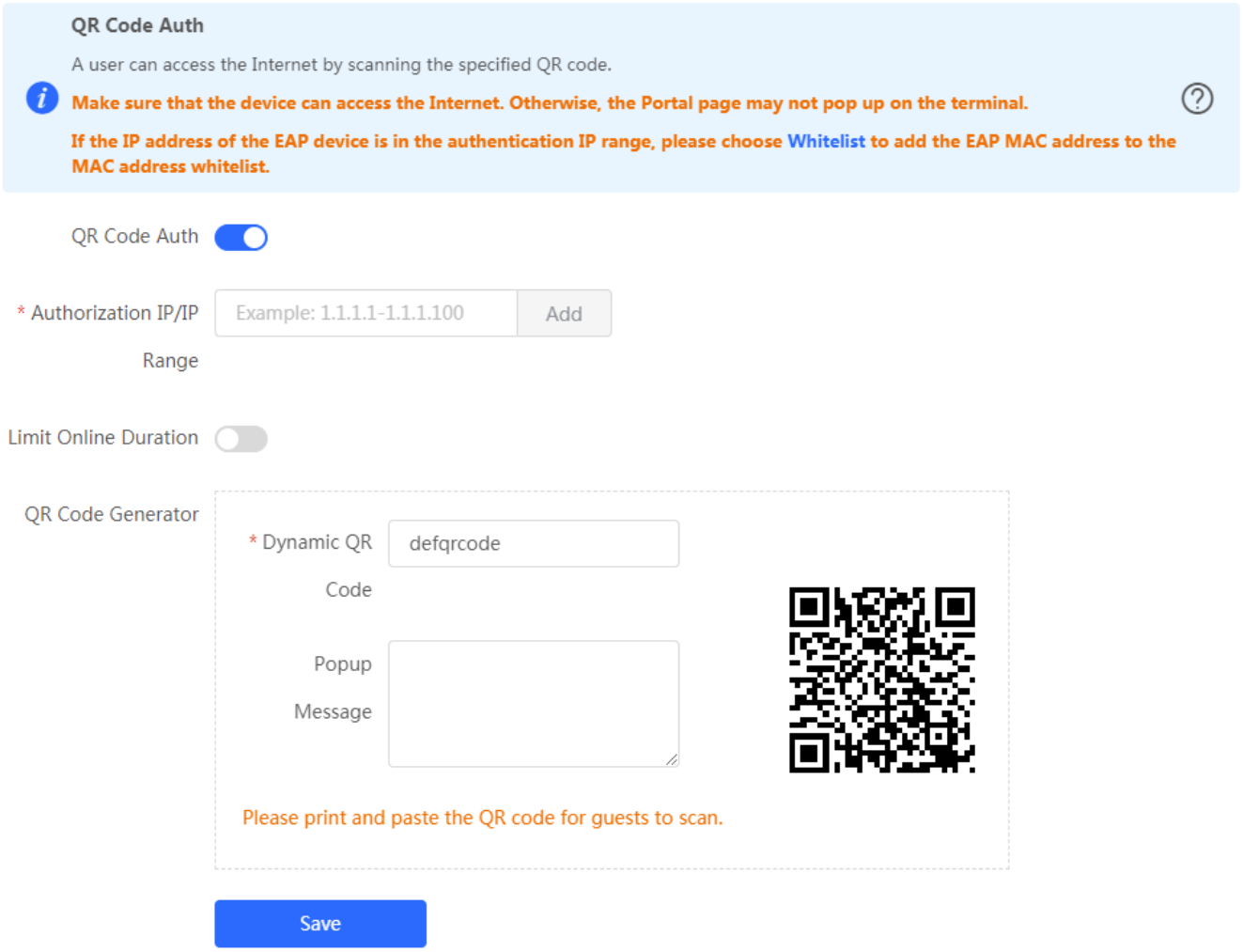
3.3.6.4.3 Authorized Auth

Figure 3-3-98 Authorized Auth



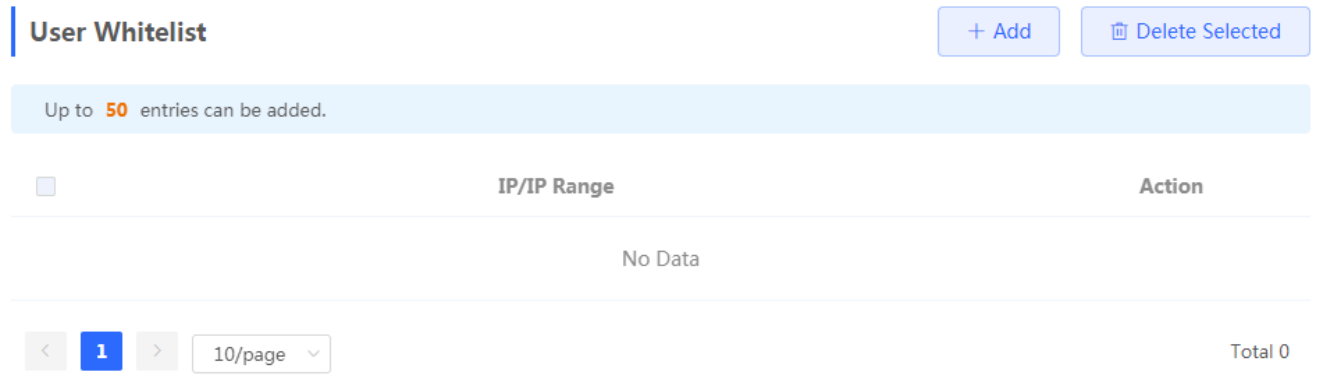
3.3.6.4.4 QR Code Auth

Figure 3-3-99 QR Code Auth



3.3.6.4.5 Whitelist

Figure 3-3-100 User Whitelist



Click **Add** to add a User In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-101 Add User

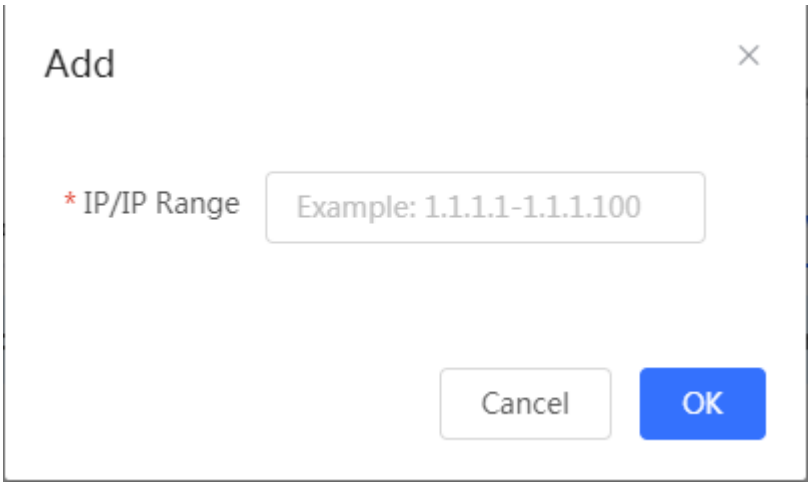
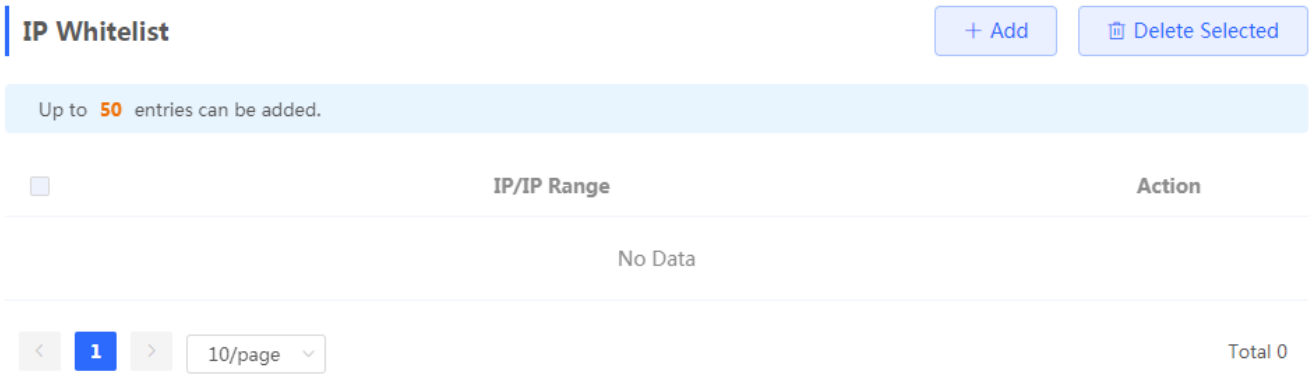


Figure 3-3-102 IP Whitelist



Click **Add** to add an IP address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-103 Add IP

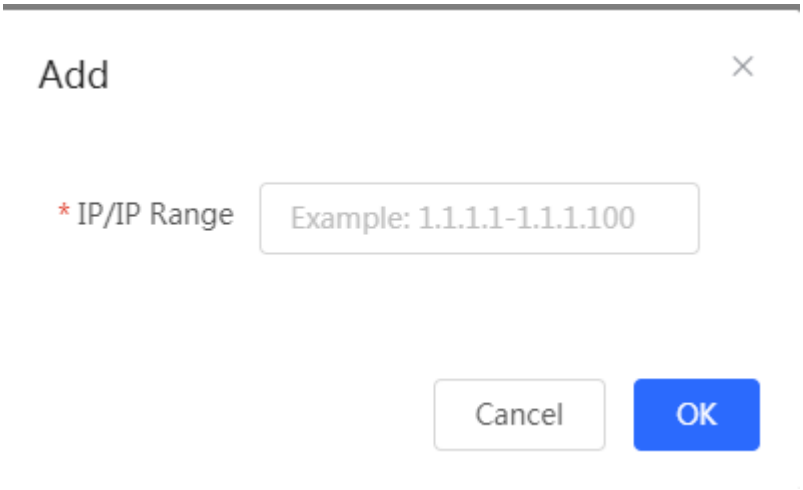
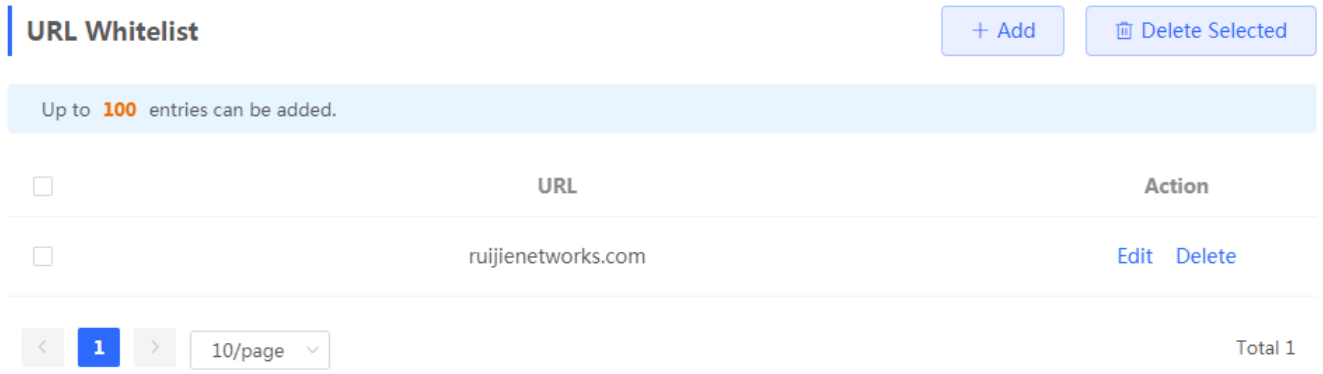


Figure 3-3-104 URL Whitelist



Click **Add** to add a URL. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-105 Add URL

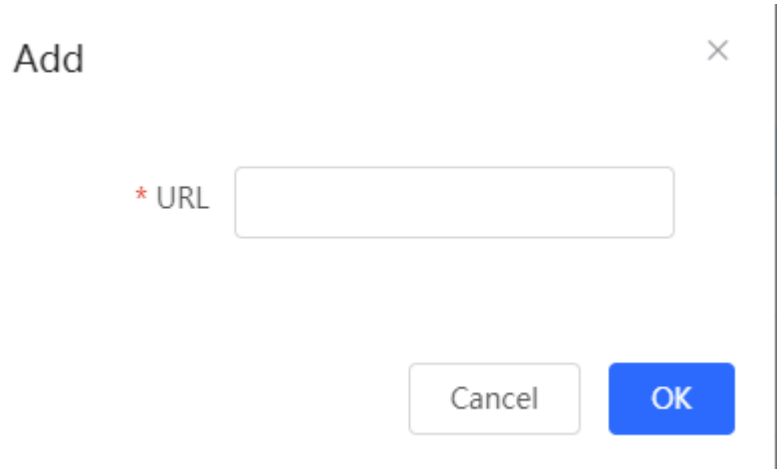
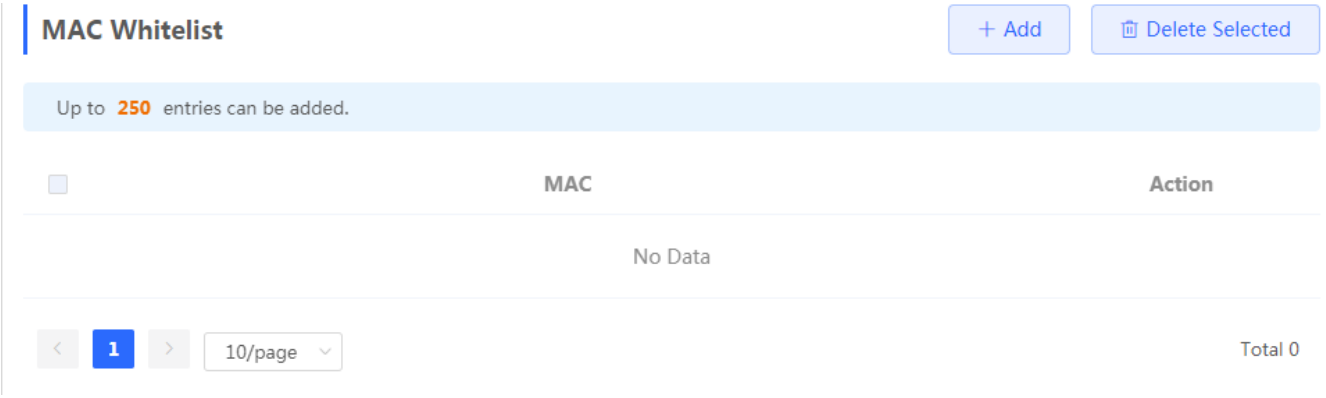


Figure 3-3-106 MAC Whitelist



Click **Add** to add a MAC address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-107 Add MAC

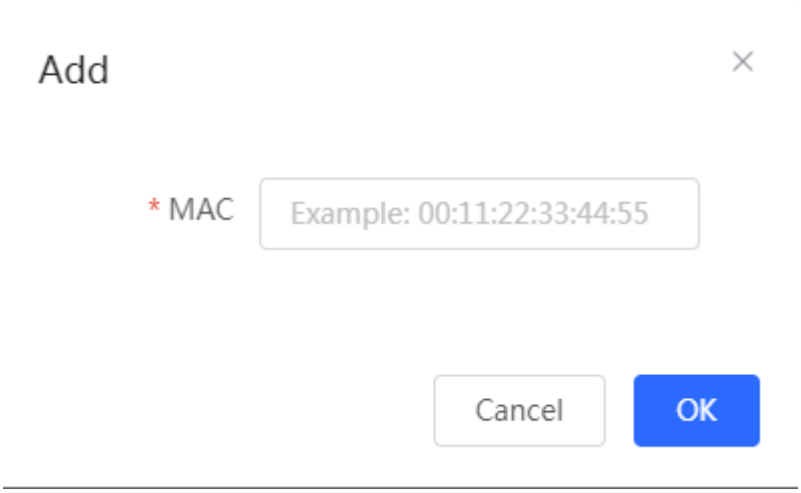
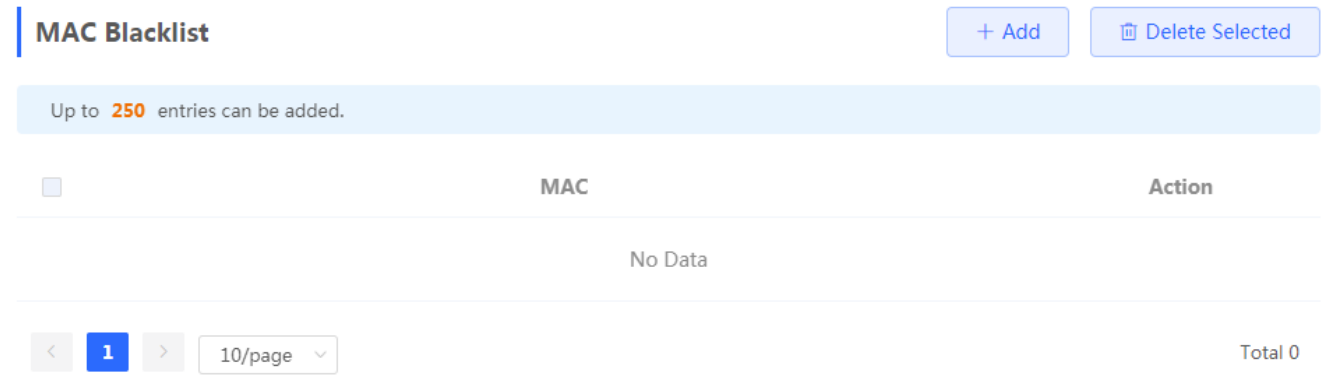
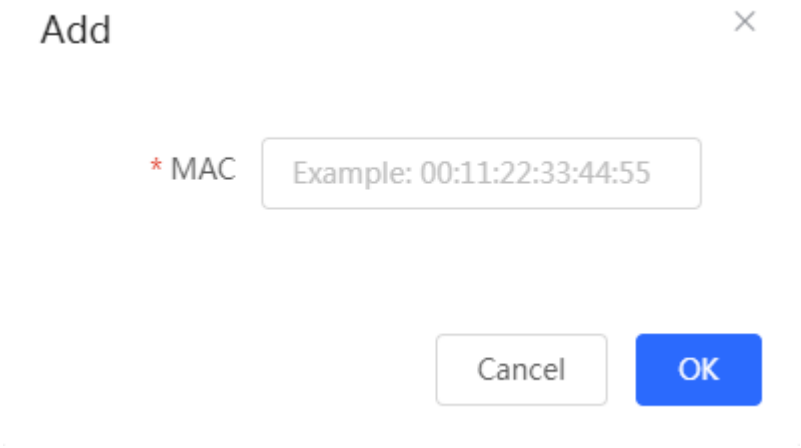


Figure 3-3-108 MAC Blacklist



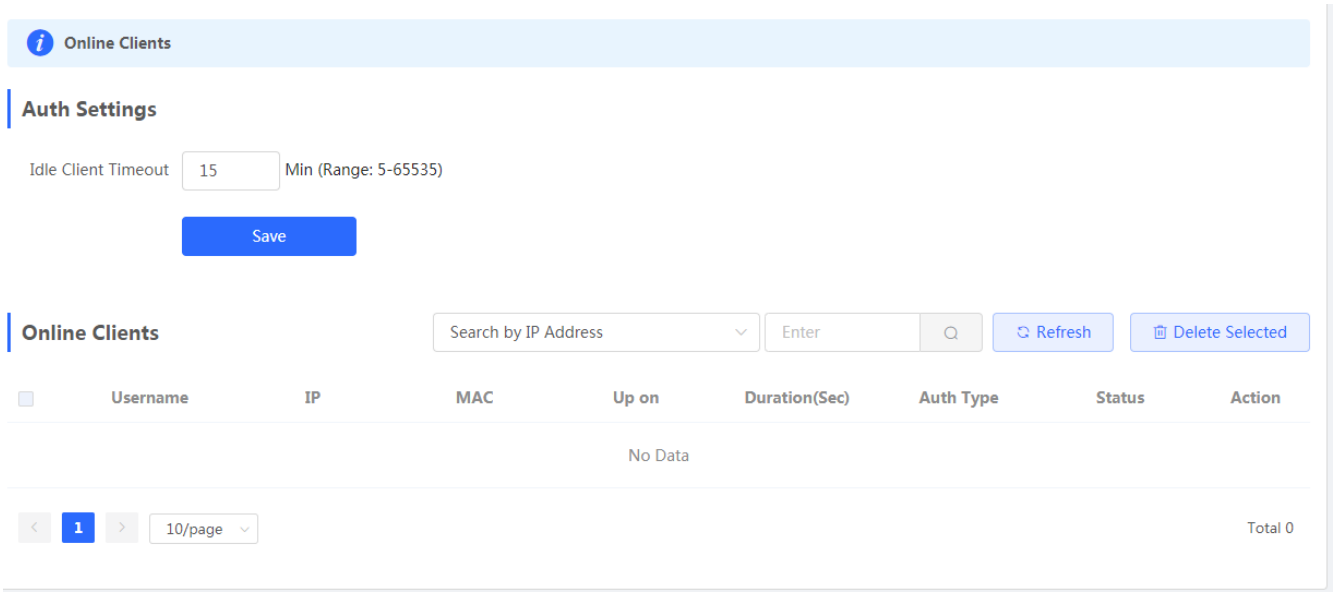
Click **Add** to add a MAC address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-109 Add MAC



3.3.6.4.6 Online Users

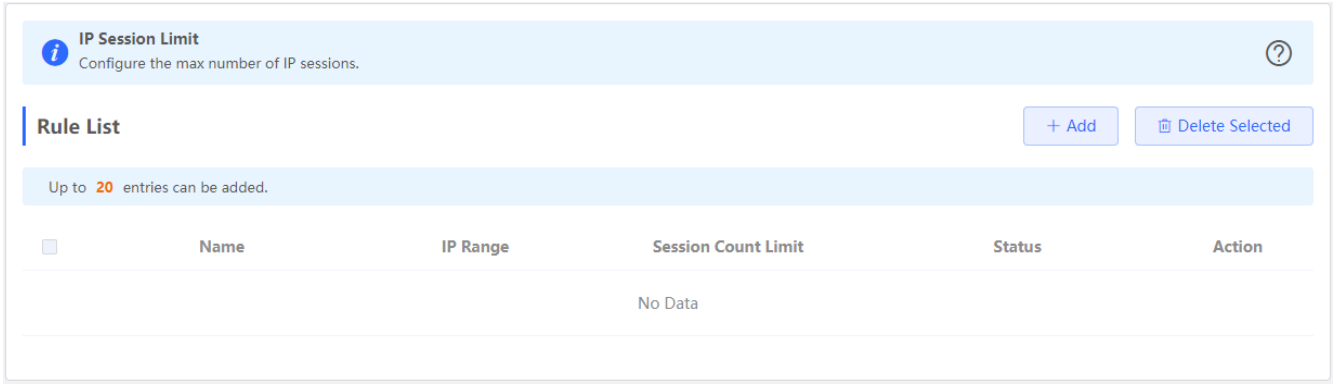
Figure 3-3-110 Online Users



3.3.6.5 Session Limit

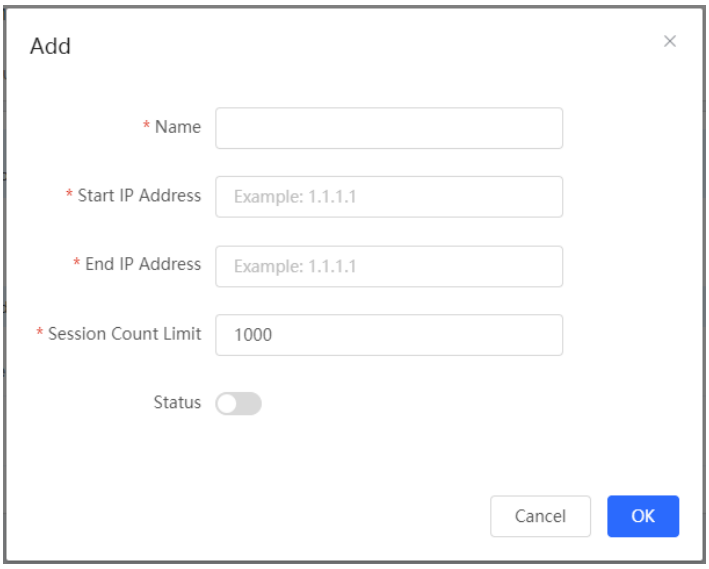
The **Session Limit** module allows you to add, delete and edit session limit polices.

Figure 3-3-111 IP Session Limit



Click **Add** to add a session limit policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-112 Add Session Limit Policy

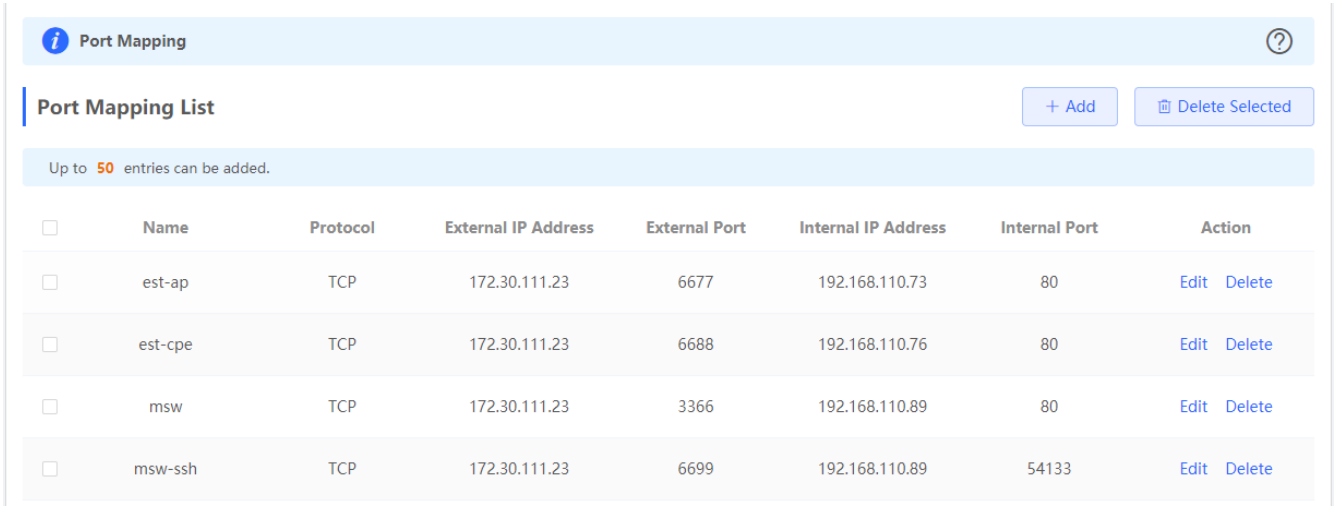


3.3.6.6 Port Mapping

3.3.6.6.1 Port Mapping

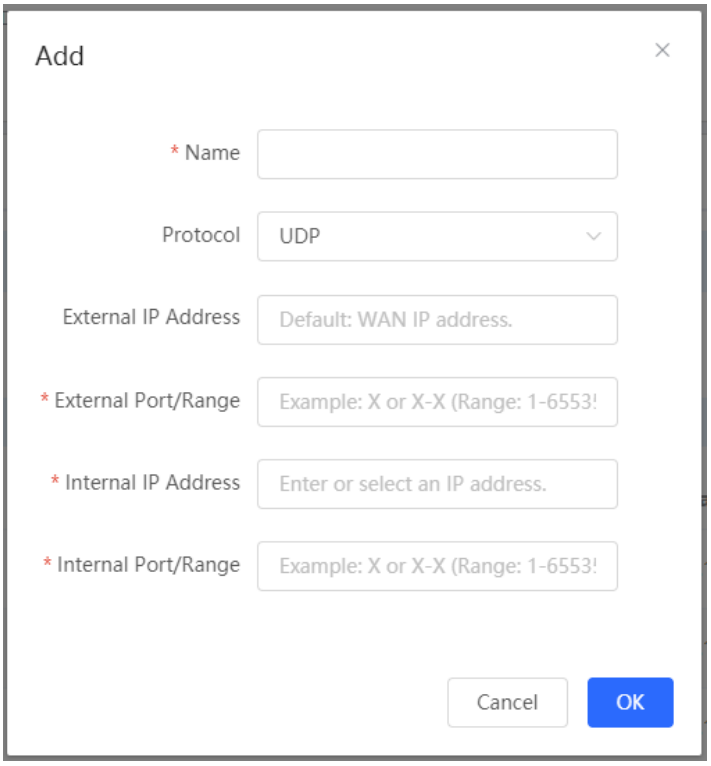
The **Port Mapping** module allows you to add, delete and edit port mapping policies.

Figure 3-3-113 Port Mapping List



Click **Add** to add a port mapping policy. In the displayed dialog box, configure settings and click **OK**.

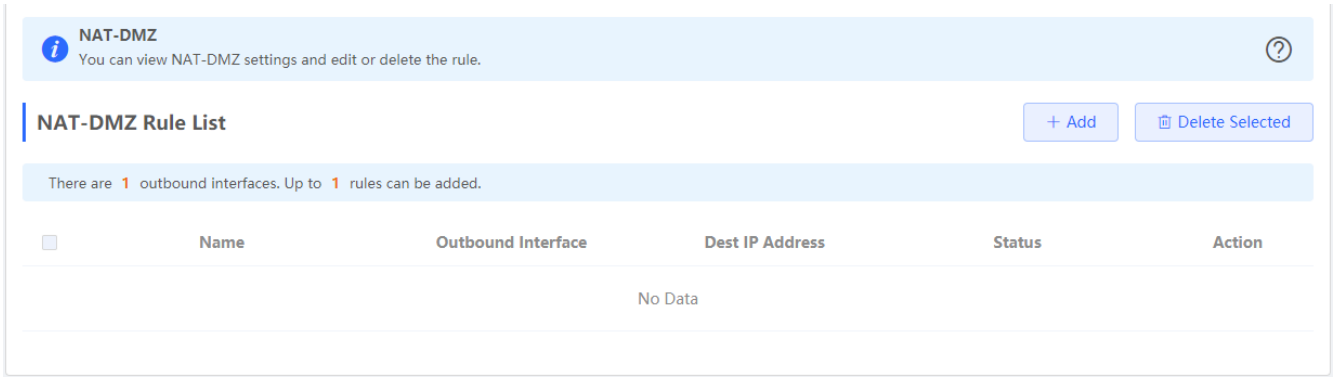
Figure 3-3-114 Add Port Mapping Policy



3.3.6.6.2 NAT-DMZ

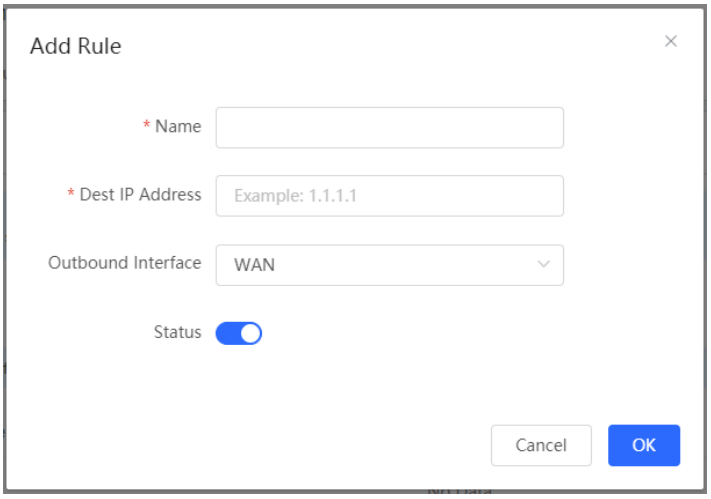
The **NAT-DMZ** module allows you to add, delete and edit NAT-DMZ rules.

Figure 3-3-115 NAT-DMZ Rule List



Click **Add** to add a NAT-DMZ rule. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-116 Add NAT-DMZ Rule

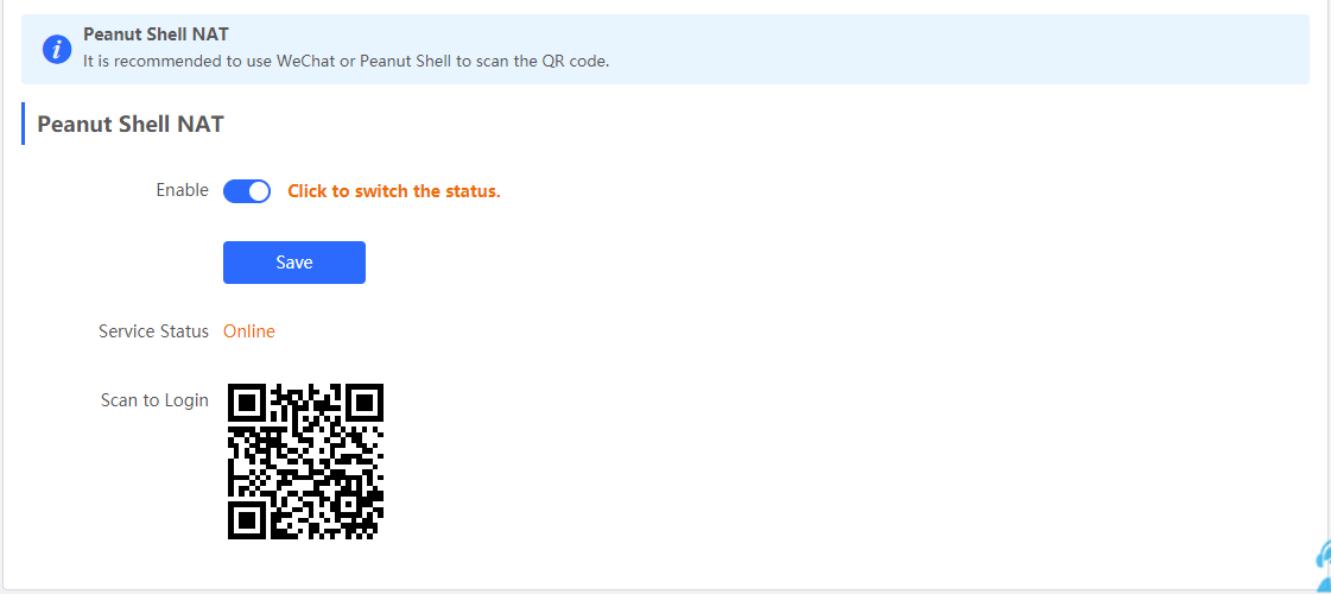


3.3.6.7 Dynamic DNS

3.3.6.7.1 Peanut Shell NAT

It is recommended to use WeChat or Peanut Shell to scan the QR code.

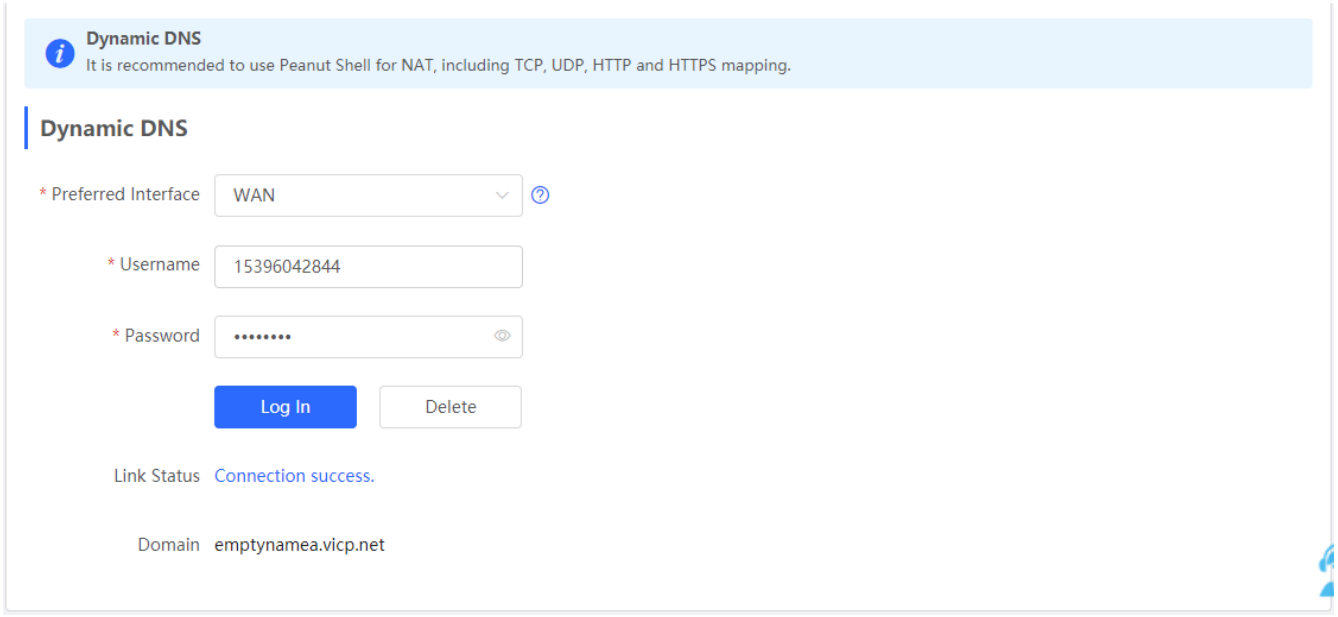
Figure 3-3-117 Peanut Shell NAT



3.3.6.7.2 Dynamic DNS

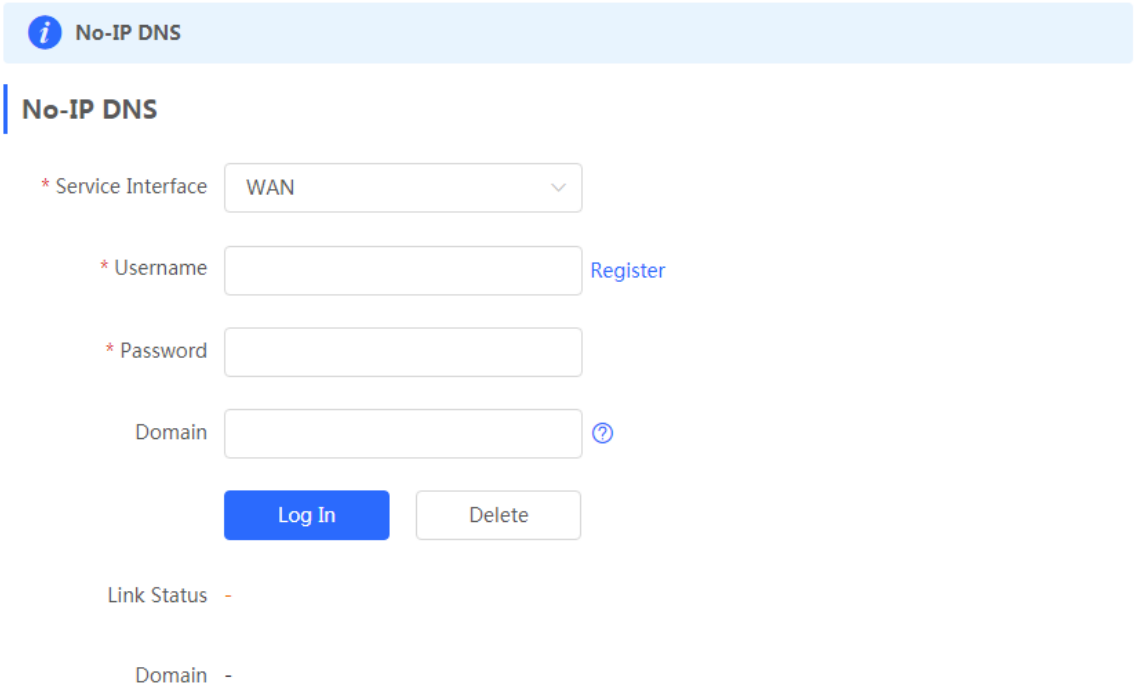
It is recommended to use Peanut Shell for NAT, including TCP, UDP, HTTP and HTTPS mapping.

Figure 3-3-118 Dynamic DNS



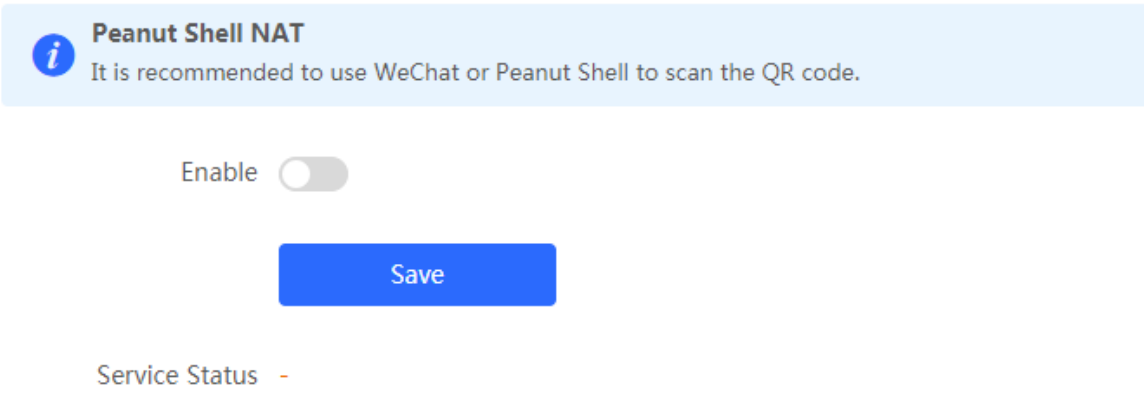
3.3.6.7.3 No-IP DNS

Figure 3-3-119 No-IP DNS



3.3.6.7.4 DynDNS

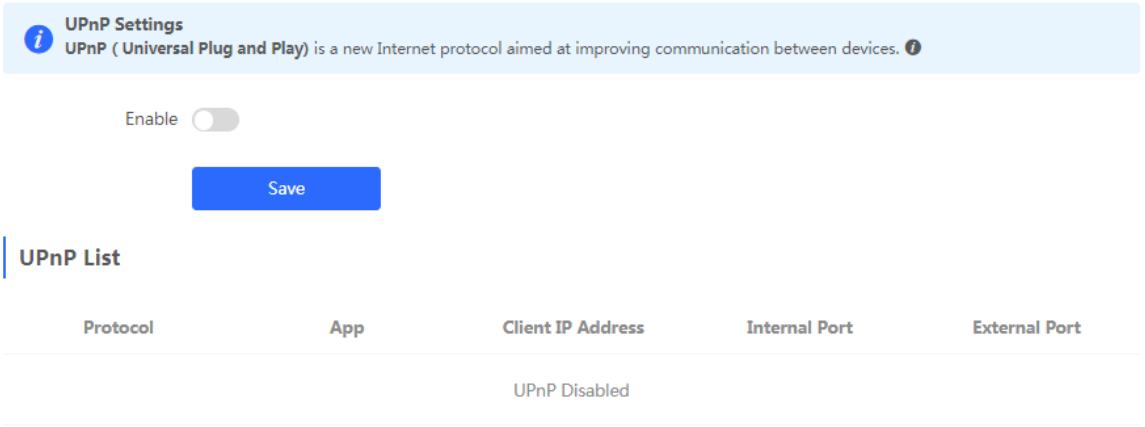
Figure 3-3-120 Local DNS



3.3.6.8 UPnP Settings

UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving communication between devices.

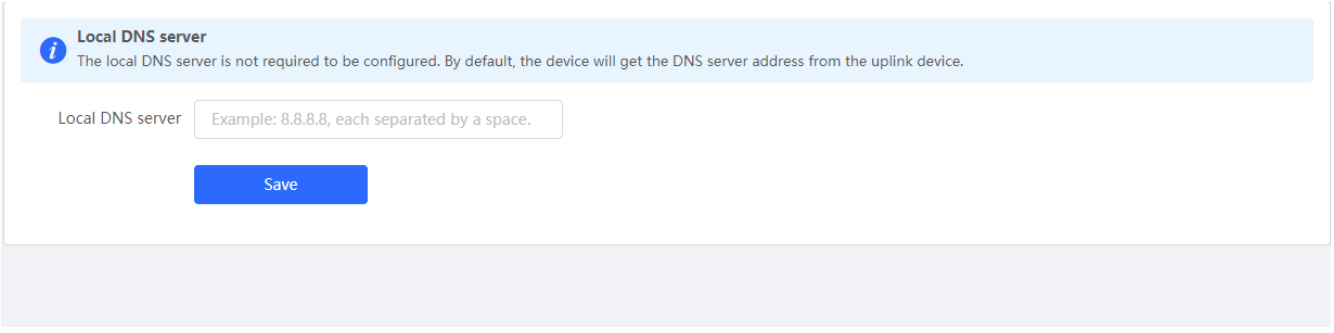
Figure 3-3-121 UPnP Settings



3.3.6.9 Local DNS

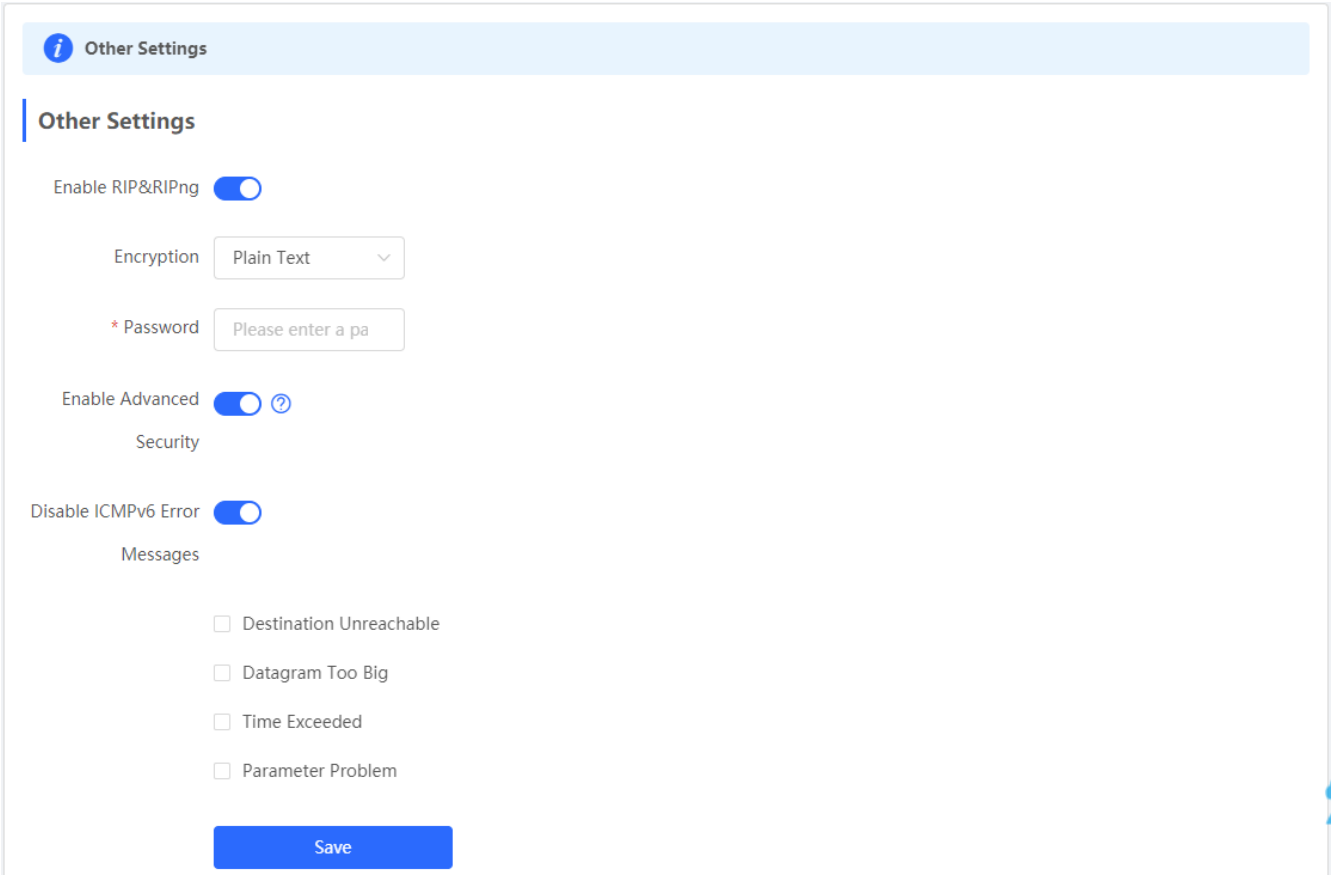
The **Local DNS** module allows you to configure a local DNS server.

Figure 3-3-122 Local DNS



3.3.6.10 Other Settings

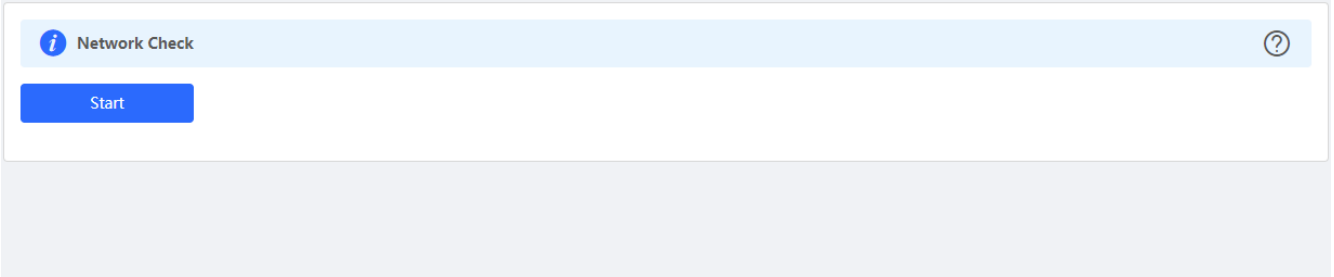
Figure 3-3-123 Other Settings



3.3.7 Diagnostics

3.3.7.1 Network Check

Figure 3-3-124 Network Check

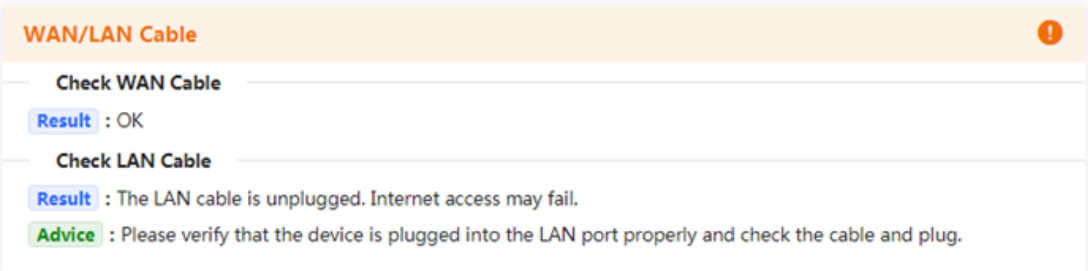


Click **Start**, and click **OK** in the confirmation box. After the test finishes, the result will be displayed.

Figure 3-3-125 Result

If any problem occurs, the result will be displayed as follows:

Figure 3-3-126 Issue & Advice

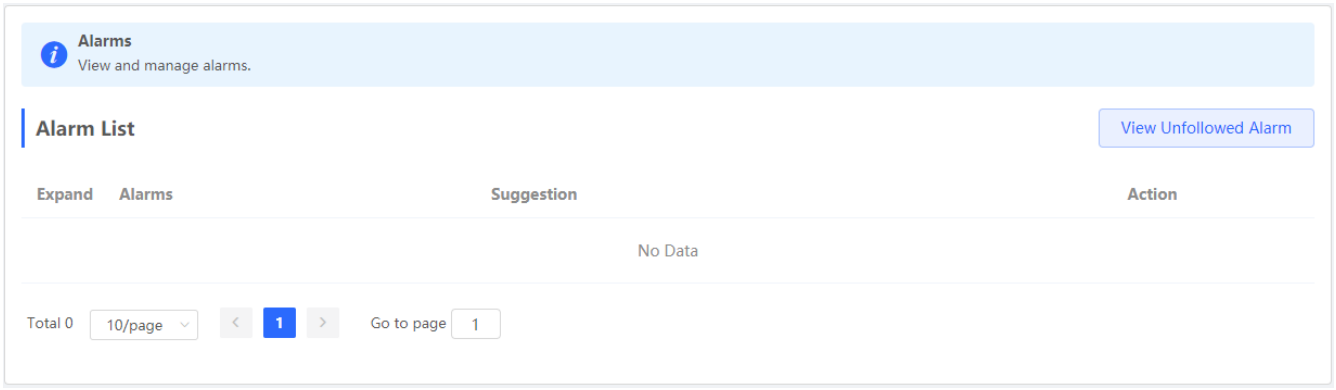


Please fix the problem by taking the suggested action.

3.3.7.2 Alarms

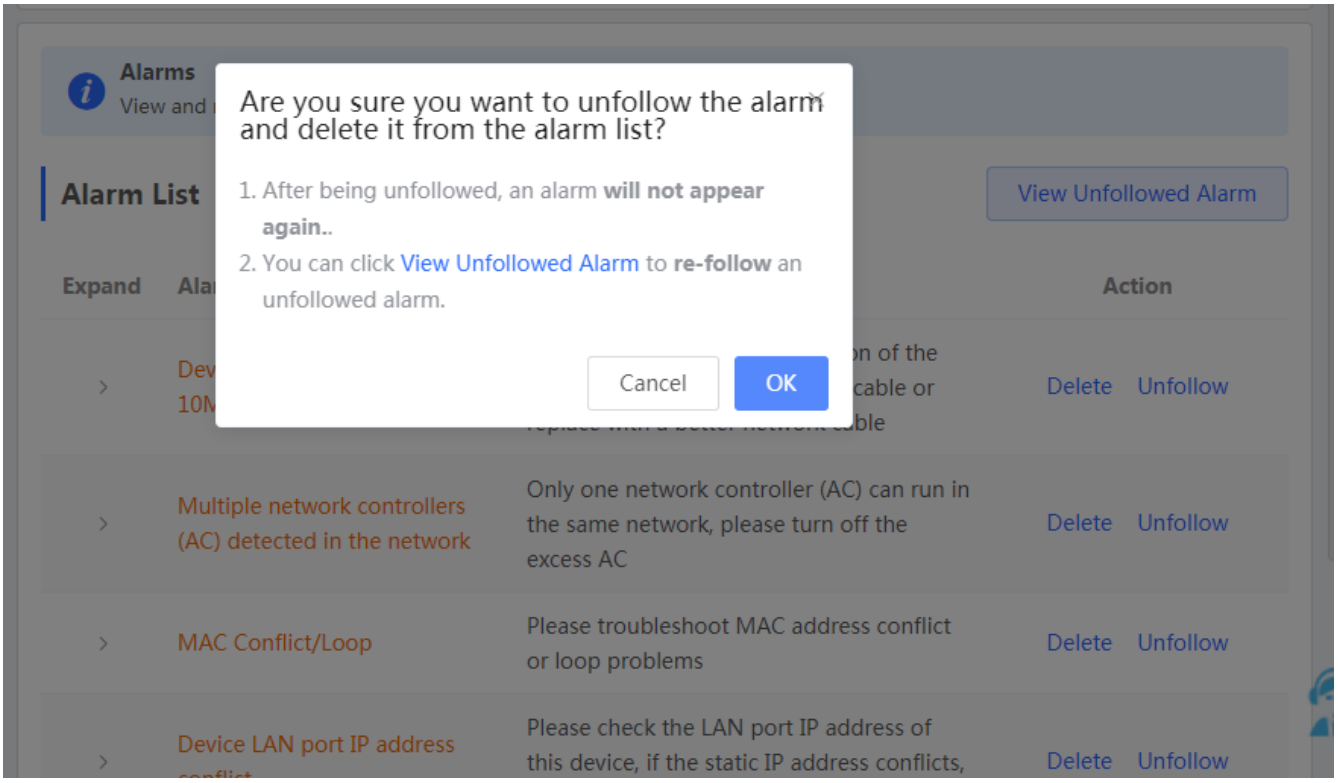
The **Alarms** module allows you to view and manage alarms in the network.

Figure 3-3-127 Alarms



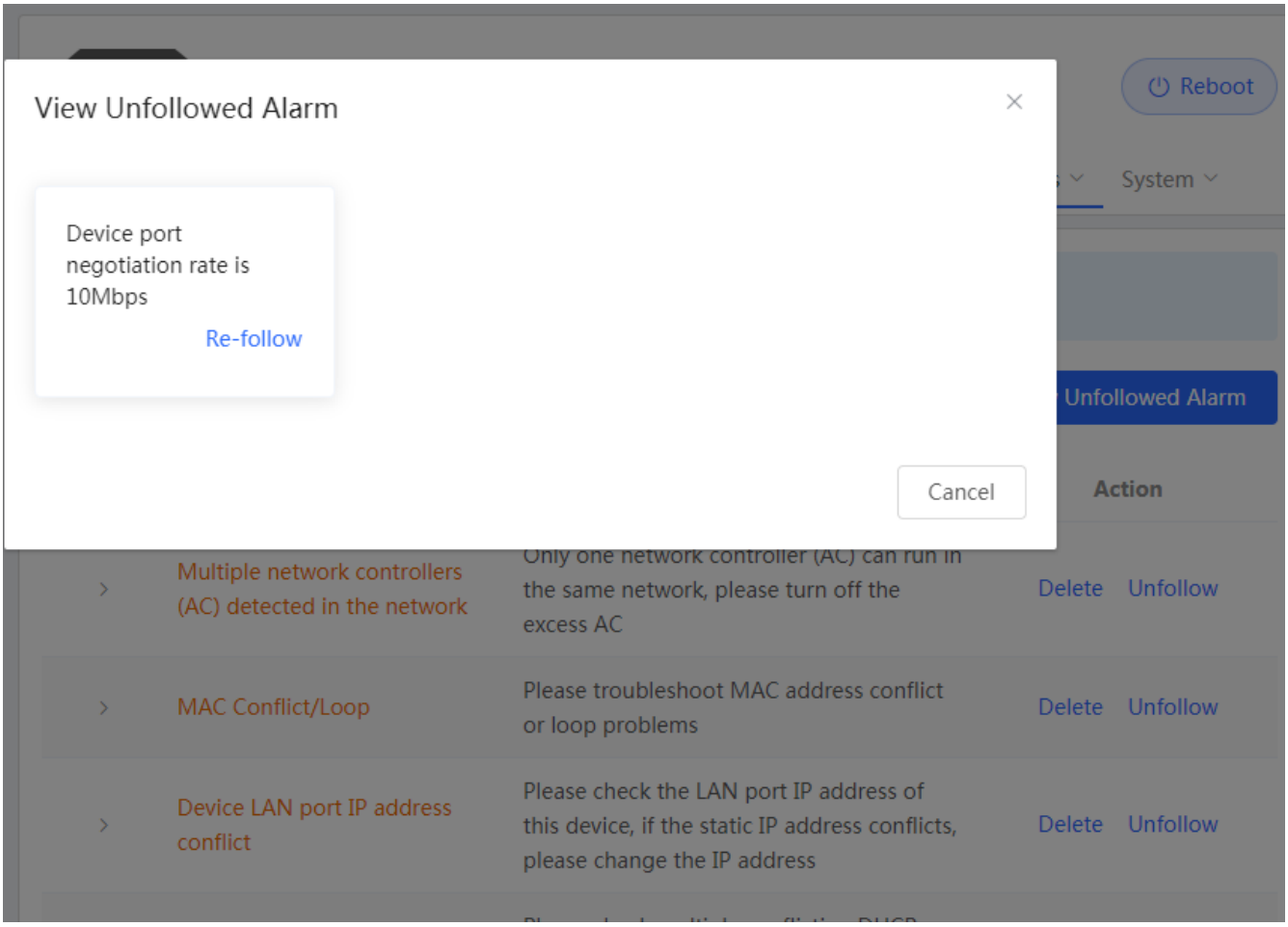
Click **Unfollow** in the **Action** column to unfollow an alarm. In the confirmation box, click **OK**.

Figure 3-3-128 Unfollow Alarm



Click **View Unfollowed Alarm**, and you can view and follow the alarm again.

Figure 3-3-129 Re-follow Alarm



3.3.7.3 Network Tools

The **Network Tools** module provides the following network tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

Figure 3-3-130 Ping Test and Result

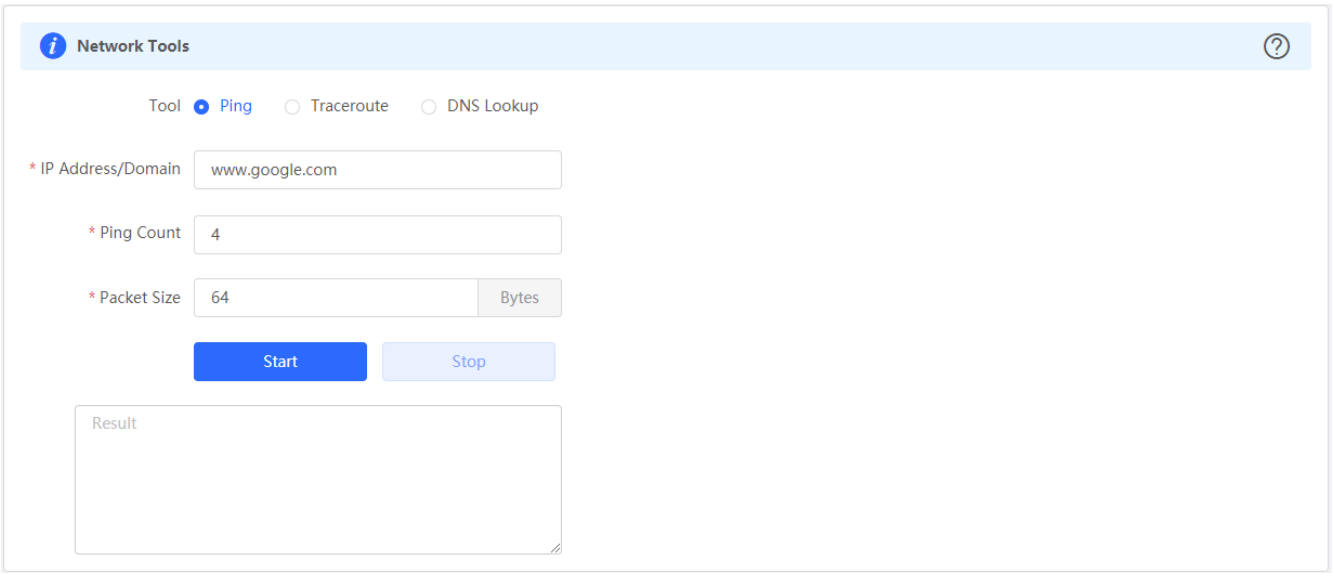


Figure 3-3-131 Traceroute Test and Result

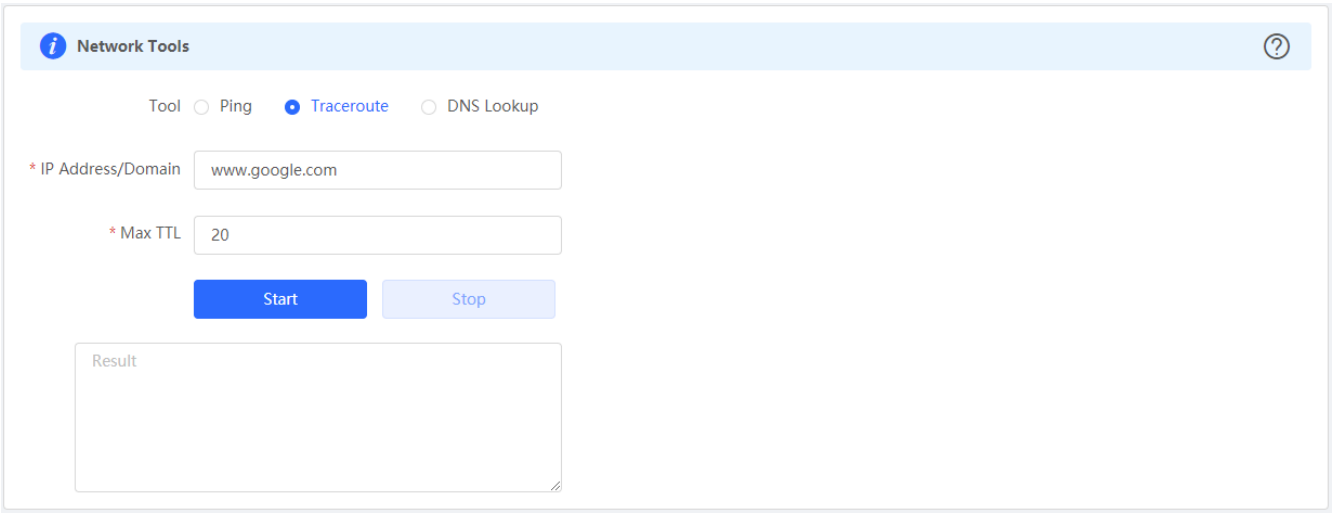
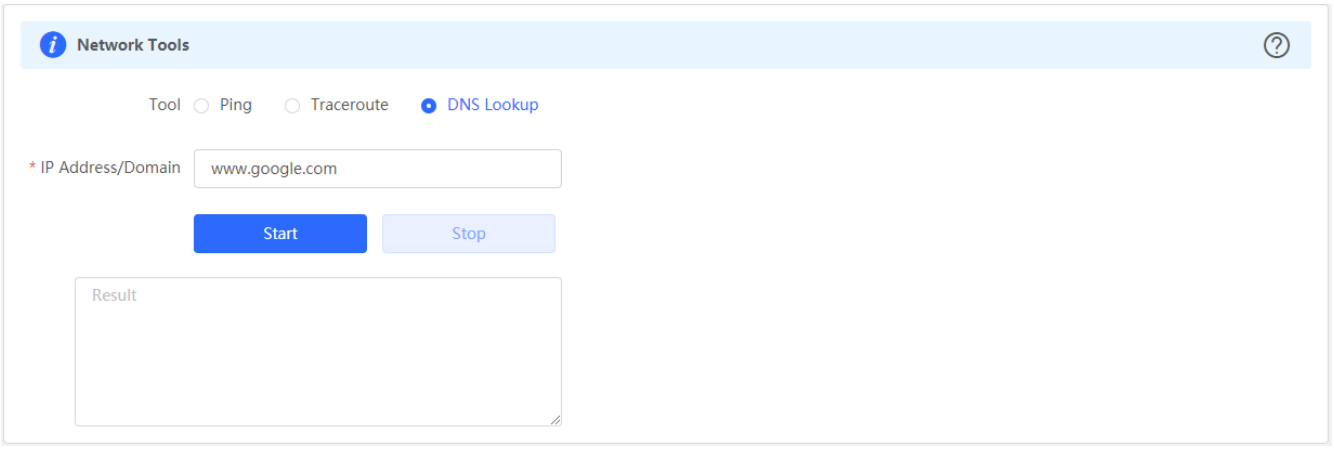


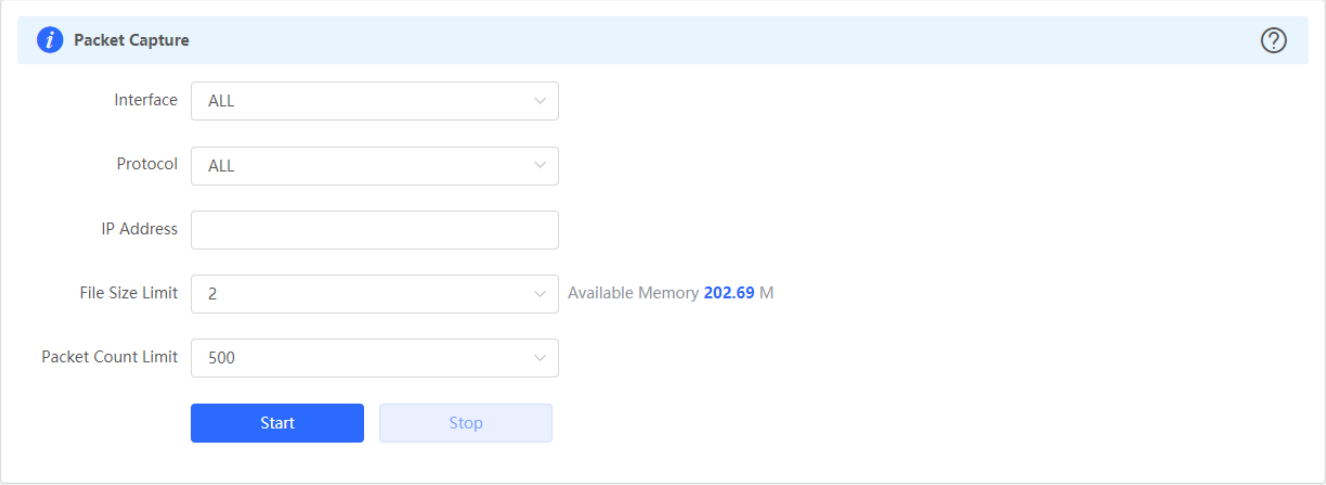
Figure 3-3-132 DNS Lookup Test and Result



3.3.7.4 Packet Capture

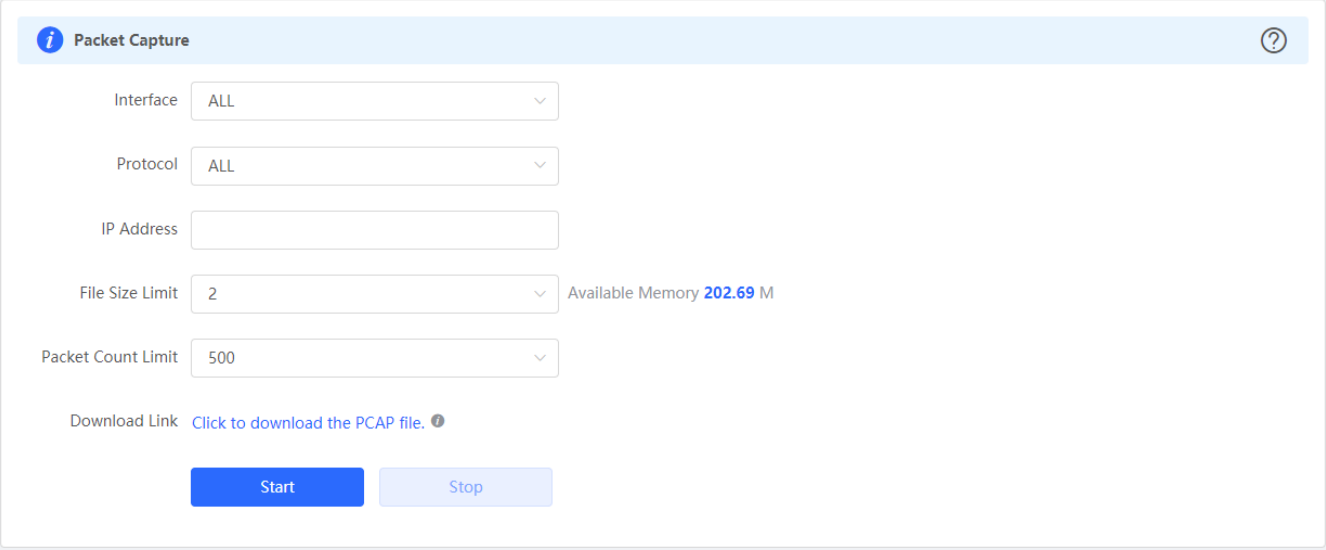
The **Packet Capture** module allows you to perform packet capture and download the result for troubleshooting.

Figure 3-3-133 Packet Capture



Specify an IP address and click **Start**. After a few seconds, click **Stop**.

Figure 3-3-134 Start Packet Capture

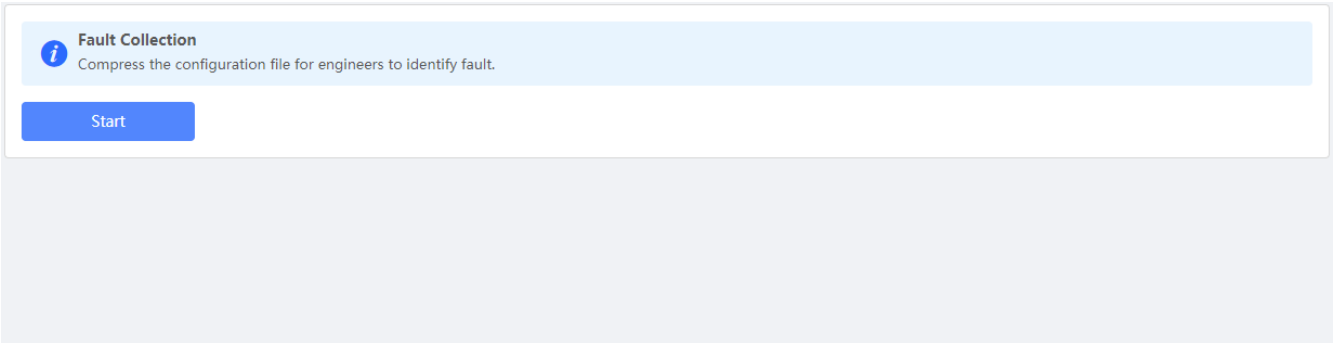


Click to download the packet capture result in the PCAP format.

3.3.7.5 Fault Collection

The **Fault Collection** module allows you to collect faults by one click and download the fault information to the local device.

Figure 3-3-135 Fault Collection

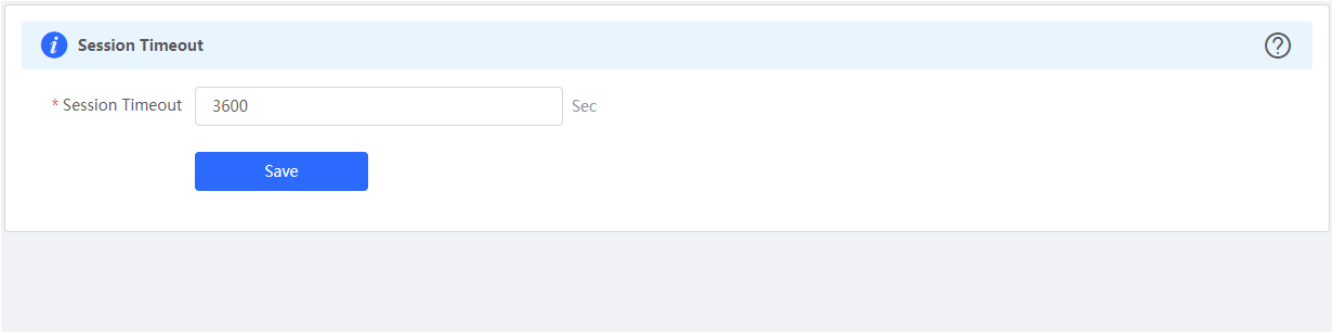


3.3.8 System

3.3.8.1 Session Timeout

The **Session Timeout** module allows you to set the session timeout period for login to the eWeb management system.

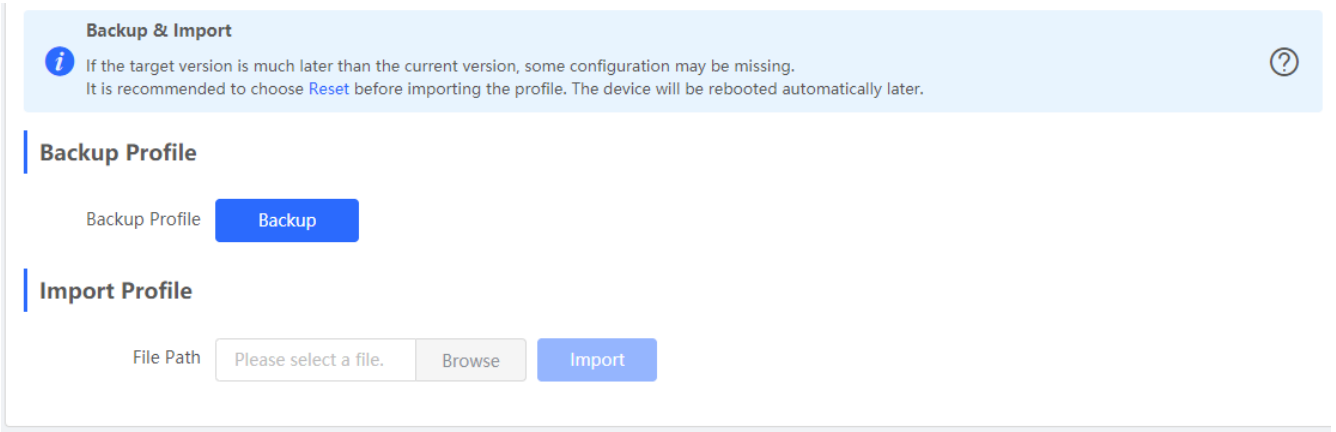
Figure 3-3-136 Session Timeout



3.3.8.2 Backup & Import

The **Backup & Import** module allows you to import a configuration file and apply the imported settings. It also allows exporting the configuration file to generate a backup.

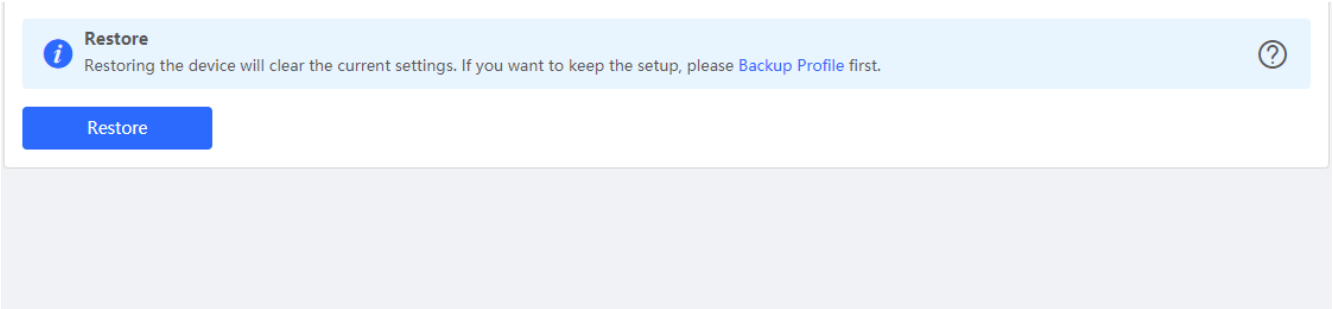
Figure 3-3-137 Backup & Import



3.3.8.3 Restore

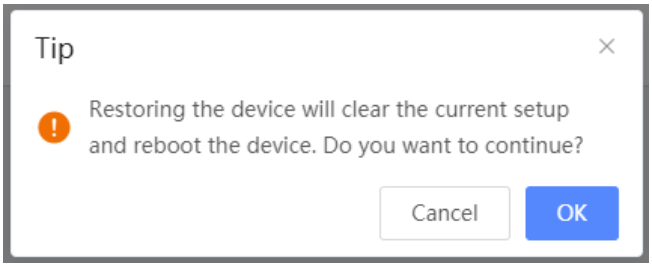
The **Restore** module allows you to restore the device to factory settings.

Figure 3-3-138 Restore



Please exercise caution if you want to restore the factory settings.

Figure 3-3-139 Confirm Restore

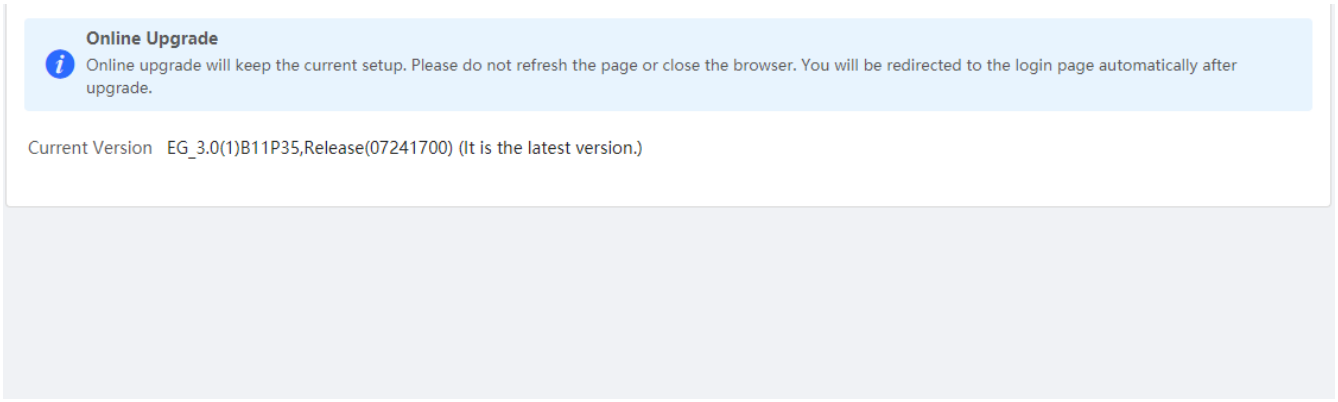


Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed..

3.3.8.4 Online upgrade

Click **Upgrade Now**. The device downloads the upgrade package from the network, and upgrades the current version. The upgrade operation retains configuration of the current device. Alternatively, you can select **Download File** to the local device and import the upgrade package on the **Local Upgrade** page. If there is no available new version, the device displays a prompt indicating that the current version is the latest.

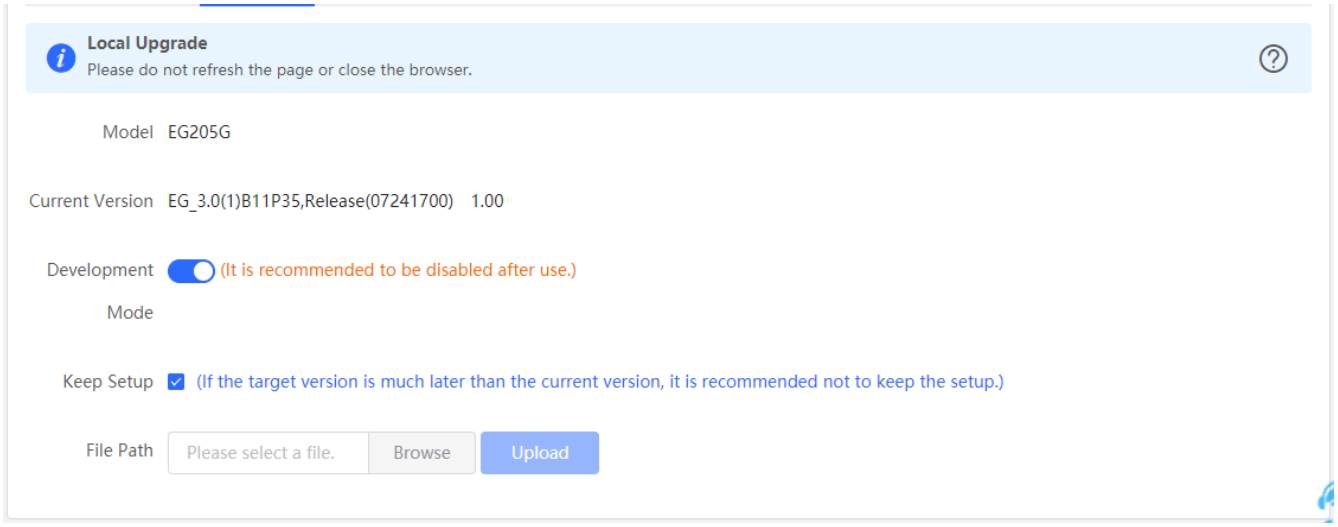
Figure 3-3-140 Online Upgrade



3.3.8.5 Local Upgrade

Click **Browse** to select an upgrade package, and click **Upload**. After uploading and checking the package, the device displays the upgrade package information and a prompt asking for upgrade confirmation. Click **OK** to start the upgrade.

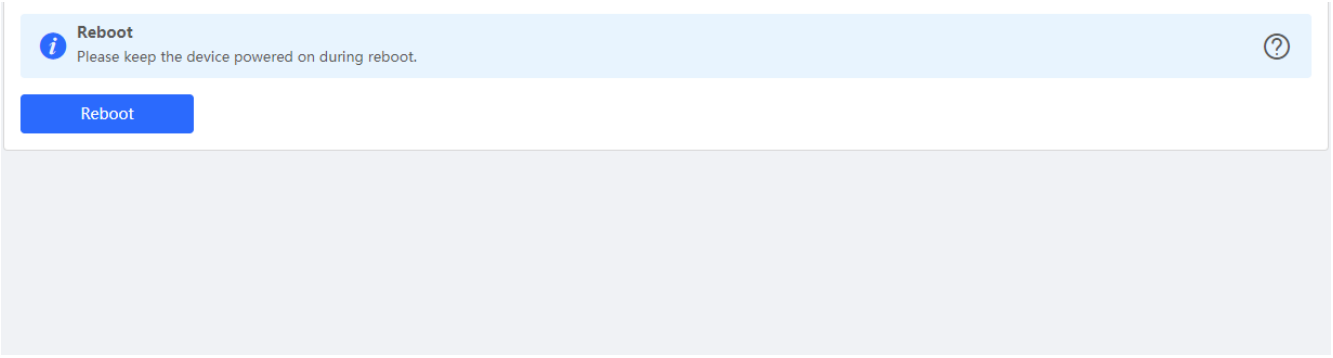
Figure 3-3-141 Local Upgrade



3.3.8.6 Reboot

The **Reboot** module allows you to reboot the device immediately.

Figure 3-3-142 Reboot

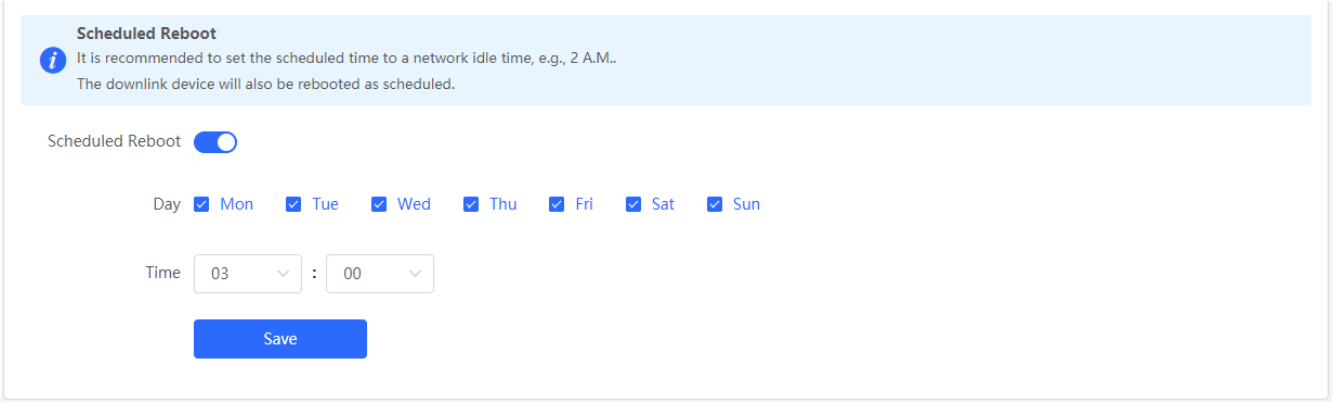


Click **Reboot**, and click **OK** in the confirmation box. The device is rebooted and you need to log into the eWeb management system again after the reboot. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the eWeb service becomes available, you will be redirected to the login page of the eWeb management system.

3.3.8.7 Scheduled Reboot

The **Scheduled Reboot** module allows you to reboot the device at a scheduled time.

Figure 3-3-143 Scheduled Reboot



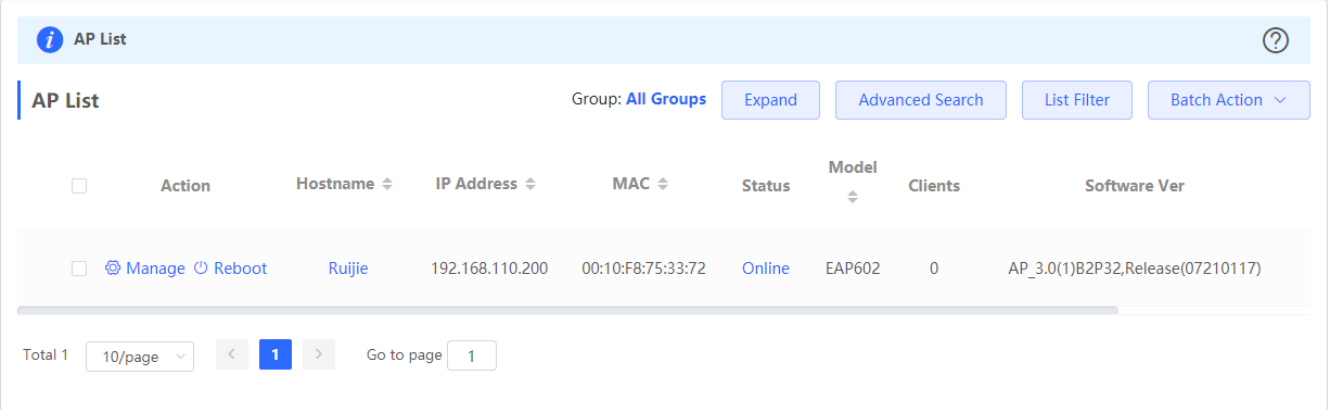
Enable scheduled reboot, select the time and click **Save**.

3.4 Wireless

3.4.1 APs

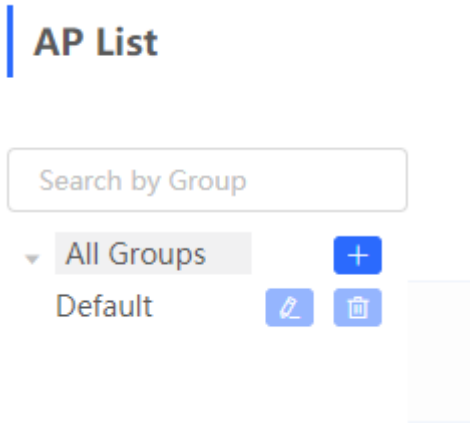
The **APs** module allows you to group, upgrade and delete APs.

Figure 3-4-1 AP List



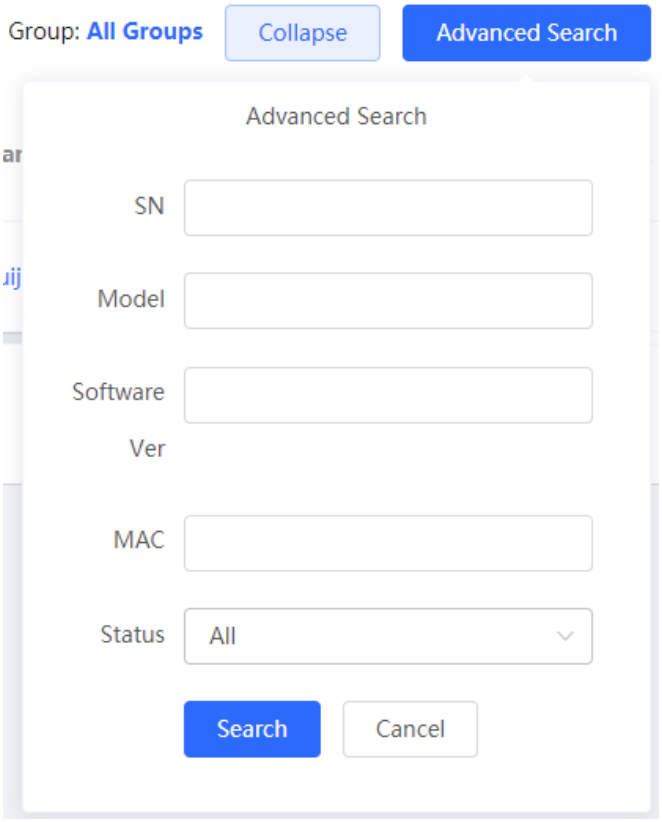
Click **Expand**, and all groups will be displayed on the left column. You can add, delete, edit and search groups. Up to 8 groups can be added.

Figure 3-4-2 Group Management



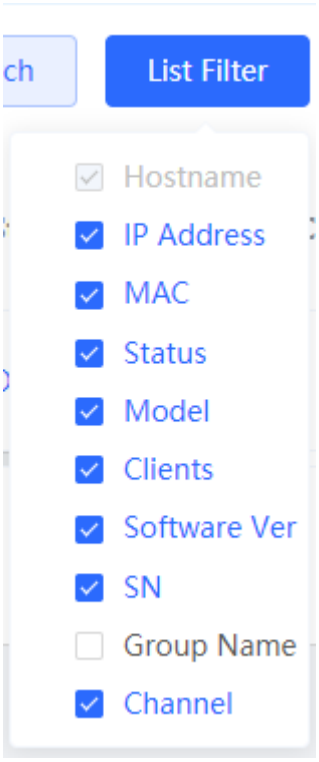
Click **Advanced Search**, and you can search APs by SN, model, software version, MAC address and status.

Figure 3-4-3 Advanced Search



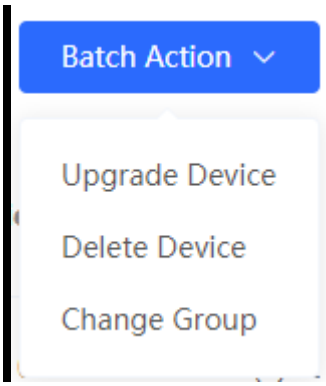
Click **List Filter**, and you can select columns to be displayed in the list.

Figure 3-4-4 List Filter



Select the target devices and click **Batch Action**. The following actions are available:

Figure 3-4-5 Batch Action



Upgrade Device: If there is a new version available, you can upgrade the devices in batches.

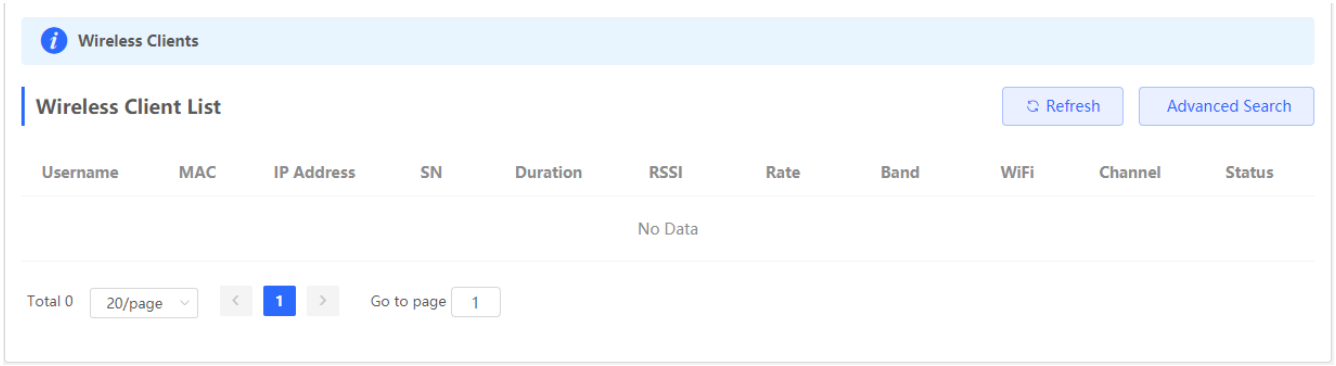
Delete Device: You can delete the devices in batches.

Change Group: You can move the devices from one group to another. The devices will be applied with the new group settings.

3.4.2 Clients

The **Clients** module displays the wireless clients.

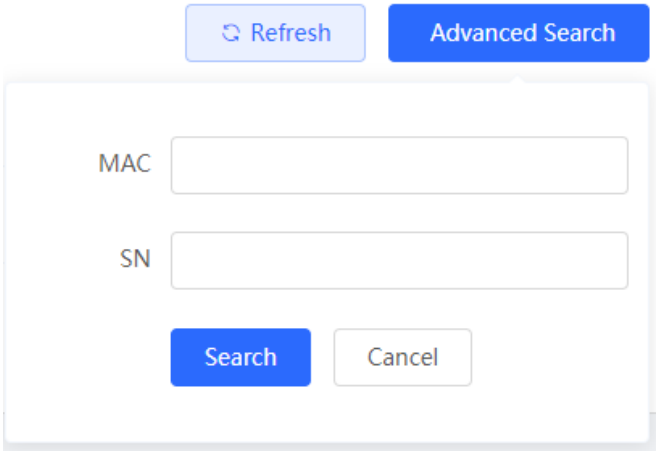
Figure 3-4-6 Wireless Client List



Click **Advanced Search**, and you can search clients by SN and MAC address.

This is a fuzzy search. You can enter an incomplete MAC address or part of an SN.

Figure 3-4-7 Advanced Search

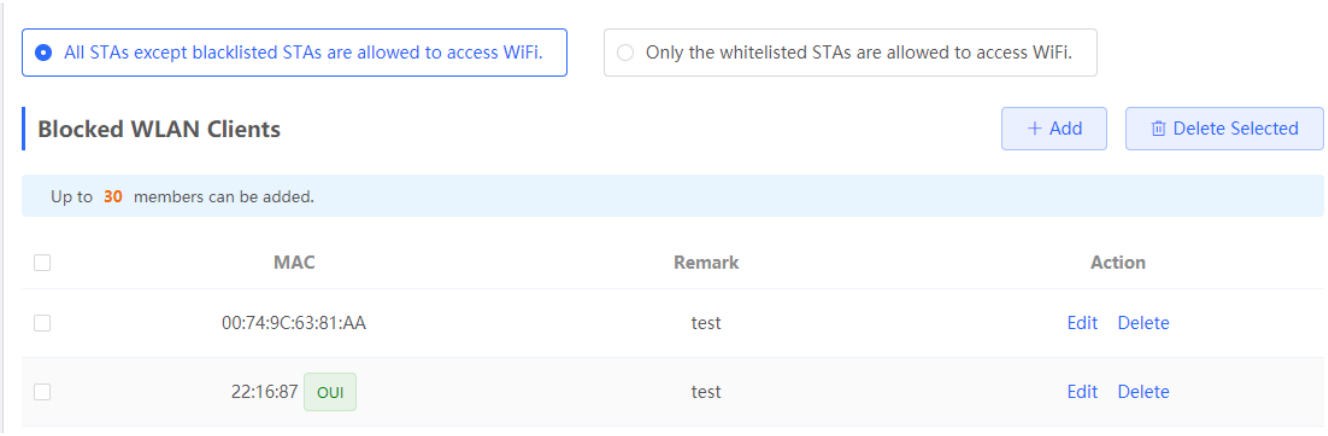


3.4.3 Blacklist/Whitelist

The **Blacklist/Whitelist** module allows you to configure global blacklist/whitelist and SSID-based blacklist/whitelist.

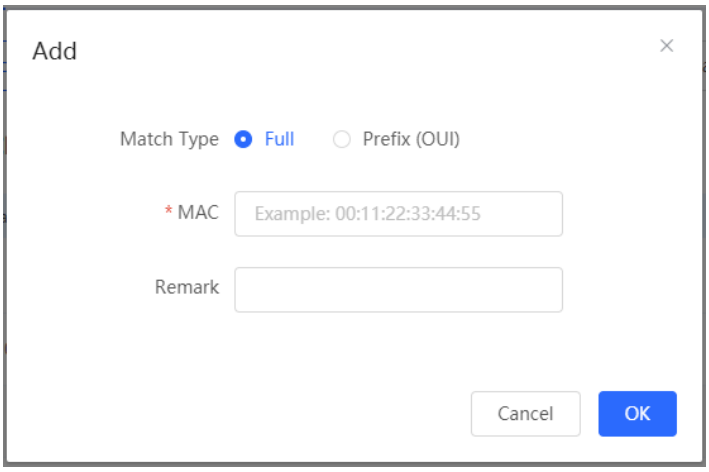
3.4.3.1 Global Blacklist/Whitelist

Figure 3-4-8 Global Blacklist/Whitelist



Click **Add** to add a blacklisted or whitelisted client. In the displayed dialog box, configure settings and click **OK**.

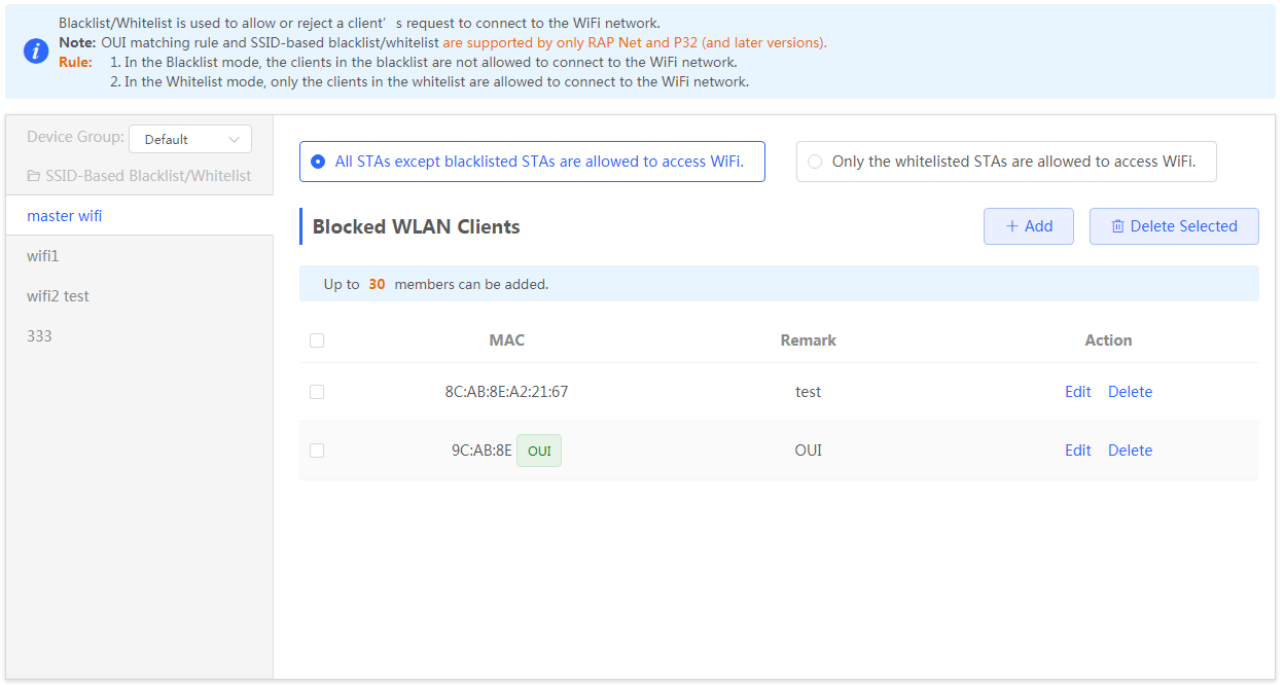
Figure 3-4-9 Add Client



3.4.3.2 SSID-based Blacklist/Whitelist

Select an SSID from the left column and configure its blacklist or whitelist.

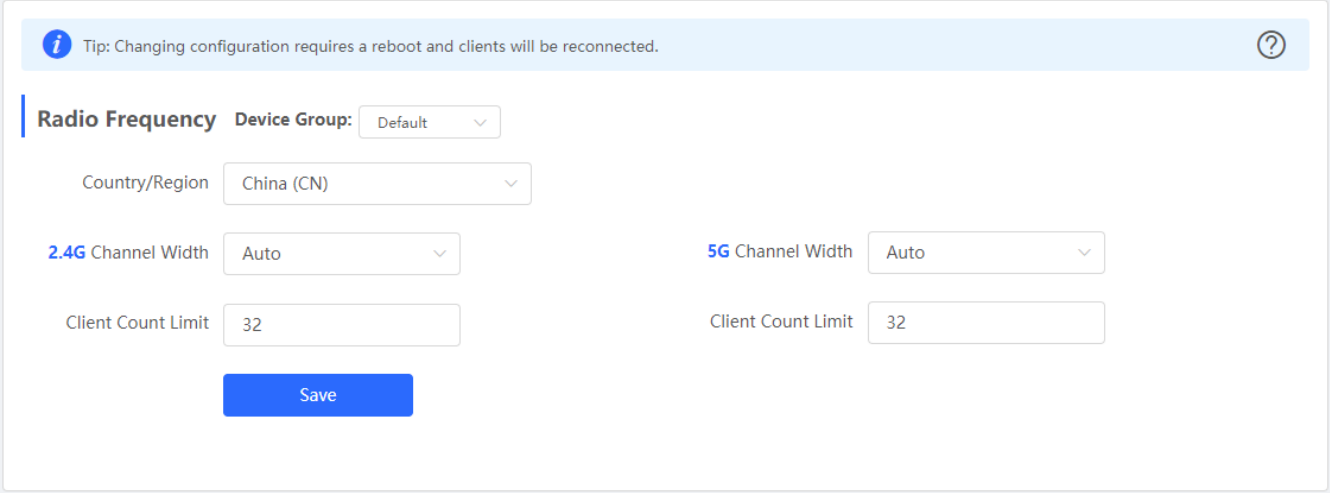
Figure 3-4-10 SSID-basd Blacklist/Whitelist



3.4.4 Radio Frequency

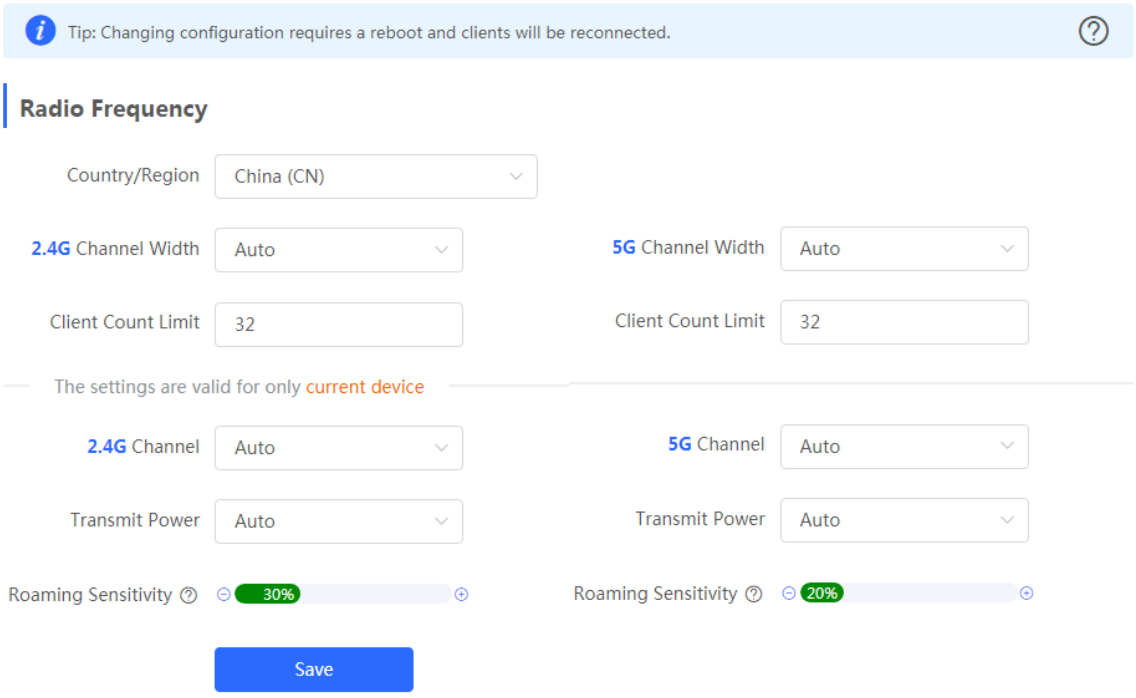
The **Radio Frequency** module allows you to configure client count limit and channel width.

Figure 3-4-11 Radio Frequency (EG Device)



Only the AP supports power and roaming sensitivity settings.

Figure 3-4-12 Radio Frequency (EAP)



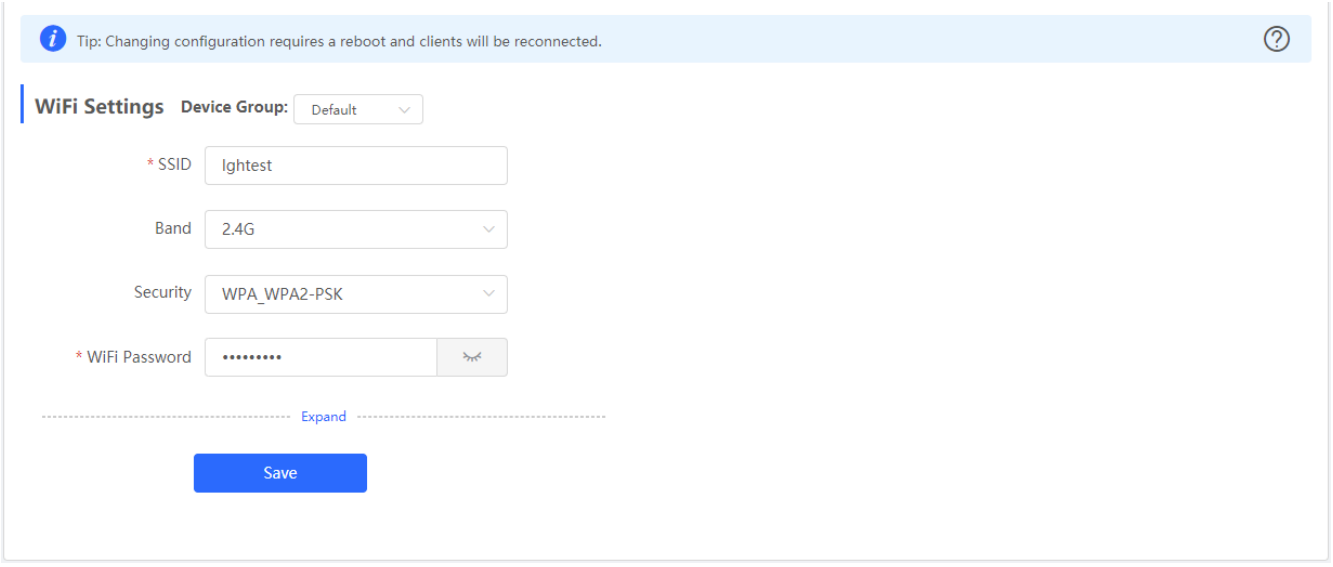
3.4.5 WiFi

The **WiFi** module allows you to configure WiFi settings for all devices.

3.4.5.1 WiFi Settings

The **WiFi Settings** module allows you to configure the primary WiFi.

Figure 3-4-13 WiFi Settings



3.4.5.2 Guest WiFi

The guest WiFi is disabled by default. You can enable guest WiFi on this page or homepage.

AP isolation is enabled by default and cannot be edited.

Set a schedule, and the guest WiFi will be enabled only during this period time. When the time expires, the guest WiFi will be disabled.

Figure 3-4-14 Guest WiFi

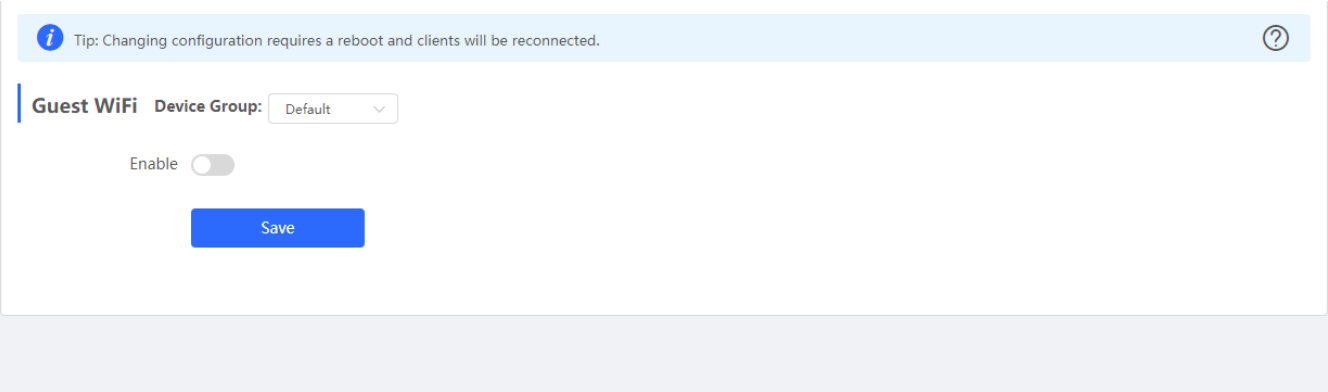
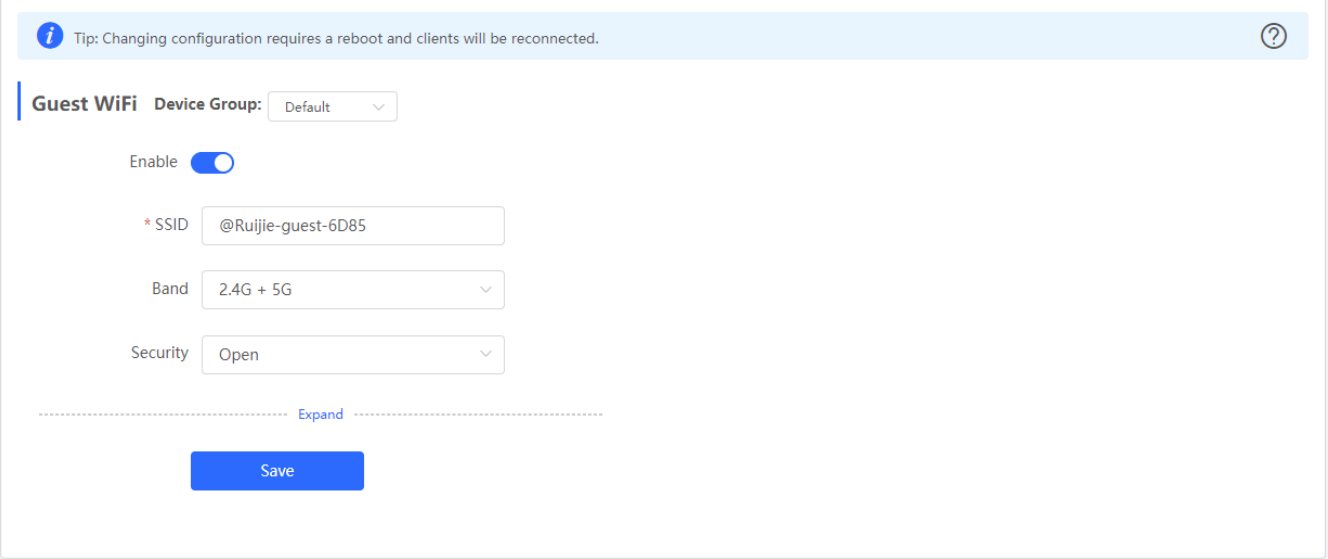


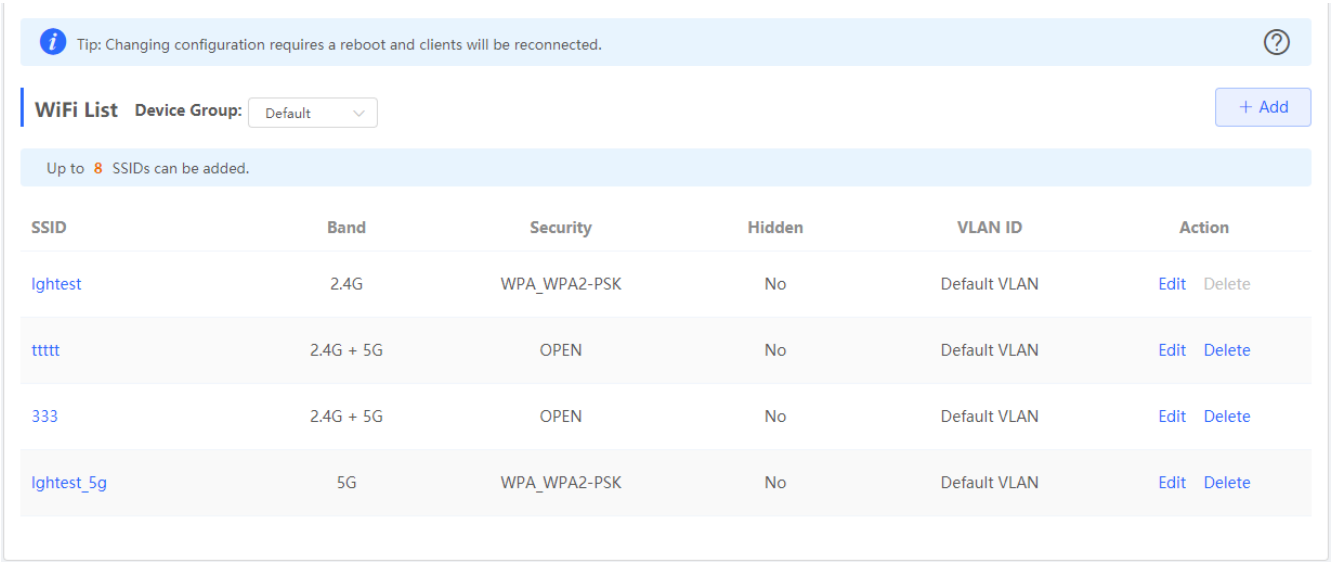
Figure 3-4-15 Enable Guest WiFi



3.4.5.3 WiFi List

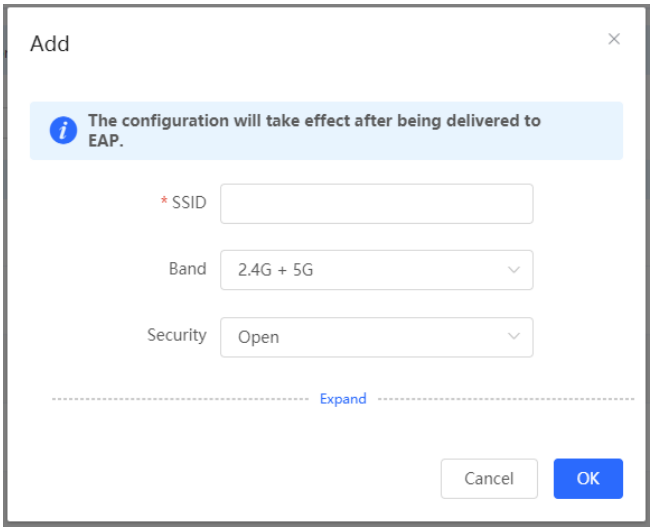
The **WiFi List** displays all WiFi networks. The primary WiFi is also listed here and cannot be deleted.

Figure 3-4-16 WiFi List



Click **Add** to add a WiFi network. In the displayed dialog box, configure settings and click **OK**.

Figure 3-4-17 Add WiFi

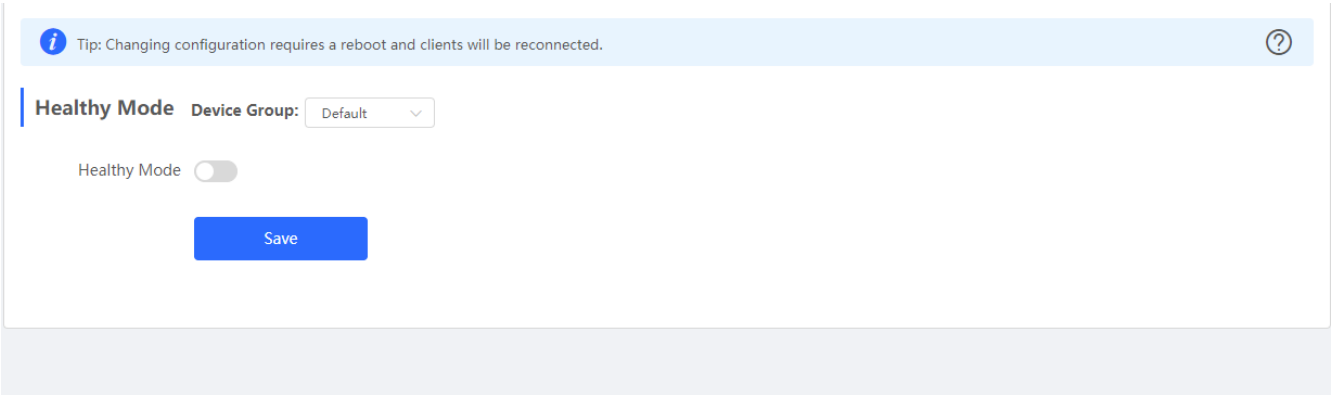


You can click in the upper right corner to see description about each configuration item.

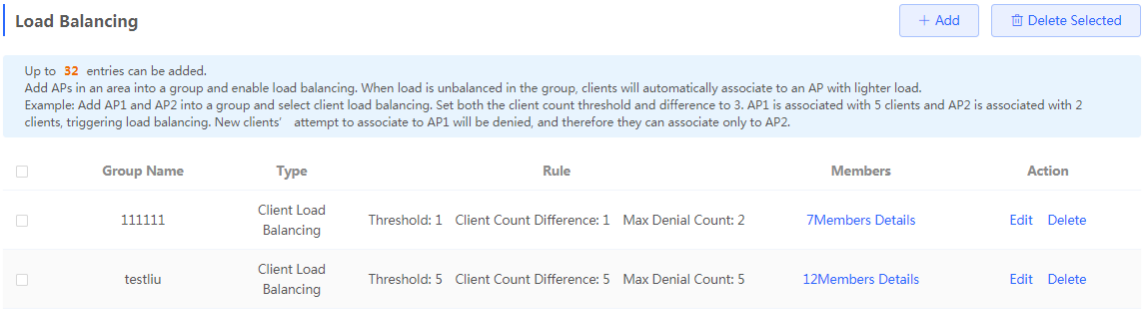
3.4.5.4 Healthy Mode

The **Healthy Mode** module allows you to enable health mode and set a schedule.

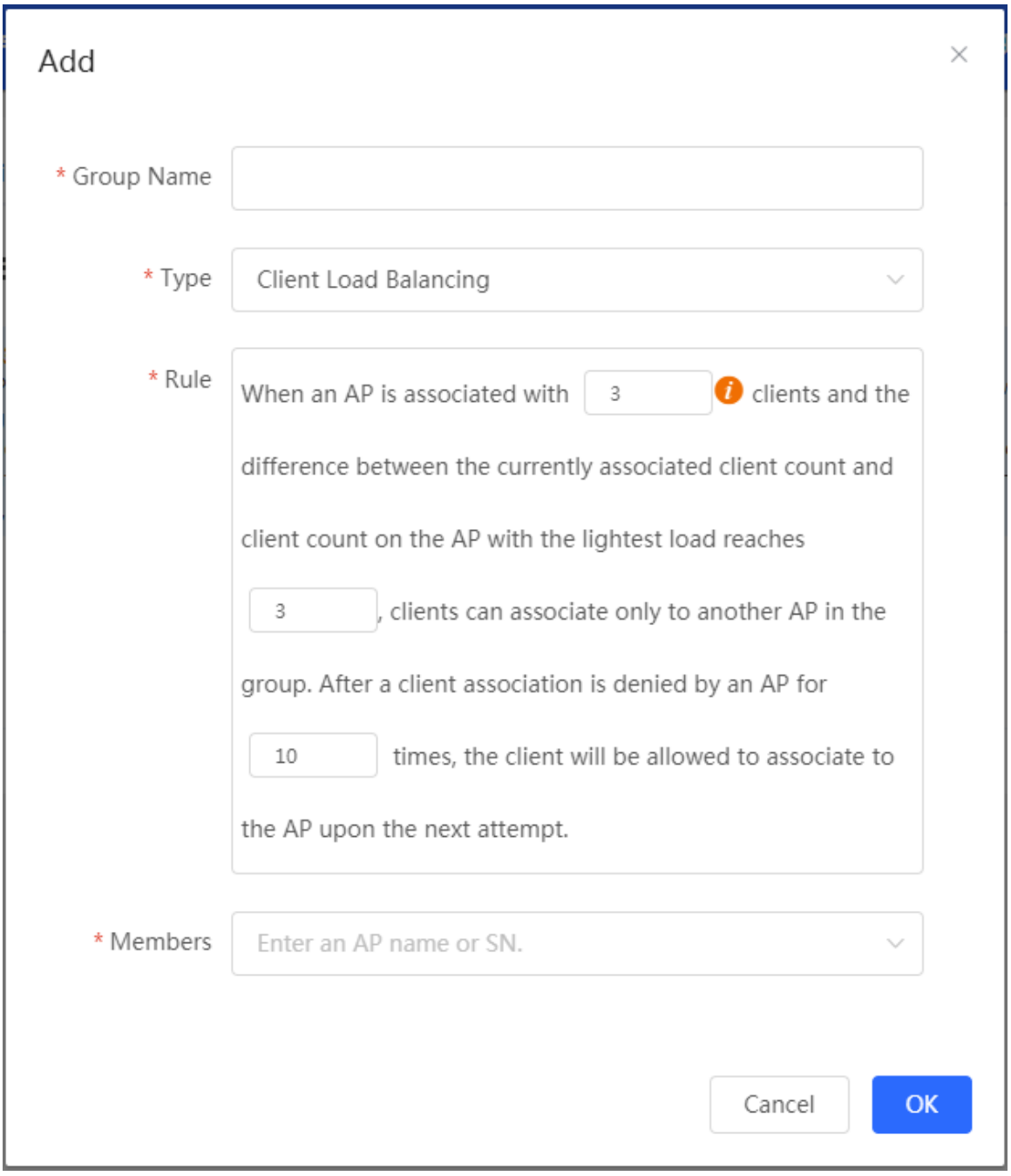
Figure 3-4-18 Healthy Mode



3.4.5.5 Load Balancing



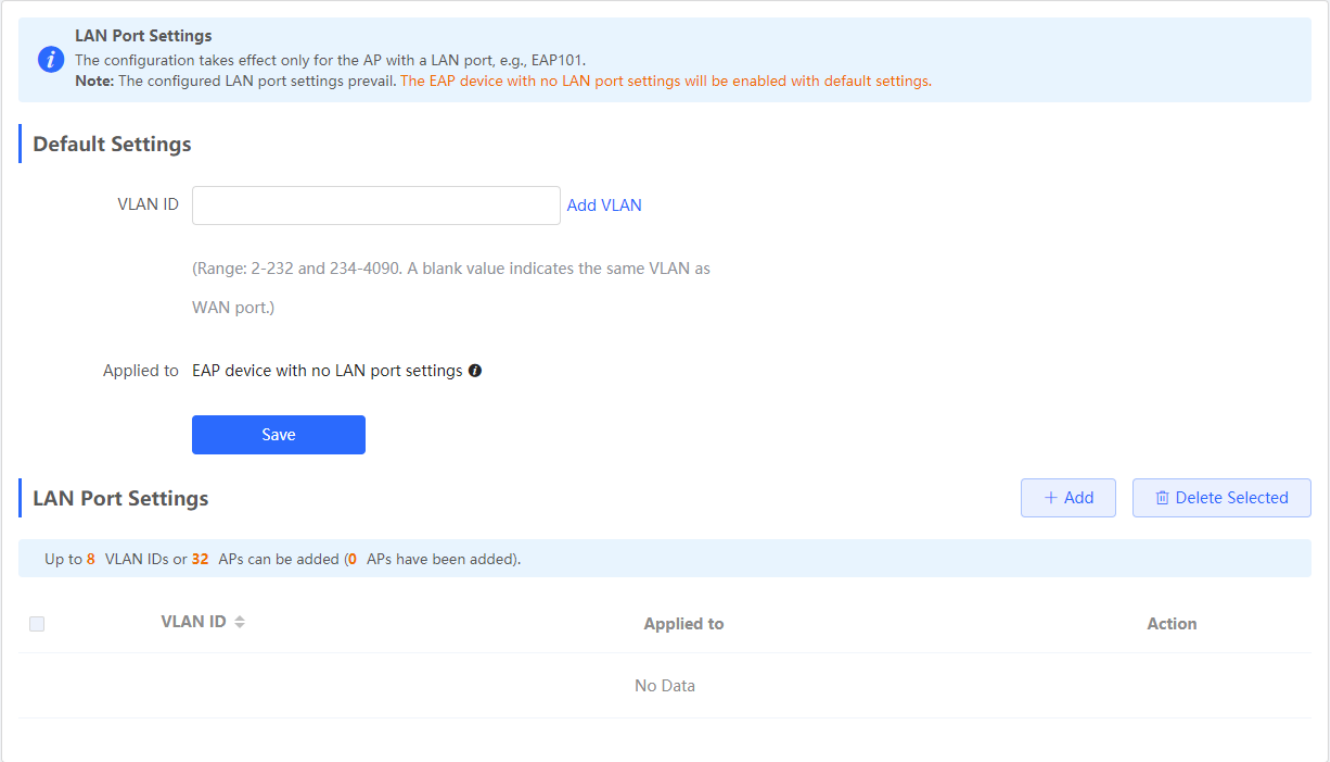
Click **Add** to add a Load Balancing. In the displayed dialog box, configure settings and click **OK**.



3.4.6 LAN Ports

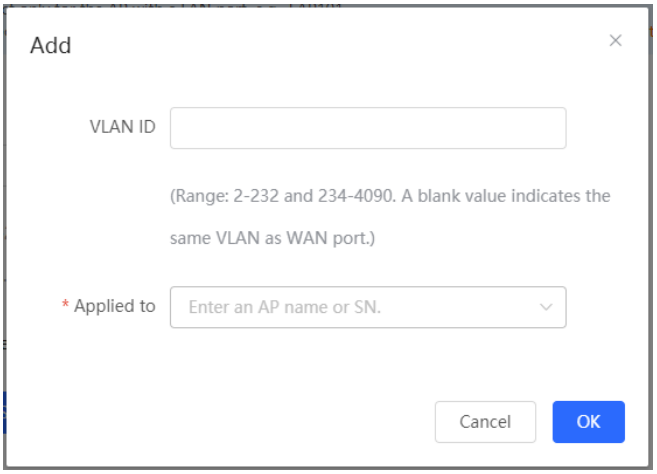
The **LAN Ports** module allows you to configure LAN ports.

Figure 3-4-19 LAN Ports



Click **Add** to add a LAN port. In the displayed dialog box, configure settings and click **OK**.

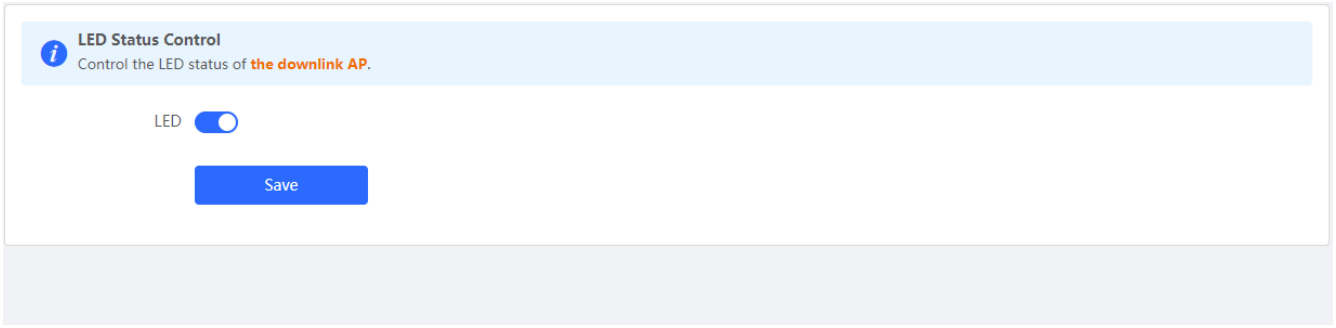
Figure 3-4-20 Add LAN Port



3.4.7 LED

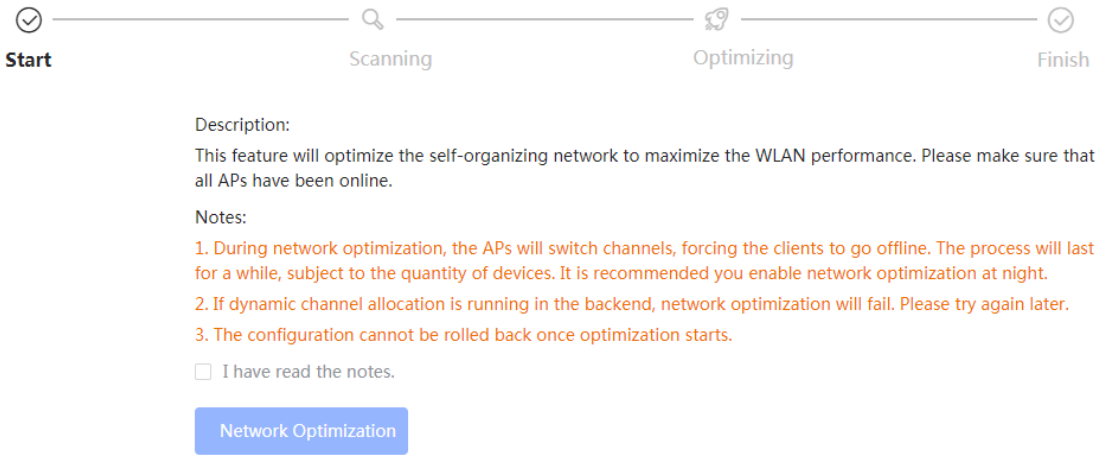
The **LED** module allows you to enable LED.

Figure 3-4-21 LED

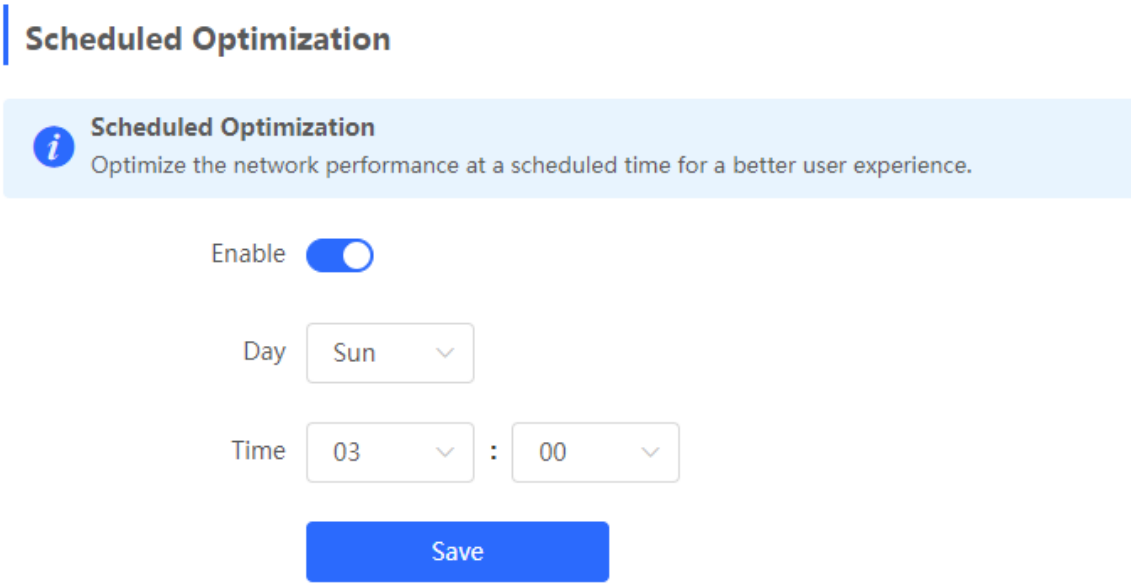


3.4.8 WIO

3.4.8.1 Network Optimization

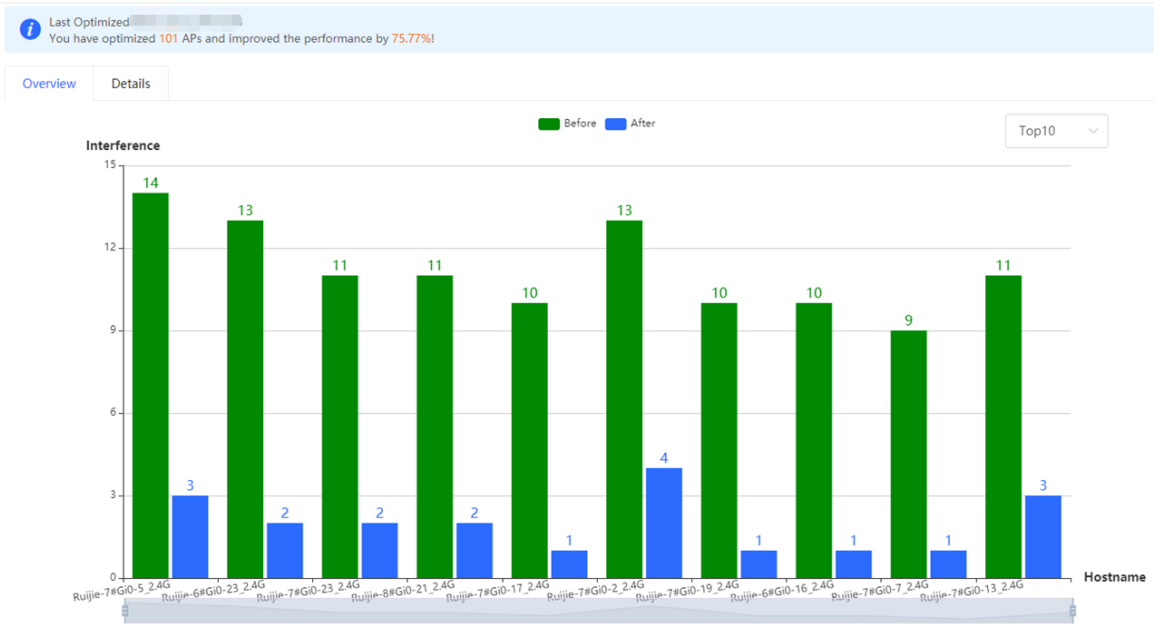


Scheduled Optimization

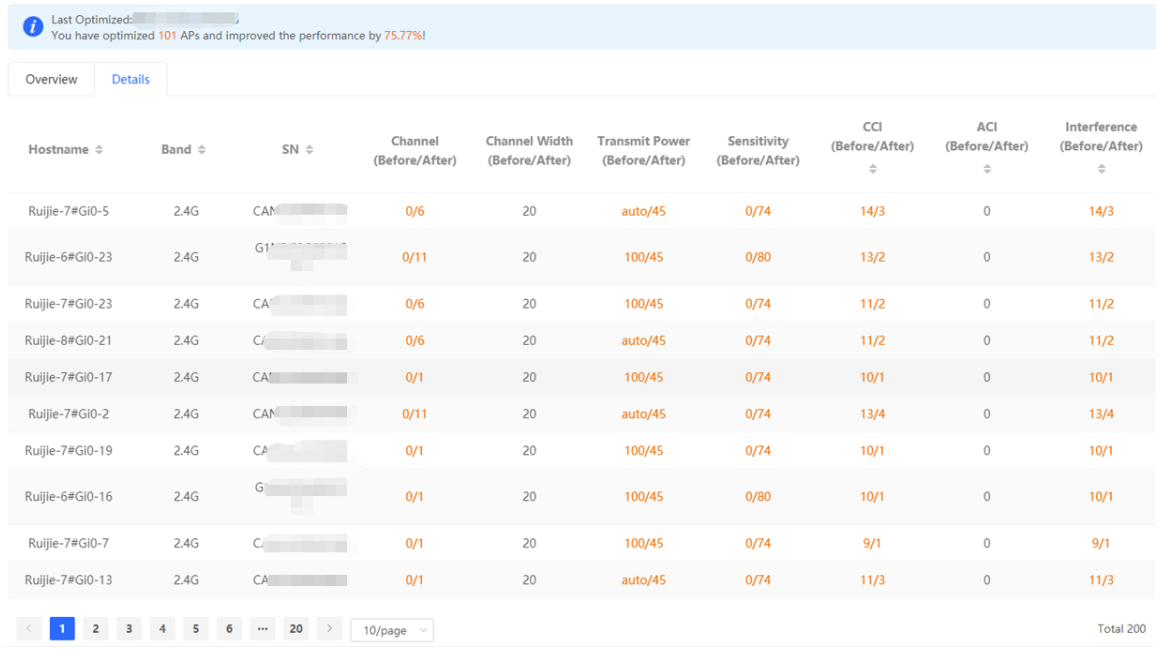


3.4.8.2 Optimization Record

Overview



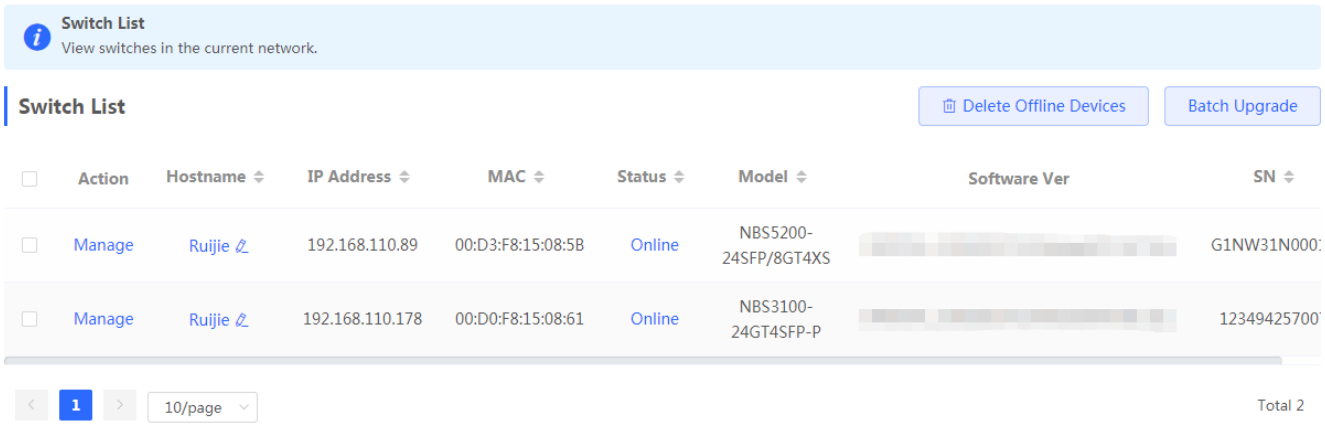
Details



3.5 Switches

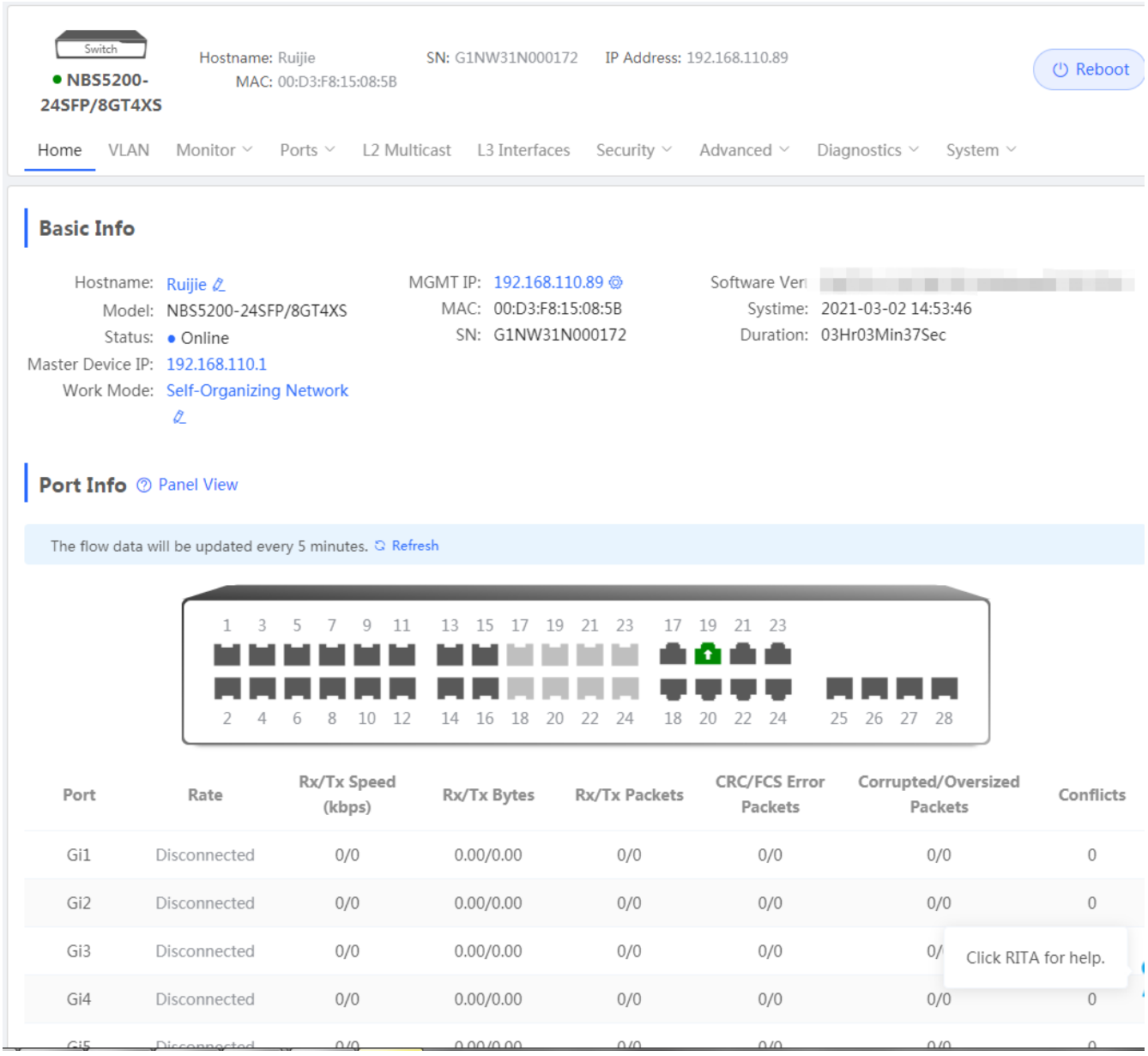
The **Switches** page displays all switches in the current network.

Figure 3-5-1 Switch List



Click **Manage** in the **Action** column, and the switch management page will be displayed.

Figure 3-5-2 Switch Management



See *Ruijie RG-NBS Series Switches Web-Based Configuration Guide* for details.

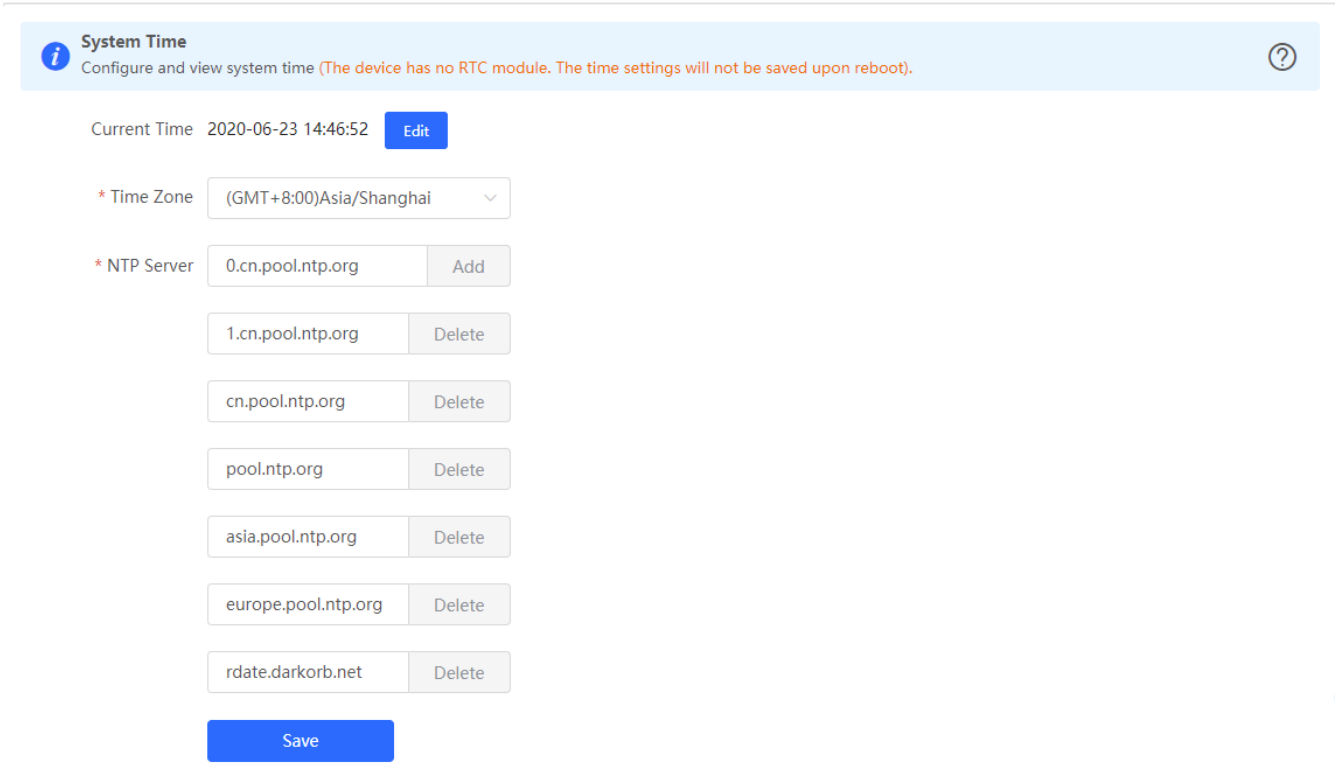
3.6 System

3.6.1 Time

The **Time** module allows you to set the system time. The system time is synchronized with the NTP server by default.

Select a time zone and set at least one NTP server, and click **Save**.

Figure 3-6-1 System Time

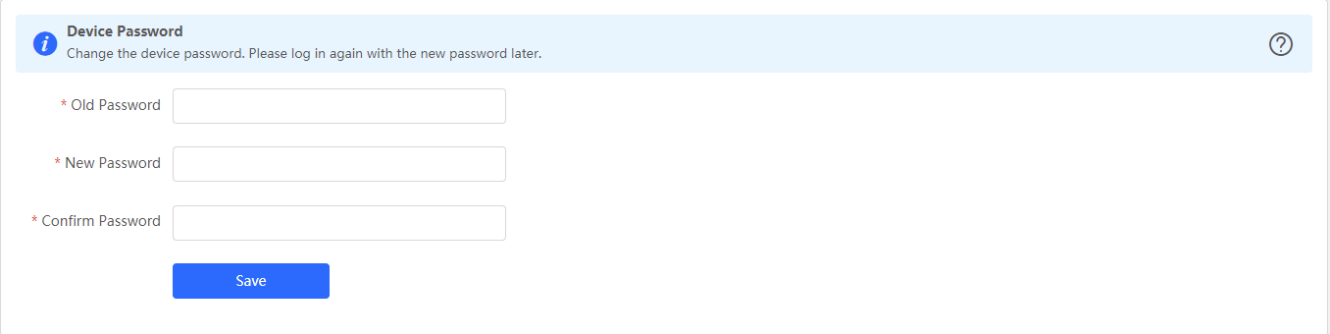


You can also edit the tiime manually by clicking **Edit**.

3.6.2 Password

The **Device Password** module allows you to set the device's login password. You need to log into the system again after changing the password.

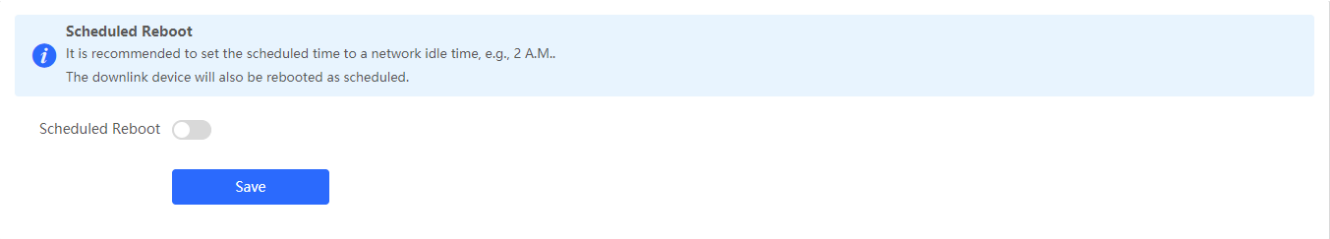
Figure 3-6-2 Device Password



3.6.3 Scheduled Reboot

The **Scheduled Reboot** module allows you to reboot all devices at a scheduled time.

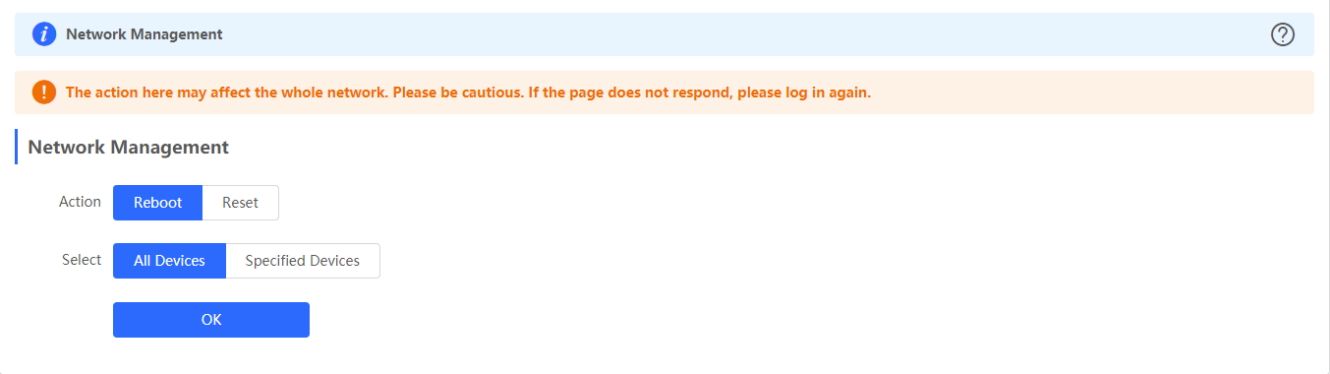
Figure 3-6-3 Scheduled Reboot



3.6.4 Reboot & Reset

The **Reboot & Reset** module allows you to reboot or reset all devices in the network.

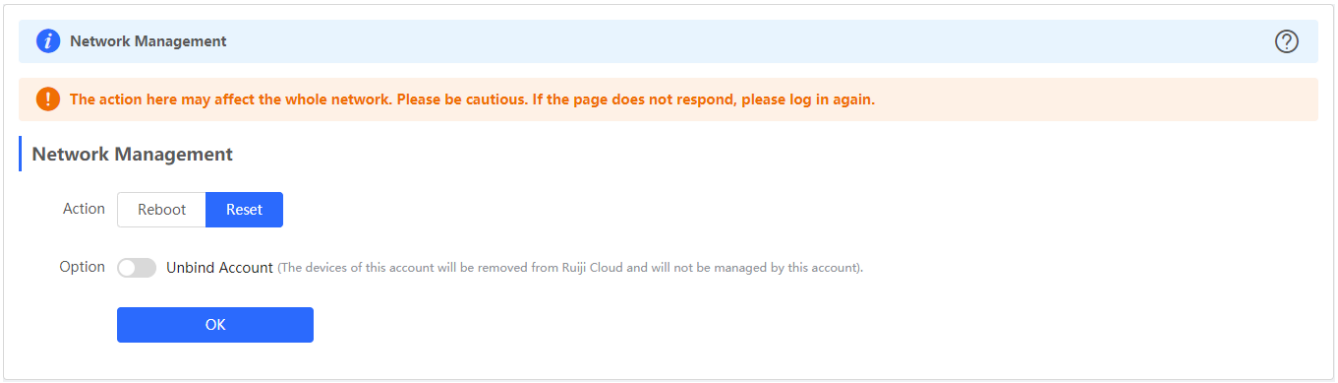
Figure 3-6-4 Reboot



If you click **Reboot**, you will be allowed to select all devices or specified devices for the action.

If you click **Reset**, all devices in the network will be reset to the factory settings. You can select whether to unbind the account.

Figure 3-6-5 Reset


Network Management
The action here may affect the whole network. Please be cautious. If the page does not respond, please log in again.
Network Management
Action
Reboot
Reset
Option
Unbind Account (The devices of this account will be removed from Ruiji Cloud and will not be managed by this account).
OK

4 FAQs

Q1: I failed to log into the eWeb management system. What can I do?

Perform the following steps:

(1) Check that the network cable is properly connected to the LAN port of the device and the corresponding LED indicator blinks or is steady on.

(2) Before accessing the configuration GUI, set the IP assignment mode to **Obtain an IP address automatically** (recommended), so that the server with DHCP enabled can automatically assign an IP address to the PC. To designate a static IP address to the PC, set the IP address of the PC in the same network segment as the IP address of the management interface. For example, if the default IP address of the management interface is 192.168.110.1 and the subnet mask is 255.255.255.0, set the IP address of the PC to 192.168.110.X (X is any integer ranging from 2 to 254), and the subnet mask is 255.255.255.0.

(3) Run the **ping** command to test the connectivity between the PC and the device.

(4) If the login failure persists, restore the device to factory settings.

Q2: What can I do if I forget my username and password? How to restore the factory settings?

To restore the factory settings, power on the device, and press and hold the **Reset** button for 5s or more, and release the **Reset** button after the system LED indicator blinks. The device automatically restores the factory settings and restarts. The original configuration will be lost after the factory settings are restored. After the restoration, the default management address is http://10.44.77.200. You can set the username and password upon first login.

Q3: The subnet mask value needs to be specified to divide the address range for certain functions. What are the common subnet mask values?

A subnet mask is a 32-bit binary address that is used to differentiate between the network address and host address. The subnet and the quantity of hosts in the subnet vary with the subnet mask.

Common subnet mask values include 8 (default subnet mask 255.0.0.0 for class A networks), 16 (default subnet mask 255.255.0.0 for class B networks), 24 (default subnet mask 255.255.255.0 for class C networks), and 32 (default subnet mask 255.255.255.255 for a single IP address).