Ruijie Reyee RG-RAP73HD Access Point ReyeeOS 1.220

Web-based Configuration Guide

Document Version: V1.0
Date: 2023-05-31

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Audience

This document is intended for:

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

Technical Support

- Official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee
- 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

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

This manual introduces the product model, port type and CLI for your reference. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Contents

1 Fast Internet Access

1.1 Configuration Environment Requirements

1.1.1 PC

- Browser: Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/Internet Explorer kernel-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- Resolution: 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

1.2 Default Configuration

1.2.1 Connecting to the Access Point

You can open the management page and complete Internet access configuration only after connecting a client to the access point in either of the following ways:

- Wired Connection

Connect a local area network (LAN) port of the access point to the network port of the PC, and set the IP address of the PC. See Configuring the IP Address of the Management Client.

- Wireless Connection

On a mobile phone or laptop, search for wireless network @Ruijie-SXXXX (XXXX is the last four digits of the MAC address of each device). In this mode, you do not need to set the IP address of the management Client, and you can skip the operation in Configuring the IP Address of the Management Client.

1.2.2 Configuring the IP Address of the Management Client

Configure an IP address for the management client in the same network segment as the default IP address of the device (The default device IP address is 10.44.77.254, and the subnet mask is 255.255.255.0.) so that the management client can access the device. For example, set the IP address of the management client to 10.44.77.100.

Table 1-1 **Default eWeb Configuration**

Item	Default
IP address	10.44.77.254
Username/Password	A username is not required when you log in for the first time. The default password is **admin**.

Caution

- Make sure that the client can access the Eweb system as long as it can ping the access point.
- The IP address of the management client cannot be set to 10.44.77.253, because this IP address is reserved by the device. If the management client uses this IP address, it cannot access the device.

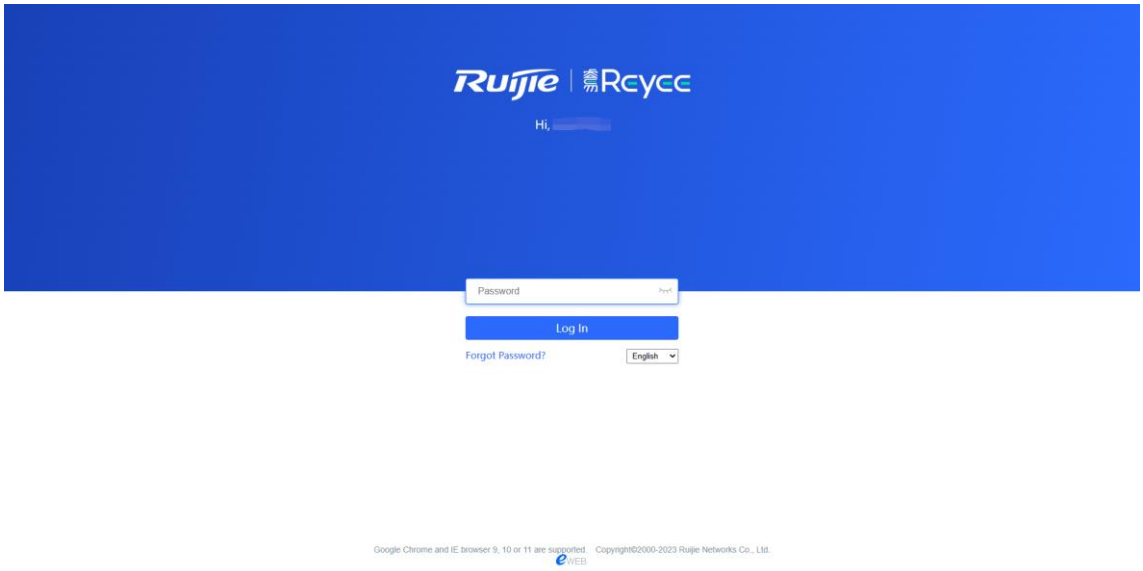
1.2.3 Logging in to the eWeb Page

(1) Enter the IP address (10.44.77.254 by default) of the access point in the address bar of the browser to open the login page.

Note

If the static IP address of the device is changed, or the device obtains a new dynamic IP address, the new IP address can be used to access the web management system of the device as long as the management client and the device are in the same network segment of a LAN.

(2) On the web page, enter the password and click **Log In** to enter the eWeb management system.



You can use the default password **admin** to log in to the device for the first time. For security purposes, you are advised to change the default password as soon as possible after logging in, and to regularly update your password thereafter.

If you forget the IP address or password, hold down the **Reset** button on the device panel for more than 5 seconds when the device is connected to the power supply to restore factory settings. After restoration, you can use the default IP address and password to log in.

Caution

Restoring factory settings will delete the existing configuration and you are required to configure the device again at your next login. Therefore, exercise caution when performing this operation.

1.3 Work Mode

The device can work in the router mode or AP mode. The displayed system menu page and function ranges vary with the work mode. The RAP works in the AP mode by default. If you want to switch the work mode, see Switching Work Mode.

1.3.1 AP Mode

The device performs L2 forwarding and does not support the DHCP address pool function. In AP mode, the device often networks with devices supporting the routing function. IP addresses of downlink wireless clients are assigned and managed by the uplink device (supporting the DHCP address pool) of the AP in a unified manner, and the AP only transparently transmits data.

1.3.2 Router Mode

The device supports NAT routing and forwarding. The addresses of wireless clients can be assigned by the AP and wireless network data is routed and forwarded by the AP. NAT is supported in this mode. When an AP works in the router mode, it supports device networking, network-wide configuration, and AP-specific radio functions.

There are three Internet types available: PPPoE, DHCP mode and static IP address mode. You can connect the device to an Ethernet cable or an upstream device.

Caution

After switching to the router mode, the device's LAN IP address will change to 192.168.120.1. Please obtain an IP address automatically for your management client and enter 10.44.77.254 into the address bar of the browser to log in to Eweb again.

1.4 Configuration Wizard (Router Mode)

Upon first login, you can perform quick configuration procedures to configure the Internet type, Wi-Fi network and management password.

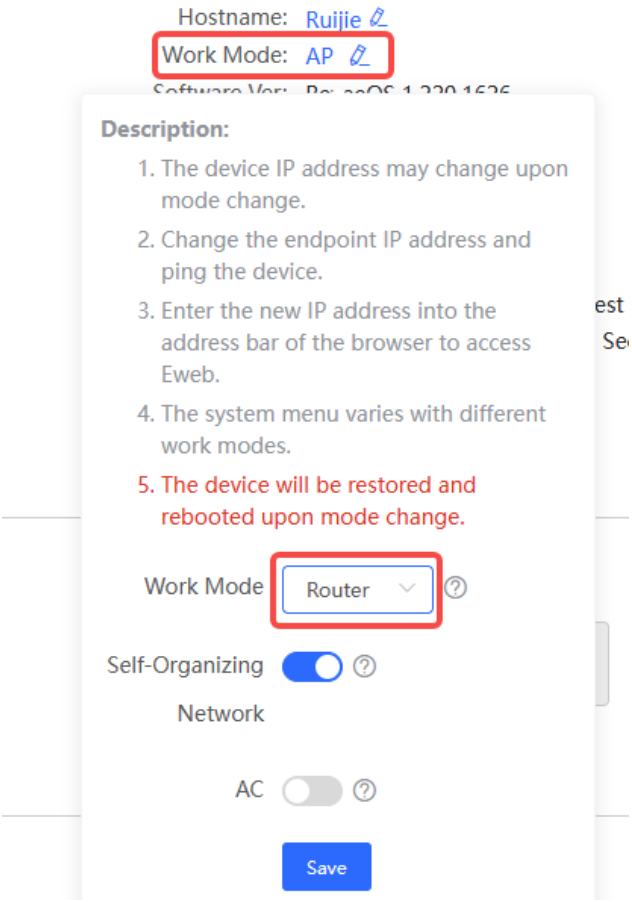
1.4.1 Getting Started

(1) Connect the device to a power supply and connect the port of the device to an upstream device with an Ethernet cable. Or you can connect an Ethernet cable to the device.

(2) Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet access may fail due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection type:

- Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
- In the PPPoE mode, a username, a password, and possibly a service name are needed.
- In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.

(3) The device works in the AP mode by default. If you want to switch the work mode to the router mode, perform the configuration on the work mode setting page. See Switching Work Mode for more details.



1.4.2 Configuration Steps

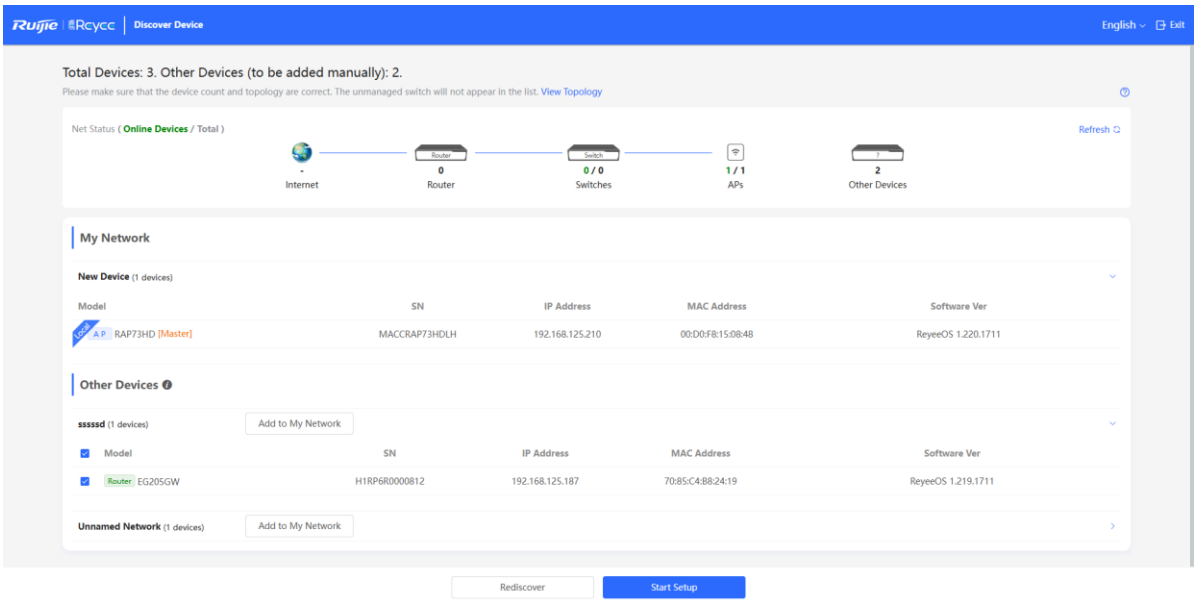
1. Add a Device to Network

You can manage and configure all devices in the network in batches by default. Please verify the device count and network status before configuration.

Note

New devices will join in a network automatically after being powered on. You only need to verify the device count.

If a new device is detected not in the network, click **Add to My Network** and enter its management password to add the device manually.



1. Creating a Network Project

Click **Start Setup** to configure the Internet connection type, Wi-Fi network and management password.

(1) **Network Name**: Identify the network where the device is located.

(2) **Internet**: Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).

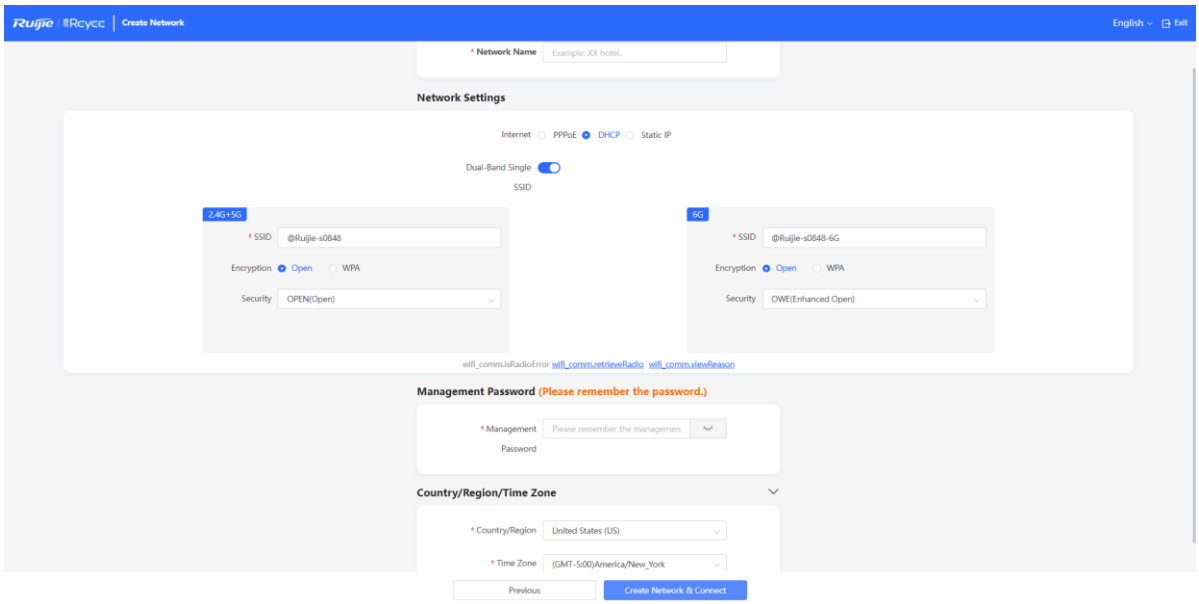
- **DHCP**: The access point detects whether it can obtain an IP address via DHCP by default. If the access point connects to the Internet successfully, you can click **Next** without entering an account.
- **PPPoE**: Click **PPPoE**, and enter the username, password, and service name. Click **Next**.
- **Static IP**: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.

(3) **SSID and Wi-Fi Password**: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.

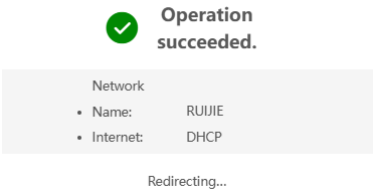
(4) **Management Password**: The password is used for logging in to the management page.

(5) **Country/Region**: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.

(6) **Time Zone**: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.



Click **Create Network & Connect**. The device will deliver the initialization and check the network connectivity.



The device can access the Internet now. Bind the device with a Ruijie Cloud account for remote management. Follow the instruction to log in to Ruijie Cloud for further configuration.

Note

- If your device is not connected to the Internet, click **Exit** to exit the configuration wizard.
- Please log in again with the new password if you change the management password.

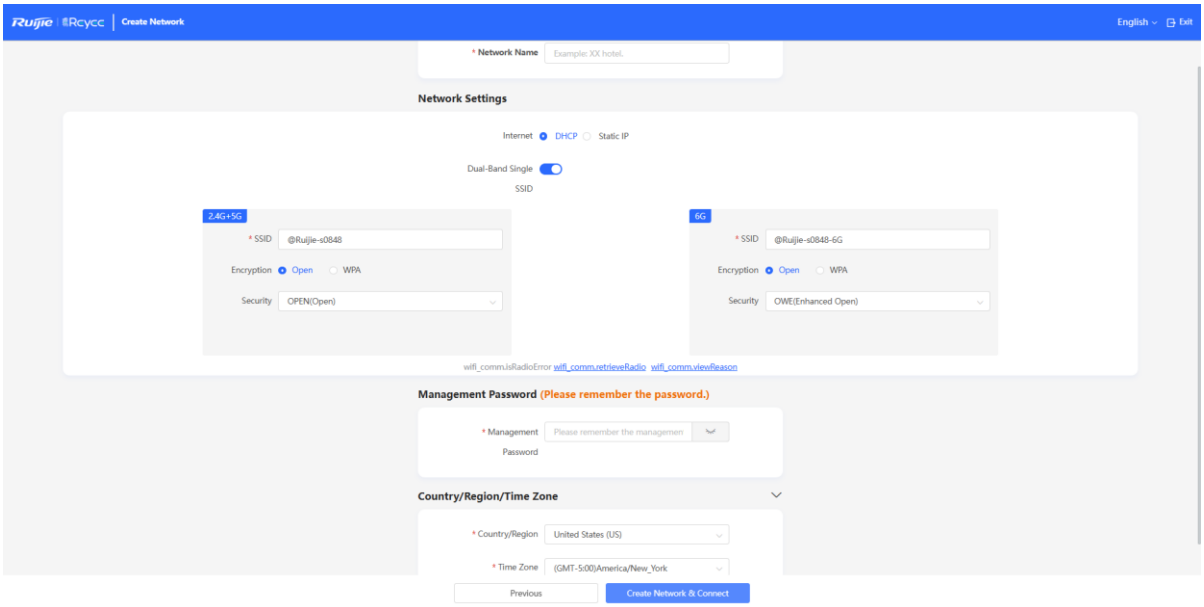
1.5 Configuration Wizard (AP Mode)

1.5.1 Getting Started

- Power on the device and connect the device to an upstream device.
- Make sure that the device can access the Internet.

1.5.2 Configuration Steps

The device obtains the IP address through the DHCP by default. Configure the SSID, Wi-Fi password and management password. The default Internet connection type is DHCP mode. You are advised to use the default value. See Configuration Steps for details.



1.6 Introduction to the eWeb GUI

To facilitate flexible device management, the Web page displays different system configuration menus in different work modes. For details about the work mode, see Switching Work Mode.

Note

When the self-organizing network is enabled, the Eweb GUI is subject to the master device in the network. If the master device supports the dual management webpages, the slave device also displays the dual management webpages.

1.6.1 Dual Management Webpages

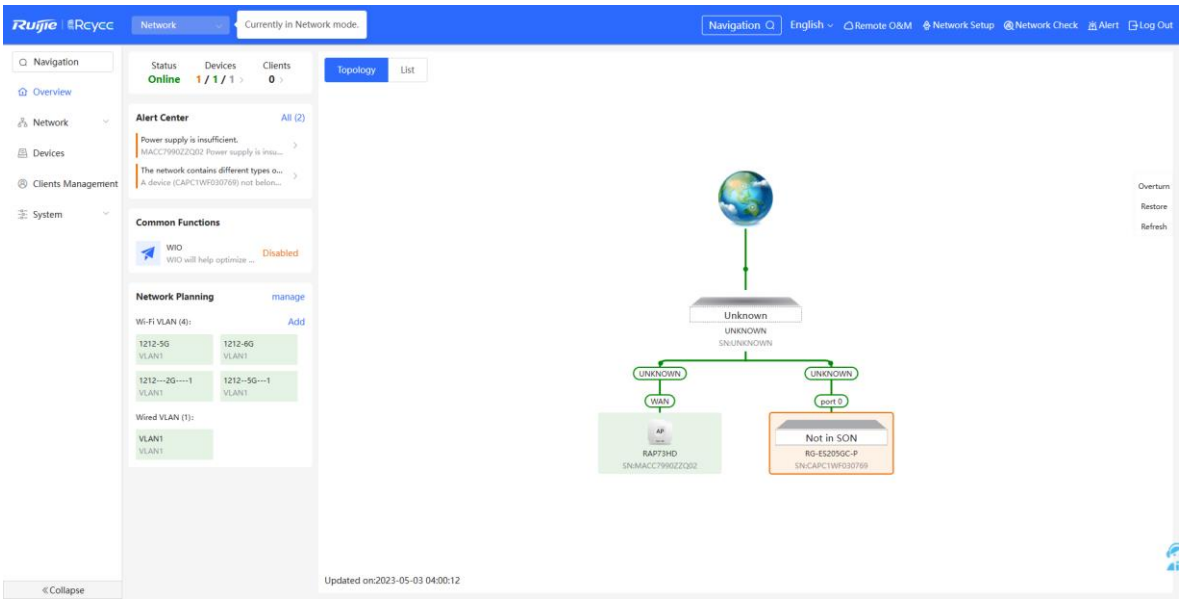
1. Introducing the Management Mode

If the self-organizing network is disabled (The function is enabled by default. See Switching Work Mode for details.), the device works in the local device mode displayed on the eWeb page.

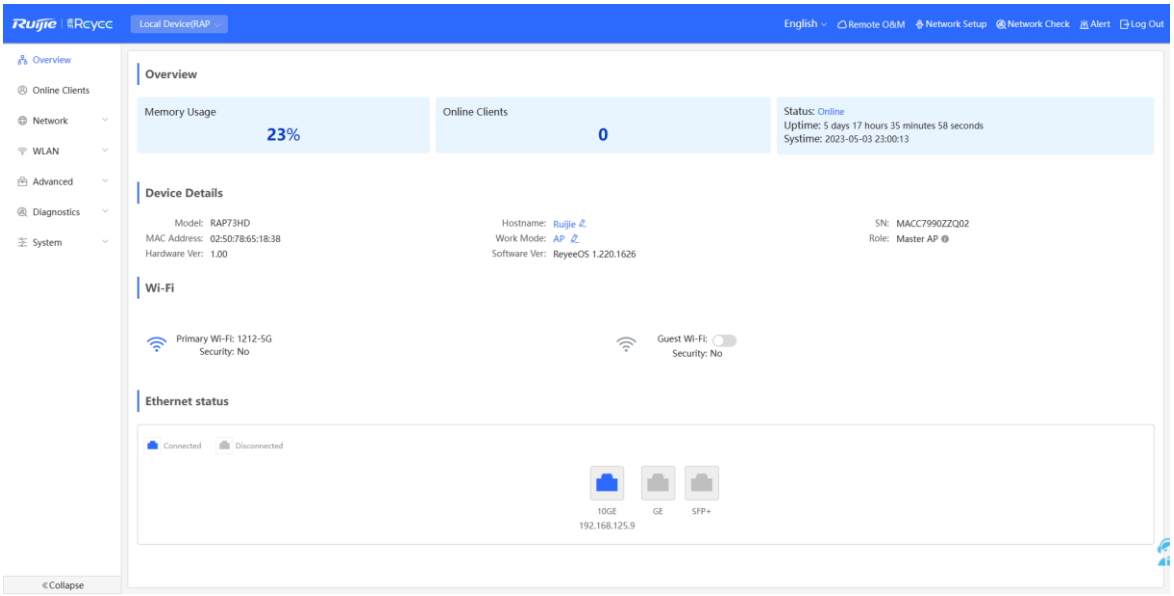
If the self-organizing network is enabled, the device can work in the network mode and the local device mode. The two modes can be switched on the eWeb page.

- **Network** mode: View the management information of all devices in the network, and configure all devices based on network management.
- **Local Device** mode: Only configure the currently logged in devices.

Network mode webpage.

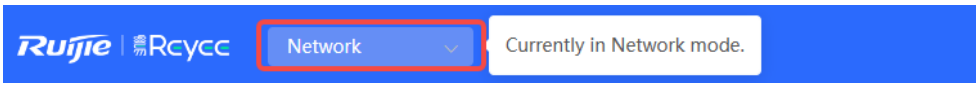


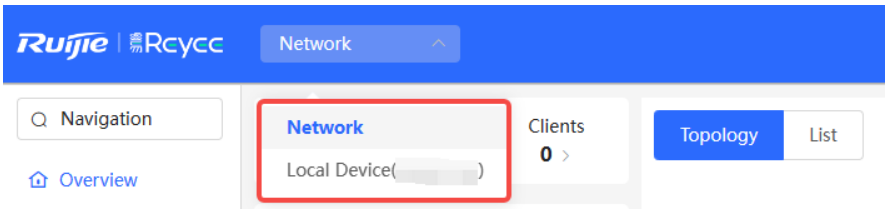
Local Device mode webpage.



2. Switching the Management Mode

Click the current management mode in the navigation bar, and select the mode in the drop-down box to switch the work mode of the device.

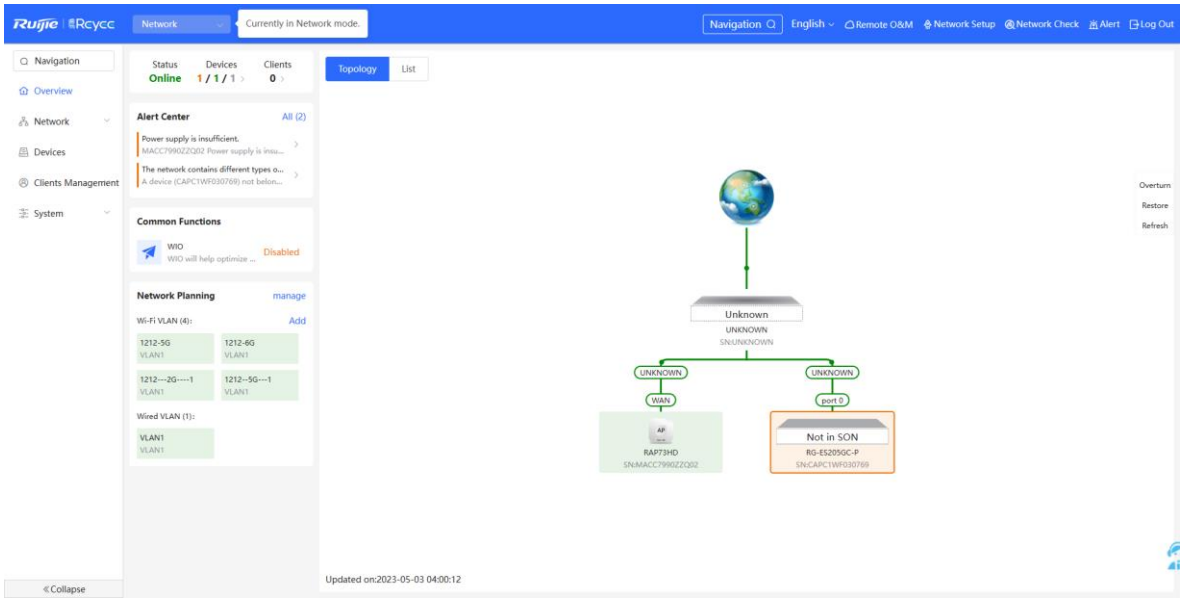



Ruijie | Reyee
Network
Navigation
Overview
Network
Local Device(
)
Clients
0
Topology
List

2 Network Monitoring

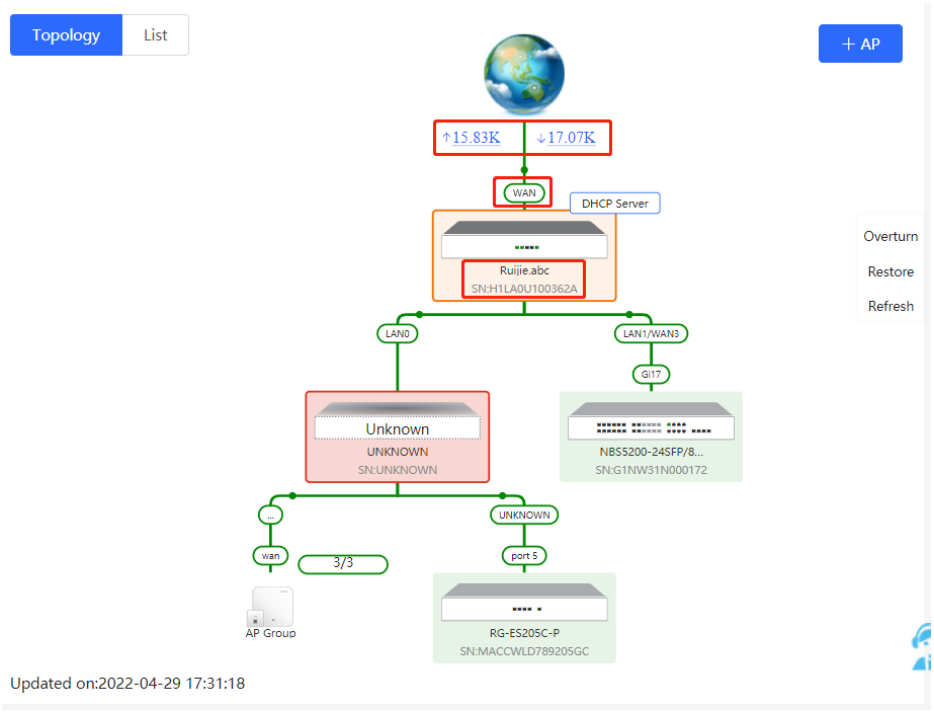
In **Network** mode, select **Overview**.

The **Overview** webpage displays the current network topology, real-time uplink and downlink flow, networking status, and the number of users. The quick access to network and device settings is also provided on the **Overview** webpage. Users can monitor, configure and manage the network status on the current page.

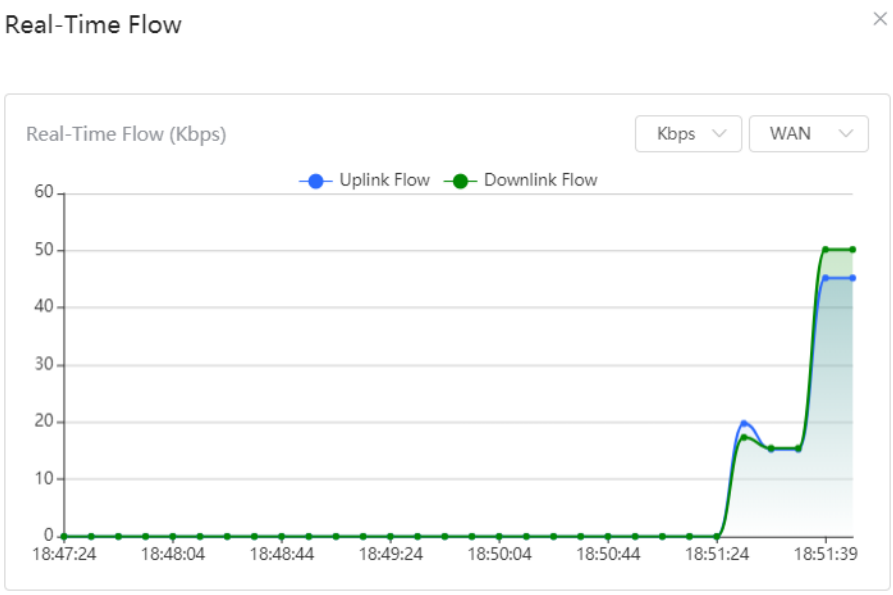


2.1 Viewing the Network Information

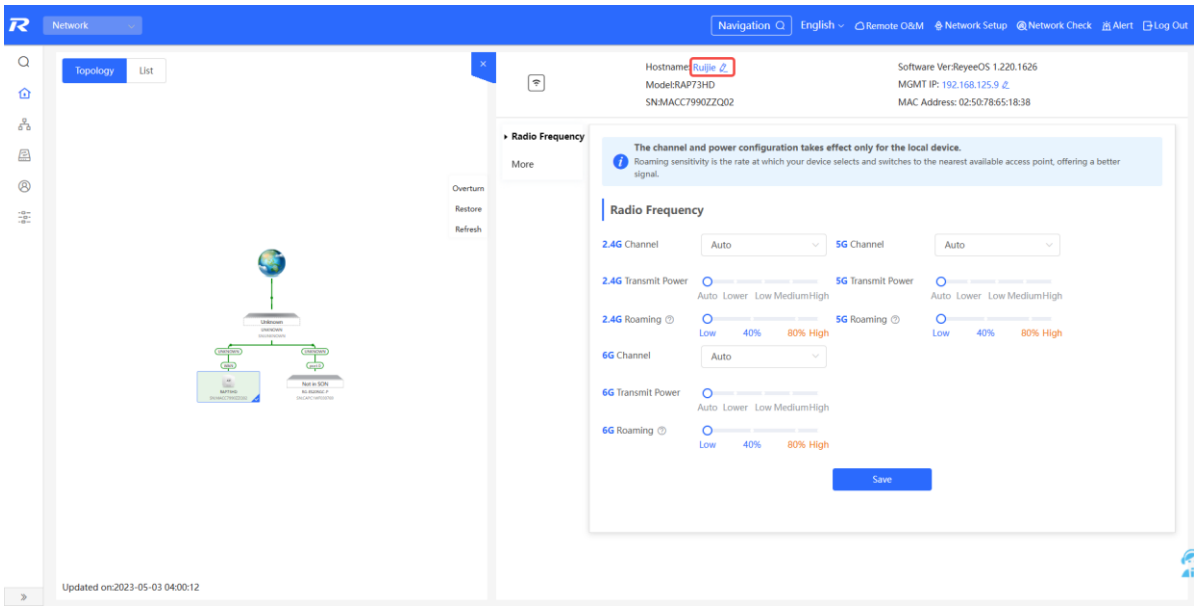
You can view the online device, port ID, device SN as well as the real-time uplink and downlink flow in the network topology.



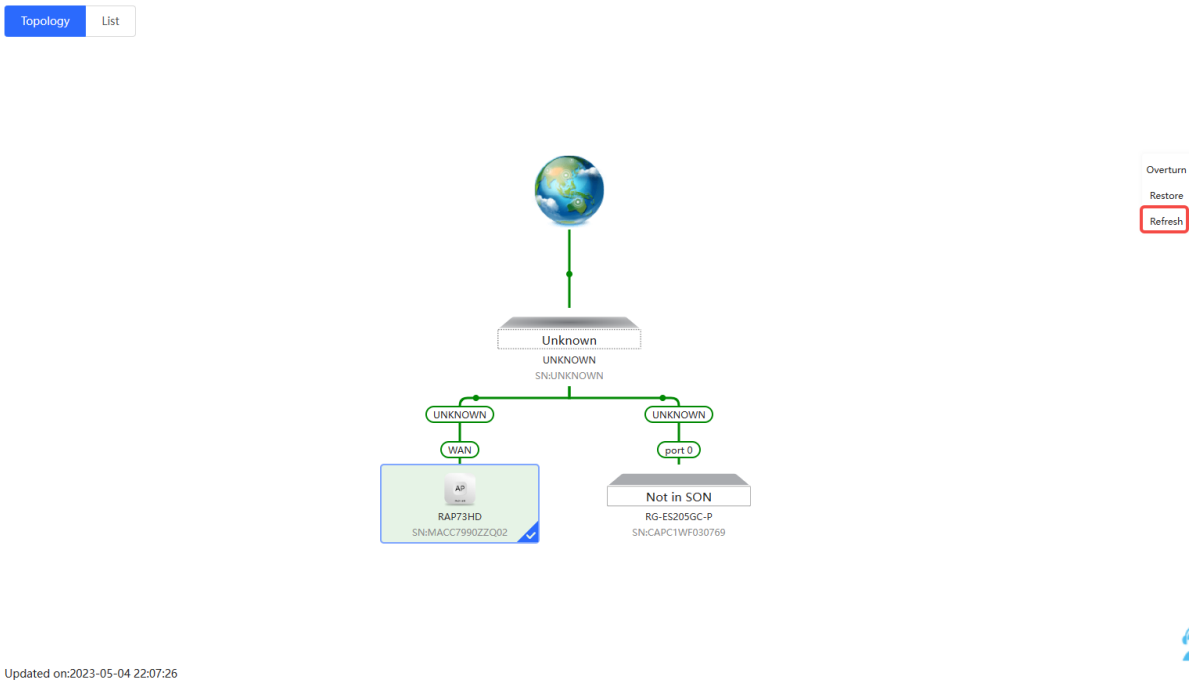
- Click the flow data and view the real-time flow.



- Click the device in the topology to view the operating status and configuration of the device and configure the device functions. The hostname is set to the product model by default. You can click to modify the hostname.



- The update time of the topology is displayed at the bottom left corner. Click **Refresh** to update the topology to the latest status. Please wait for a few minutes for the update.

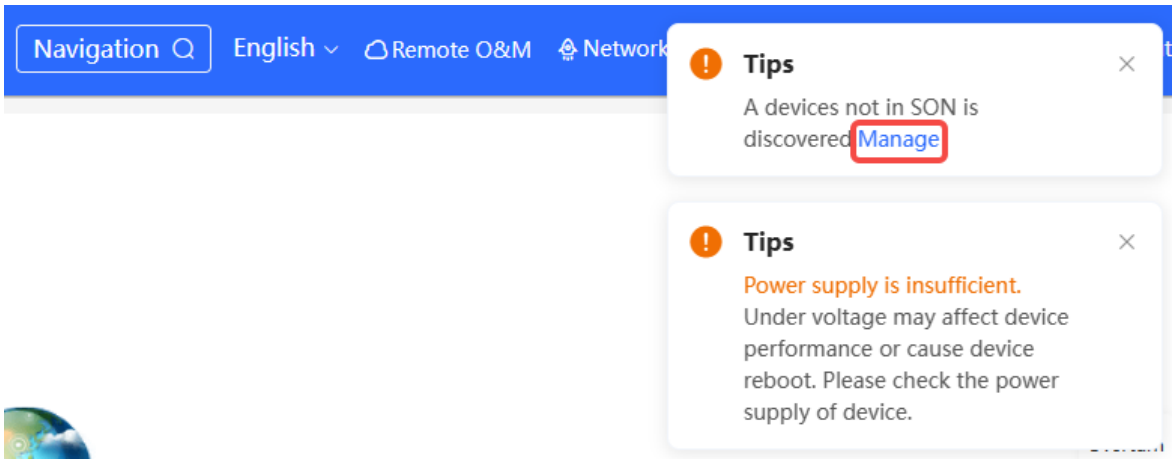


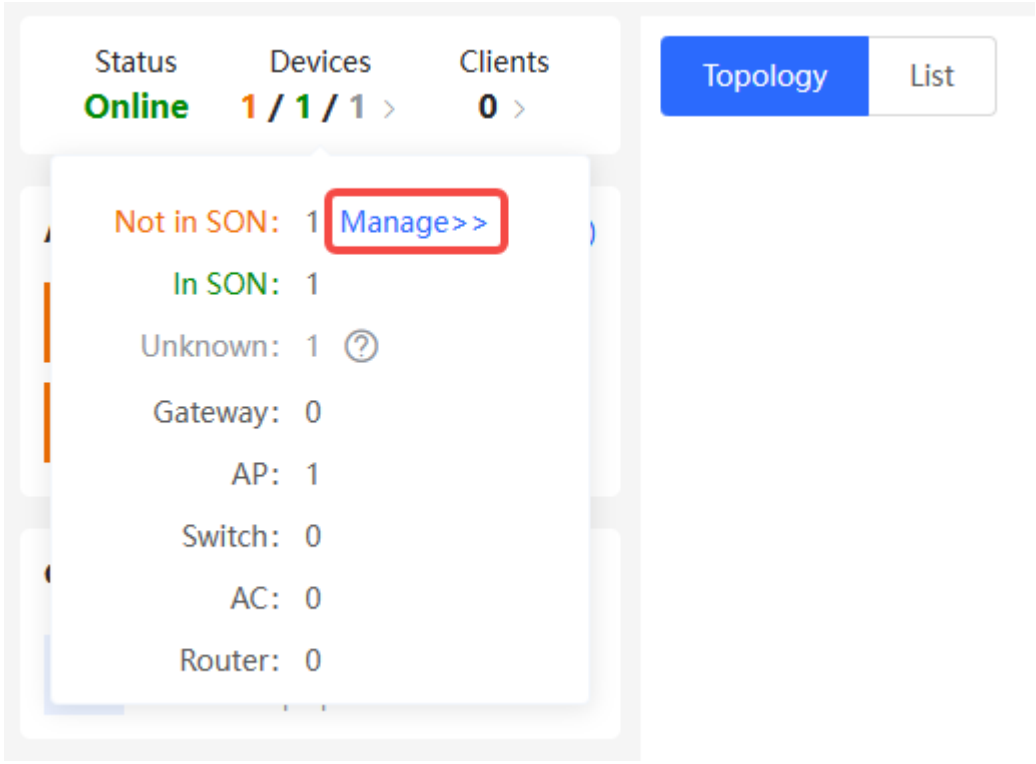
2.2 Adding Network Devices

2.2.1 Wired Connection

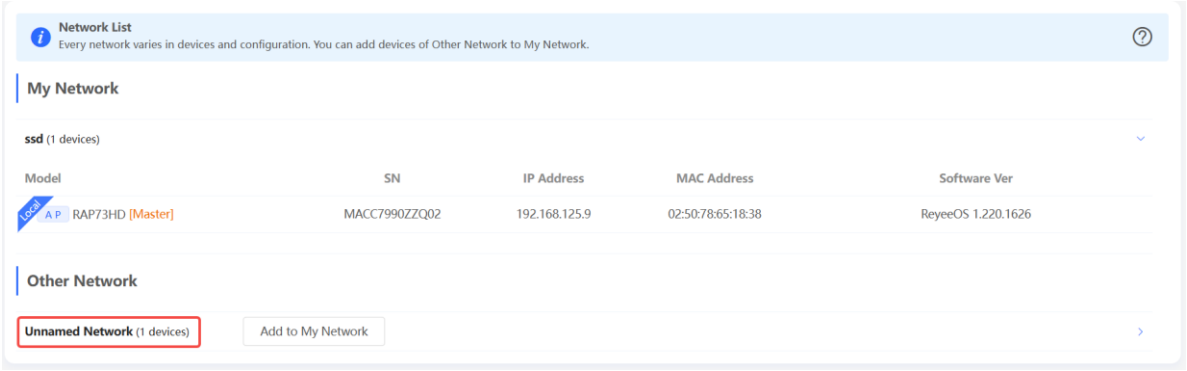
(1) If a new device is connected to the device in the network through wired connection, a prompt message will pop up, indicating that a device not in SON (Self-Organizing Network) is discovered. The number (in

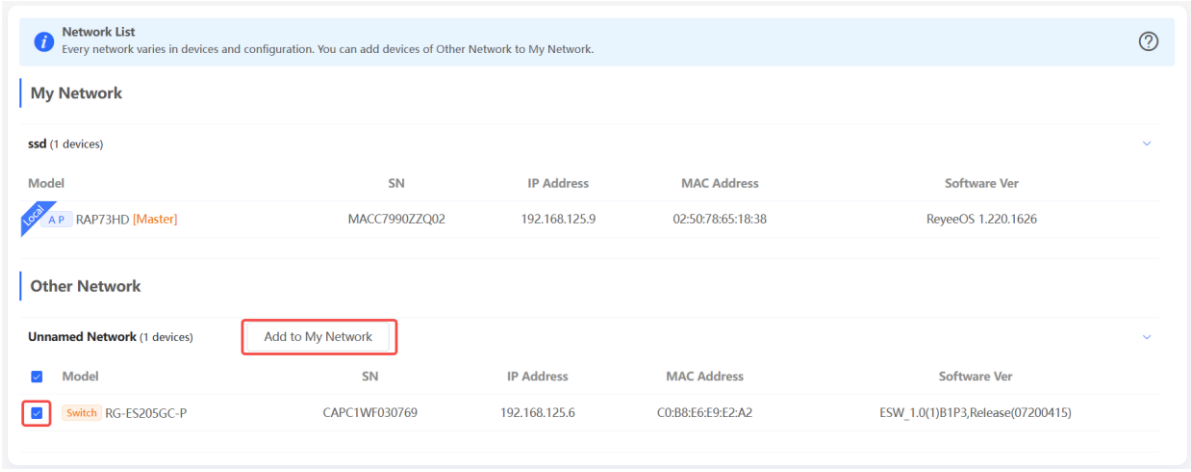
orange) of devices that are not in SON is displayed under the **Devices** at the top left corner of the page. Click **Manage>>** to add the device to the current network.



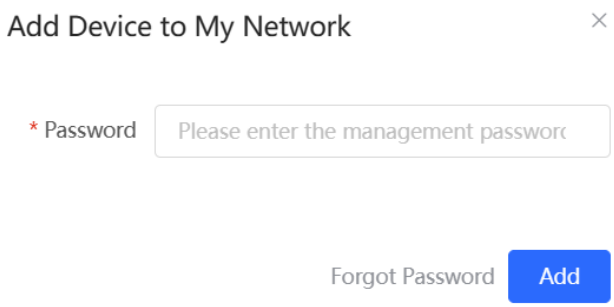


(2) Go to the **Network List** page, click **Other Network** to select the target device and click **Add to My Network**.



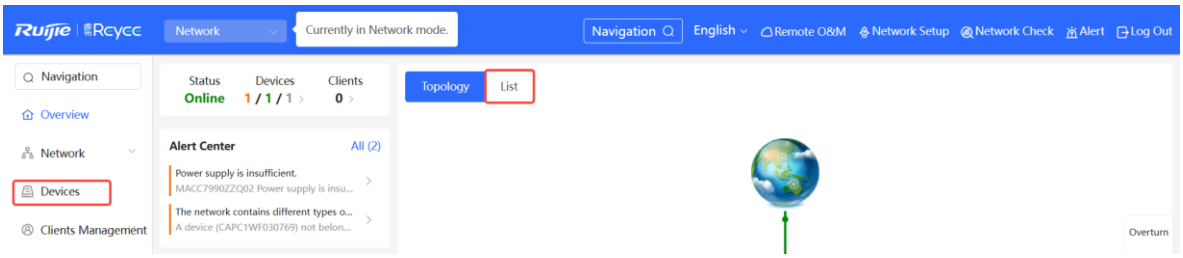


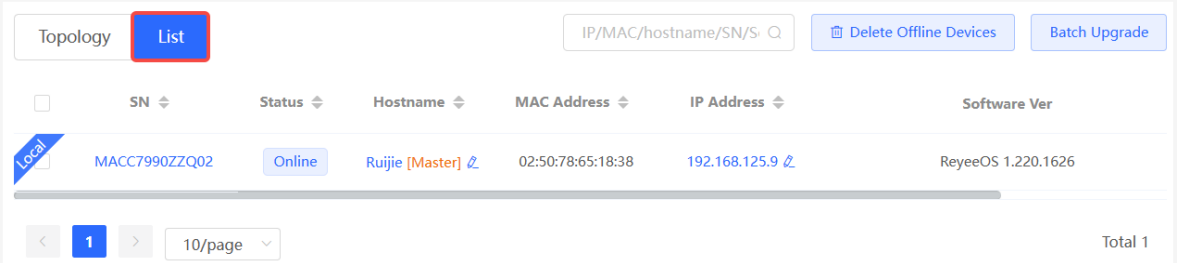
(3) If the target device is not configured yet, you can add the device directly without a password. If the device is configured with a password, please enter the management password of the device. If the password is incorrect, the device cannot be added to the network.



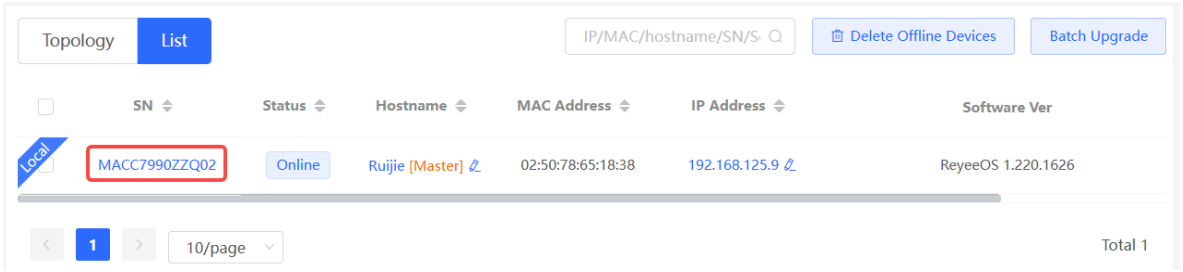
2.3 Managing Network Devices

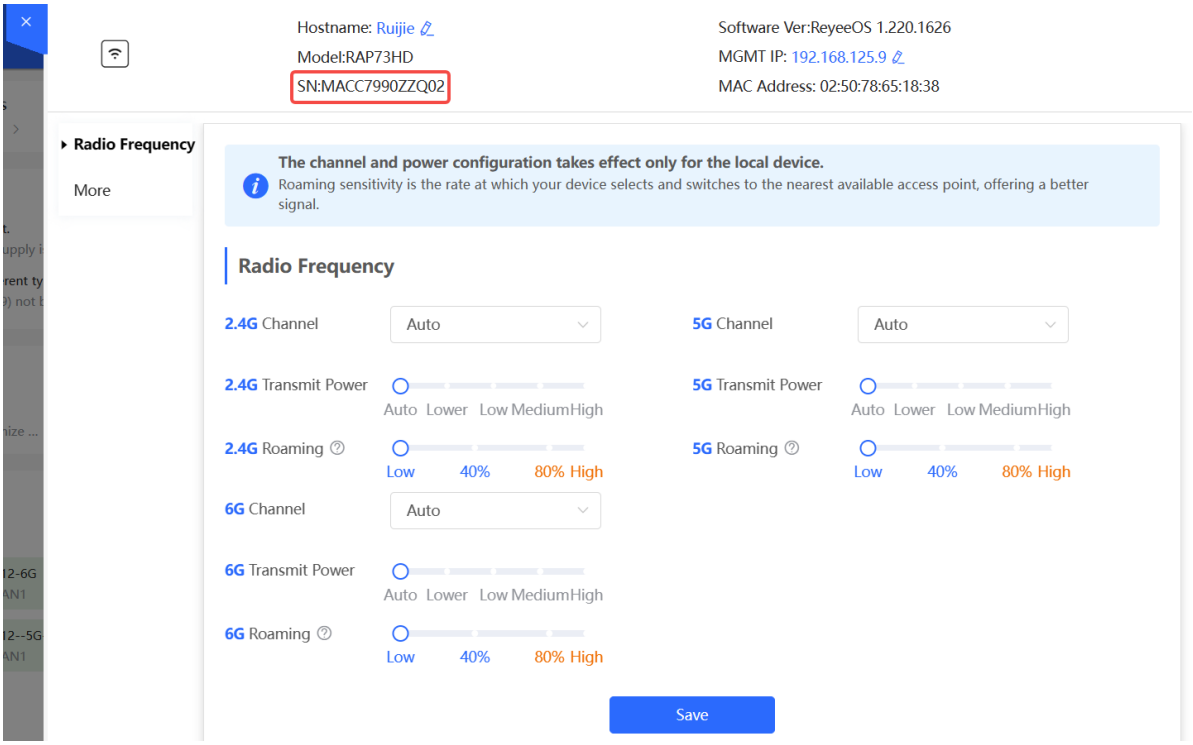
Click **List** at the top left corner of the topology or click **Devices** in the menu bar to switch to the device list view, and view the information of all devices in the self-organizing network (SON). You can perform configurations and management on all devices by logging in to only one device in the network.



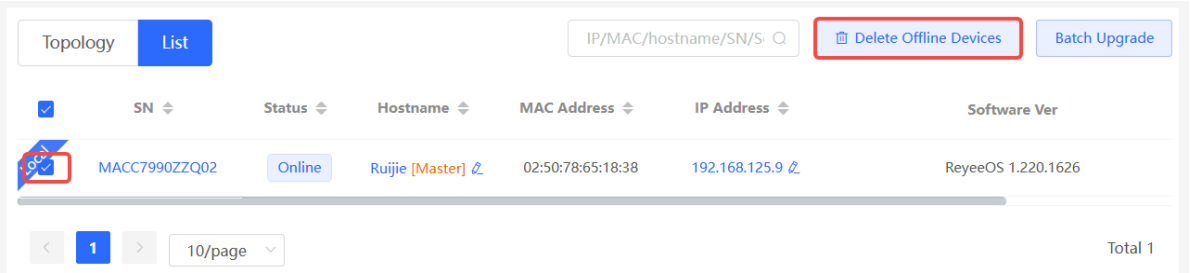


- Click **SN** to configure the specified device.



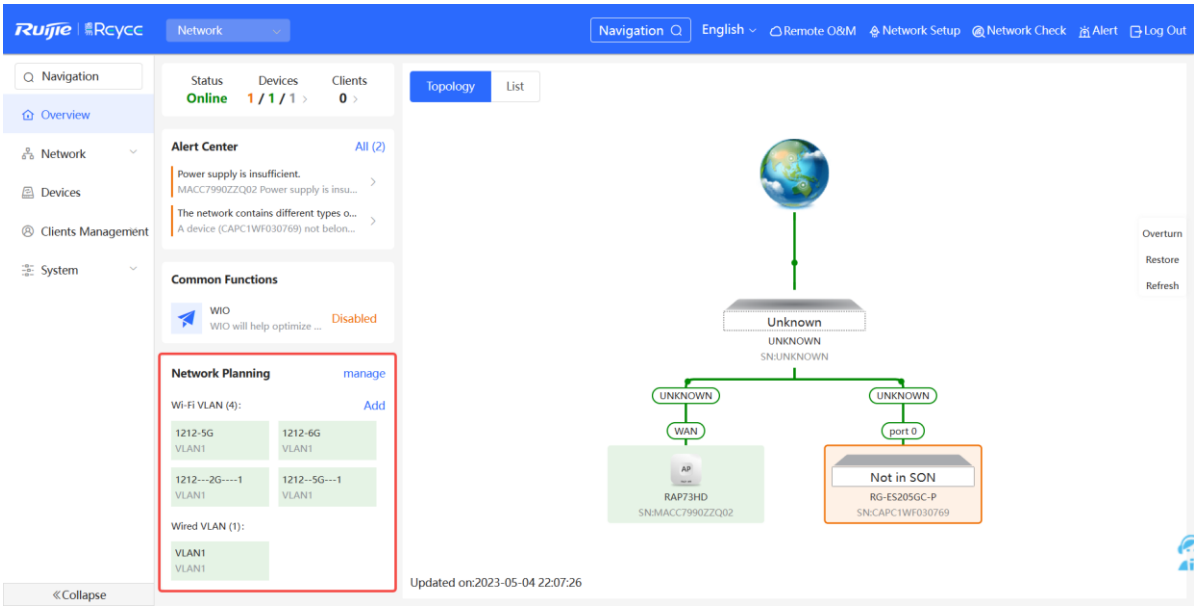


- Select the offline device and click **Delete Offline Devices** to remove the device from the list and the topology.

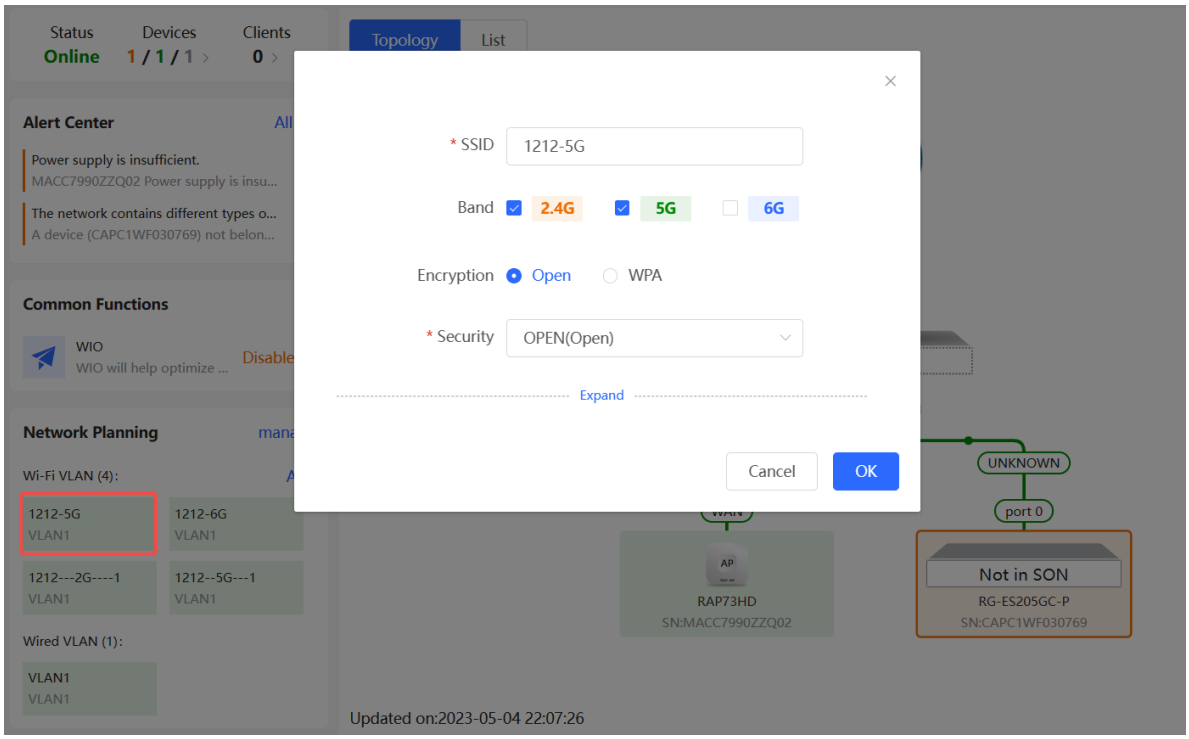


2.4 Configuring Network Planning

The **Overview** page displays the configuration of **Network Planning** at the bottom left corner, including **Wi-Fi VLAN** and **Wired VLAN**.



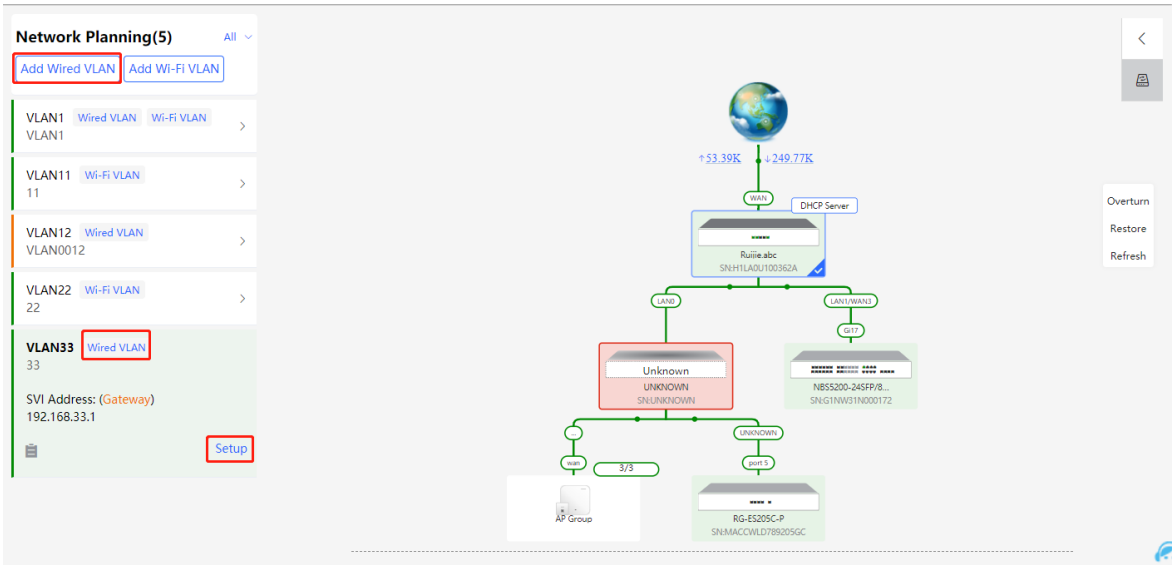
- Click **manage** to go to the **Network Planning** page for configuration (**Network** > **Network Planning**). You can add or edit the **Network Planning** configuration for the live network.
- Click **Add** to configure **Wi-Fi VLAN** or **Wired VLAN** for the live network.
- Click the SSID to edit the Wi-Fi configuration. For details, see Chapter 3 Wi-Fi Network Settings.



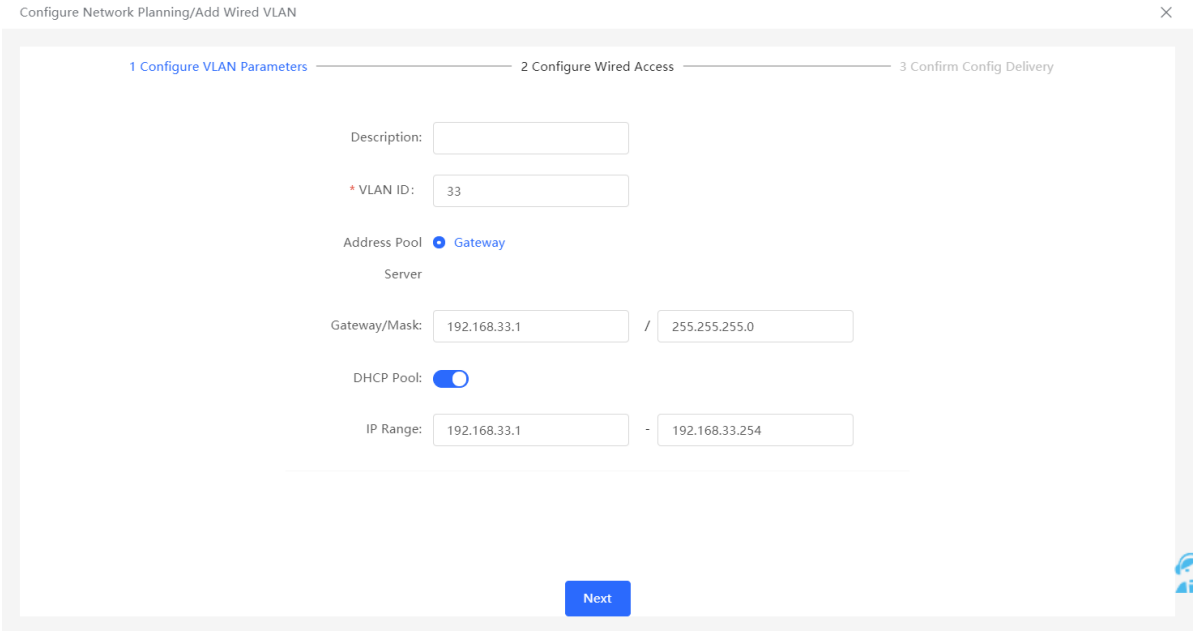
2.4.1 Configuring Wired VLAN

(1) Go to the **Wired VLAN** page for configuration.

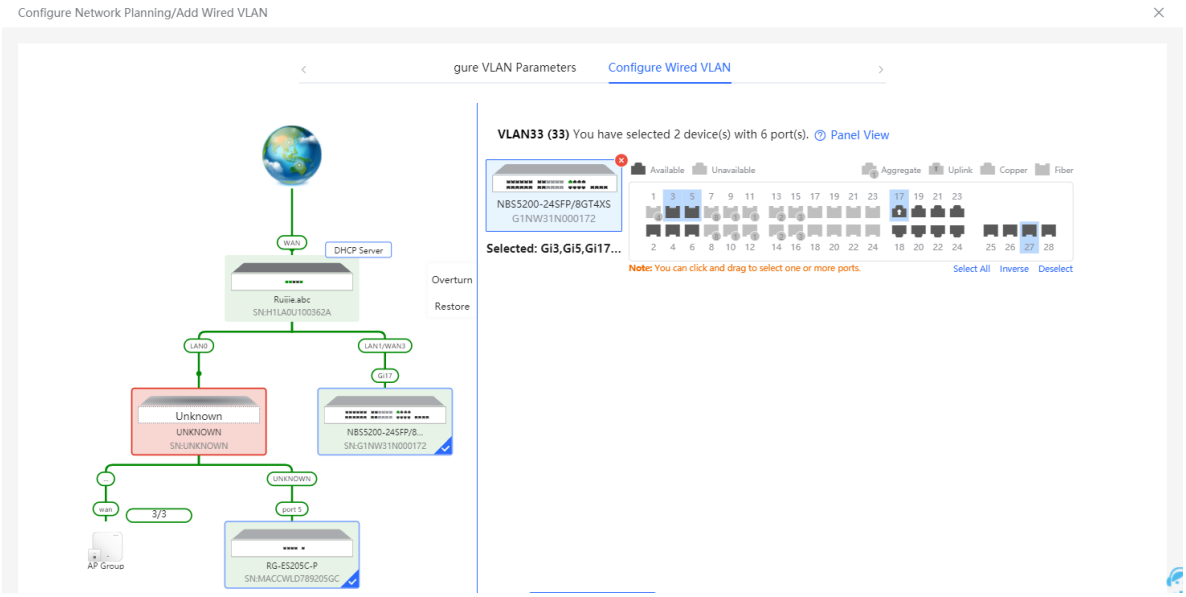
- Method 1: Click **Add** beside **Wired VLAN** in the **Network Planning** area on the **Overview** page to add the wired VLANs.
- Method 2: Click **manage** in the **Network Planning** area on the **Overview** page to go to the **Network Planning** page for configuration (**Network** > **Network Planning**). Click **Add Wired VLAN** to add the wired VLANs to the live network or select the available wired VLANs. Click **Setup** to configure the wired VLANs.



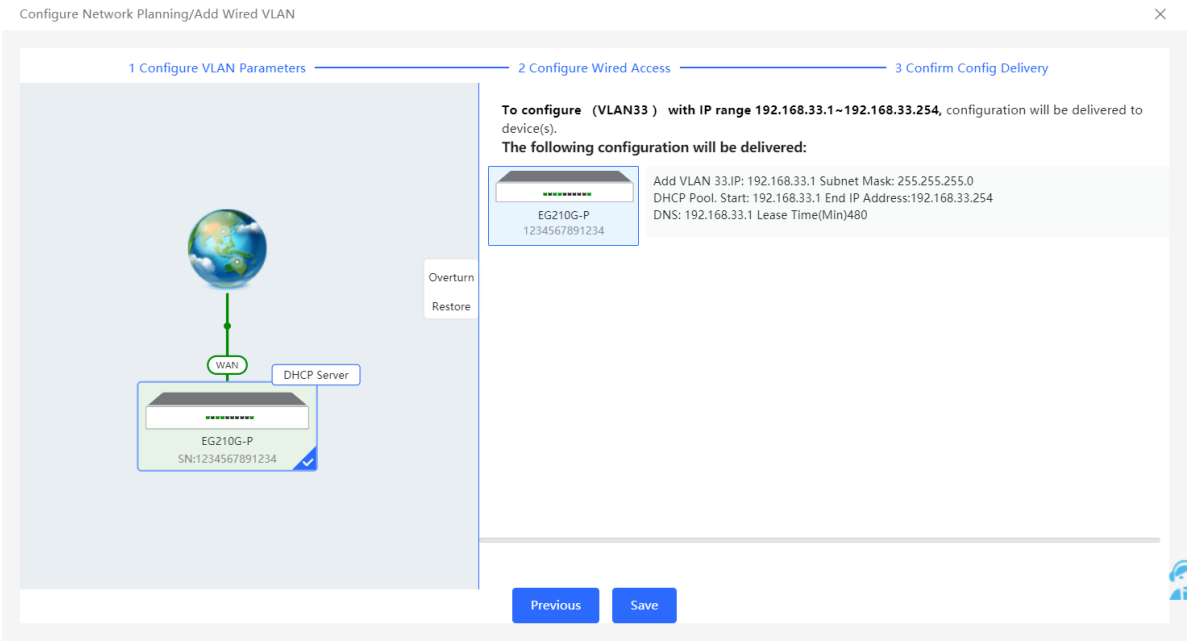
(2) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.



(3) Select the target switch in the topology and all member ports in the VLAN, and click **Next**.



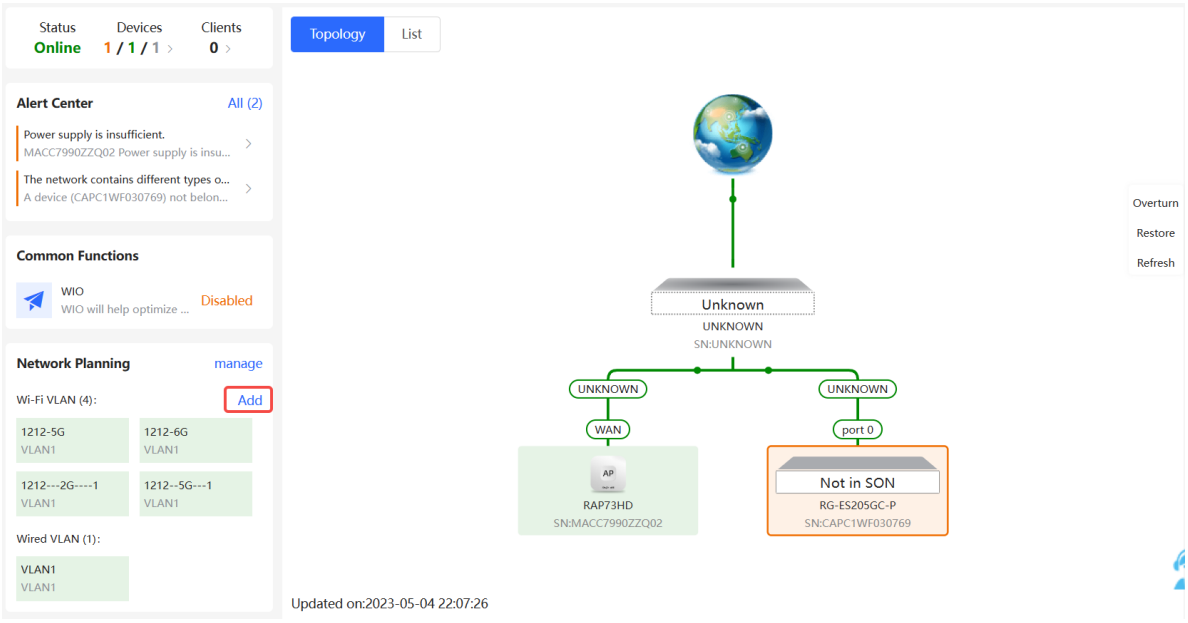
(4) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



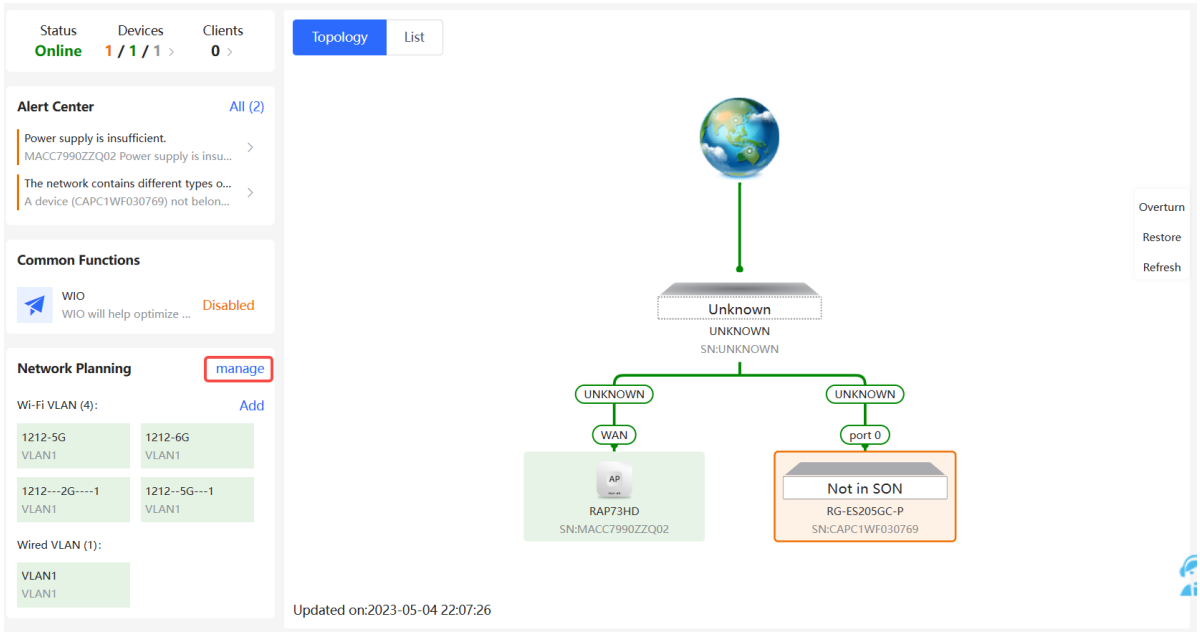
2.4.2 Configuring Wi-Fi VLAN

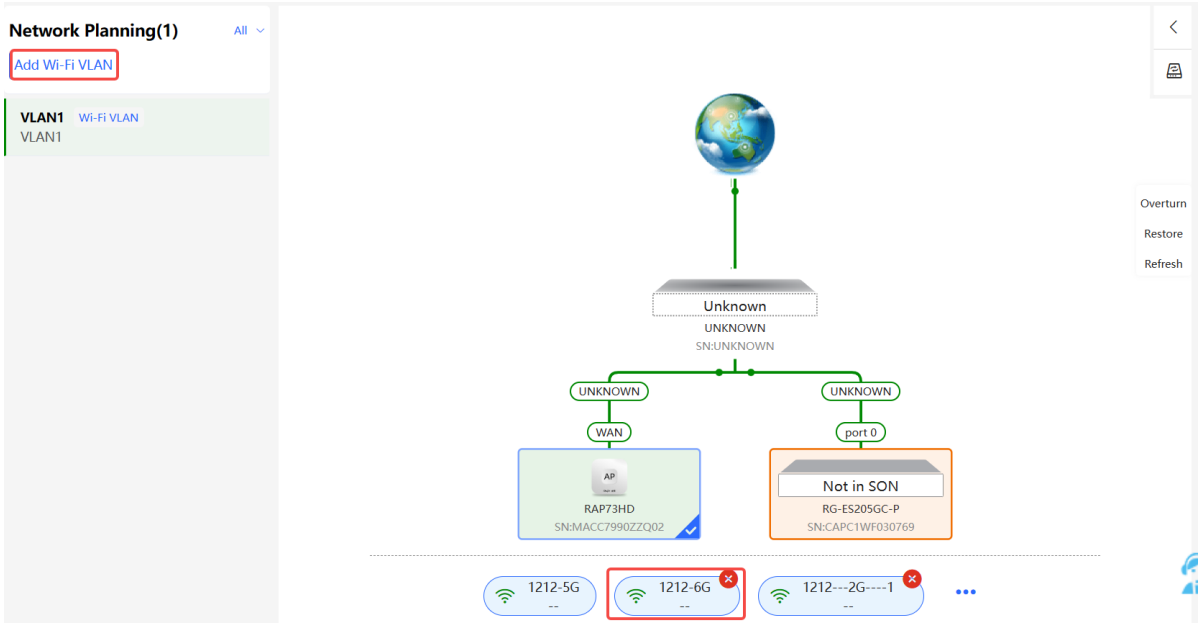
(1) Go to the **Wired VLAN** page for configuration.

- Method 1: Click **Add** beside **Wi-Fi VLAN** in the **Network Planning** area on the **Overview** page to add the Wi-Fi VLANs.

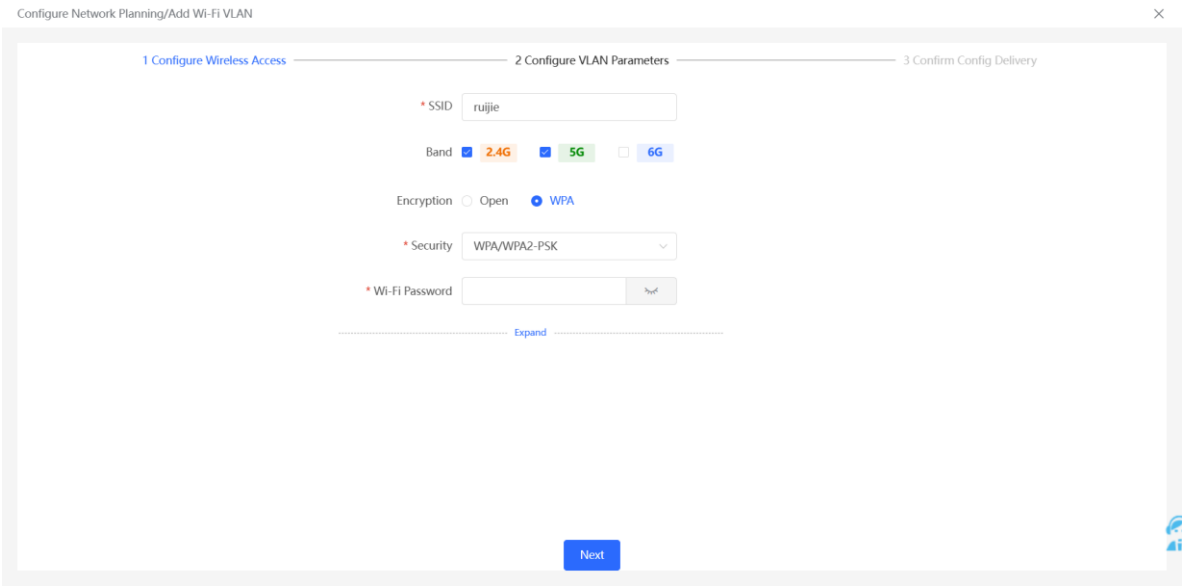


- Method 2: Click **manage** in the **Network Planning** area on the **Overview** page to go to the **Network Planning** page for configuration (**Network** >> **Network Planning**). Click **Add Wi-Fi VLAN** to add the Wi-Fi VLANs to the live network or select the available Wi-Fi VLANs.

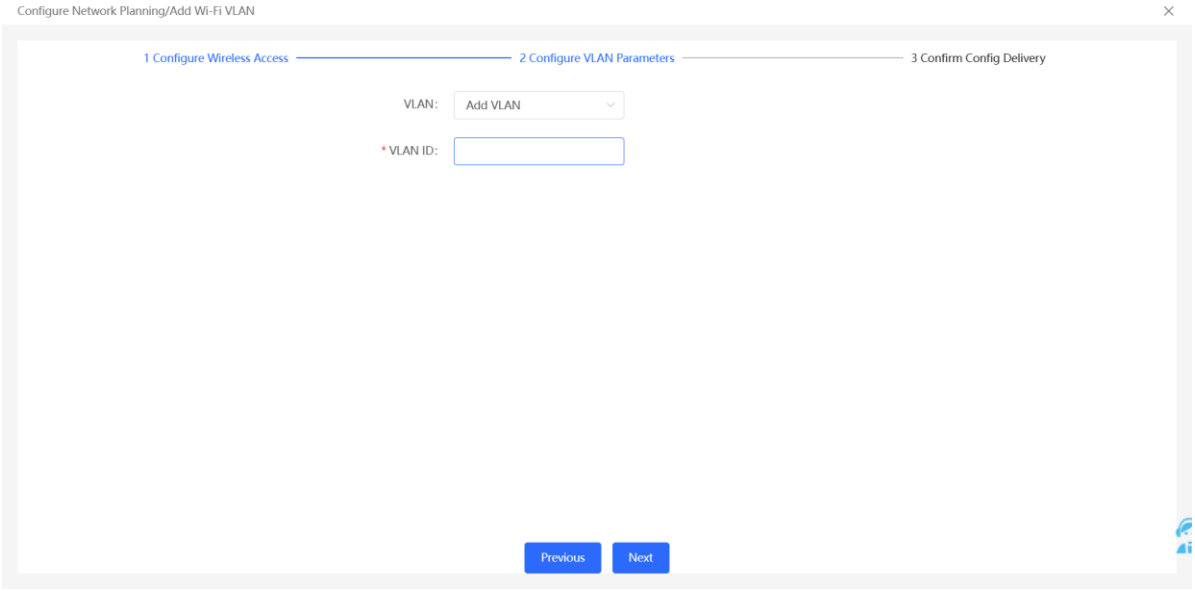




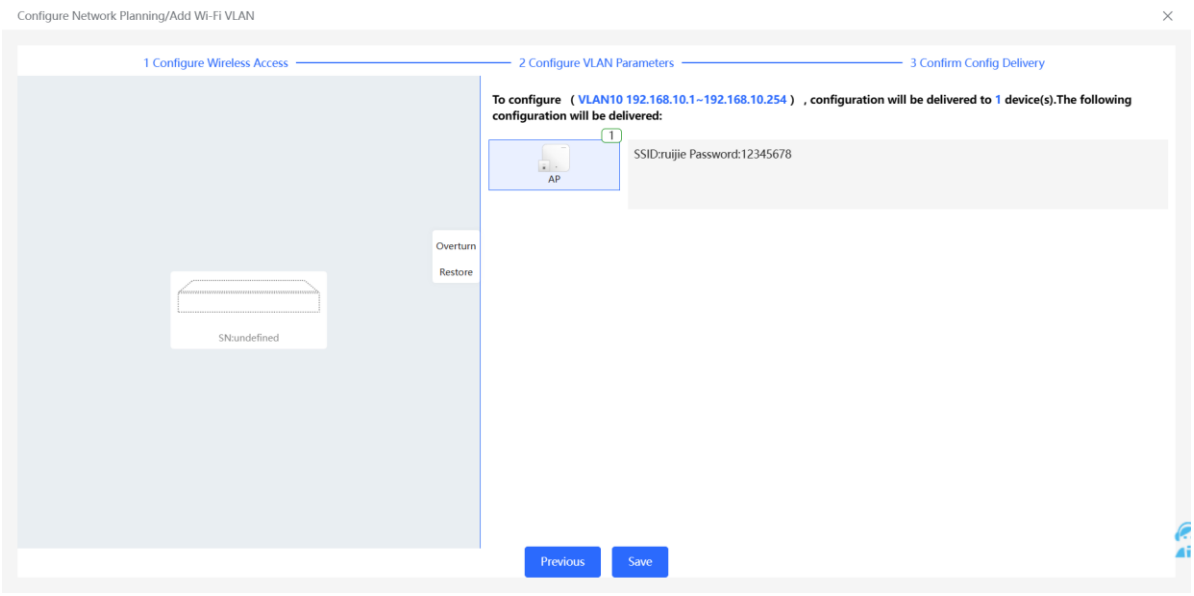
(1) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.



(2) Configures the VLAN and VLAN ID for wireless access.

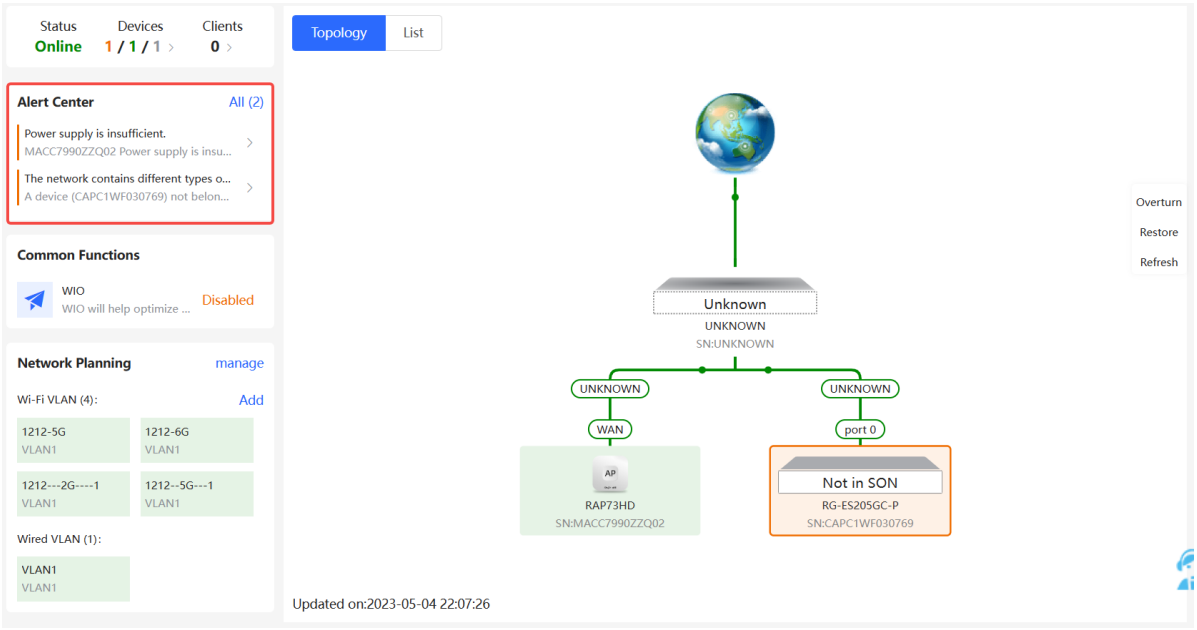


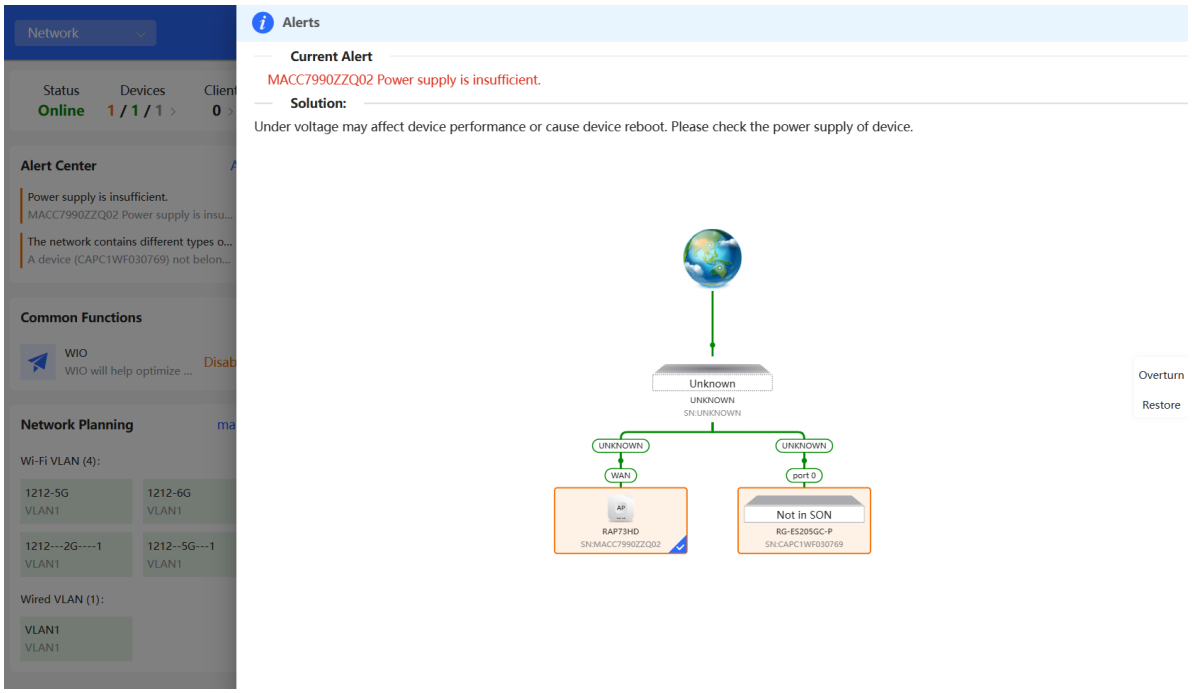
(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



2.5 Troubleshooting Fault Alerts

The **Overview** page displays the fault alerts and handling suggestions if faults occur in the network. Click the fault alert in **Alert Center** to view the faulty device, fault details and handling suggestions, and troubleshoot device faults by referring to the handling suggestions.




Network
Status
Online
Devices
1 / 1 / 1
Client
0
Alert Center
Power supply is insufficient.
MACC7990ZZQ02 Power supply is insu...
The network contains different types o...
A device (CAPC1WF030769) not belon...
Common Functions
WIO
WIO will help optimize ...
Disab
Network Planning
ma
Wi-Fi VLAN (4):
1212-5G
VLAN1
1212-6G
VLAN1
1212---2G----1
VLAN1
1212--5G---1
VLAN1
Wired VLAN (1):
VLAN1
VLAN1
Alerts
Current Alert
MACC7990ZZQ02 Power supply is insufficient.
Solution:
Under voltage may affect device performance or cause device reboot. Please check the power supply of device.
Unknown
UNKNOWN
SN:UNKNOWN
UNKNOWN
UNKNOWN
WAN
port 0
AP
RAP73HD
SN:MACC7990ZZQ02
Not in SON
RG-ES205GC-P
SN:CAPC1WF030769
Overturn
Restore

3 Wi-Fi Network Settings

Note

Wi-Fi network settings covers the Wi-Fi settings of the currently logged in devices and the management of all wireless devices in the network. In **Network** mode, the Wi-Fi network settings are synchronized to all wireless devices in the network. You can configure device groups to limit the synchronization range. For details, see Configuring AP Groups.

3.1 Configuring AP Groups

3.1.1 Overview

After the self-organizing network is enabled, the device can act as the master AP/AC to perform batch configuration and management on the downlink APs in groups. Group the APs before the configurations are delivered.

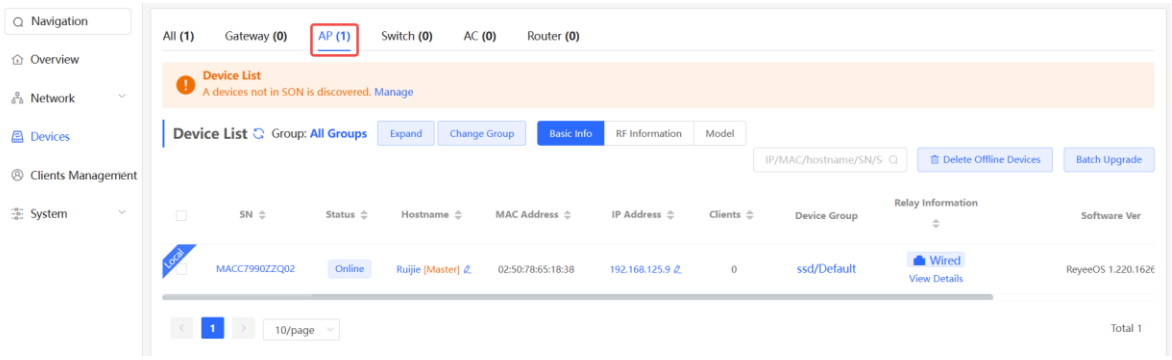
Note

If you specify a group when setting up a wireless network, the corresponding configuration will take effect on the wireless devices in the specified group.

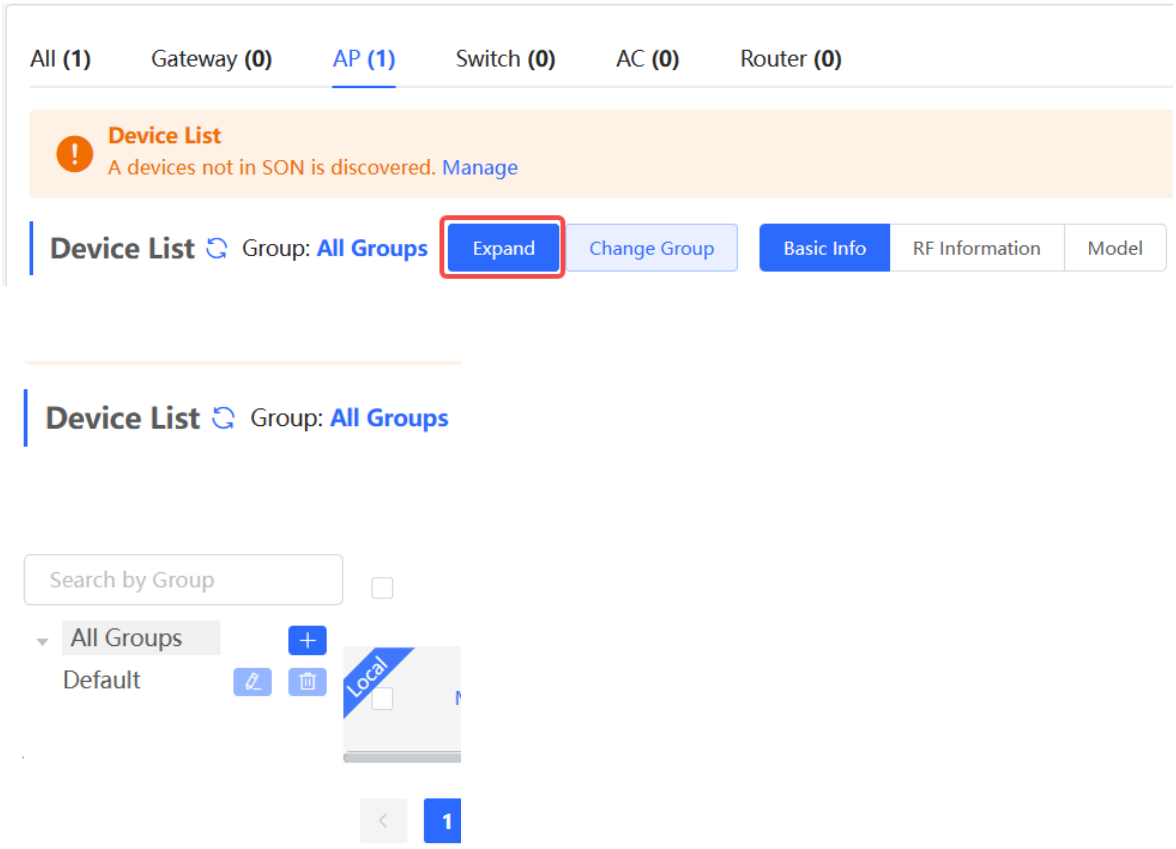
3.1.2 Procedures

In **Network** mode, choose **Devices** >> **AP**

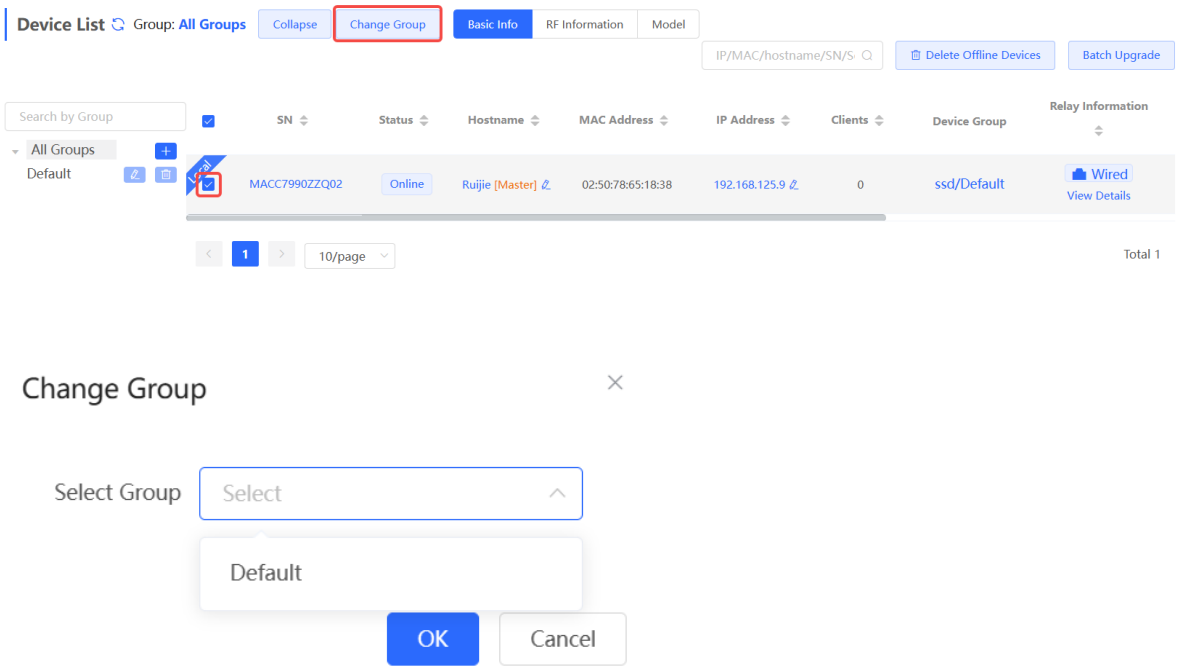
(1) View the information of all APs in the current network, including the basic information, RF information and models. You can click **SN** to configure the device.



(2) Click **Expand** to view all groups on the left part of the **Device List** page. Click + to create a new group. Up to 8 groups can be added. You can click to edit the group name and click to delete the group. The default group cannot be deleted and its name cannot be edited.



(3) Click the group name on the left part to view all devices in this group. A device can only belong to a group. By default, all devices belong to the default group. Select an entry in the list and click **Change Group** to move the target device to a specified group, and then the device will apply the configurations of this group. Click **Delete Offline Devices** to remove the offline device from the list.



3.2 Configuring SSID and Wi-Fi Password

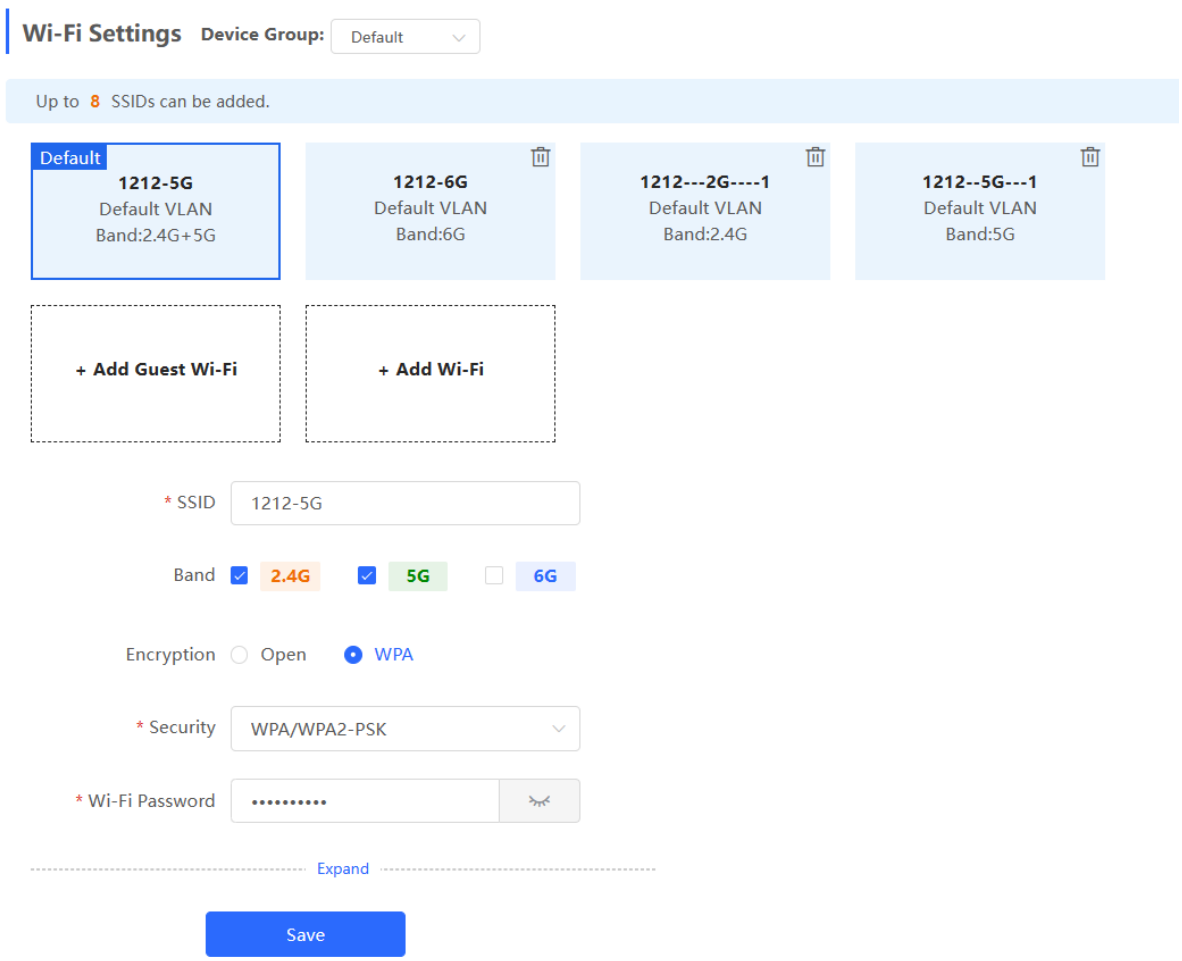
(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click the target Wi-Fi network, change the SSID and Wi-Fi password of the Wi-Fi network, and click Save. The "Open" encryption type indicates that the Wi-Fi network is an open network where wireless clients can connect to the Internet without a password, while the "WPA" encryption signifies a password-protected Wi-Fi network where wireless clients need to provide a password for accessing the Internet. The password is 8-16 characters long. Only letters, numbers and special characters <=>[]!@#$*(). are allowed.

Caution

After the configuration is saved, all online clients will be disconnected from the Wi-Fi network. You have to enter the new password to connect to the Wi-Fi network.



3.3 Hiding the SSID

3.3.1 Overview

Hiding the SSID can prevent unauthorized clients from accessing the Wi-Fi network and enhance network security. After this function is enabled, the mobile phone or PC cannot search out the SSID. Instead, you have to manually enter the correct SSID and Wi-Fi password. Remember the SSID so that you can enter the correct SSID after the function is enabled.

3.3.2 Configuration Steps

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi >**> **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, turn on **Hide SSID** in the expanded settings and click **Save**.

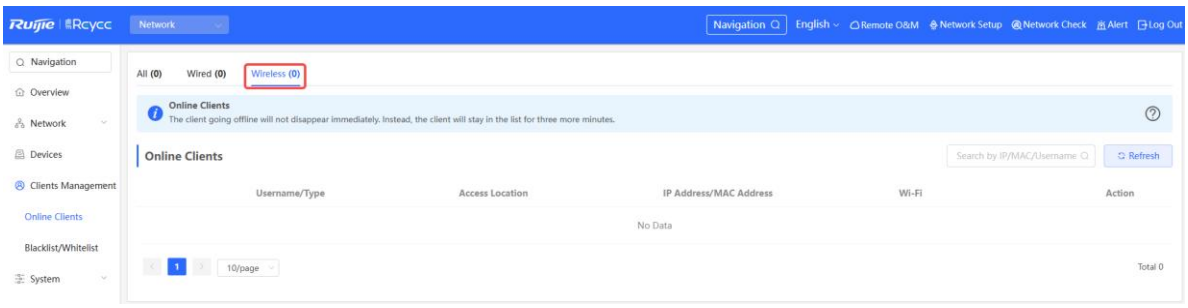
Caution

After the configuration is saved, you have to manually enter the SSID and Wi-Fi password before connecting any device to the Wi-Fi network. Therefore, exercise caution when performing this operation.

3.4 Checking Wireless Clients

If the self-organizing network is disabled, choose **WLAN** > **Clients**

If the self-organizing network is enabled, in **Network** mode, choose **Clients Management** >> **Online Clients** >> **Wireless**

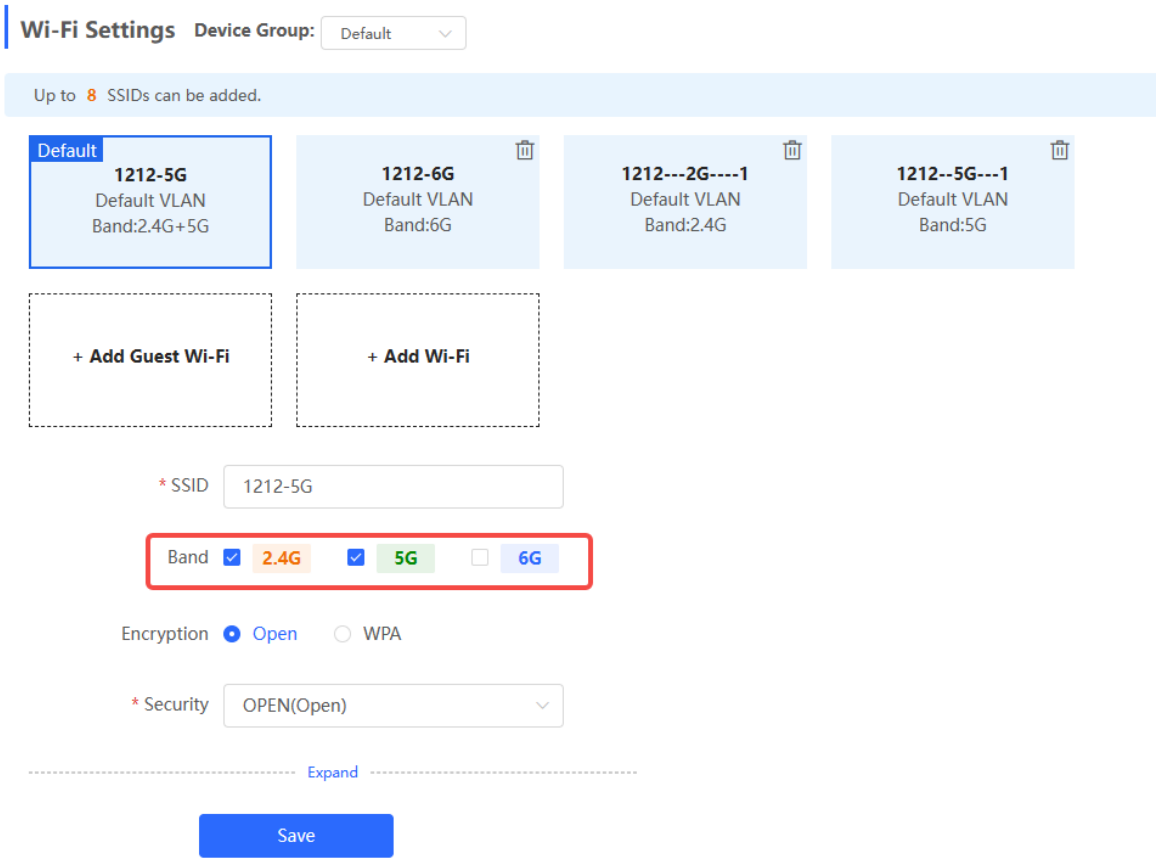


3.5 Configuring Wi-Fi Band

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Set the frequency band for the Wi-Fi signal. Both the 2.4 GHz, 5 GHz, and 6 GHz frequency bands are supported. The 6 GHz frequency band has a faster transmission rate and less interference compared to the 2.4 GHz and 5 GHz frequency bands, but it is usually not as good as the 2.4 GHz and 5 GHz frequency bands in terms of signal coverage and wall penetration. The 5 GHz frequency band has a faster transmission rate and less interference compared to the 2.4 GHz frequency band, but it is usually not as good as the 2.4 GHz frequency band in terms of signal coverage and wall penetration. You can select the signal frequency band according to the actual needs. The default frequency band is 2.4 GHz + 5 GHz or 6 GHz. When 2.4 GHz + 5 GHz is selected, Wi-Fi signals are emitted simultaneously in the 2.4 GHz and 5 GHz frequency bands. When 6 GHz is selected, Wi-Fi signals are broadcasted in the 6GHz frequency band.



3.6 Configuring Band Steering

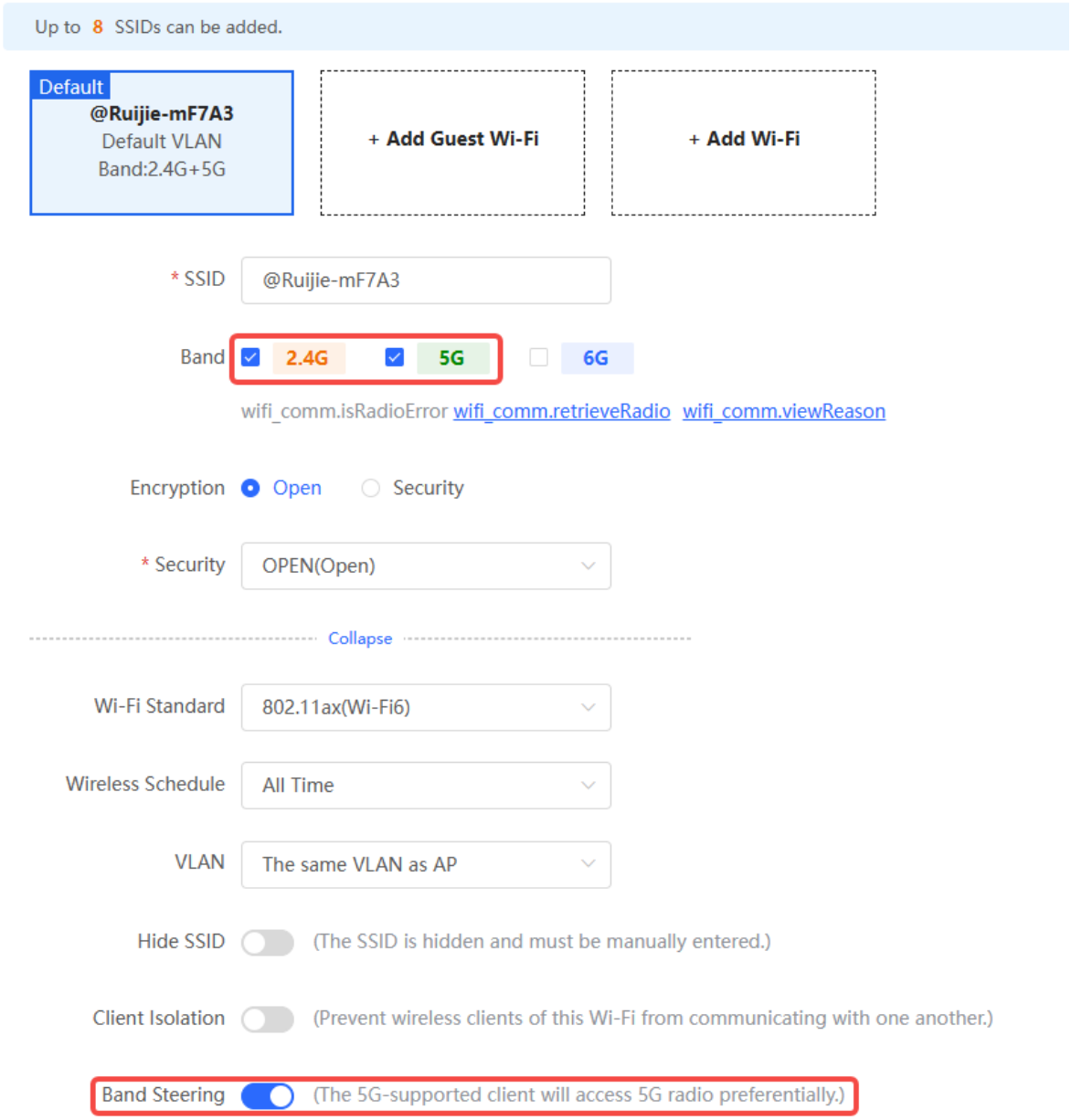
Caution

This function can be enabled only after the dual-band integration (**Band** is set to **2.4G + 5G**) is enabled on the Wi-Fi network. A client automatically selects a band only when the SSIDs of the 2.4 GHz and 5 GHz bands are the same.

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi >> Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Collapse**, turn on **Band Steering** in the expanded settings, and click **Save**. After the function is enabled, the client supporting 5 GHz selects the 5G Wi-Fi network preferentially.



3.7 Configuring Wi-Fi 6

Caution

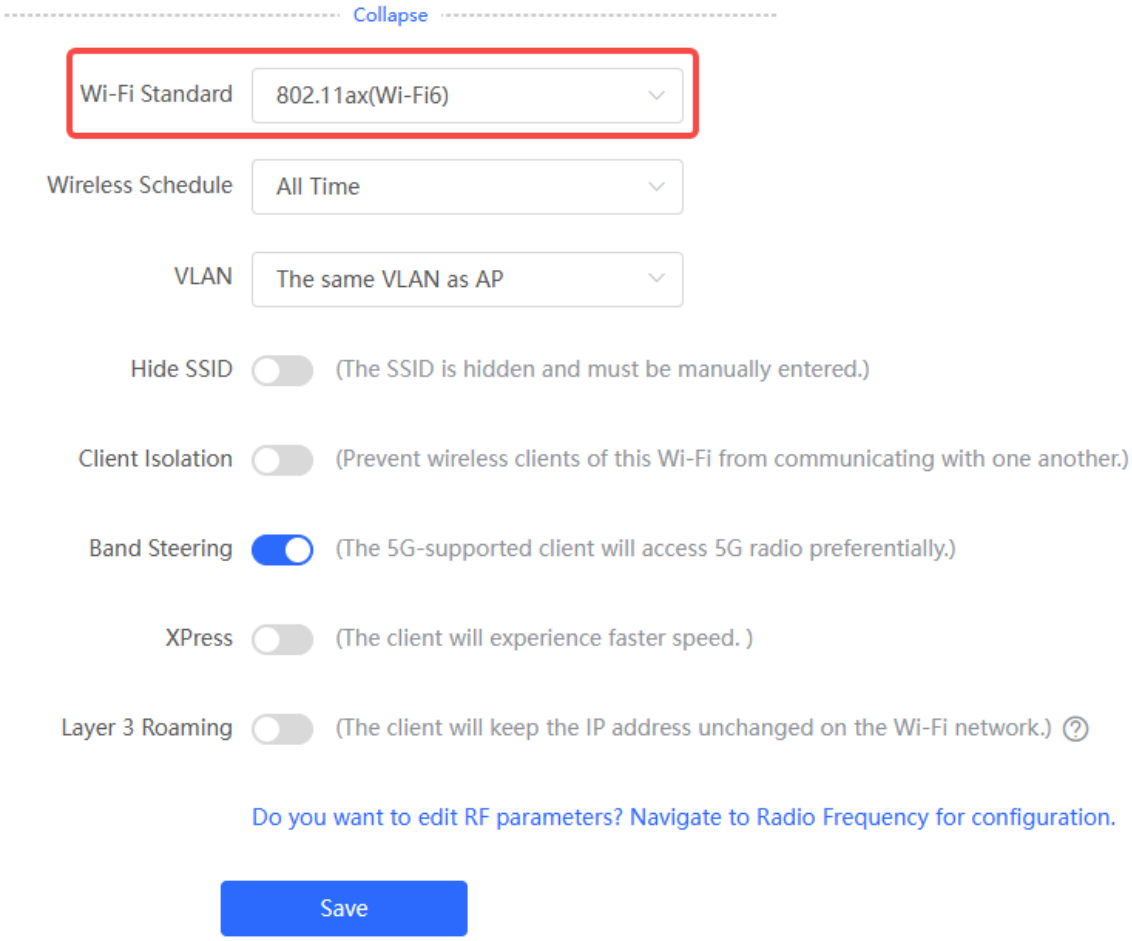
The function takes effect only on APs supporting the IEEE 802.11ax protocol. In addition, access clients must support IEEE 802.11ax so that clients can enjoy high-speed Internet access experience brought by Wi-Fi 6. If clients do not support Wi-Fi 6, you can disable this function.

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi Settings**. Select the target Wi-Fi.

- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Advanced Settings**, select **802.11ax(Wi-Fi6)** as the Wi-Fi standard, and click **Save**. Once done, configure the wireless mode to Wi Fi 6, which enables faster Internet speeds for wireless users for better network experience.



3.8 Configuring Wi-Fi 7

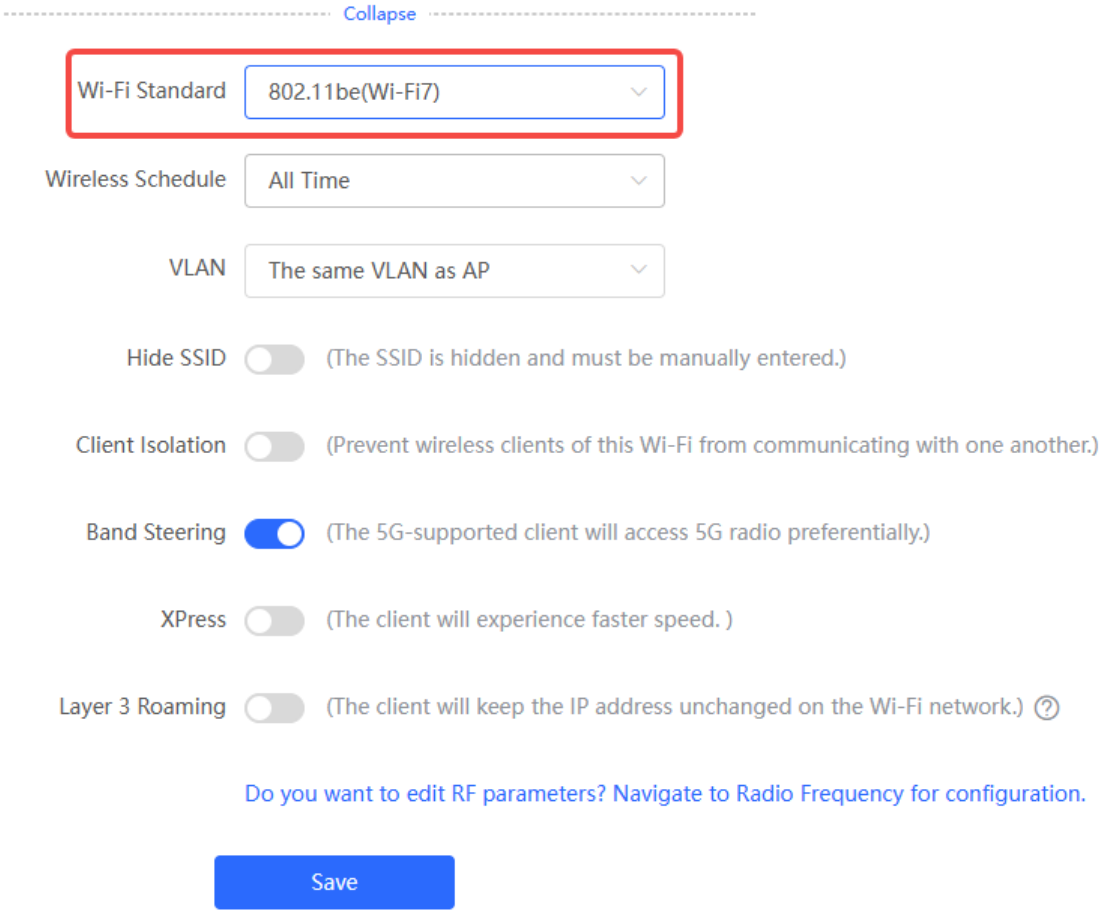
Caution

This configuration is only applicable to access points that support the 802.11be protocol, and the connected STAs must also support the 802.11be protocol.

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(1) Click **Advanced Settings**, select **802.11be(Wi-Fi7)** as the Wi-Fi standard, and click **Save**.

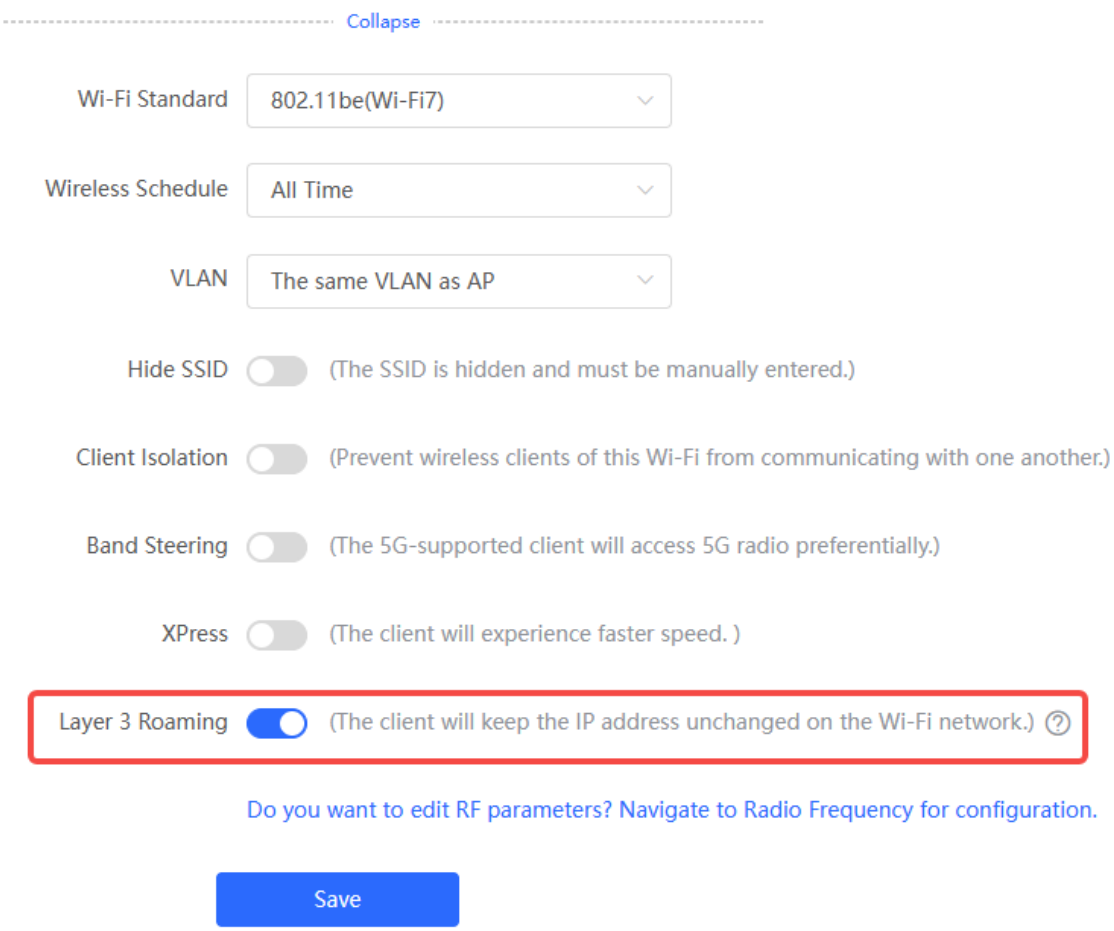


3.9 Configuring Layer-3 Roaming

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi >> Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Collapse**, turn on **Layer 3 Roaming** in the expanded settings and click **Save**. The client will keep the IP address unchanged in this Wi-Fi network, improving roaming experience across VLANs.

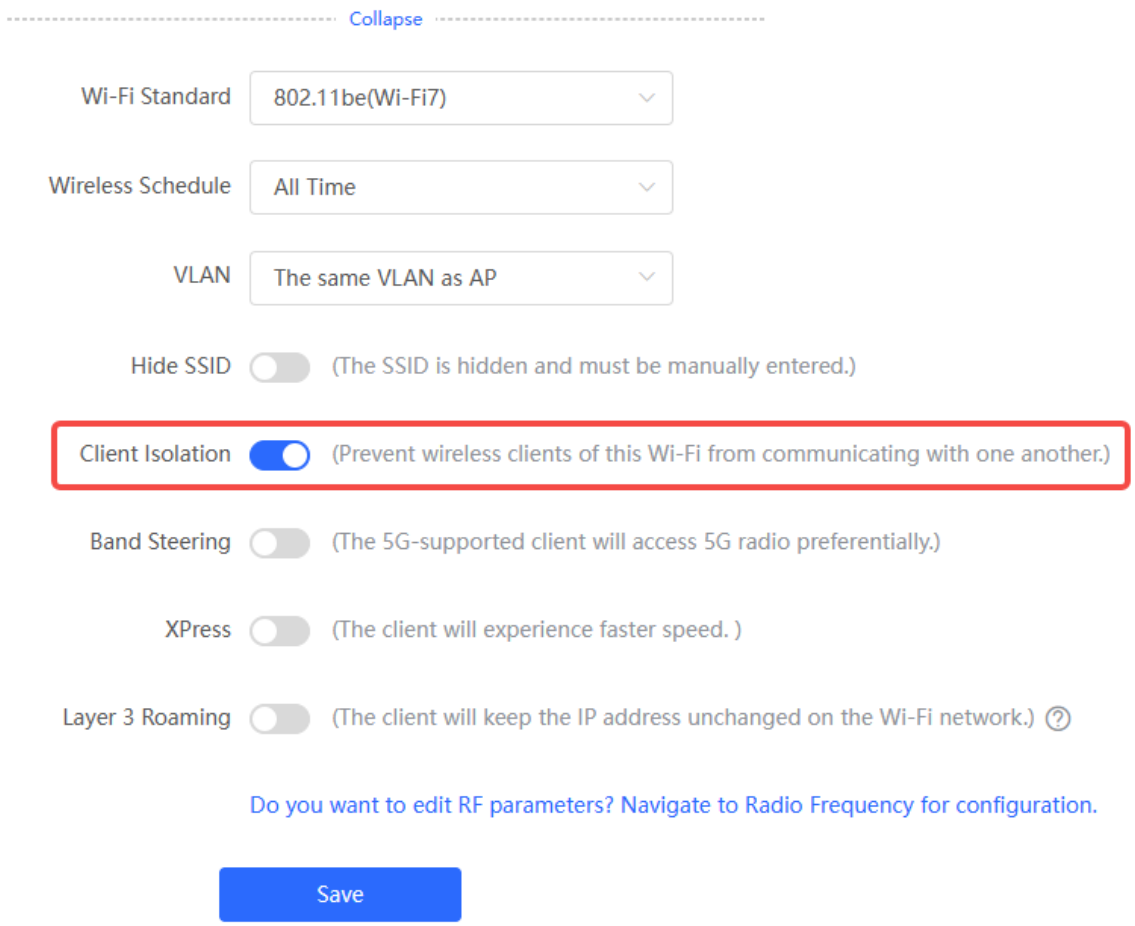


3.10 Configuring Client Isolation

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(1) Click **Collapse**, turn on **Client Isolation** in the expanded settings and click **Save**. The clients joining in this Wi-Fi network will be isolated. The clients associated with the same access point cannot access each other.

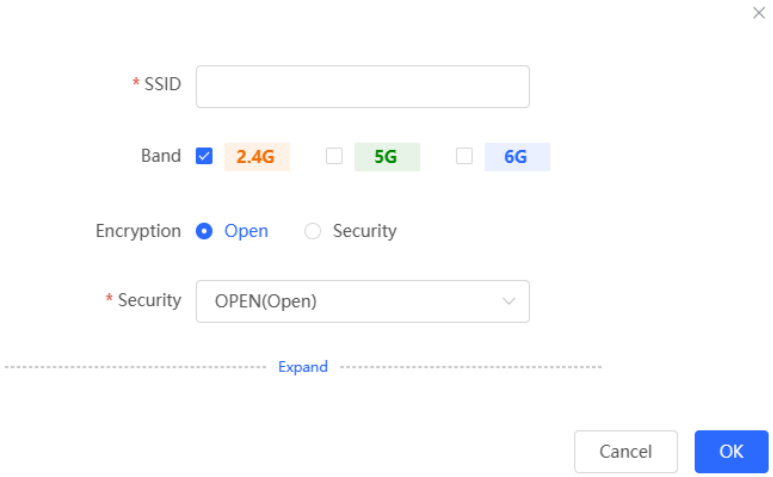


3.11 Adding a Wi-Fi Network

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi Settings**.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**.

(2) Click **Add**, enter the SSID and Wi-Fi password and click **OK** to add a Wi-Fi network. Click **Expand** to configure more Wi-Fi features in the expanded settings. After the Wi-Fi network is added successfully, it will be displayed in the list. The client will be able to scan the new Wi-Fi network.



3.12 Configuring a Guest Wi-Fi

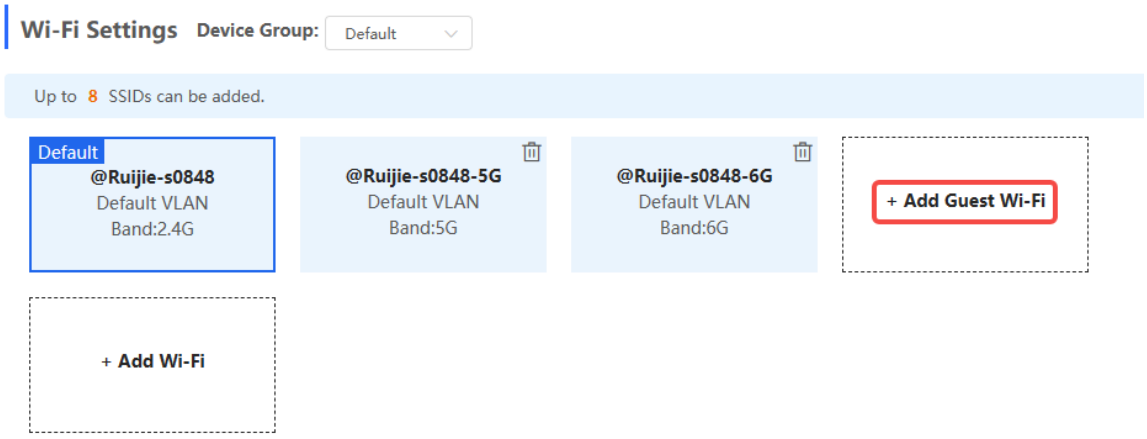
3.12.1 Overview

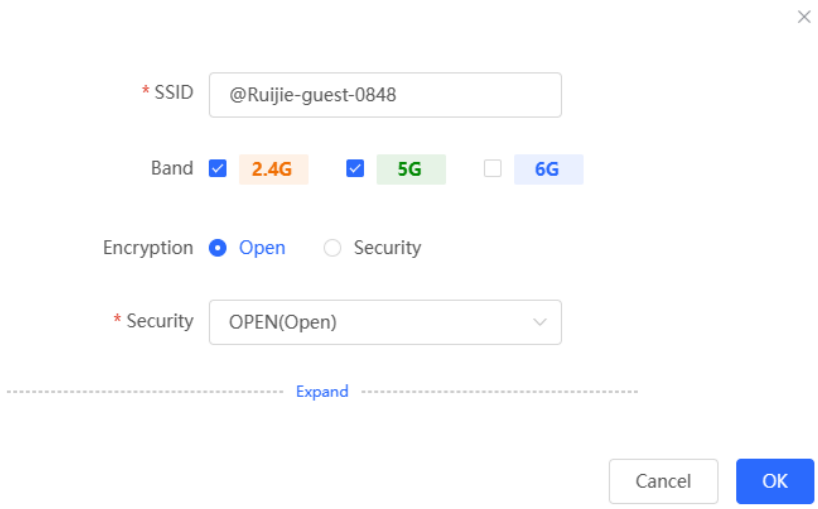
This Wi-Fi network is provided for guests and is disabled by default. It supports client isolation, that is, access clients are isolated from each other. They can only access the Internet via Wi-Fi, but cannot access each other, improving security. The guest Wi-Fi network can be turned off as scheduled. When the time expires, the guest network is off.

3.12.2 Configuration Steps

Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi Settings**.

Click **Add Guest Wi-Fi** to configure the SSID and password of the Guest Wi-Fi. Click **Expand** to configure the effective time period and other Wi-Fi features in the expanded settings. Click **Save**, and the guest Wi-Fi network will be created. Guests can access the guest Wi-Fi network by entering the SSID and Wi-Fi password.





3.13 Configuring Wi-Fi Blocklist or Allowlist

3.13.1 Overview

You can configure the global or SSID-based blocklist and allowlist. The MAC address supports full match and OUI match.

Wi-Fi blocklist: Clients in the Wi-Fi blocklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blocklist are free to access the Internet.

Wi-Fi allowlist: Only clients in the Wi-Fi allowlist can access the Internet. Clients that are not added to the Wi-Fi allowlist are prevented from accessing the Internet.

Caution

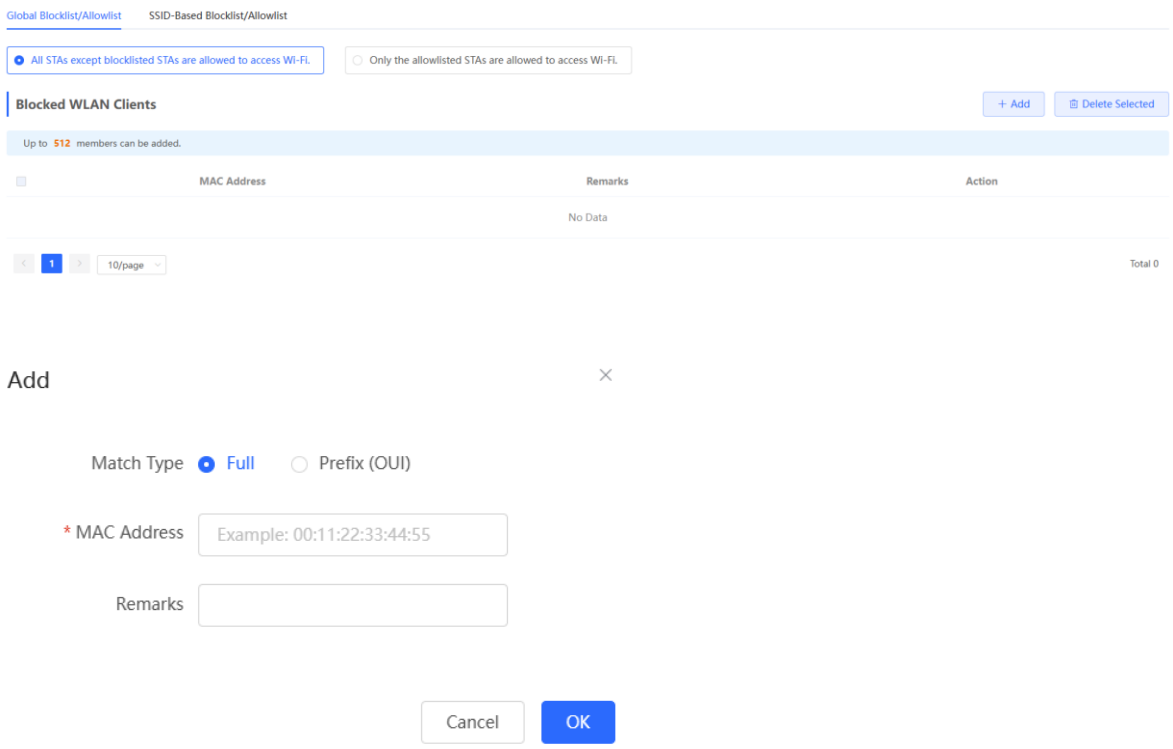
If the allowlist is empty, the allowlist does not take effect. In this case, all clients are allowed to access the Internet.

3.13.2 Configuration Steps

1. Configuring a Global Blocklist/Allowlist

Choose **Clients Management** (**WLAN**)>> **Blocklist/Allowlist** >> **Global Blocklist/Allowlist**

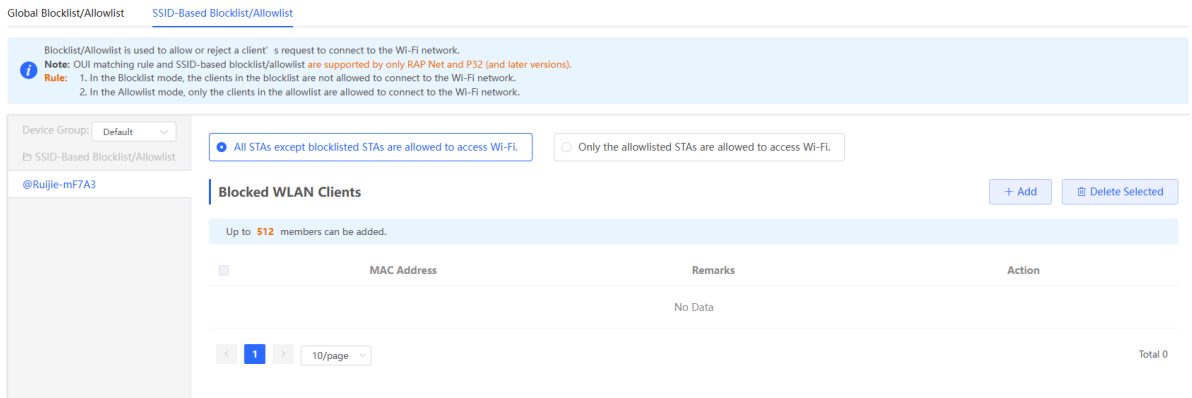
Select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. In the **Add** window, enter the MAC address and remark of the target client and click **OK**. If a client is already associated with the access point, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blocklist will be forced offline and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the access point.



2. Configuring an SSID-based Blocklist/Allowlist

Choose **Clients Management** (**WLAN**)>> **Blocklist/Allowlist** >> **SSID-Based Blocklist/Allowlist**

Select a target Wi-Fi network from the left column, select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. The SSID-based blocklist and allowlist will restrict the client access to the specified Wi-Fi.



3.14 Optimizing Wi-Fi Network

3.14.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can

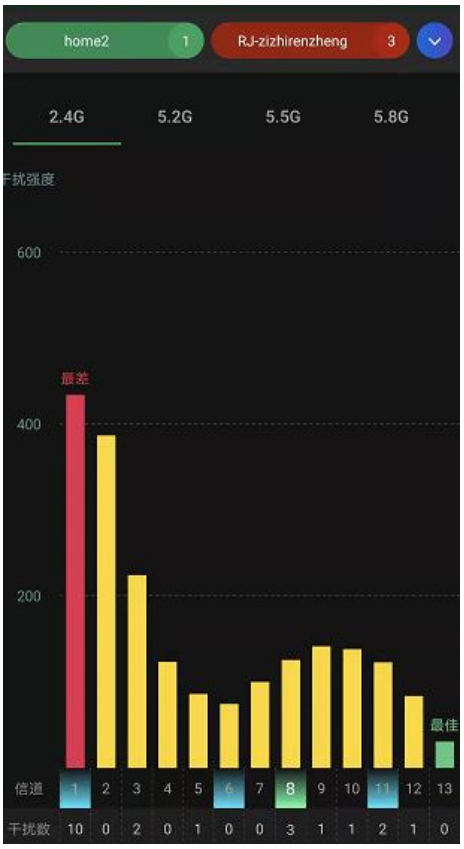
optimize the network with one single click, analyze the wireless environment around the access point and select appropriate parameters.

Caution

After being optimized, the Wi-Fi network will restart, and clients need to reconnect to the W-Fi network. Therefore, exercise caution when performing this operation.

3.14.2 Getting Started

Install Wi-Fi Moho or other Wi-Fi scanning app on the mobile phone and check interference analysis results to find out the best channel.



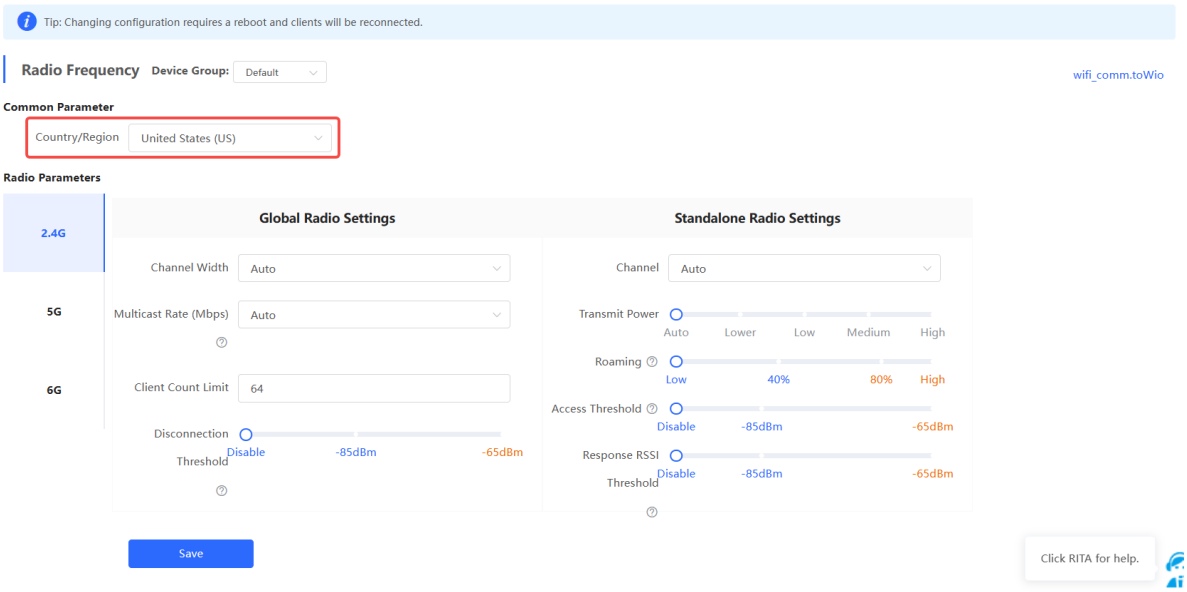
3.14.3 Optimizing the Radio Channel

- Configure the master device. Choose **Network** (**WLAN**) >> **Radio Frequency**.
- Configure the slave device. Choose **Devices** >> Select the target device in the device list and click **SN** >> **Radio Frequency**.

Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. The more devices in a channel, the greater the interference.

Note

The available channel is related to the country or region code. Select the local country or region.



3.14.4 Optimizing the Channel Width

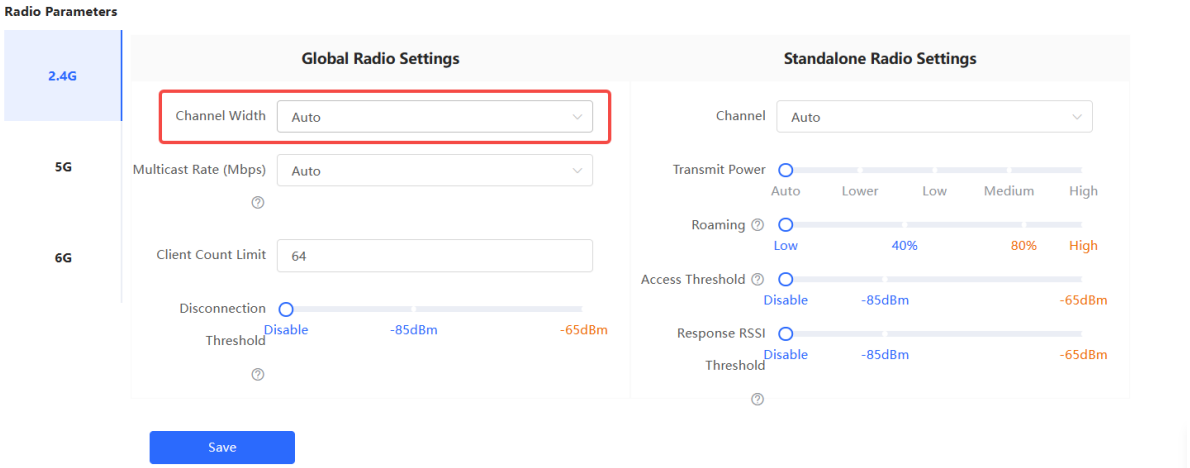
Choose **Network** (**WLAN**) >> **Radio Frequency.**

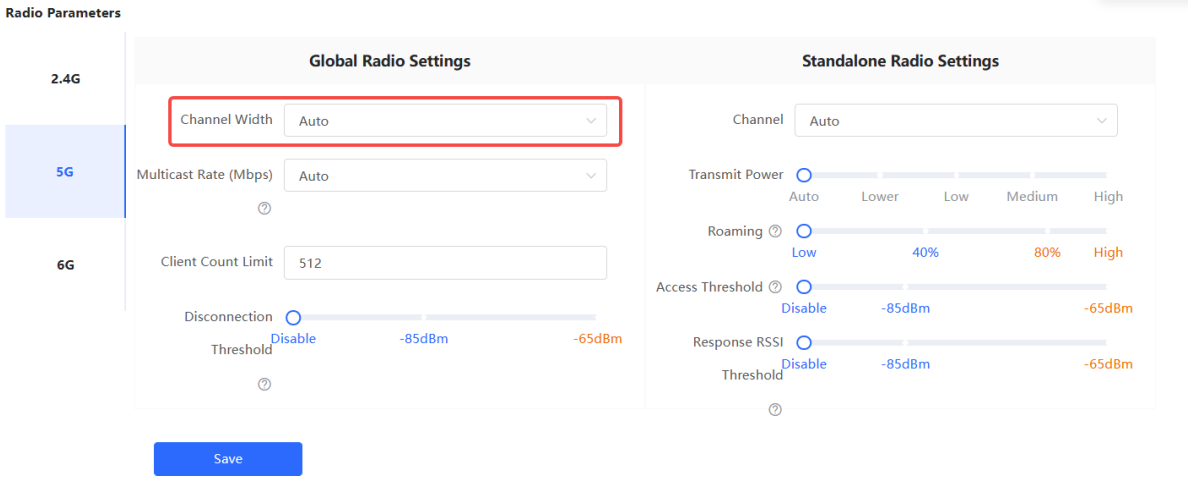
A network with a lower channel width is more stable, while a network with a higher channel width is susceptible to interference. If the interference is severe, choose a lower channel width to avoid network stalling to a certain extent. The 2.4 GHz frequency band supports bandwidths of 20 MHz and 40 MHz, while the 5 GHz frequency band supports bandwidths of 20 MHz, 40 MHz, 80 MHz, and 160 MHz. In addition, the latest 6 GHz frequency band supports an even wider range of bandwidths, including 20 MHz, 40 MHz, 80 MHz, 160 MHz, and 320 MHz.

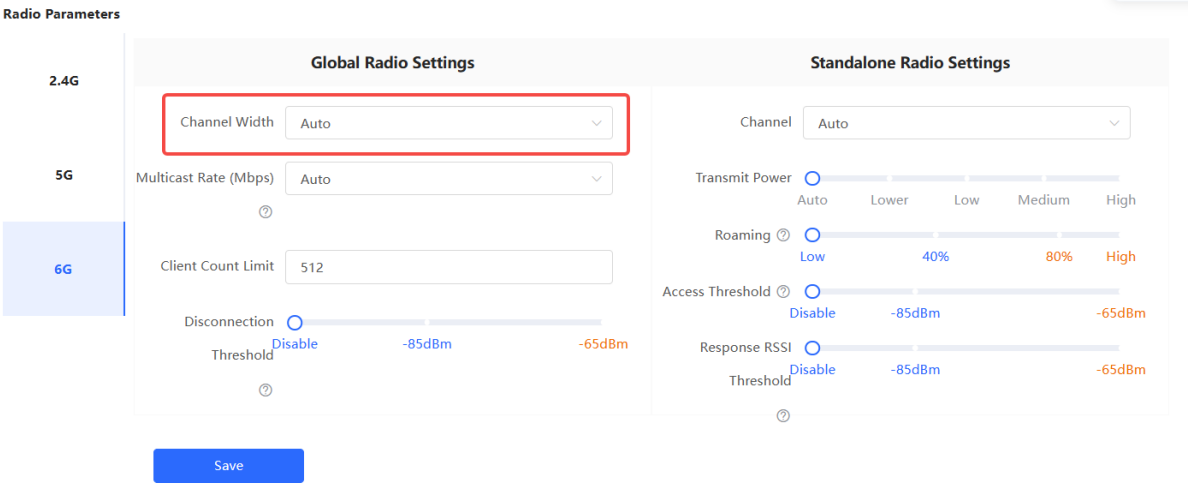
The default value is **Auto**, indicating that the channel width is automatically selected based on the environment. After changing the channel width, click **Save** to make the configuration take effect immediately.

Caution

In the self-organizing network mode, the channel width settings will be synchronized to all devices in the network.


Radio Parameters
2.4G
5G
6G
Global Radio Settings
Channel Width
Auto
Multicast Rate (Mbps)
Auto
Client Count Limit
64
Disconnection Threshold
Disable
-85dBm
-65dBm
Standalone Radio Settings
Channel
Auto
Transmit Power
Auto
Lower
Low
Medium
High
Roaming
Low
40%
80%
High
Access Threshold
Disable
-85dBm
-65dBm
Response RSSI Threshold
Disable
-85dBm
-65dBm
Save

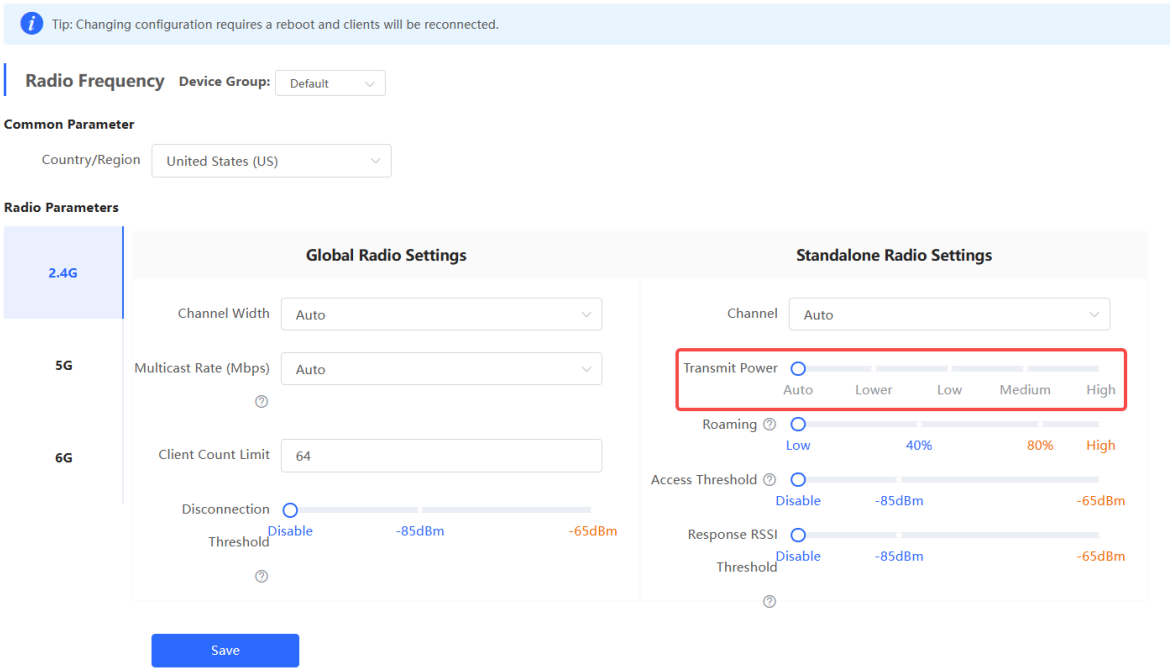

Radio Parameters
2.4G
5G
6G
Global Radio Settings
Channel Width
Auto
Multicast Rate (Mbps)
Auto
Client Count Limit
512
Disconnection Threshold
Disable
-85dBm
-65dBm
Standalone Radio Settings
Channel
Auto
Transmit Power
Auto
Lower
Low
Medium
High
Roaming
Low
40%
80%
High
Access Threshold
Disable
-85dBm
-65dBm
Response RSSI Threshold
Disable
-85dBm
-65dBm
Save


Radio Parameters
2.4G
5G
6G
Global Radio Settings
Channel Width
Auto
Multicast Rate (Mbps)
Auto
Client Count Limit
512
Disconnection Threshold
Disable
-85dBm
-65dBm
Standalone Radio Settings
Channel
Auto
Transmit Power
Auto
Lower
Low
Medium
High
Roaming
Low
40%
80%
High
Access Threshold
Disable
-85dBm
-65dBm
Response RSSI Threshold
Disable
-85dBm
-65dBm
Save

3.14.5 Optimizing the Transmit Power

- Configure the master device. Choose **Network** (**WLAN**) >> **Radio Frequency**.
- Configure the slave device. Choose **Devices** >> Select the target device in the device list and click **SN** >> **Radio Frequency**.

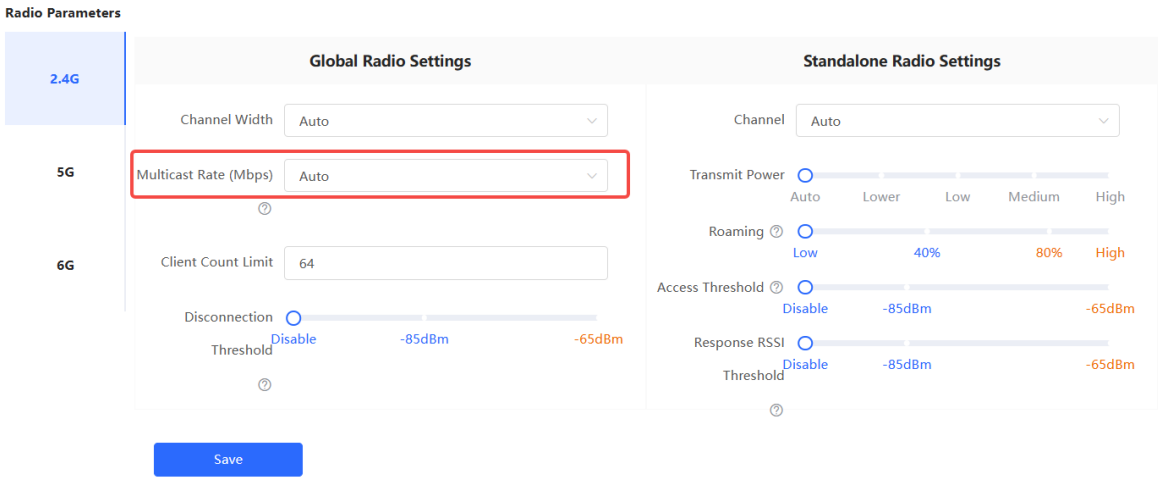
A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. In a high-density scenario, you are advised to set the transmit power to a small value. The **Auto** mode is recommended, indicating automatic adjustment of the transmit power. After adjusting the configuration, click **Save**.



3.14.6 Configuring the Multicast Rate

Choose **Network** (**WLAN**) >> **Radio Frequency**.

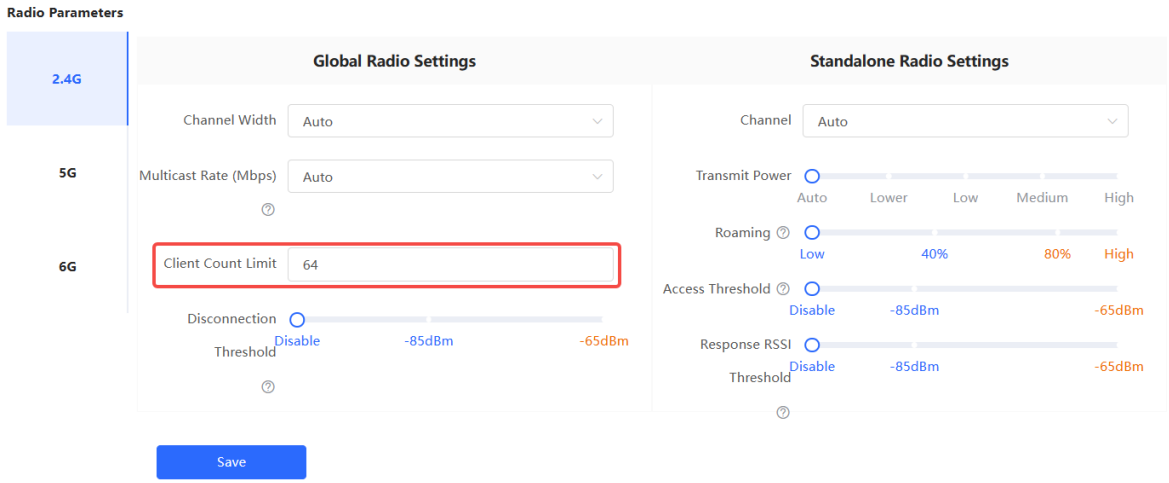
If the multicast rate is too high, the packet loss rate of multicast packets may increase. If the multicast rate is too low, the radio interface may become busy. When network stalling is serious, you are advised to configure a high multicast rate. When network stalling is minor, configure a medium multicast rate. After adjusting the configuration, click **Save**.



3.14.7 Configuring the Client Limit

Choose **Network** (**WLAN**) >> **Radio Frequency.**

If the access point is associated with too many clients, it will have a lower performance, affecting user experience. After you configure the threshold, new clients over the threshold will not be allowed to access the Wi-Fi network. You can lower the threshold if there is requirement for bandwidth per client. You are advised to keep the default settings unless there are special cases. After adjusting the configuration, click **Save**.



Note

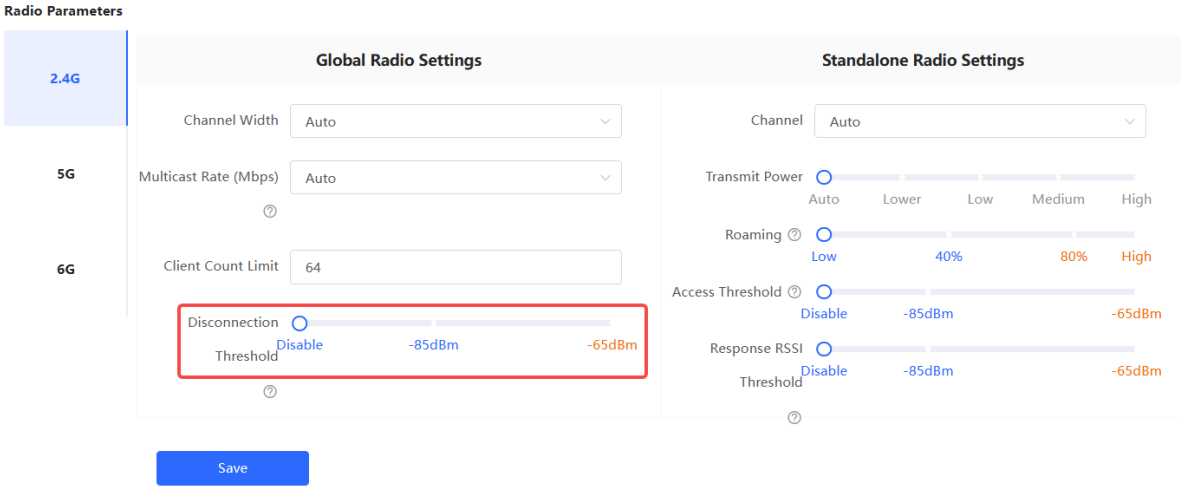
In the self-organizing network mode, the client limit refers to the maximum number of clients accessing all Wi-Fi networks in the current AP group.

3.14.8 Configuring the Kick-off Threshold

Choose **Network** (**WLAN**) >> **Radio Frequency.**

In the case of multiple Wi-Fi signals, setting the kick-off threshold can improve the wireless signal quality to a certain extent. The farther the client is away from the access point, the lower the signal strength is. If the signal is lower than the kick-off threshold, the Wi-Fi will be disconnected, and the client will be forced offline and select a nearer Wi-Fi signal.

However, the higher the kick-off threshold is, the easier it is for the client to be kicked offline. To ensure normal Internet access, you are advised to disable the kick-off threshold or set the value to less than -75dBm. After adjusting the configuration, click **Save**.



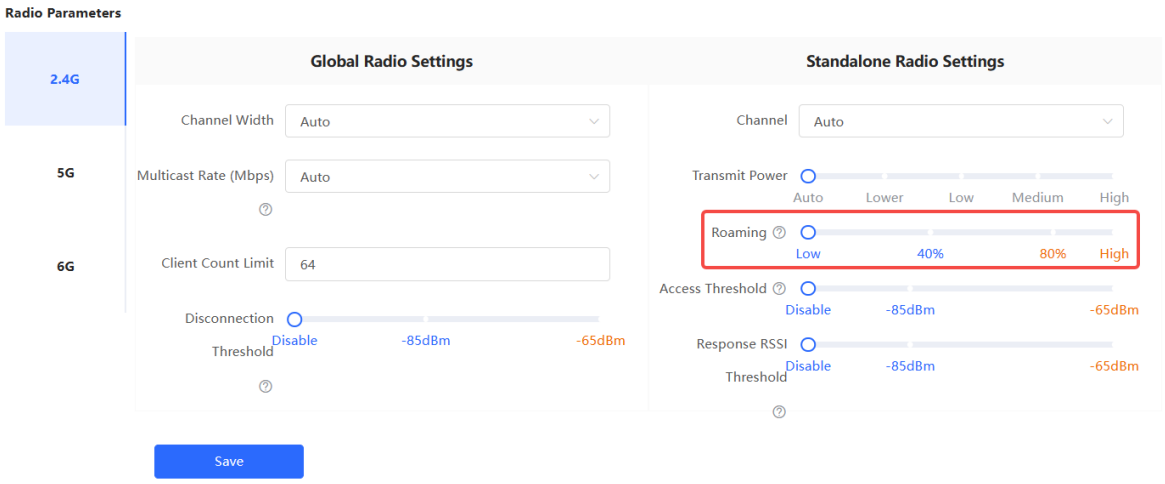
Caution

In the self-organizing network mode, the kick-off threshold settings will be synchronized to all devices in the network.

3.14.9 Configuring the Roaming Sensitivity

- Configure the master device. Choose **Network** (**WLAN**) >> **Radio Frequency**.
- Configure the slave device. Choose **Devices** >> Select the target device in the device list and click **SN** >> **Radio Frequency**.

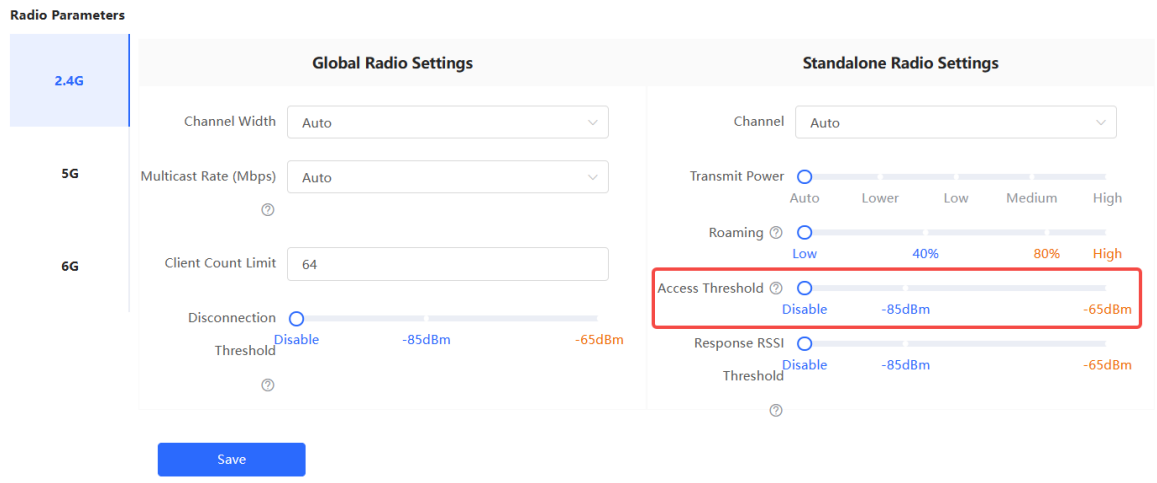
The roaming sensitivity enables the device to actively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving the sensitivity of wireless roaming. Higher the roaming sensitivity level, smaller the wireless signal coverage. To improve the signal quality for a client moving within more than one Wi-Fi coverage, improve the roaming sensitivity level. You are advised to keep the default settings. After adjusting the configuration, click **Save**.



3.14.10 Configuring Access Threshold

- Configure the master device. Choose **Network** (**WLAN**) >> **Radio Frequency**.
- Configure the slave device. Choose **Devices** >> Select the target device in the device list and click **SN** >> **Radio Frequency**.

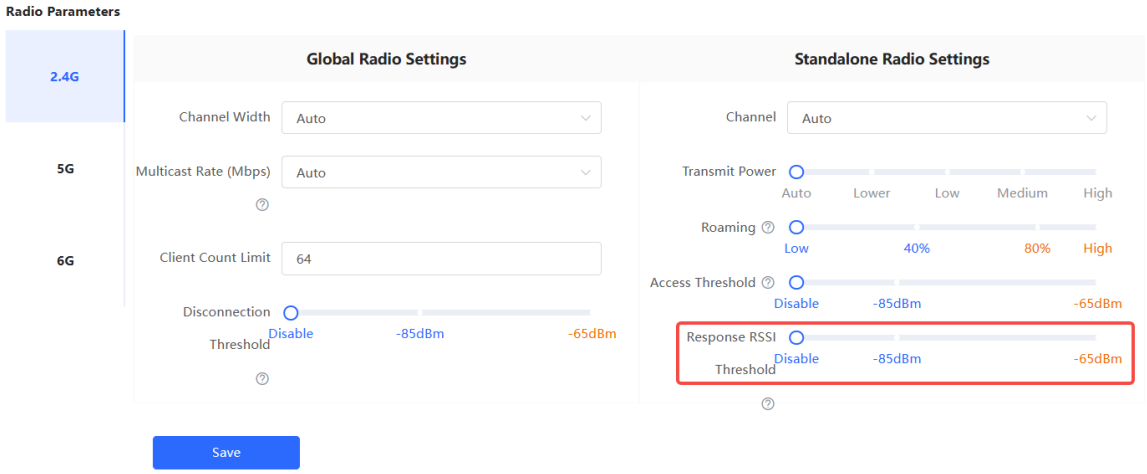
When the wireless signal of the end user is lower than the access threshold set on the device, the client cannot detect the wireless signal of the device. After adjusting the configuration, click **Save**.



3.14.11 Configuring Response RSSI Threshold

- Configure the master device. Choose **Network** (**WLAN**) >> **Radio Frequency**.
- Configure the slave device. Choose **Devices** >> Select the target device in the device list and click **SN** >> **Radio Frequency**.

When the wireless signal of the end user is lower than the response RSSI threshold configured on the device, the client cannot detect the wireless signal of the device. The smaller the response RSSI threshold is configured, the less the environmental factors interfere with the AP. However, the connection of the client may be affected. After adjusting the configuration, click **Save**.



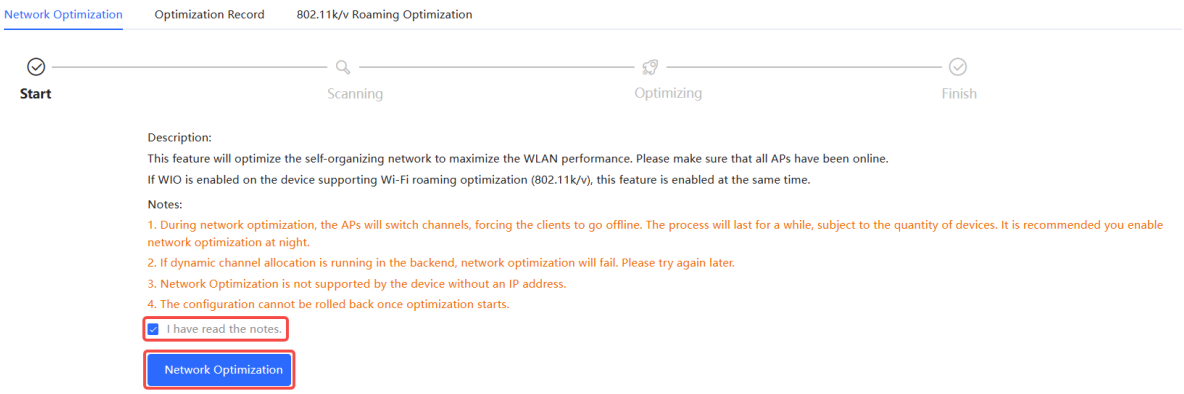
3.14.12 Configuring WIO

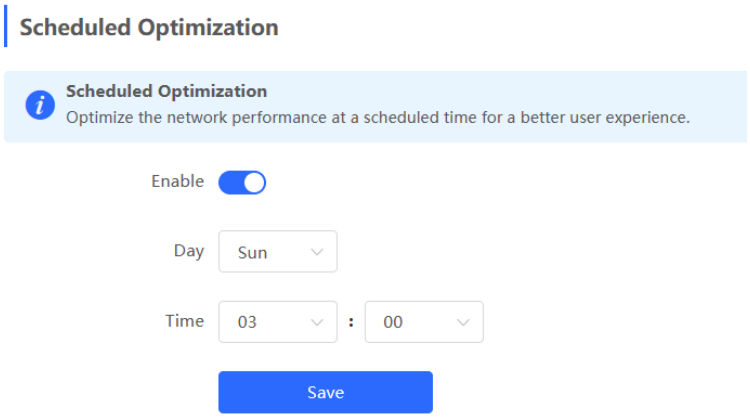
In **Network** mode, choose **Network** >> **WIO**.

Check **I have read the notes.** And click **Network Optimization** to optimize the wireless network. You are advised to set a scheduled task to optimize the wireless network in the early hours of the morning or when the network is idle.

Caution

- WIO is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.





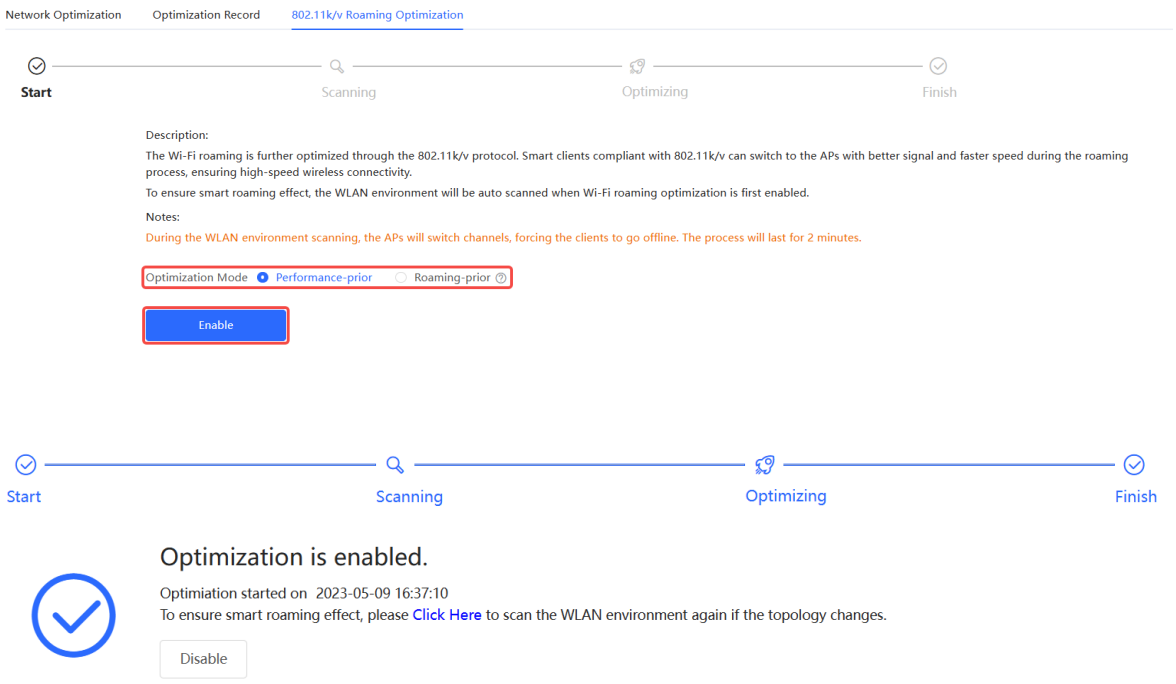
3.14.13 Configuring Wi-Fi Roaming Optimization (802.11k/v)

In **Network** mode, choose **Network** >> **WIO** >> **802.11k/v Roaming Optimization**

Choose the optimization mode, and click **Enable** to further optimize the wireless roaming performance of Wi-Fi signals through the 802.11k/v roaming protocols. Smart clients compliant with 802.11k/v can switch to the APs with better signal and faster speed during the roaming process, ensuring high-speed wireless connectivity. To ensure smart roaming effect, the WLAN environment will be auto scanned when Wi-Fi roaming optimization is first enabled.

Caution

- WIO is supported only in the self-organizing network mode.
- During the WLAN environment scanning, the APs will switch channels, forcing the clients to go offline. The process will last for 2 minutes.

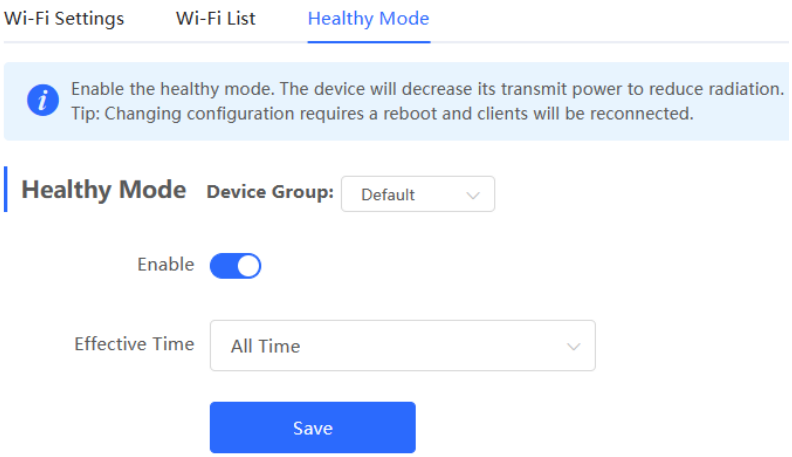


3.15 Configuring Healthy Mode

Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Healthy Mode.**

Select **Device Group** from the drop-down list box. Click **Enable** to enable the healthy mode. You are allowed to set the effective time period for the healthy mode.

After the healthy mode is enabled, the transmit power and the Wi-Fi coverage area will decrease. The healthy mode may reduce signal strength and cause network stalling. You are advised to disable it or enable it when the network is idle.

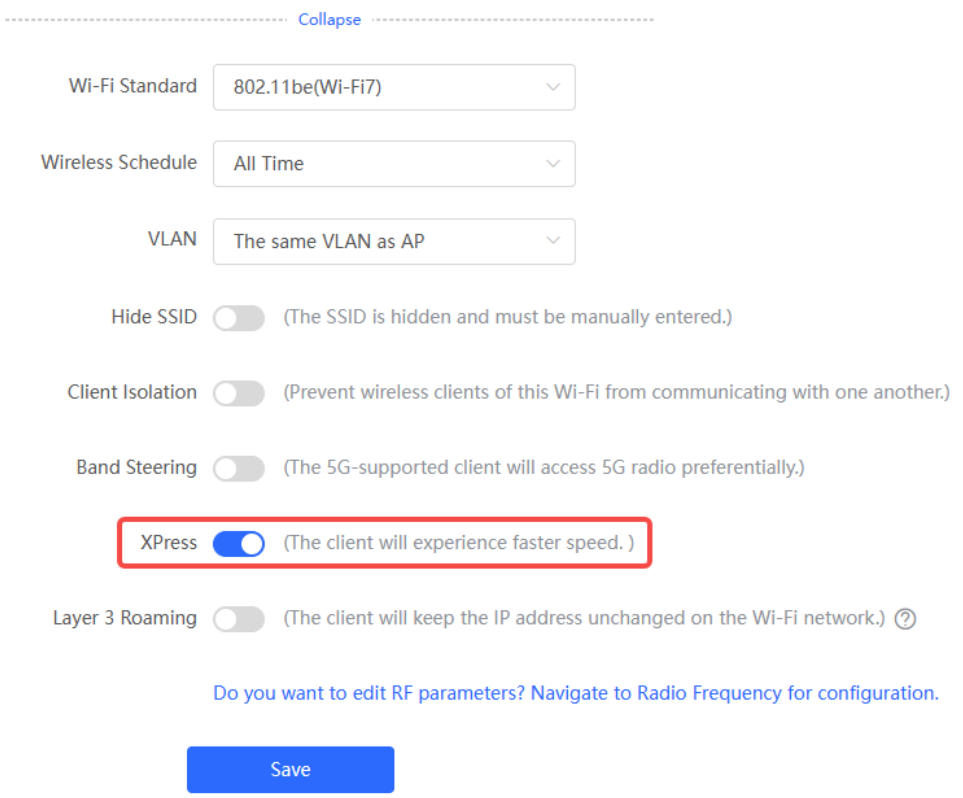


3.16 Configuring XPress

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi >> Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Collapse**, turn on **XPress** in the expanded settings and click **Save**. After XPress is enabled, the gaming traffic will be prioritized, ensuring a more stable gaming experience.

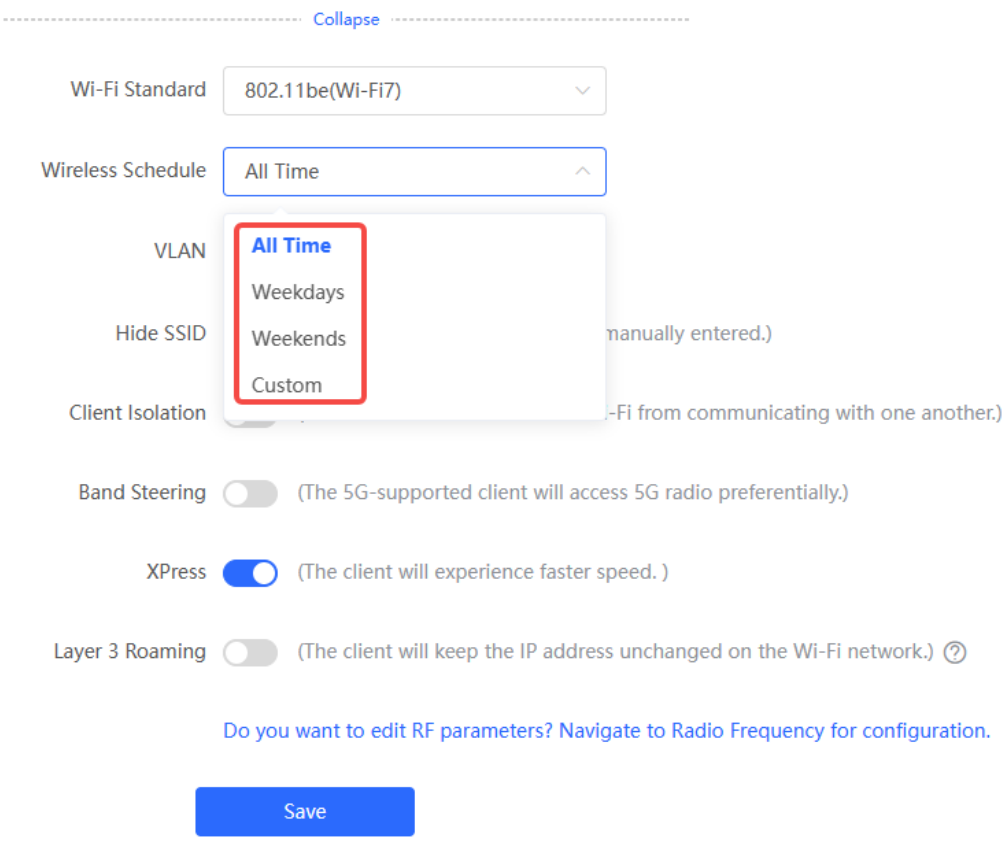


3.17 Configuring Wireless Schedule

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) >> **Wi-Fi** >> **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(1) Click **Collapse**, select a scheduled time span to turn on Wi-Fi and click **Save**. Clients will be allowed to access the Internet only in the specified time span.



3.18 Wireless Authentication

3.18.1 Overview

Wireless authentication verifies the identity of users on a wireless network. Only authenticated users can access the network, ensuring wireless network security. You can configure authentication-free for wireless STAs (IP address/MAC address), public IP addresses, and domain names. Users can directly use network services or access specific websites without entering the username, password, or other information.

To use the wireless authentication function, ensure that the AP is added to Ruijie Cloud and is online. Then, configure a portal template on Ruijie Cloud and apply it to a specific SSID. When STAs connect to this SSID and access the network, the AP allows STAs added to the authentication-free lists configured on the Eweb management system (excluding those added to the MAC address blocklist) to access the network without authentication. The AP forbids STAs whose MAC addresses are added to the MAC address blocklist configured on the Eweb management system from accessing the network. For other users or domain names, the AP redirects them to the portal authentication page. Users need to complete identity verification on the portal page.

The following four authentication modes are supported:

- One-click Login: indicates login without the username and password.
- Voucher: indicates login with a random eight-digit password.
- Account: indicates login with the account and password.
- SMS: indicates login with the phone number and code.

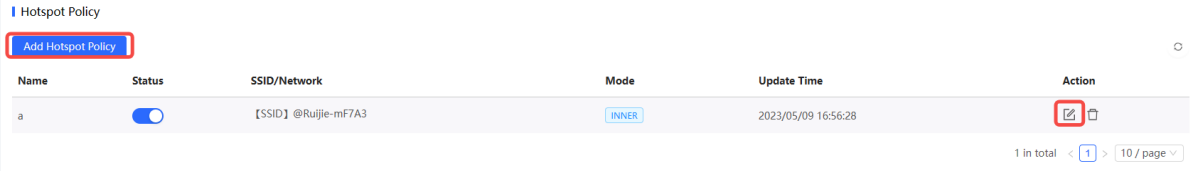
Two or more authentication modes can be configured in a portal template. When multiple authentication modes are configured, users can select an authentication mode on the portal page.

3.18.2 Configuring One-click Login on Ruijie Cloud

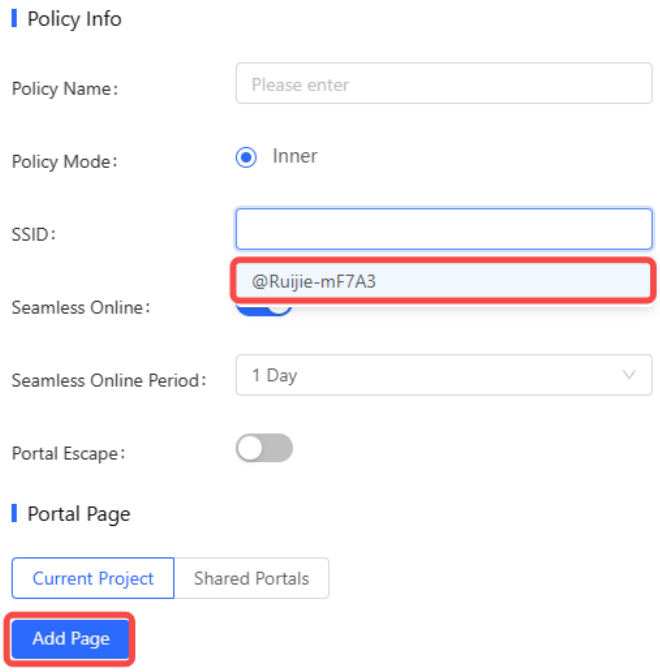
Configuring a portal template with the authentication mode set to One-click login

(1) Log in to Ruijie Cloud, choose **Project** >> **Configuration >> Auth & Accounts** >> **Authentication** >> **Hotspot Policy**, and select a network that needs to configure wireless authentication.

(2) Click **Add Hotspot Policy** to create a hotspot policy, or click  to edit the authentication mode of an existing SSID.



(1) Select the SSID to be authenticated, and click **Add Page** to enter the portal template configuration page.



(4) Configure basic settings of the portal template.

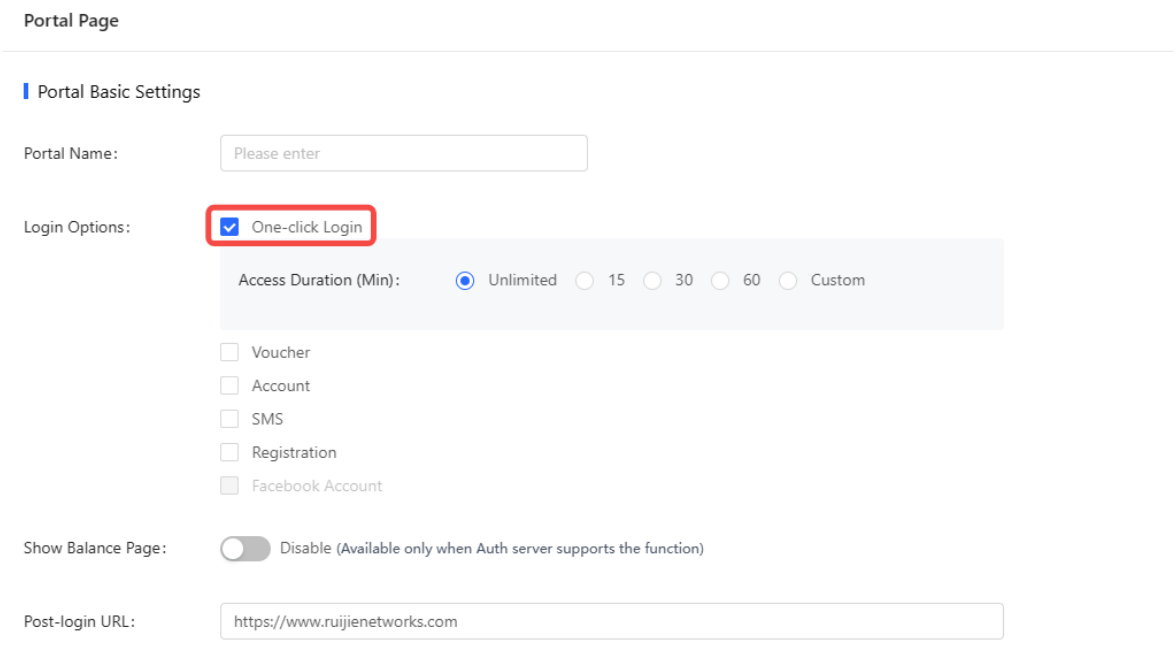


Table 3-1 **Basic Information of the Portal Template**

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Select **One-click Login**, which indicates login without the username and password. You can set the access duration and access time per day.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) On the **Portal Page** section, configure the required settings for the portal page.

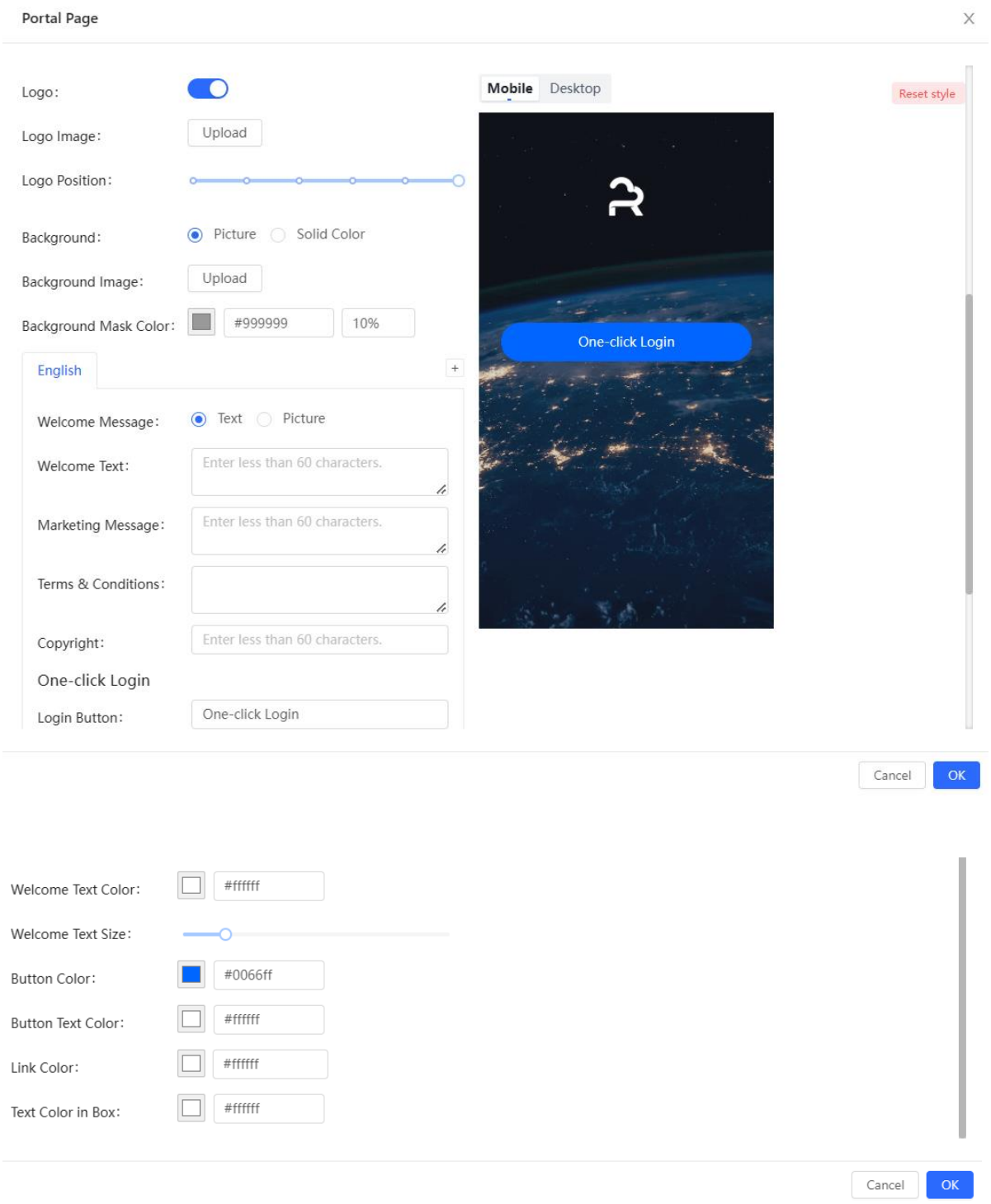


Table 3-2 **Information of the Portal Page**

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.

Parameter	Description
Background Image	When **Background** is set to **Image**, upload the background image or select the default image.
Background Mask Color	Select the background mask color. The default value is #999999.
Language	Select the language of the portal page and configure the content displayed on the portal page as required. You can click + to add portal pages in other languages. ● Welcome Message: Select the welcome message with the image or text. ● Welcome Text: Enter the welcome text. ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● One-click Login: Enter the button name (default: One-click Login) displayed on Portal page.
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

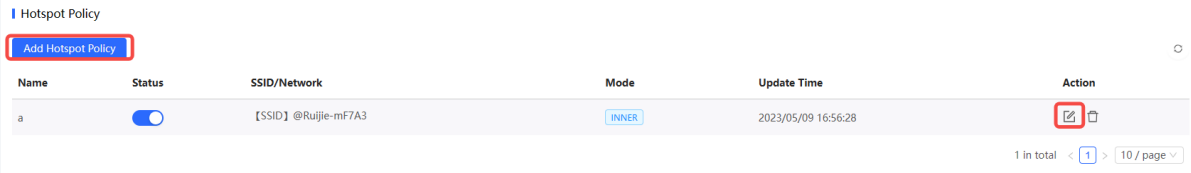
(6) After the configuration, click **OK** to save the portal template configurations.

3.18.3 Configuring Voucher Authentication on Ruijie Cloud

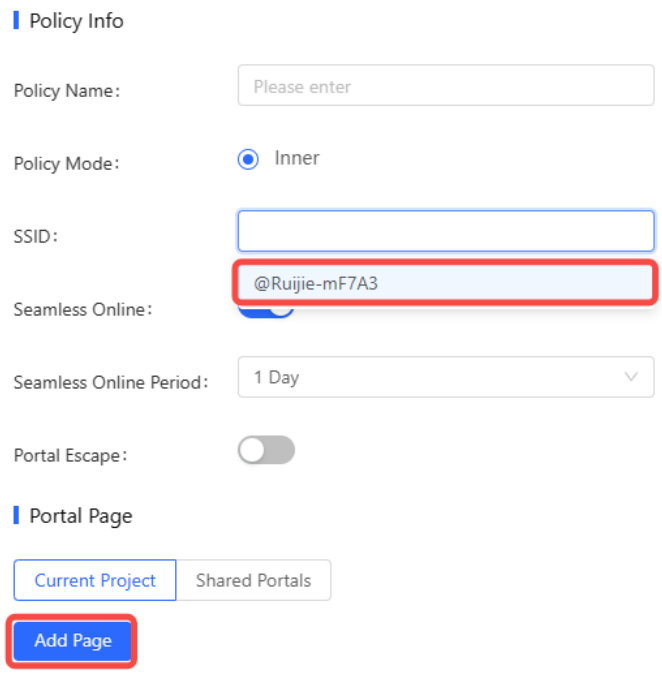
1. Configuring a Portal Template with the Authentication Mode Set to Voucher

(1) Log in to Ruijie Cloud, choose **Project** >> **Configuration >> Auth & Accounts** >> **Authentication** >> **Hotspot Policy**, and select a network that needs to configure wireless authentication.

(3) Click **Add Hotspot Policy** to create a hotspot policy, or click  to edit the authentication mode of an existing SSID.



(2) Select the SSID to be authenticated, and click **Add Page** to enter the portal template configuration page.



(4) Configure basic settings of the portal template.

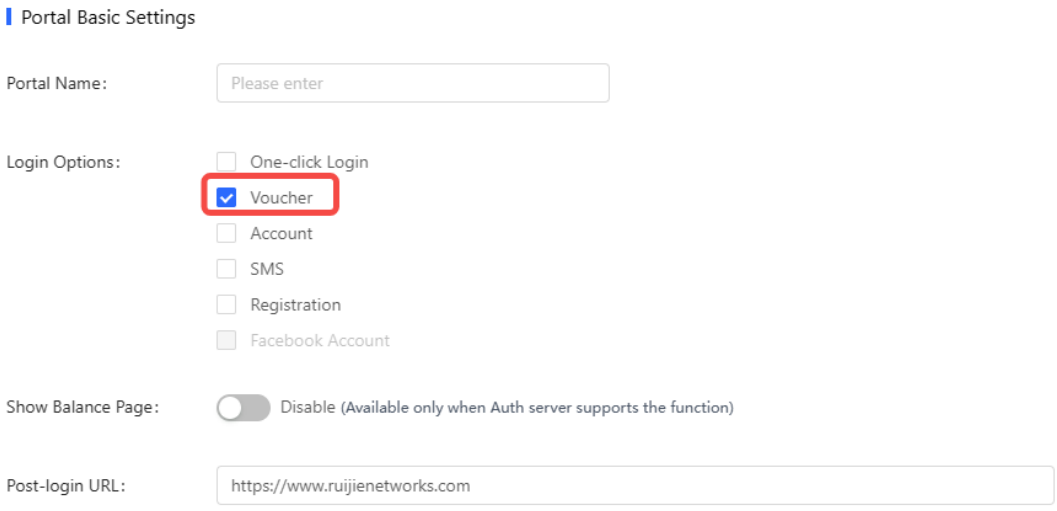


Table 3-3 **Basic Information of the Portal Template**

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Select **Voucher**, which indicates login with a random eight-digit password.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) On the **Portal Page** section, configure the required settings for the portal page.

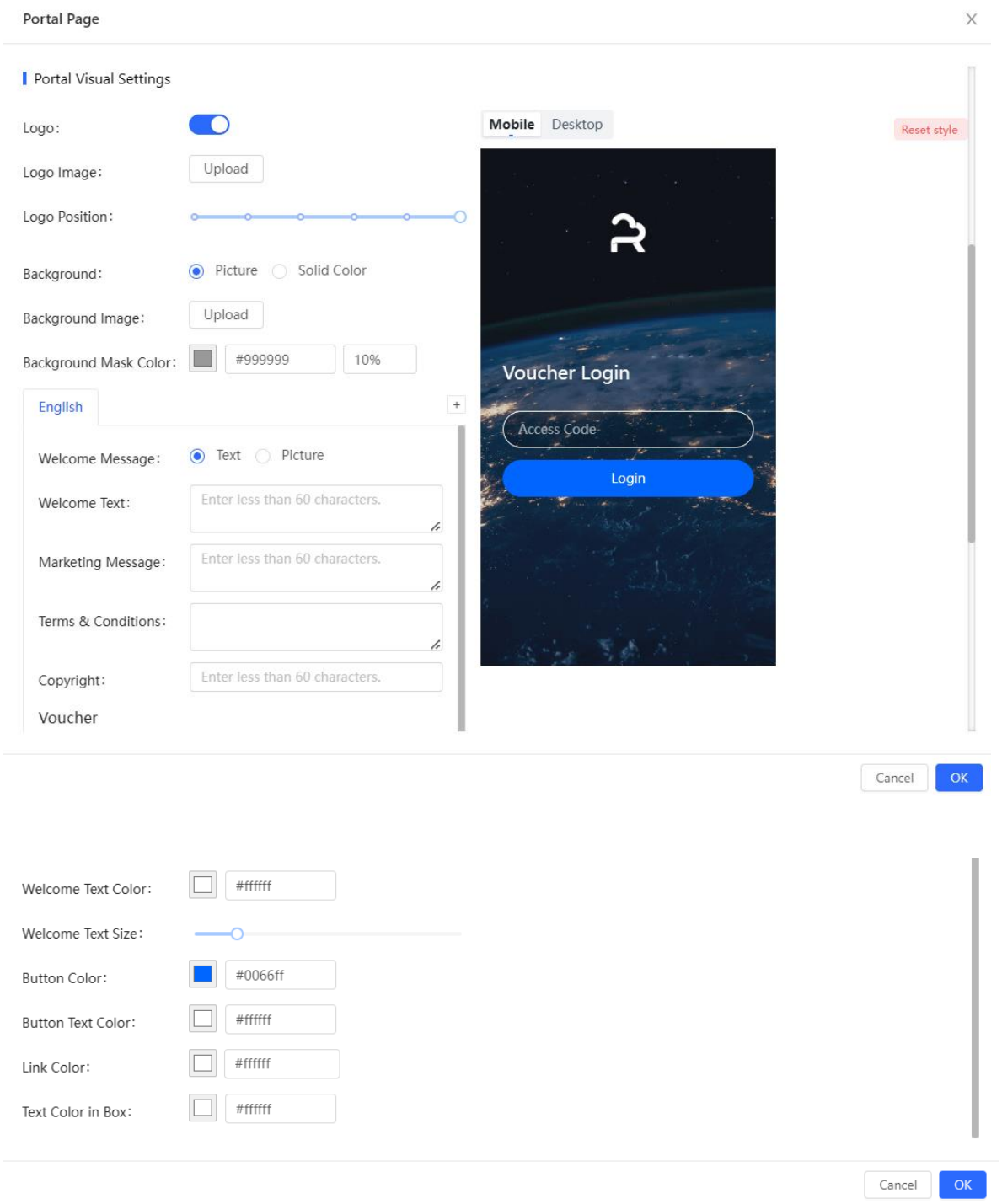
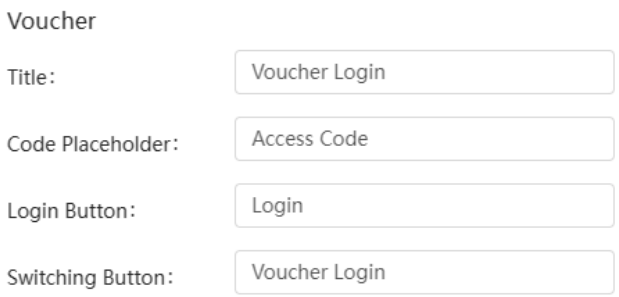


Table 3-4 **Information of the Portal Page**

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.

Parameter	Description
Background Image	When **Background** is set to **Image**, upload the background image or select the default image.
Background Mask Color	Select the background mask color. The default value is #999999.
Language	Select the language of the portal page and configure the content displayed on the portal page as required. You can click + to add portal pages in other languages. ● Welcome Message: Select the welcome message with the image or text. ● Welcome Text: Enter the welcome text. ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● Voucher: Enter the name of controls related to voucher authentication. 
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

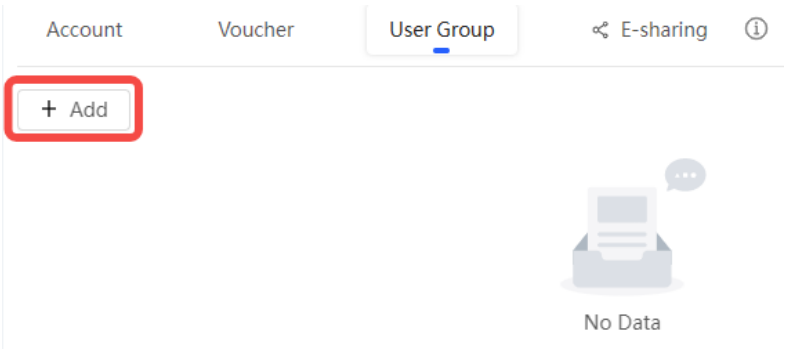
(6) After the configuration, click **OK** to save the portal template configurations.

2. Adding a Voucher

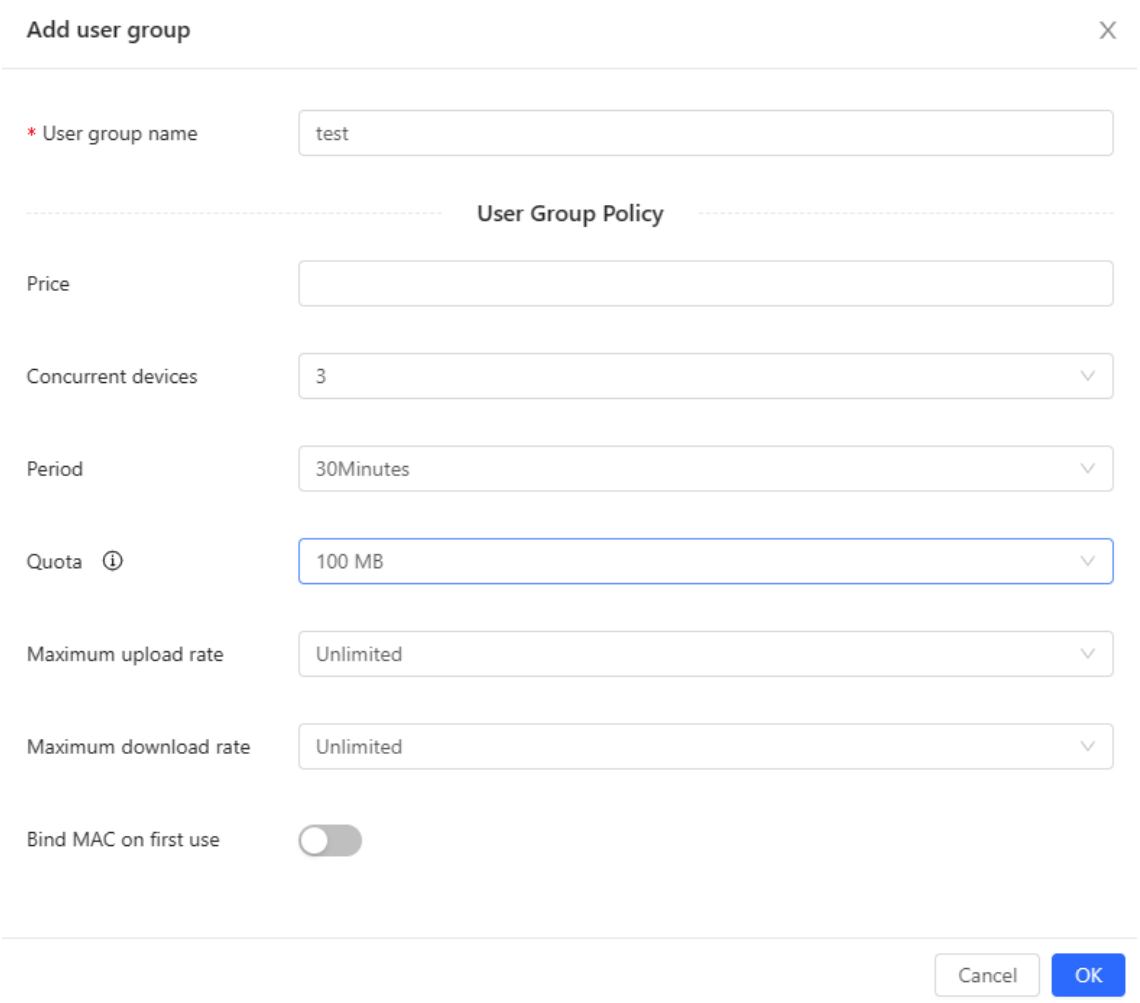
(1) Log in to Ruijie Cloud, choose **Project** >> **Configuration** >> **Auth & Accounts** >> **Accounts** >>**User Management** and select a network in this account**.**

(2) Configure a user group.

a On the **User Group** tab, click **Add**.



b Configure user group parameters. After the configuration, click **OK**.



User Group Name: indicates the user group name.

Price: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.

Concurrent Devices: indicates the number of concurrent devices for one account.

Period: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.

Quota: indicates the maximum amount of data transfer.

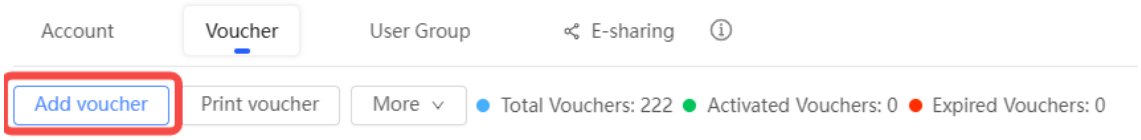
Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

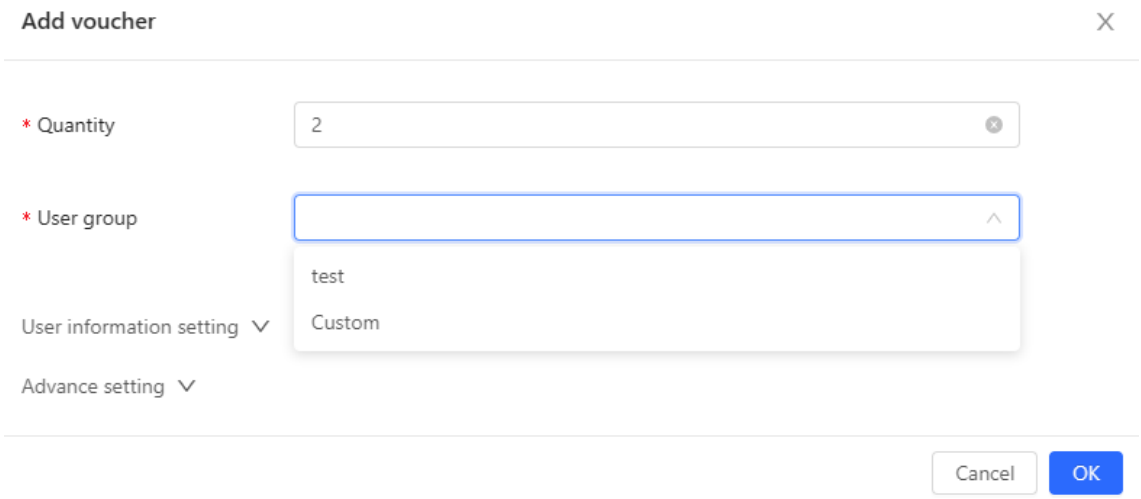
Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) Configure a voucher.

a On the **Voucher** tab, click **Add voucher**.



b Configure voucher parameters. After the configuration, click **OK**.



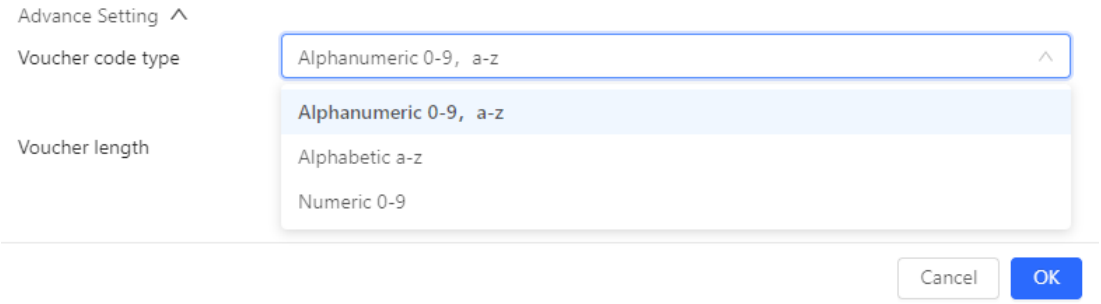
Quantity: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the vouchers are added.

User group: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click **Custom** to create a user group.

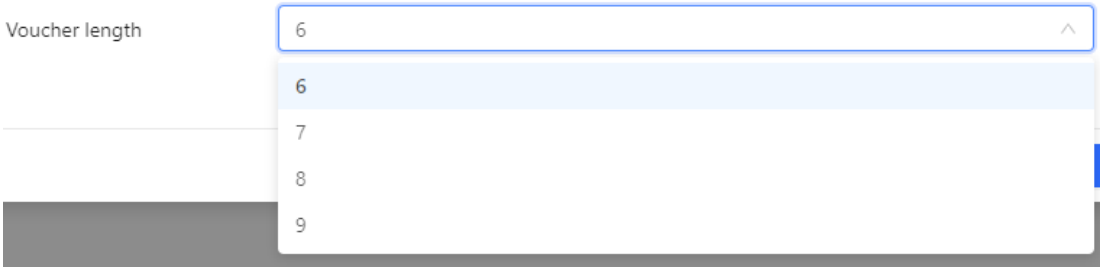
User information setting: Configure user information, which is optional.

Advance setting:

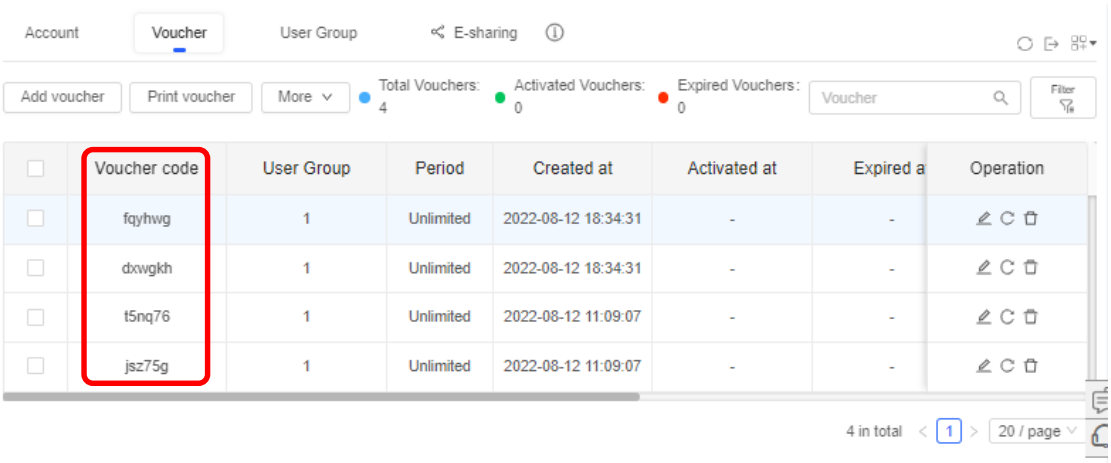
- **Voucher code type**: Set the value to Alphanumeric 0-9, a-z, Alphabetic a-z, or Numeric 0-9.



- **Voucher length**: Select the voucher length. The value ranges from 6 to 9.



(4) Obtain the voucher code from the voucher list.

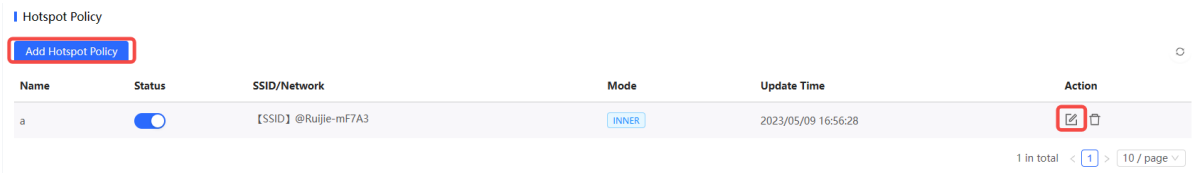


3.18.4 Configuring Account Authentication on Ruijie Cloud

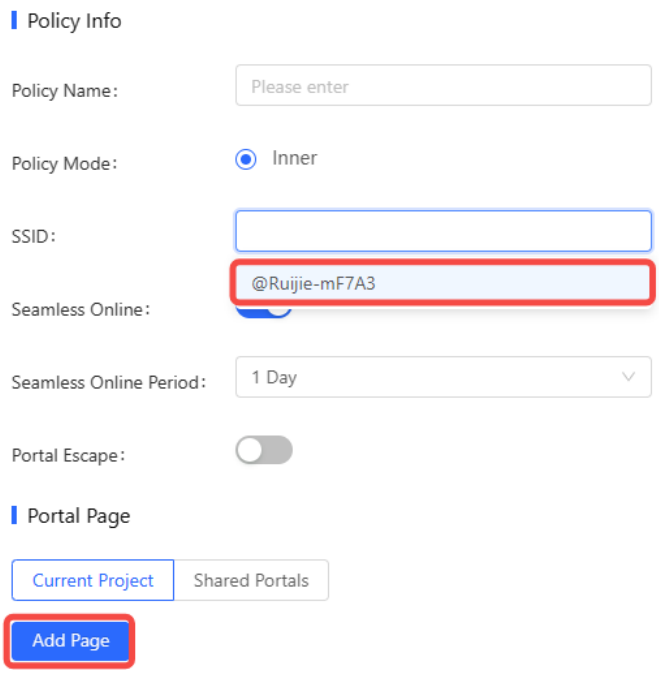
1. Configuring a Portal Template with the Authentication Mode Set to Account

(1) Log in to Ruijie Cloud, choose **Project** >> **Configuration >> Auth & Accounts** >> **Authentication** >> **Hotspot Policy**, and select a network that needs to configure wireless authentication.

(2) Click **Add Hotspot Policy** to create a hotspot policy, or click  to edit the authentication mode of an existing SSID.



(3) Select the SSID to be authenticated, and click **Add Page** to enter the portal template configuration page.



(4) Configure basic settings of the portal template.

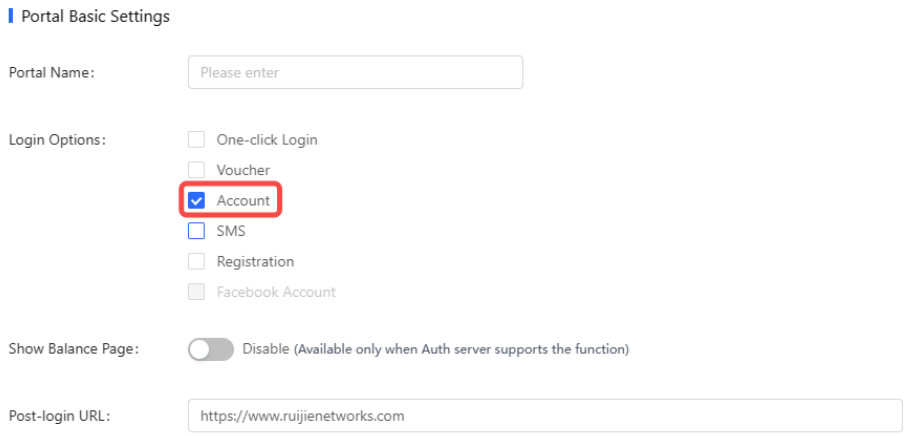


Table 3-5 **Basic Information of the Portal Template**

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Select **Account**, which indicates login with the account and password.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) On the **Portal Page** section, configure the required settings for the portal page.

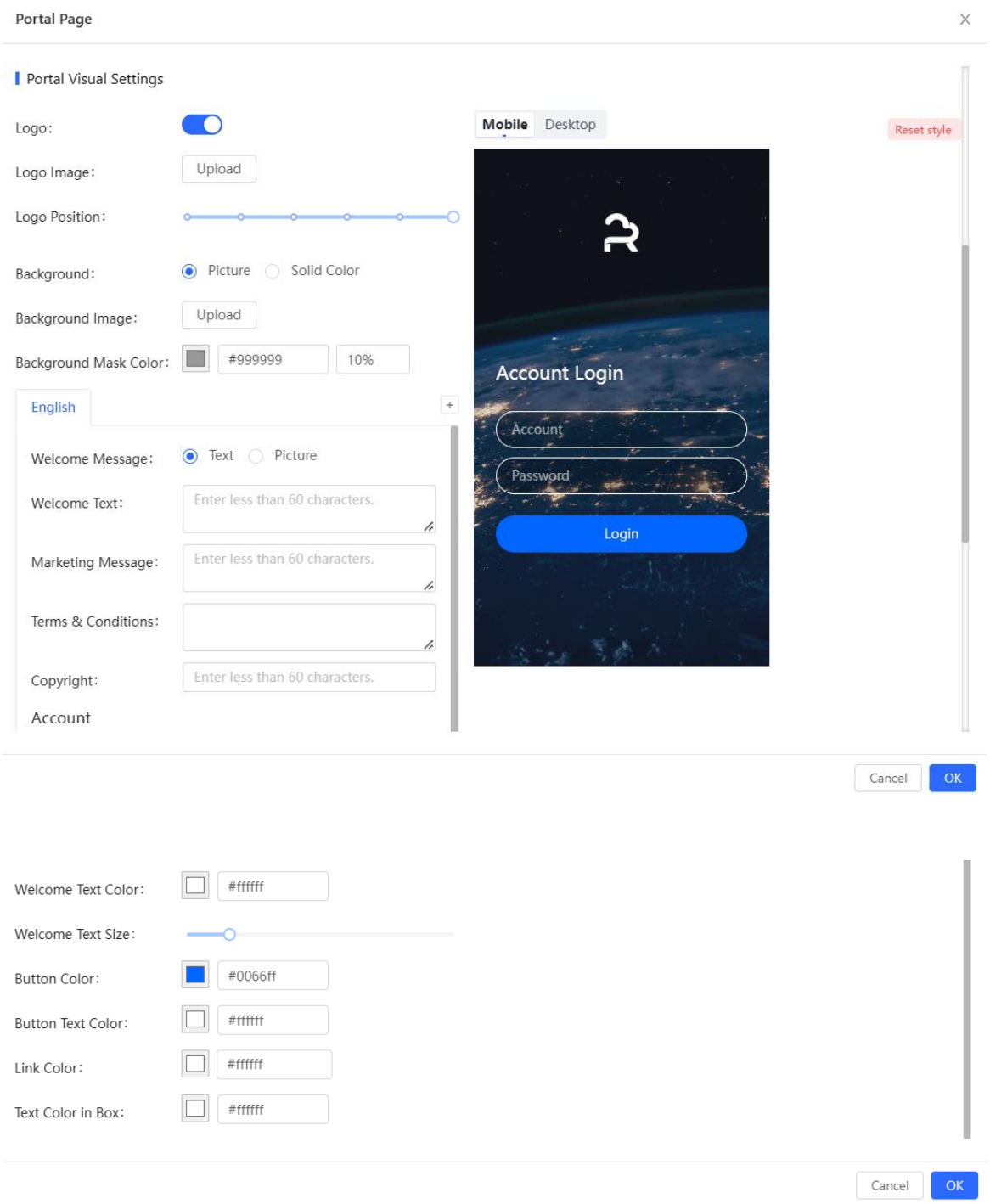
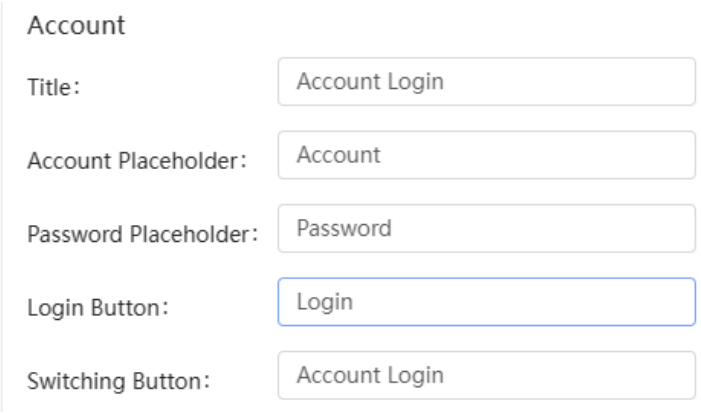


Table 3-6 **Information of the Portal Page**

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.

Parameter	Description
Background Image	When **Background** is set to **Image**, upload the background image or select the default image.
Background Mask Color	Select the background mask color. The default value is #999999.
Language	Select the language of the portal page and configure the content displayed on the portal page as required. You can click + to add portal pages in other languages. ● Welcome Message: Select the welcome message with the image or text. ● Welcome Text: Enter the welcome text. ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● Account: Enter the name of controls related to account authentication. 
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

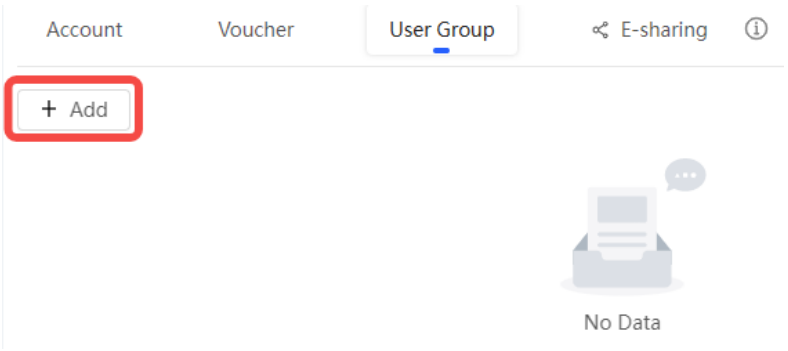
(5) After the configuration, click **OK** to save the portal template configurations.

2. Adding an Account

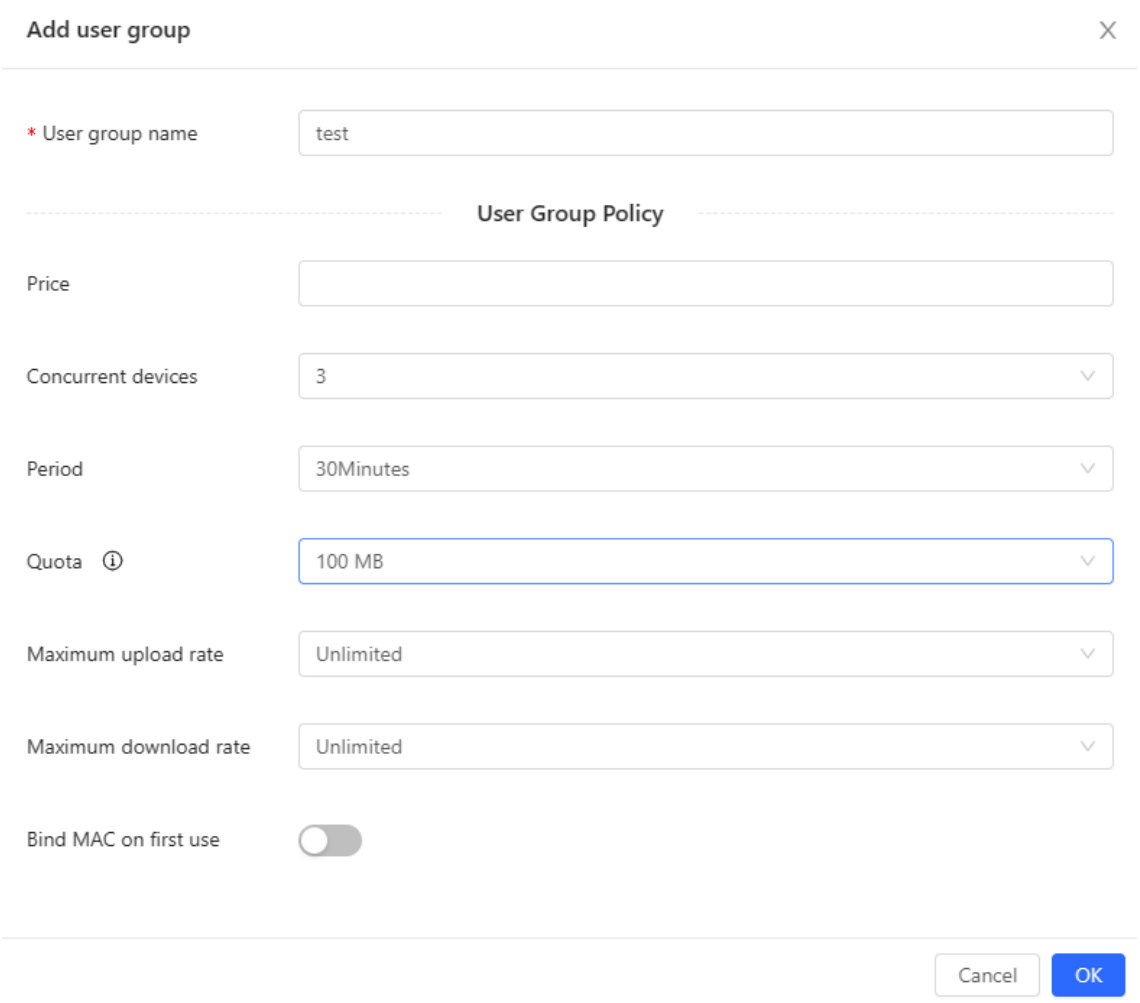
(1) Log in to Ruijie Cloud, choose **Project** >> **Configuration** >> **Auth & Accounts** >> **Accounts** >>**User Management** and select a network in this account**.**

(2) Configure a user group.

a On the **User Group** tab, click **Add**.



b Configure user group parameters. After the configuration, click **OK**.



User Group Name: indicates the user group name.

Price: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.

Concurrent Devices: indicates the number of concurrent devices for one account.

Period: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.

Quota: indicates the maximum amount of data transfer.

Maximum upload rate: indicates the maximum upload rate.

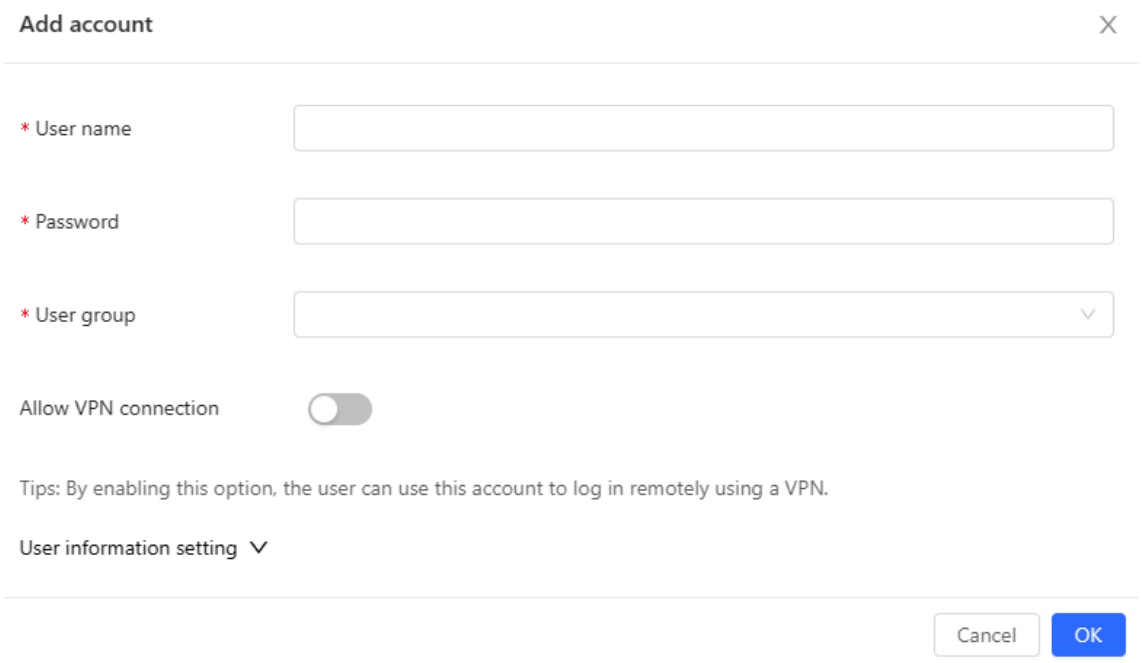
Maximum download rate: indicates the maximum download rate.

Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(1) On the **Account** tab, add an account. Accounts can be added manually or through batch import.

- Adding an account manually

  Click **Add an Account**, set parameters about the account, and click **OK**.



User name: The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.

Password: The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.

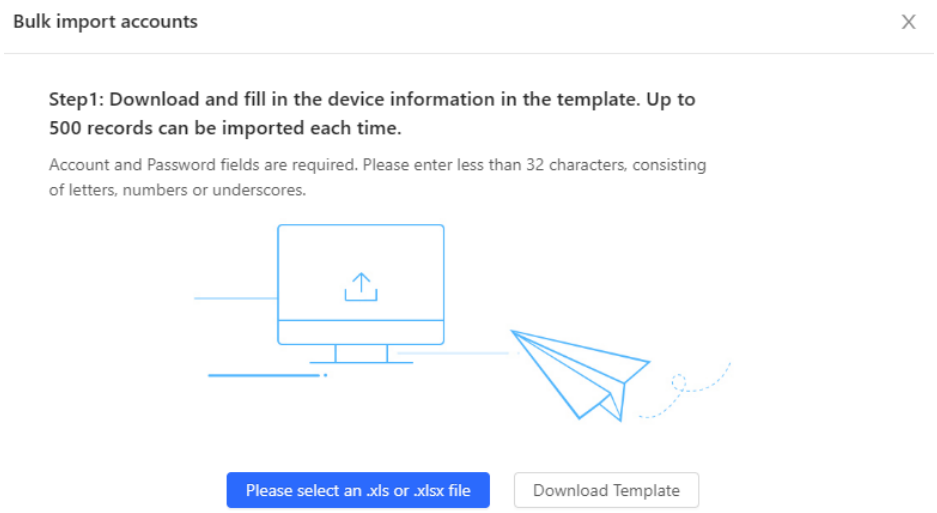
User group: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click **Custom** to create a user group.

Allow VPN connection: By enabling this option, the user can use this account to log in remotely using a VPN.

User information setting: You can expand it to have more user information displayed, including the first name, last name, email, phone number, and alias.

- Adding accounts through batch import

  a Click Bulk import.



b Click **Download Template** to download the template.

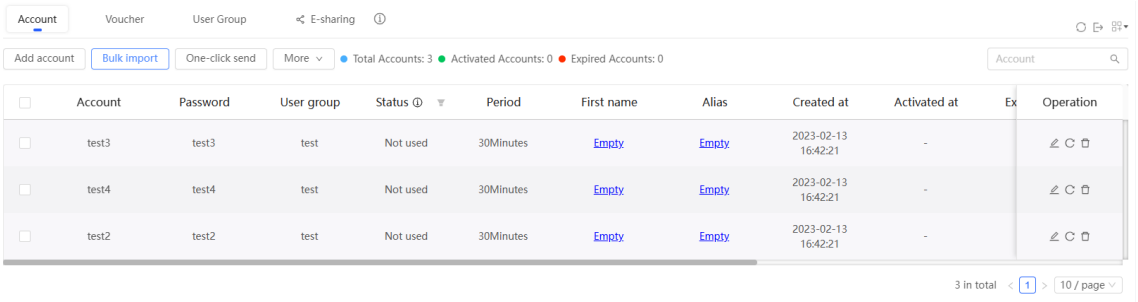
c Edit the template and save it.

Note

- **Account**, **Password**, and **User Group** are mandatory.
- Check that the user group already exists and the added accounts are not duplicate with existing accounts.

Account	Password	First name	Last name	Alias	User group	Email
test2	test2				test	
test3	test3				test	
test4	test4				test	

d Click **Please select an .xls or .xlsx file** to upload the file. After uploading, users are automatically created.



3.18.5 Configuring SMS Authentication on Ruijie Cloud

1. Adding a Twilio Account

Prerequisites

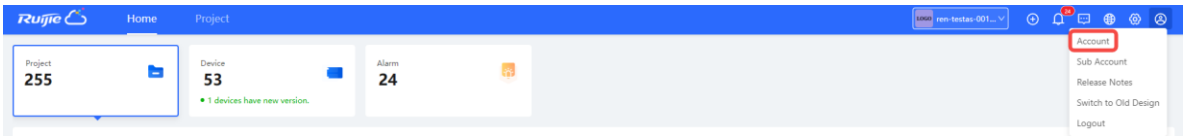
A Twilio account has been applied for from the Twilio official website (https://www.twilio.com/login).

Note

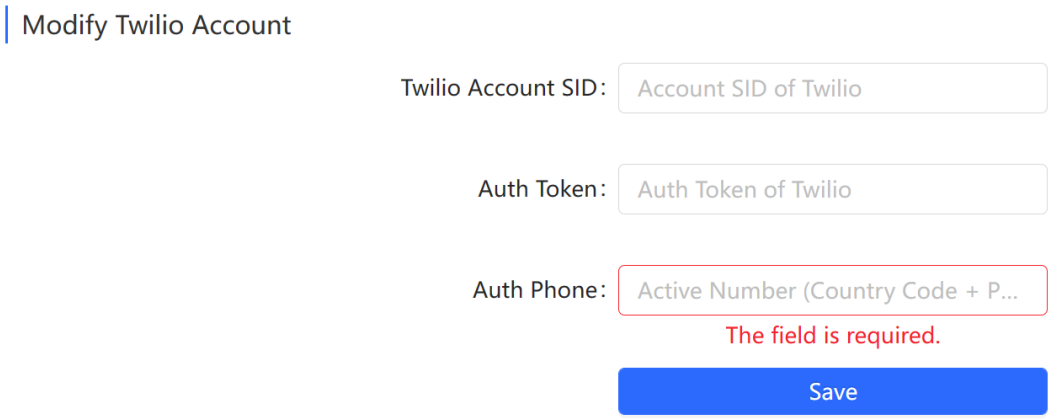
A Twilio account is used to send the SMS verification code.

Configuration Steps

(1) Log in to Ruijie Cloud and choose >> **Account**.



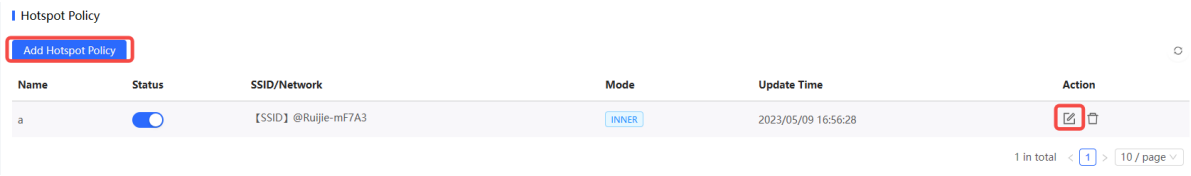
(2) Add Twilio account information and click **Save**.



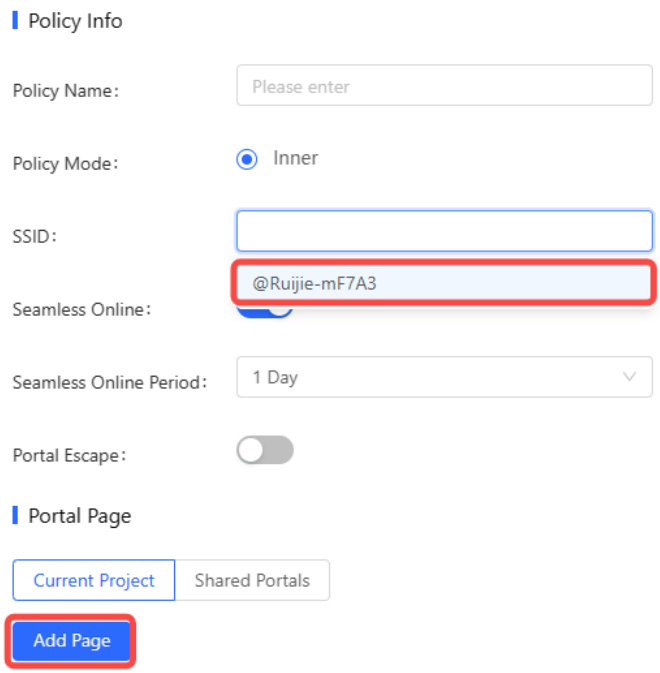
2. Configuring a Portal Template with the Authentication Mode Set to SMS

(1) Log in to Ruijie Cloud, choose **Project** >> **Configuration >> Auth & Accounts** >> **Authentication** >> **Hotspot Policy**, and select a network that needs to configure wireless authentication.

(2) Click **Add Hotspot Policy** to create a hotspot policy, or click to edit the authentication mode of an existing SSID.



(1) Select the SSID to be authenticated, and click **Add Page** to enter the portal template configuration page.



(4) Configure basic settings of the portal template.

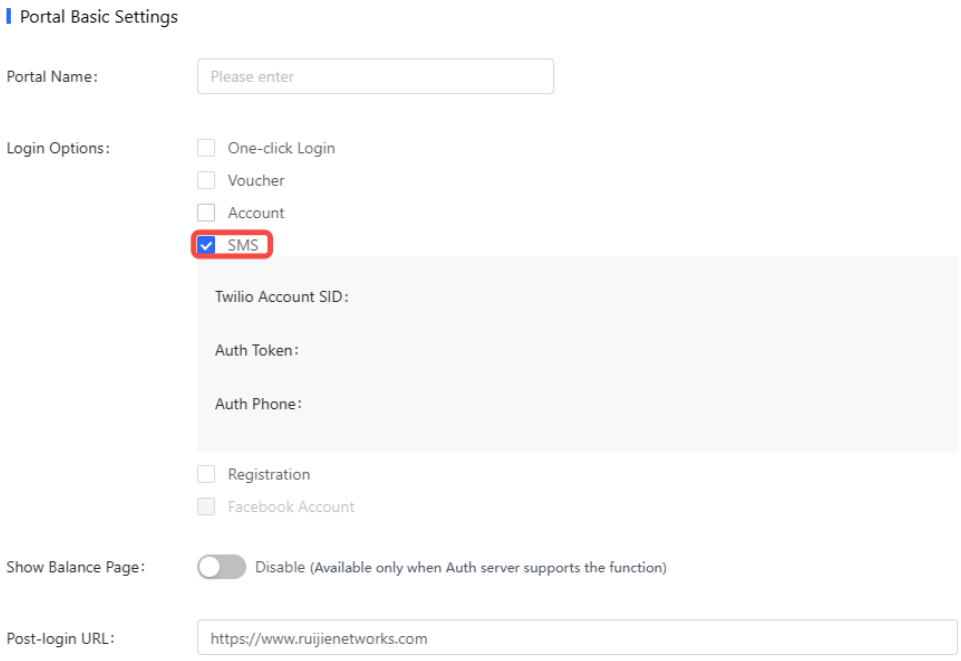


Table 3-7 **Basic Information of the Portal Template**

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Select **SMS**, which indicates login with the phone number and code.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.

Parameter	Description
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) On the **Portal Page** section, configure the required settings for the portal page.

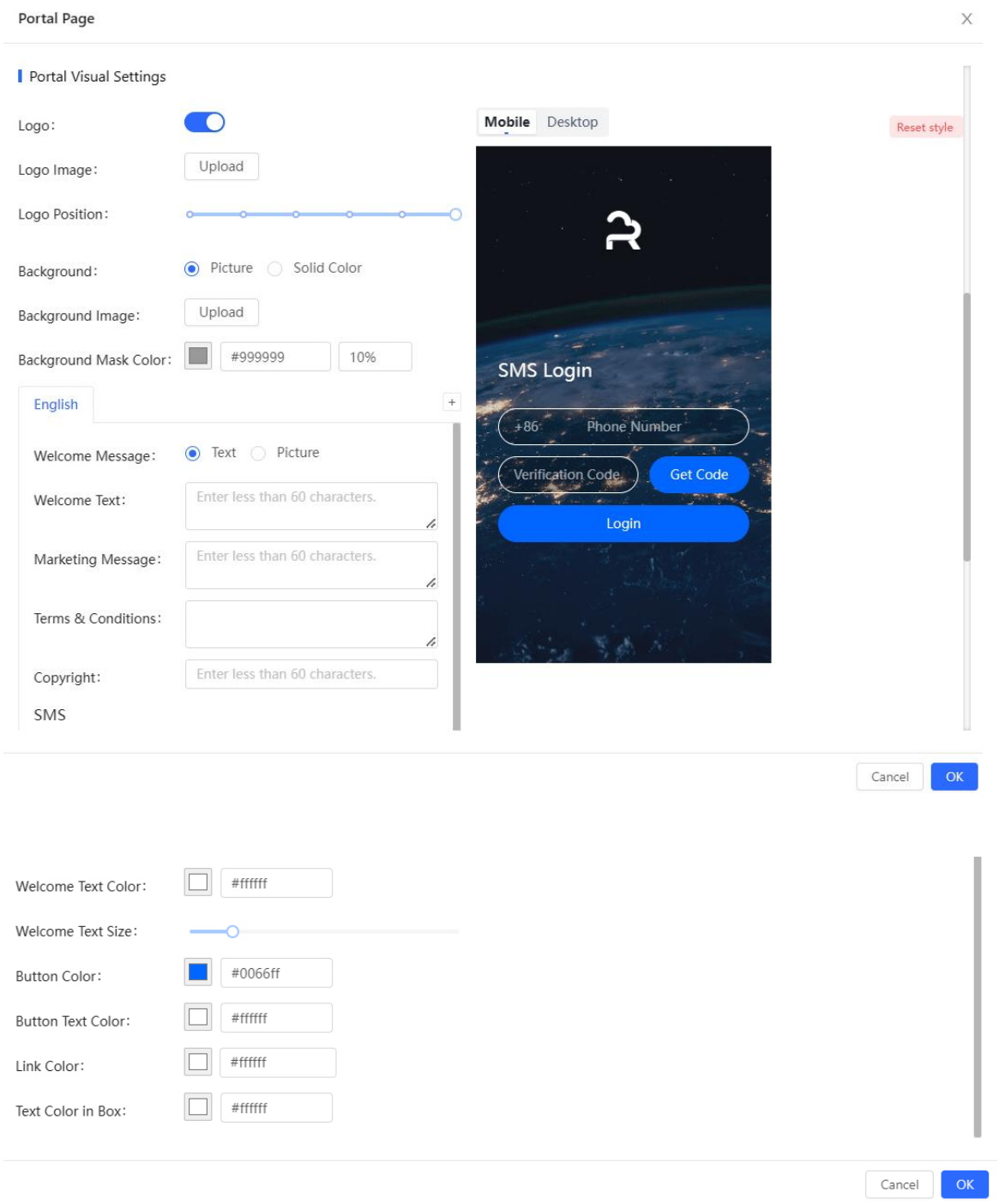
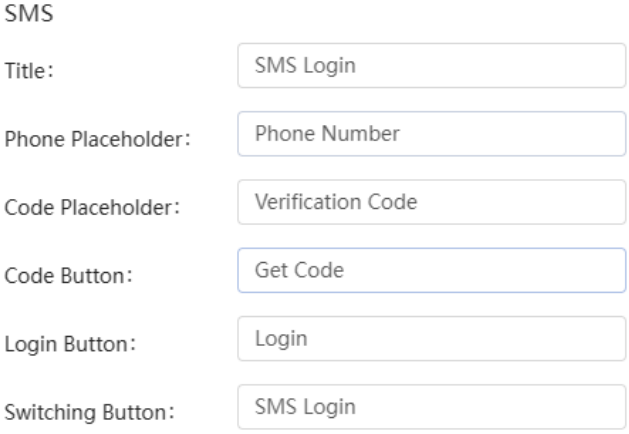


Table 3-8 **Information of the Portal Page**

Parameter	Description
Logo	Select whether to display the logo image.

Parameter	Description
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.
Background Image	When **Background** is set to **Image**, upload the background image or select the default image.
Background Mask Color	Select the background mask color. The default value is #999999.
Language	Select the language of the portal page and configure the content displayed on the portal page as required. You can click + to add portal pages in other languages. ● Welcome Message: Select the welcome message with the image or text. ● Welcome Text: Enter the welcome text. ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● SMS: Enter the name of controls related to SMS authentication. 
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

(5) After the configuration, click **OK** to save the portal template configurations.

3.18.6 Configuring an Authentication-Free User List on eWeb Management System

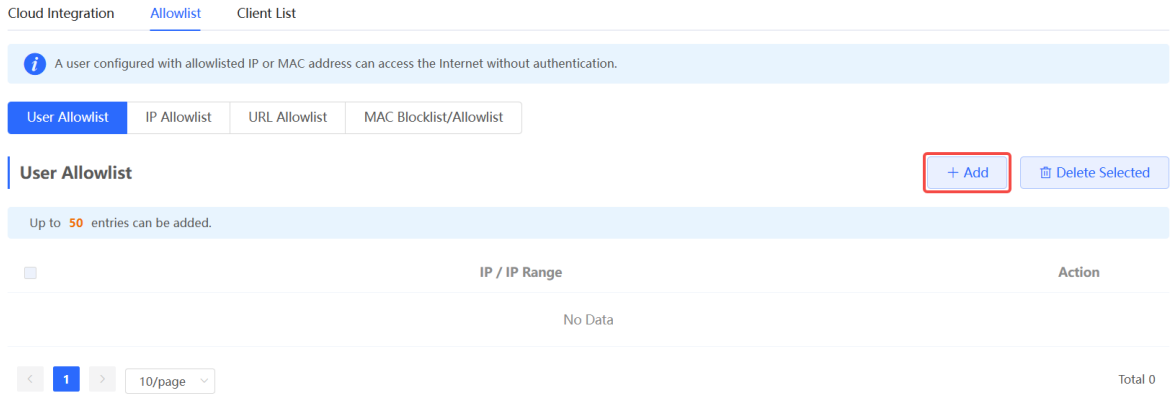
You can configure authentication-free for wireless STAs (IP address/MAC address), public IP addresses, and domain names. Users can directly use network services or access specific websites without entering the username, password, or other information.

Configuring an Authentication-Free User

1. Configuring an Authentication-Free User

(1) Choose **Network** (**WLAN**) >> **Wireless Auth** >> **Allowlist >> User Allowlist.**

(2) Click **Add** to open the configuration page.

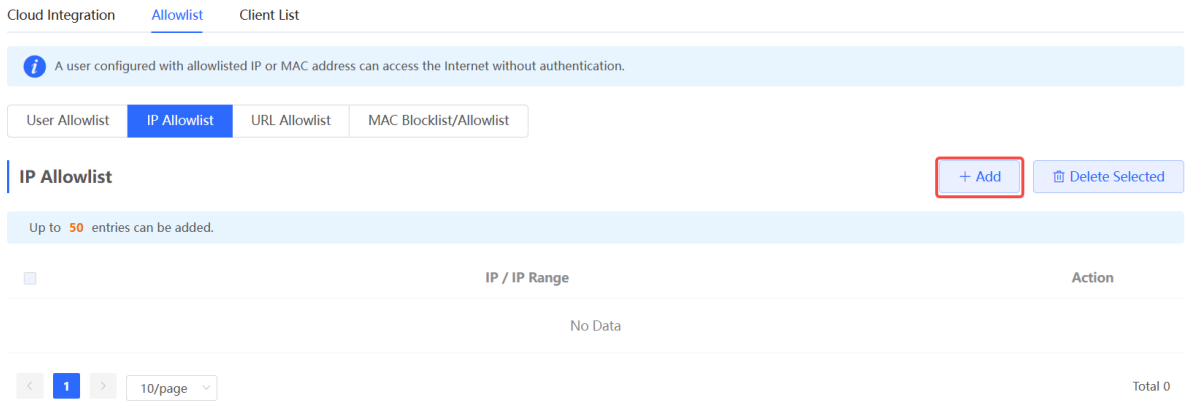


(3) Configure an STA IP address or IP address range. After the configuration, click **OK** to save the configurations.

2. Configuring an Authentication-Free Public IP Address

(1) Choose **Network** (**WLAN**) >> **Wireless Auth** >> **Allowlist >> IP Allowlist.**

(2) Click **Add** to open the configuration page.

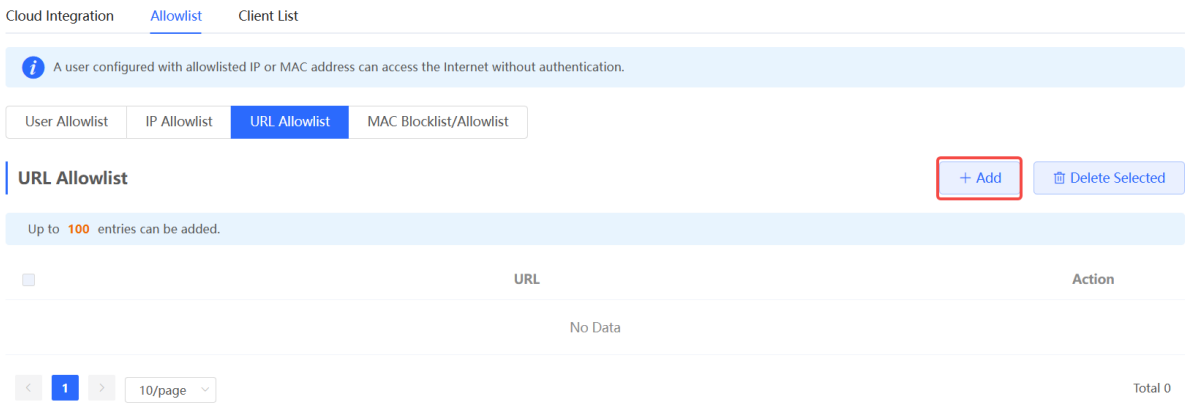


(3) Configure a public IP address or public IP address range. After the configuration, click **OK** to save the configurations.

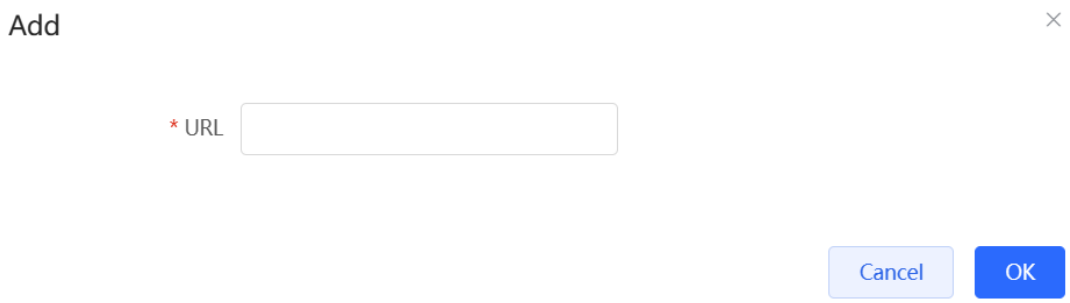
3. Configuring a URL Allowlist

(1) Choose **Network** (**WLAN**) >> **Wireless Auth** >> **Allowlist >> URL Allowlist.**

(2) Click **Add** to open the configuration page.



(3) Configure authentication-free websites. After the configuration, click **OK**.

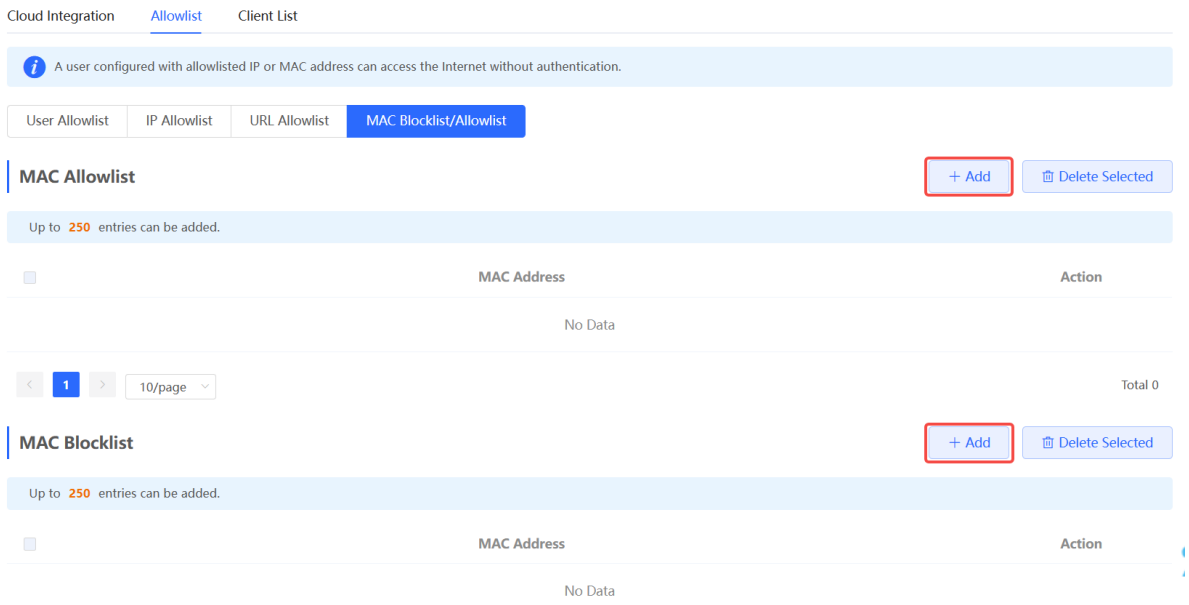


4. Configuring a MAC Address Allowlist and Blocklist

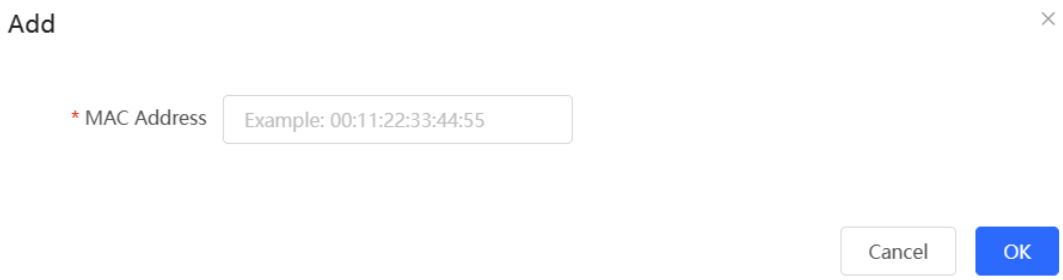
STAs whose MAC addresses are added to the MAC address allowlist can access the network without authentication, and STAs whose MAC addresses are added to the MAC address blocklist are forbidden to access the network.

(1) Choose **Network** (**WLAN**) >> **Wireless Auth** >> **Allowlist >> MAC Blocklist/Allowlist.**

(2) Click **Add** to open the MAC address allowlist or blocklist configuration page.



(3) Configure the MAC address of a wireless STA. After the configuration, click **OK**.

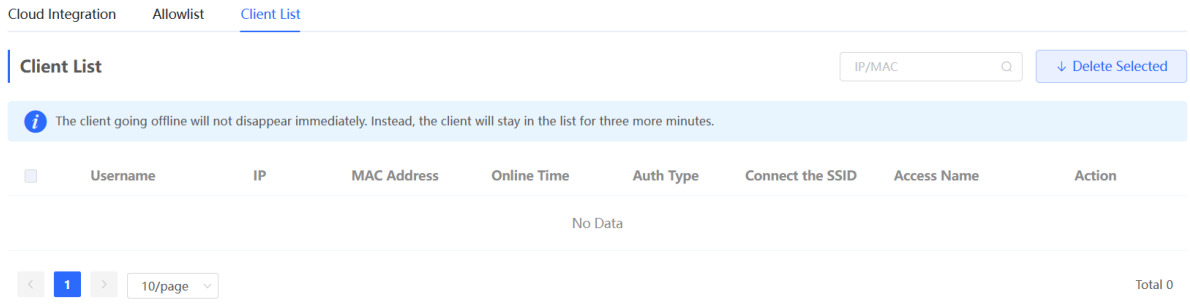


3.18.7 Displaying Authenticated Users on Eweb Management System

Choose **Network** (**WLAN**) > **Wireless Auth** > **Client List** to display authenticated users.

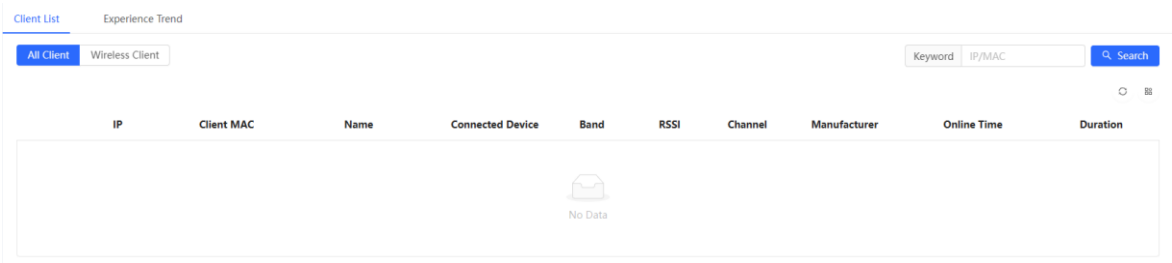
Note

The client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes.



3.18.8 Displaying Authenticated Users on Ruijie Cloud

Log in to Ruijie Cloud, choose **Project** >> **Monitoring >> Clients** >> **Auth Client**, and select a network that needs to display authenticated users.



4 Network Settings

4.1 Switching Work Mode

4.1.1 Work Mode

See Work Mode for details.

4.1.2 Self-Organizing Network Discovery

When setting the work mode, you can set whether to enable the self-organizing network discovery function. This function is enabled by default.

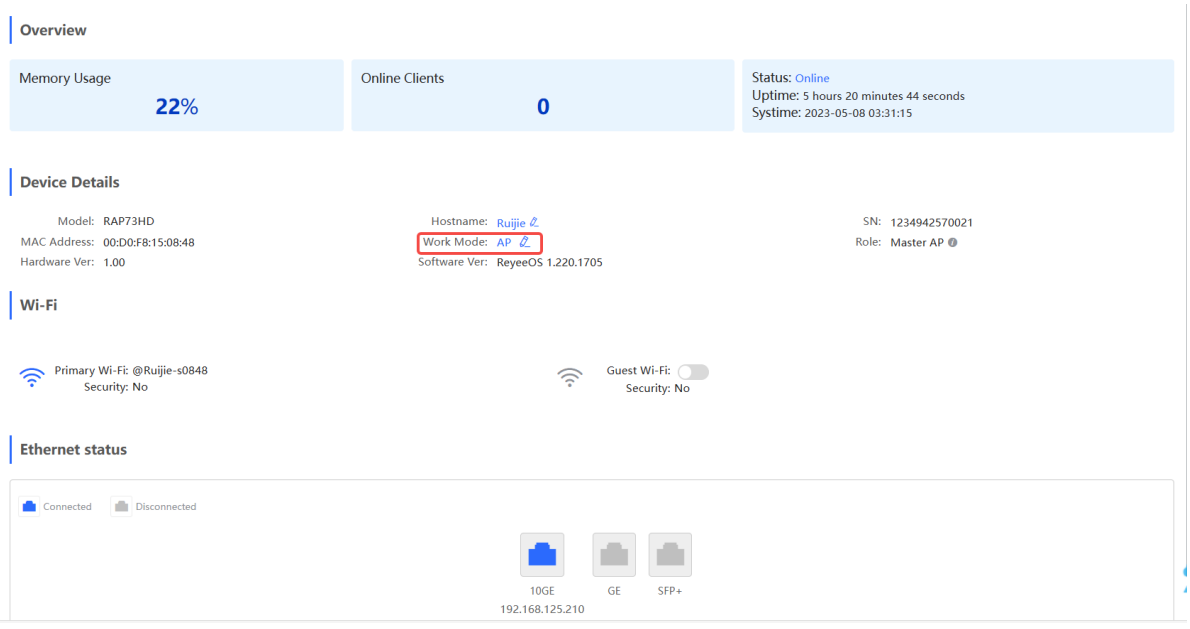
After the self-organizing network discovery function is enabled, the device can be discovered in the network and discover other devices in the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the Web management page of any device in the network to check information about all devices in the network. After this function is enabled, clients can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

If the self-organizing network discovery function is disabled, the device will not be discovered in the network and it runs in standalone mode. After logging in to the Web page, you can configure and manage only the currently logged in device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the self-organizing network discovery function.

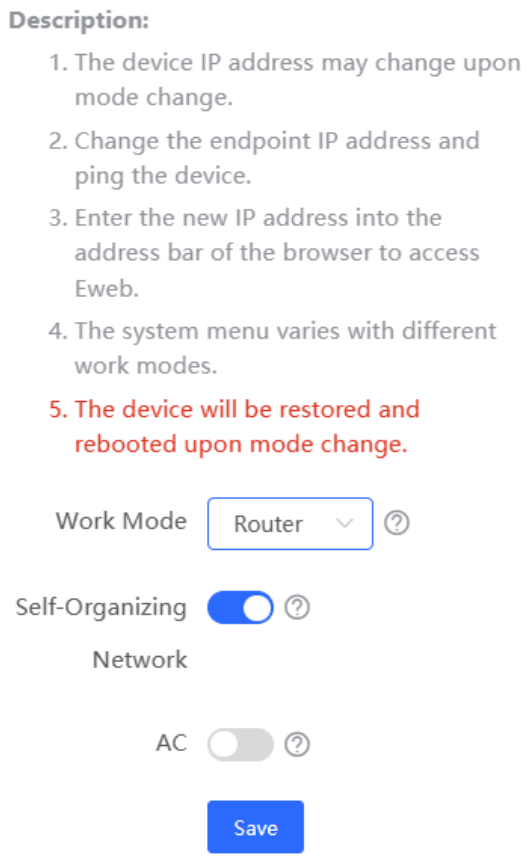
4.1.3 Configuration Steps

In **Local Device** mode, choose **Overview** >> **Device Details.**

Click **Work Mode** to edit the work mode of the device.



AC function switch: If a device works in the router mode and the self-organizing network discovery function is enabled, you can enable or disable the AC function. After the AC function is enabled, the device in the router mode supports the virtual AC function and can manage downlink devices. If this function is disabled, the device needs to be elected as an AC in self-organizing network mode and then manage downlink devices.



Note

- By enabling self-organizing network, you can view the device's role on the self-organizing network. See Viewing Device Role.
- After being switched to the router mode, the device restores to factory settings. The IP address of the LAN port changes to 192.168.120.1, and the DHCP server function is enabled. You are advised to configure the PC to obtain an IP address automatically, and enter 10.44.77.254 in the address bar of your browser to configure the AP in router mode.

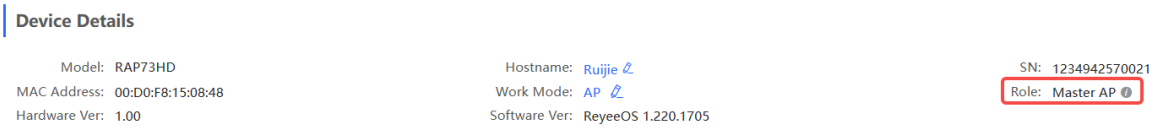
4.1.4 Viewing Device Role

In **Local Device** mode, choose **Overview** >> **Device Details**.

If the self-organizing network is enabled, you can view the device role on the **Device Details** page.

Master AP/AC: The device can manage downlink devices.

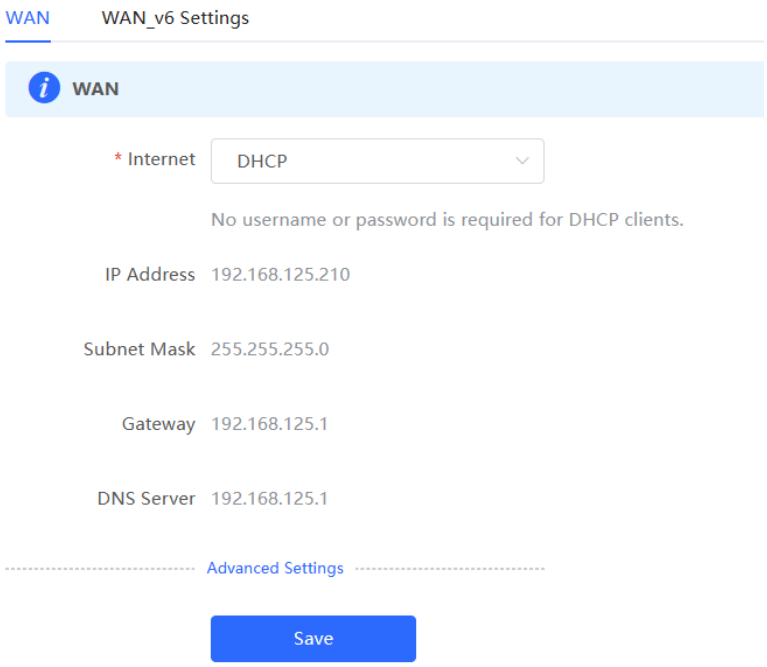
Slave AP/Device: The device has been managed by an AC. The slave Aps are managed by the master AP/AC in a unified manner. Some wireless network settings cannot be edited alone, and thus the master AP/AC delivers configurations to edit the network settings in a unified manner.



4.2 Configuring Internet Connection Type (IPv4)

In **Local Device** mode, choose **Network** >>**WAN**

Select the Internet connection type after confirming with the ISP. For detailed configuration, see Work Mode. After completing the configuration, click **Save**.



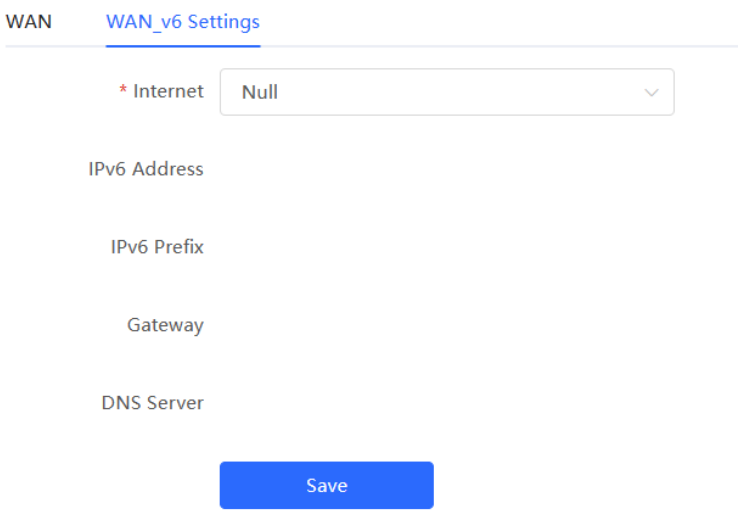
The device supports the following Internet connection types:

- **PPPoE**: This Internet connection type is supported only when the device works in routing mode. You need to manually configure the PPPoE username and password.
- **DHCP**: The current device will act as a DHCP client and apply for the IPv4 address/prefix from the upstream network device.
- **Static IP**: If this Internet connection type is selected, you need to manually configure a static IPv4 address, subnet mask, gateway address, and DNS server.

4.3 Configuring Internet Connection Type (IPv6)

In **Local Device** mode, choose **Network** >>**WAN** >> **WAN_v6 Settings**

Select the Internet connection type after confirming with the ISP. For detailed configuration, see Work Mode. After completing the configuration, click **Save**.



The device supports the following Internet connection types:

- **DHCP**: The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device.
- **Static IP**: If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server.
- **Null**: The IPv6 function is disabled on the current WAN port.

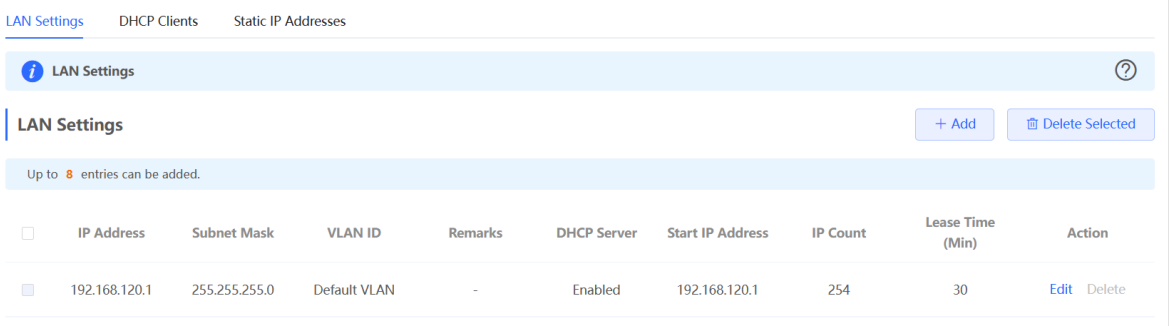
4.4 Configuring LAN Port

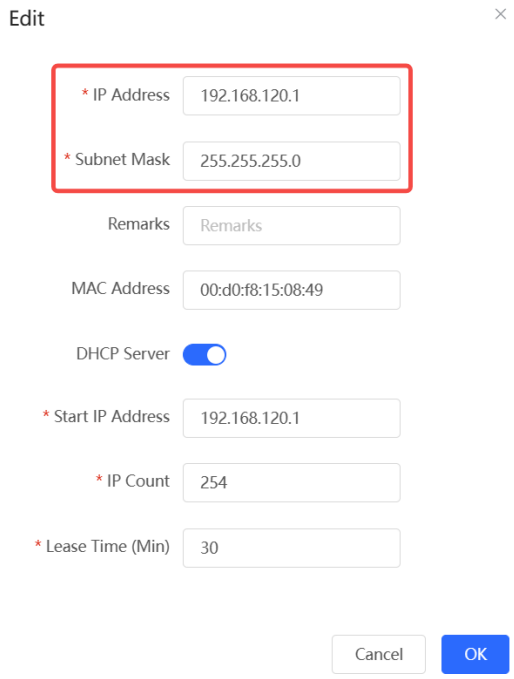
Caution

This function is supported only when the device is in router mode.

In **Local Device** mode, choose **Network** >> **LAN** >> **LAN Settings**

Click **Edit**. In the displayed dialog box, enter the IP address and subnet mask, and click **OK**. Change the IP address of the LAN port. Enter the new IP address in the browser and log in to the device again to configure and manage the device.





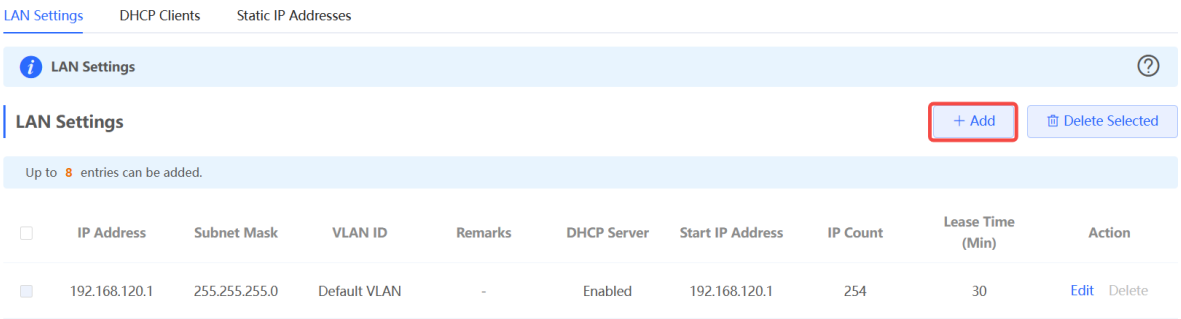
4.5 Creating a VLAN

Caution

This function is supported only when the device is in router mode.

In **Local Device** mode, choose **Network** >> **LAN** >> **LAN Settings**

A LAN can be classified into multiple VLANs. Click **Add** to create a VLAN.



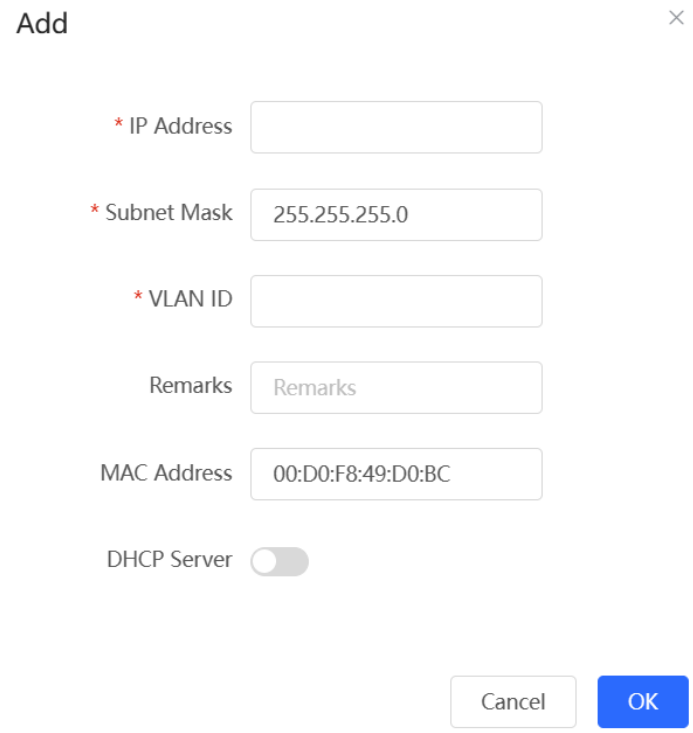


Table 4-1 **VLAN Configuration**

Parameter	Description
IP Address	IP address of the VLAN interface. The default gateway of devices that access the Internet through the current LAN should be set to this IP address.
Subnet Mask	Subnet mask of the IP address of the VLAN interface.
VLAN ID	VLAN ID.
Remarks	VLAN description.
MAC Address	MAC address of the VLAN interface.
DHCP Server	Enable the DHCP server function. After it is enabled, devices on the LAN can automatically obtain IP addresses. After the DHCP service is enabled, you need to configure the start IP address to be assigned, number of IP addresses to be assigned, and address lease term for the DHCP server, and other DHCP server options. For details, see Configuring DHCP Server.

Caution

VLAN configuration is associated with the configuration of the uplink device. Therefore, refer to the configuration of the uplink device when configuring a VLAN.

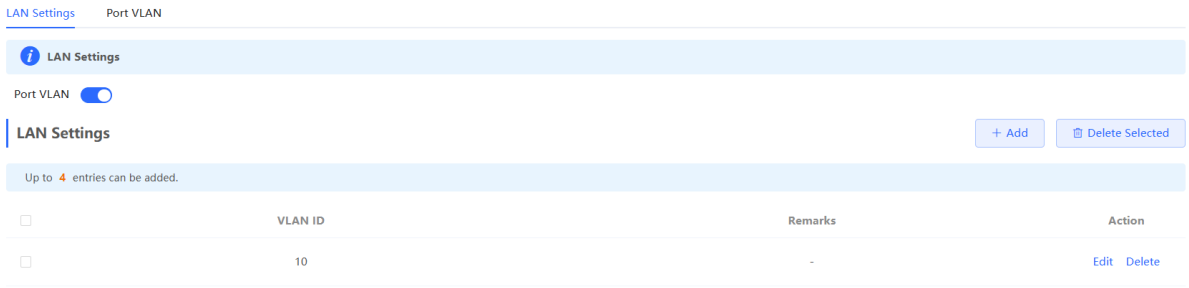
4.6 Configuring Port VLAN

Caution

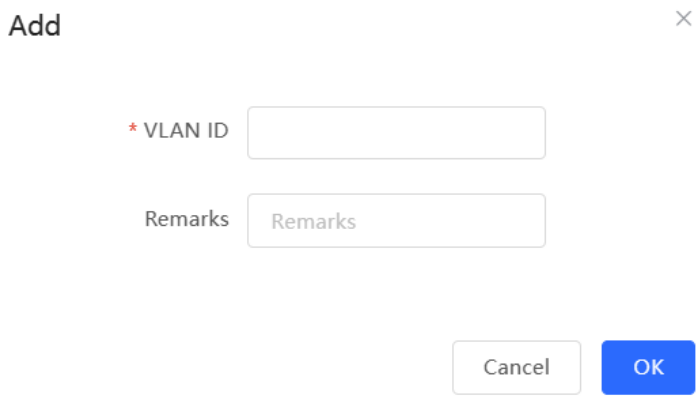
The port VLAN can be configured only when the device works in AP mode.

In **Local Device** mode, choose **Network** >> **LAN**

(1) On the **LAN Settings** tab page, turn on **Port VLAN**, and click **OK** in the confirmation dialog box.

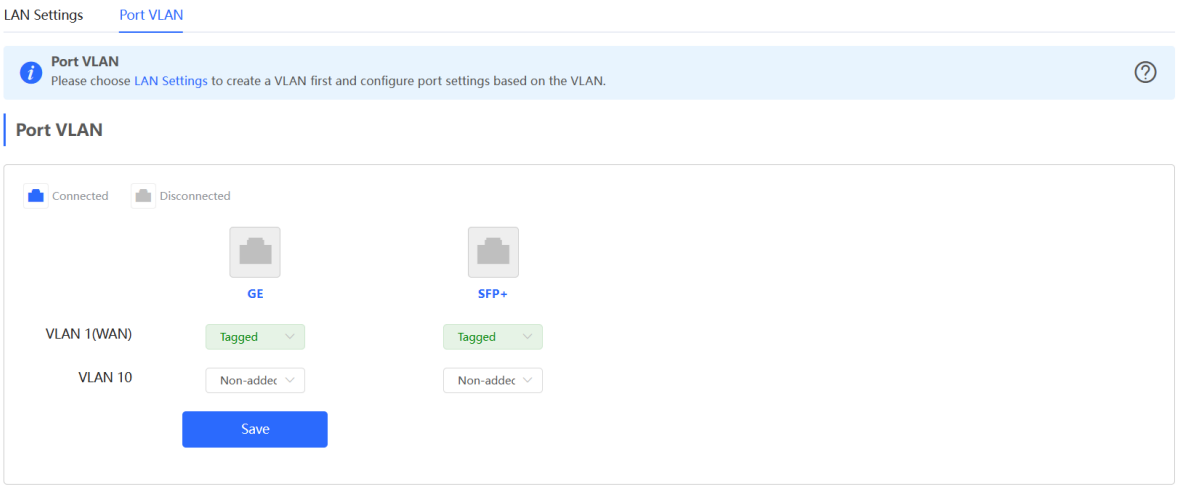


(2) Click **Add**. Enter the VLAN ID and description, and click **OK** to create a VLAN. The added VLAN is used to set the VLAN, to which a port belongs.



(3) Switch to the **Port VLAN** tab page and configure VLANs for the port. Click the option box below the port, select the mapping between a VLAN and the port from the drop-down list box, and click **Save**.

- **UNTAG**: Configure the VLAN as the native VLAN of the port. That is, when receiving a packet from this VLAN, the port removes the VLAN tag from the packet and forwards the packet. When receiving an untagged packet, the port adds the VLAN tag to the packet and forwards the packet through the VLAN. Only one VLAN can be configured as an untagged VLAN on each port.
- **TAG**: Configure the VLAN as an allowed VLAN of the port, but the VLAN cannot be the native VLAN. That is, VLAN packets carry the original VLAN tag when they are forwarded by the port.
- **Not Join**: Configure the port not to allow packets from this VLAN to pass through. For example, if VLAN 10 and VLAN 20 are not added to port 2, port 2 will neither receive nor send packets from or to VLAN 10 and VLAN 20.



4.7 Changing MAC Address

In **Local Device** mode, choose **Network** >> **WAN**

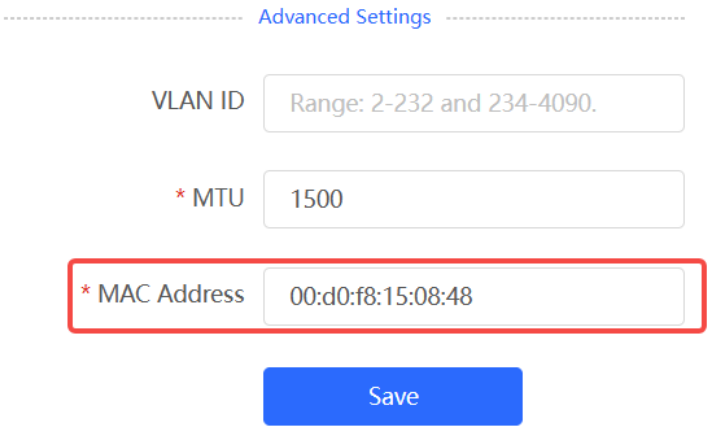
ISPs may restrict the access of devices with unknown MAC addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port.

Click to expand **Advanced Settings**, enter the MAC address, and click **Save**. You do not need to change the default MAC address unless in special cases.

In the router mode, change the MAC address of the LAN port on **Network** > **LAN**.

Caution

Changing the MAC address will disconnect the device from the network. You need to reconnect the device to the network or restart the device. Therefore, exercise caution when performing this operation.

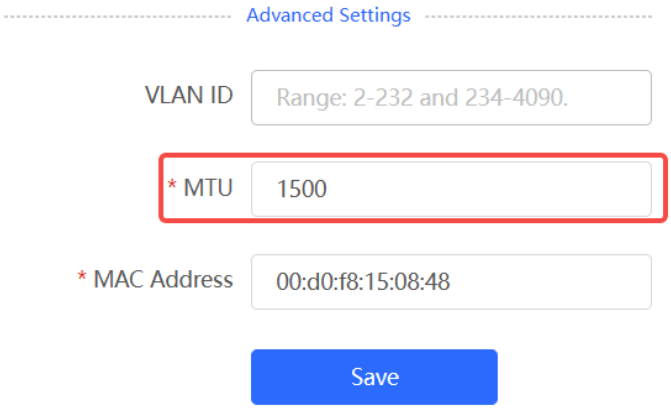


4.8 Changing MTU

In **Local Device** mode, choose **Network** >> **WAN**

WAN interface MTU indicates the maximum transmission unit (MTU) allowed by the WAN interface. The default value is 1500 bytes, indicating the maximum data forwarding efficiency. Sometimes, ISP networks restrict the speed of large data packets or forbid large data packets from passing through. As a result, the network speed is unsatisfactory or even the network is disconnected. In this case, you can set the MTU value to a smaller value.

Click **Advanced Settings**, enter the MTU value, and click **Save**.



4.9 Configuring DHCP Server

Caution

This function is supported only when the device is in router mode.

4.9.1 DHCP Server

In the router mode, the DHCP server function can be enabled on the device to automatically assign IP addresses to clients so that clients connected to the LAN ports or Wi-Fi network of the device obtain IP addresses for Internet access.

4.9.2 Configuring the DHCP Server Function

In **Local Device** mode, choose **Network** >> **LAN** >> **LAN Settings**

DHCP Server: The DHCP server function is enabled by default in the router mode. You are advised to enable the function if the device is used as the sole router in the network. When multiple routers are connected to the upper-layer device through LAN ports, disable this function.

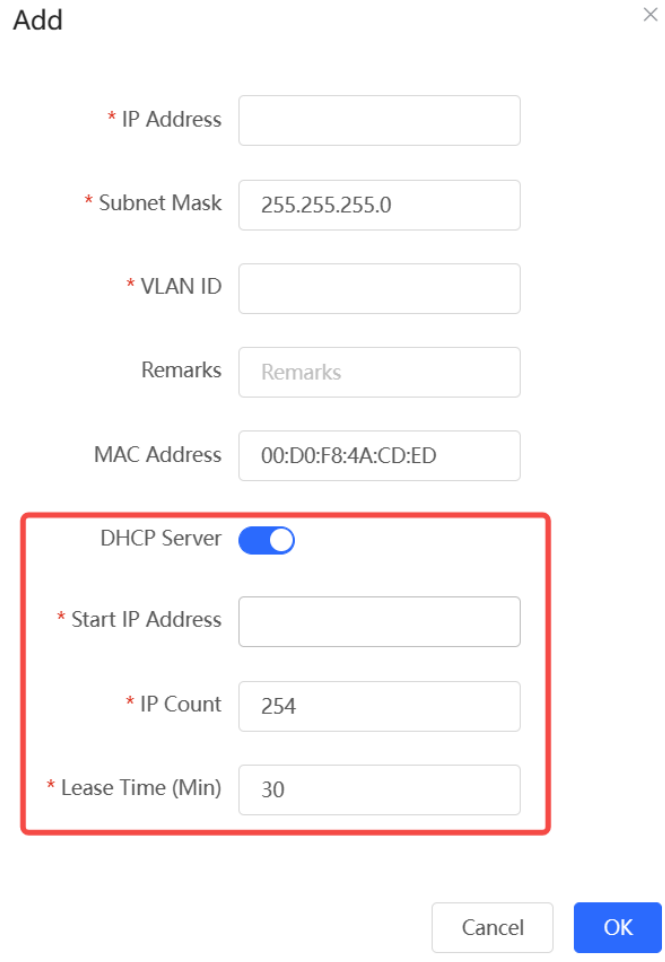
Caution

If the DHCP server function is disabled on all devices in the network, clients cannot automatically obtain IP addresses. You need to enable the DHCP server function on one device or manually configure a static IP address for each client for Internet access.

Start: Enter the start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, no IP address can be obtained from the address pool.

IP Count: Enter the number IP addresses in the address pool.

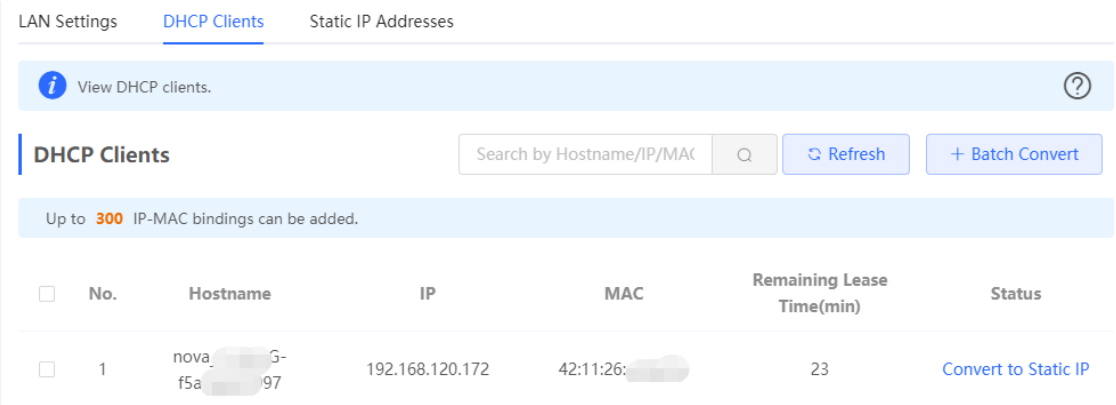
Lease Time (Min): Enter the address lease term. When a client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease term expires. After the client connection is restored, the client can request an IP address again. The default lease term is 30 minutes.



4.9.3 Displaying Online DHCP Clients

In **Local Device** mode, choose **Network** >> **LAN** >> **DHCP Clients**

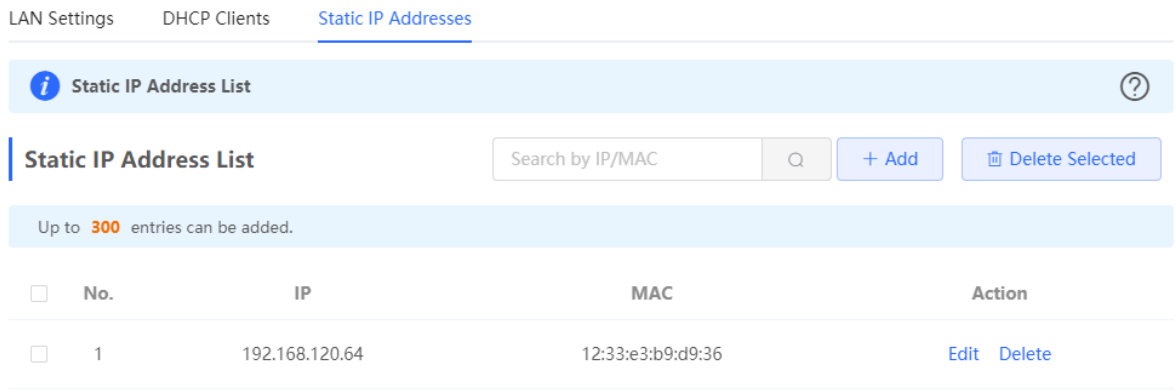
Check information about an online client. Click **Convert to Static IP**. Then, the static IP address will be obtained each time the client connects to the network.



4.9.4 Displaying the DHCP Static IP Address List

In **Local Device** mode, choose **Network** >> **LAN** >> **Static IP Addresses**

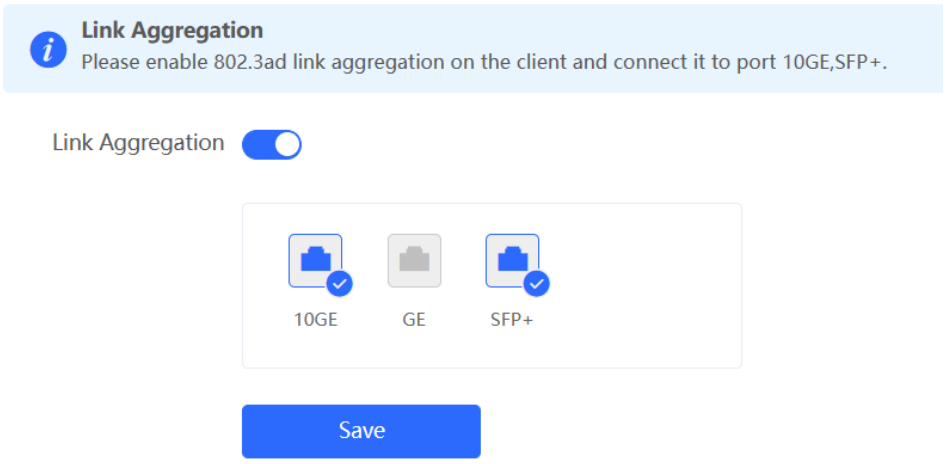
Click **Add**. In the displayed static IP address binding dialog box, enter the MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the client connects to the network.



4.10 Link Aggregation

In **Local Device** mode, choose **Advanced**>> **Link Aggregation**

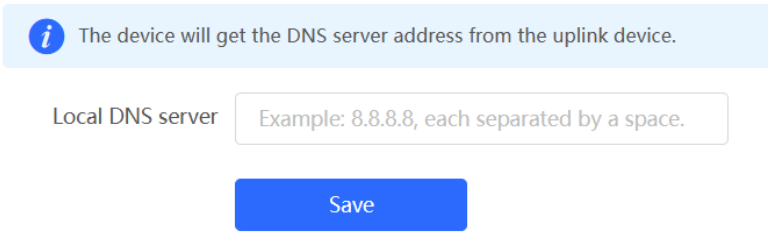
Link Aggregation can improve the throughput in the network and deal with link congestion.



4.11 Configuring DNS

In **Local Device** mode, choose **Advanced** >> **Local DNS**

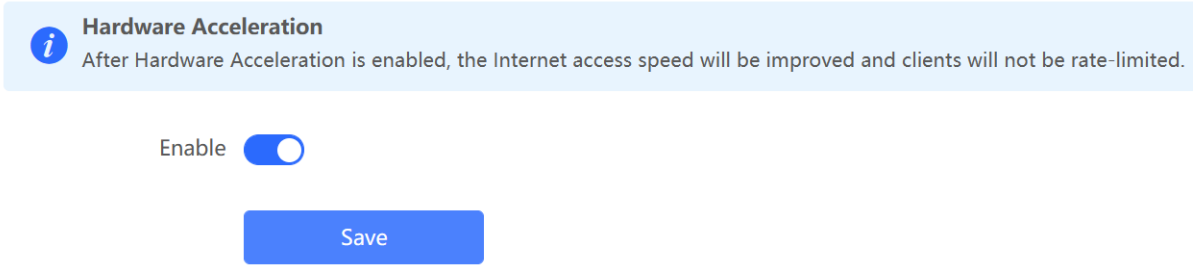
Enter the IP address of the DNS server and click **Save**. The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default. The default configuration is recommended. The available DNS service varies from region to region. You can consult the local ISP.



4.12 Hardware Acceleration

In **Local Device** mode, choose **Advanced** >> **Hardware Acceleration**

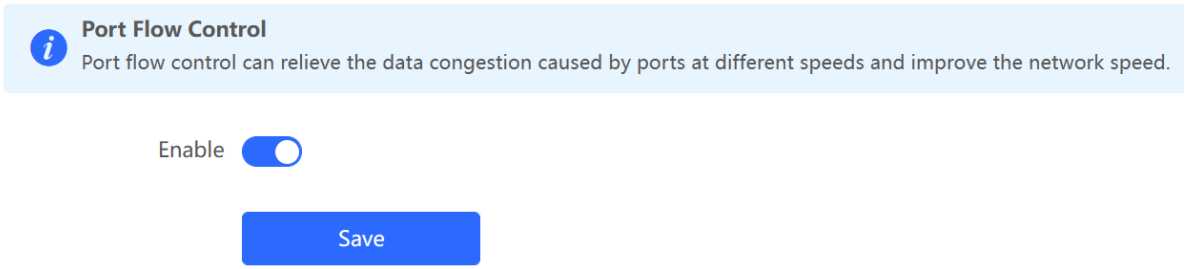
After Hardware acceleration is enabled, the Internet access speed will be improved.



4.13 Configuring Port Flow Control

In **Local Device** mode, choose **Advanced** >> **Port Settings**

When the LAN ports work at different rates, data congestion may occur, which can slow down the network speed and affect the Internet access experience. Enabling port flow control can help mitigate this problem.



4.14 Configuring ARP Binding

Caution

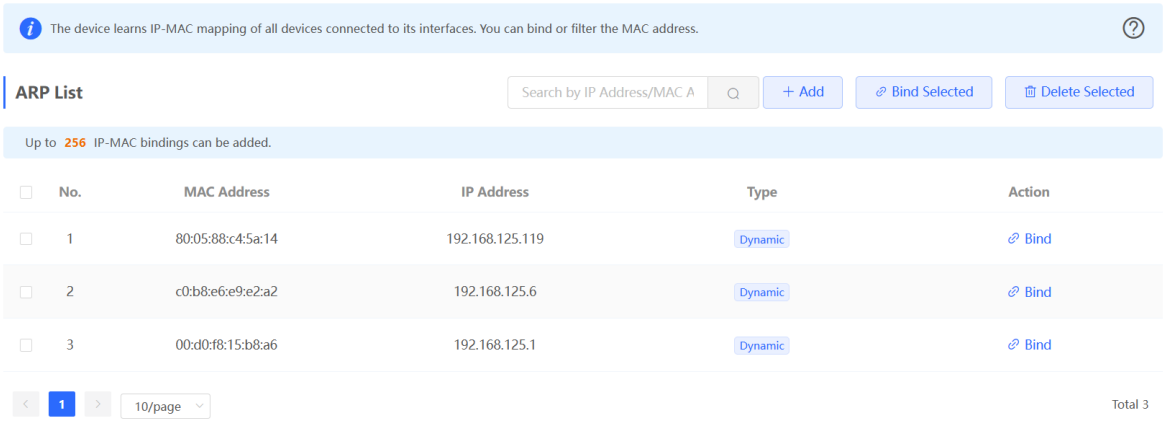
This function is supported only when the device is in router mode.

The device learns the IP and MAC addresses of network devices connected to ports of the device and generates ARP entries. You can bind ARP mappings to improve network security.

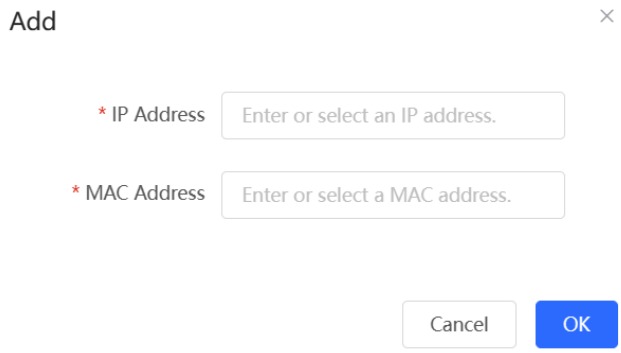
In **Local Device** mode, choose **Security** >> **ARP List**

ARP mappings can be bound in two ways:

(1) Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them. To remove the binding between a static IP address and a MAC address, click **Delete** in the **Action** column.



(2) Click **Add**, enter the IP address and MAC address to be bound, and click **OK**. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the address mapping.



4.15 Configuring LAN Ports

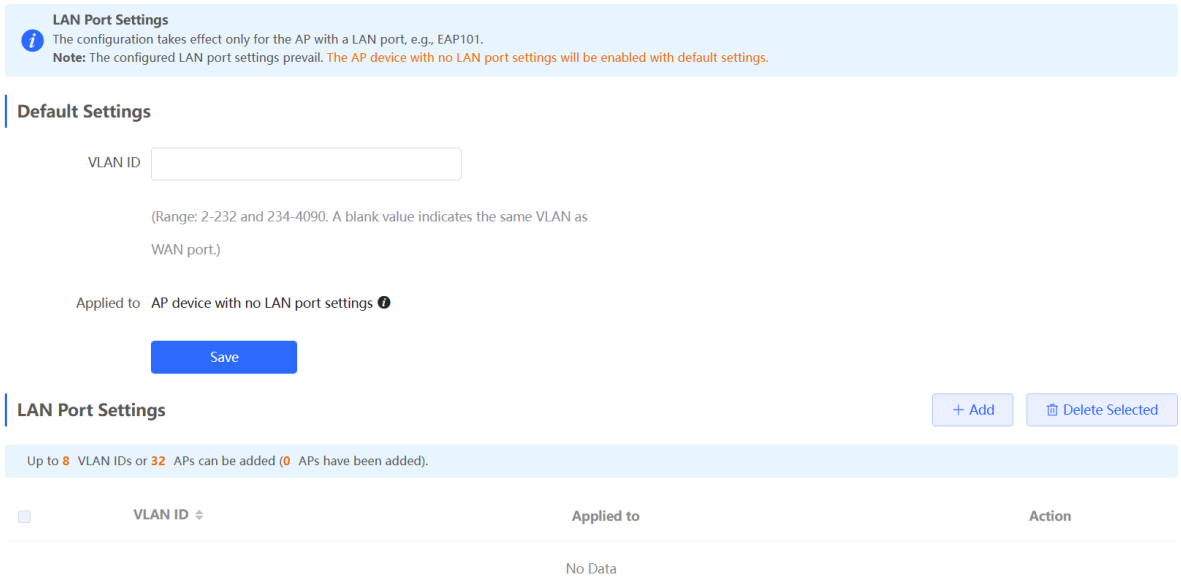
Caution

The configuration takes effect only on APs having wired LAN ports.

Choose **Network** (**WLAN**)>> **LAN Ports**

Enter the VLAN ID and click **Save** to configure the VLAN, to which the AP wired ports belong. If the VLAN ID is null, the wired ports and WAN port belong to the same VLAN.

In self-organizing network mode, the AP wired port configuration applies to all APs having wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially. Click **Add** to add the AP wired port configuration. For APs, to which no configuration is applied in **LAN Port Settings**, the default configuration of the AP wired ports will take effect on them.



4.16 IPv6 Settings

Note

This function is supported only when the device is in router mode.

4.16.1 Overview

Internet Protocol Version 6 (IPv6) is the next generation IP protocol designed by the Internet Engineering Task Force (IETF) to replace IPv4 and solve the IPv4 problems such as address depletion.

4.16.2 IPv6 Basic

1. IPv6 Address Format

IPv6 increases the length of the address from 32 bits in IPv4 to 128 bits, and therefore has a larger address space than IPv4.

The basic format of an IPv6 address is **X:X:X:X:X:X:X:X**. The 128-bit IPv6 address is divided into eight 16-bit sections that are separated by colons (:), and 16 bits in each section are represented by four hexadecimal characters (0–9 and A–F). Each **X** represents a 4-character hexadecimal number.

For example: 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:0:1, 1080:0:0:0:8:800:200C:417A

The number **0** in the IPv6 address can be abbreviated as follows:

- The starting 0s can be omitted. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be written as 2001:CD:34:78:A:B:1200:2100.
- Consecutive 0s can be replaced by two colons (::). For example, **800:0:0:0:0:0:0:1** can be written as **800::1**. Consecutive 0s can be replaced by two colons only when the 16-bit section contains all 0s, and the two colons can only appear once in the address.

2. IPv6 Prefix

An IPv6 address consists of two parts:

- Network prefix: It contains n bits, and is equivalent to the network ID in an IPv4 address.
- Interface identifier: It contains (128 - n) bits, and is equivalent to the host ID in an IPv4 address.

The length of the network prefix is separated from the IPv6 address by a slash (/). For example, **12AB::CD30:0:0:0:0/60** indicates that the length of the prefix used for routing in the address is 60 bits.

3. Special IPv6 Address

There are also some special IPv6 addresses, for example:

fe80::/8 is a link local address, and equivalent to 169.254.0.0/16 in IPv4.

fc00::/7 is a local address, and similar to 10.0.0.0/8, 172.16.0.0/16, or 192.168.0.0/16 in IPv4.

ff00::/12 is a multicast address, and similar to 224.0.0.0/8 in IPv4.

4. NAT66

IPv6-to-IPv6 Network Address Translation (NAT66) is the process of converting the IPv6 address in an IPv6 packet header to another IPv6 address. NAT66 prefix translation is an implementation of NAT66. It replaces the IPv6 address prefix in the packet header with another IPv6 address prefix to achieve IPv6 address translation. NAT66 can realize mutual access between an intranet and Internet.

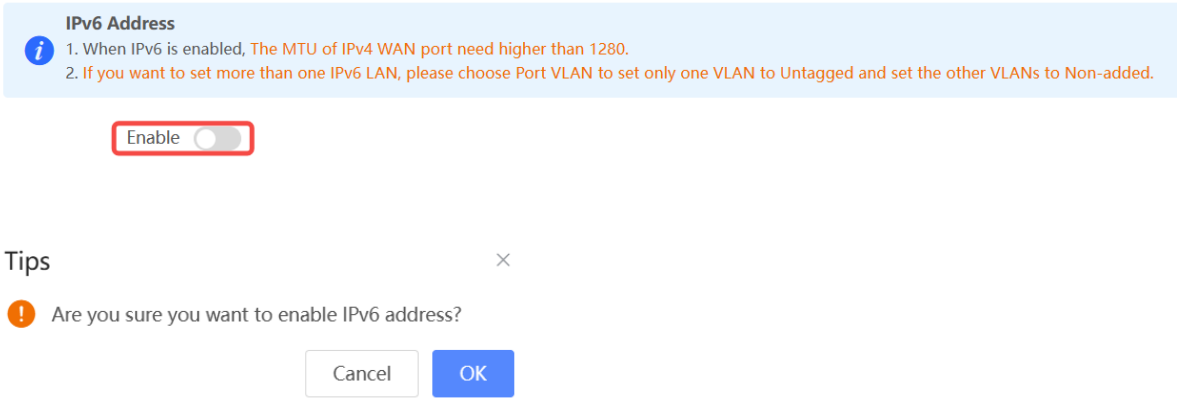
4.16.3 IPv6 Address Assignment Methods

- Manual configuration: The IPv6 address/prefix and other network configuration parameters are manually configured.
- Stateless Address Autoconfiguration (SLAAC): The link local address is generated based on the interface ID, and then the local address is automatically configured based on the prefix information contained in the route advertisement packet.
- Stateful address autoconfiguration, that is, DHCPv6: DHCPv6 is divided into the following two types:
  - DHCPv6 autoconfiguration: The DHCPv6 server automatically configures the IPv6 address/prefix and other network configuration parameters.
  - DHCPv6 Prefix Delegation (PD): The lower-layer network device sends a prefix allocation application to the upper-layer network device. The upper-layer network device assigns an appropriate address prefix to the lower-layer device. The lower-layer device automatically subdivides the obtained prefix (generally less than 64 bits in length) into subnet segments with 64-bit prefix length, and then advertises the subdivided address prefixes to the user link directly connected to the IPv6 host through the route to realize automatic address configuration of the host.

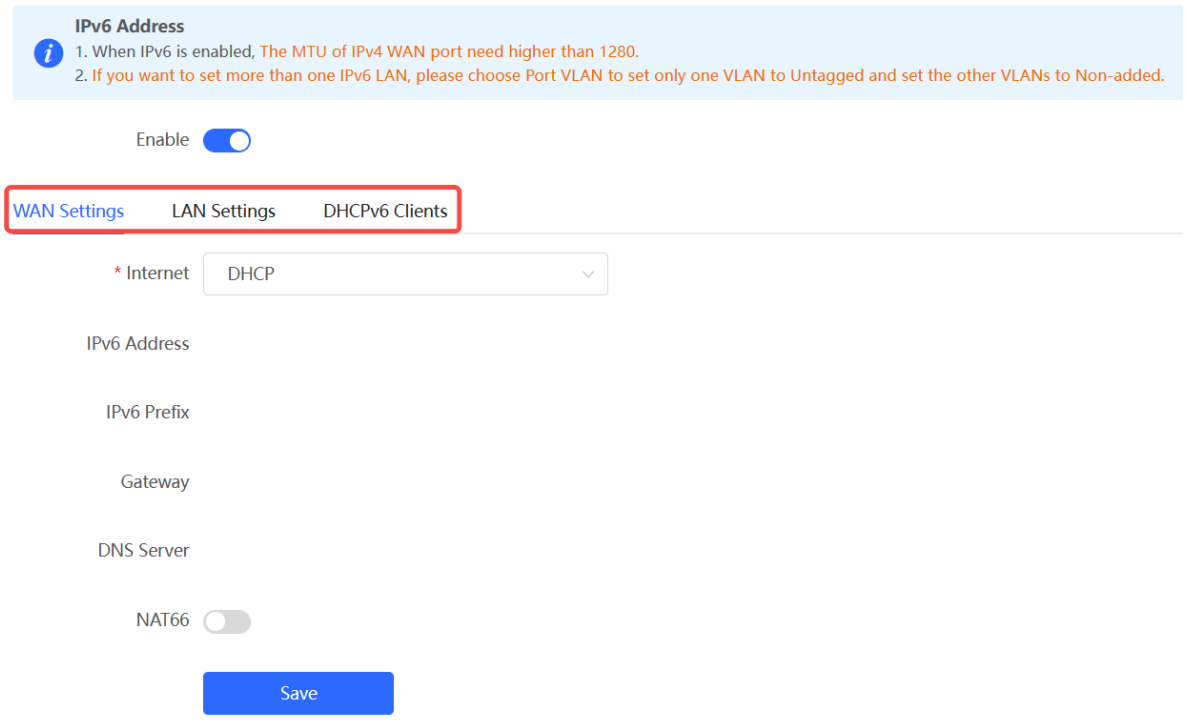
4.16.4 Enabling IPv6

In **Local Device** mode, choose **Network** >> **IPv6 Address**

Click **Enable**, and then click **OK** in the dialog box that appears to enable IPv6.



After the IPv6 function is enabled, you can set the IPv6 addresses for WAN and LAN ports, view DHCPv6 clients, and set static DHCPv6 addresses for clients.



4.16.5 Configuring the IPv6 Address for the WAN Port

In **Local Device** mode, choose **Network>>IPv6 Address >> WAN Settings**

Configure the IPv6 address for the WAN port, and click **Save**.

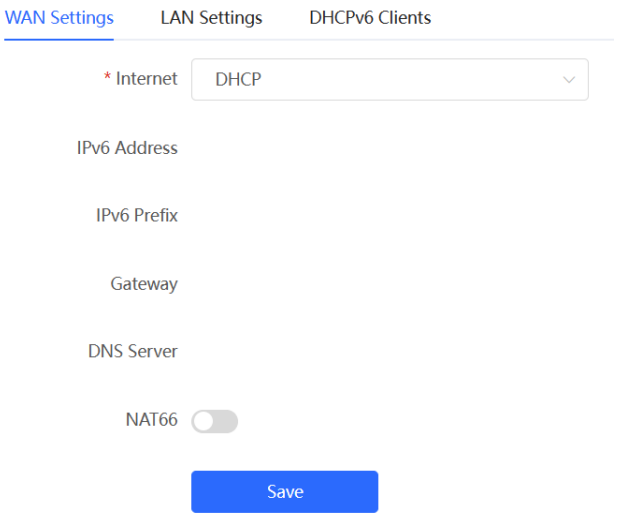


Table 4-2 **IPv6 Address Configuration Parameters of the WAN Port**

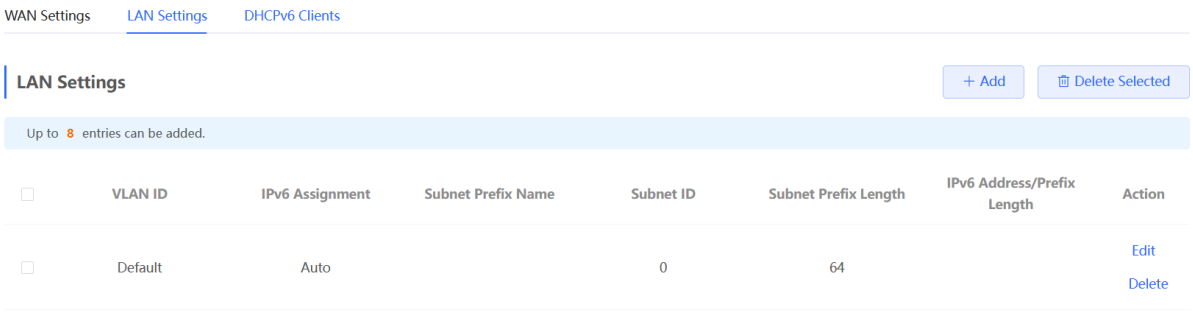
Parameter	Description
Internet	Specify the method for obtaining an IPv6 address for the WAN port.

Parameter	Description
	● **DHCP**: The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device. ● **Static IP**: If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server. ● **Null**: The IPv6 function is disabled on the current WAN port.
IPv6 Address	If **Internet** is set to **DHCP**, the automatically obtained IPv6 address is displayed. If **Internet** is set to **Static IP**, you need to manually configure this parameter.
IPv6 Prefix	If **Internet** is set to **DHCP** and the current device obtains the IPv6 address prefix from the upstream device. The obtained IPv6 address prefix is displayed.
Gateway	If **Internet** is set to **DHCP**, the automatically obtained gateway address is displayed. If **Internet** is set to **Static IP**, you need to manually configure this parameter.
DNS Server	If **Internet** is set to **DHCP**, the automatically obtained DNS server address is displayed. If **Internet** is set to **Static IP**, you need to manually configure this parameter.
NAT66	If the current device cannot access the Internet in DHCP mode or cannot obtain the IPv6 address prefix, you must enable NAT66 to assign the IPv6 address to an intranet client.

4.16.6 Configuring the IPv6 Address for the LAN Port

In **Local Device** mode, choose **Network**>>**IPv6 Address** >> **LAN Settings**

When the device accesses the network in DHCP mode, the upstream device can assign an IPv6 address to the LAN port, and assign IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the upstream device cannot assign an IPv6 address prefix to the current device, you need to manually configure an IPv6 address prefix for the LAN port, and assign IPv6 addresses to the clients in the LAN by enabling the NAT66 function (see Configuring the IPv6 Address for the WAN Port).

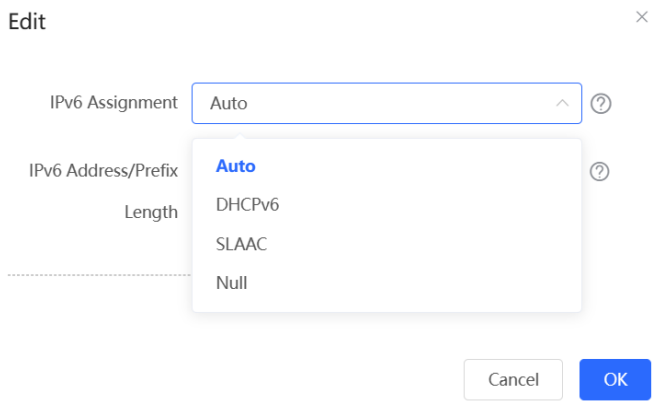


Click **Edit** corresponding to the default VLAN, and fill in a local address of no more than 64 bits in the **IPv6 Address/Prefix Length** column. This address will also be used as the IPv6 address prefix.

IPv6 Assignment specifies the method for assigning IPv6 addresses for clients. The following options are available:

- **Auto**: Both DHCPv6 and SLAAC are used to assign IPv6 addresses to clients.
- **DHCPv6**: DHCPv6 is used to assign IPv6 addresses to clients.
- **SLAAC**: SLAAC is used to assign IPv6 addresses to clients.
- **Null**: No IPv6 addresses are assigned to clients.

The setting of **IPv6 Assignment** is determined by the protocol supported by intranet clients. If you are not sure about the protocol supported by intranet clients, select **Auto**.



You can click **Advanced Settings** to configure more address attributes.

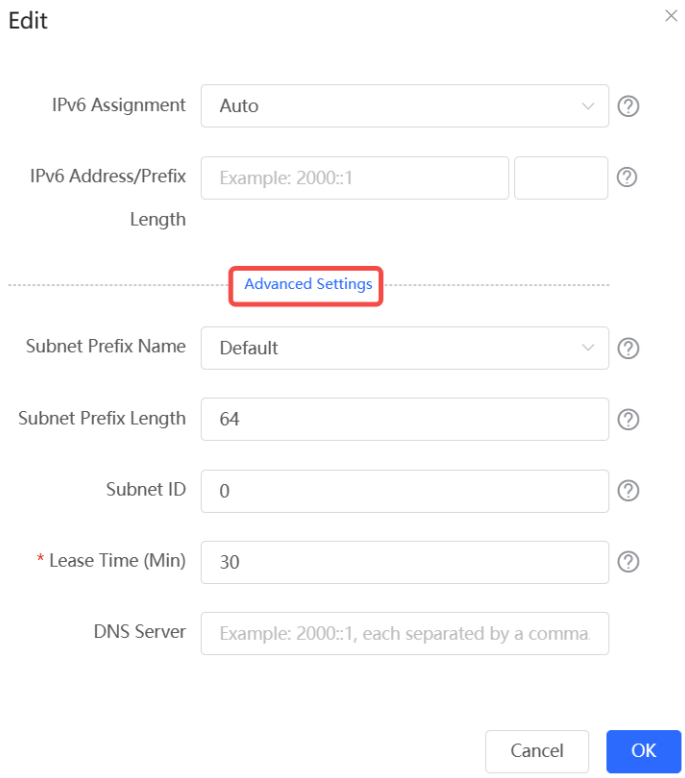


Table 4-3 **IPv6 Address Configuration Parameters of the LAN Port**

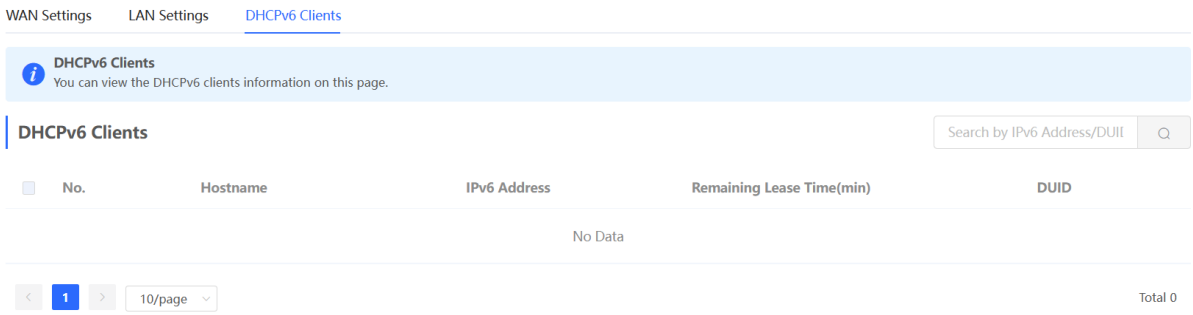
Parameter	Description
Subnet Prefix Name	Configure the interface from which the prefix is obtained, for example, **WAN_V6**. The default value is all interfaces.
Subnet Prefix Length	Configure the length of the subnet prefix. The value ranges from 48 to 64.
Subnet ID	Configure the subnet ID in hexadecimal notation. **0** indicates that the subnet ID automatically increments.
Lease Time (Min)	Configure the lease term of the IPv6 address. The unit is minutes.
DNS Server	Configure the address of the IPv6 DNS server.

4.16.7 Viewing DHCPv6 Clients

In **Local Device** mode, choose **Network** > **IPv6 Address** > **DHCPv6 Clients**.

When the device acts as a DHCPv6 server to assign IPv6 addresses to clients, you can view information about the clients that obtain IPv6 addresses from the device on the current page. The information includes the host name, IPv6 address, remaining lease term, and DHCPv6 Unique Identifier (DUID) of each client.

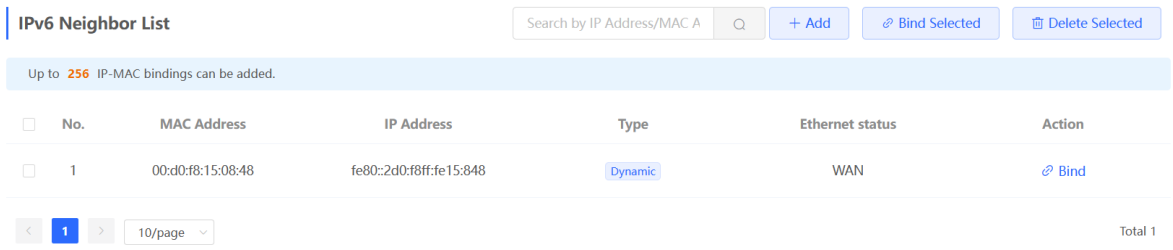
Enter an IPv6 address or DUID in the search bar, and click to quickly find the information of the specified DHCPv6 client.



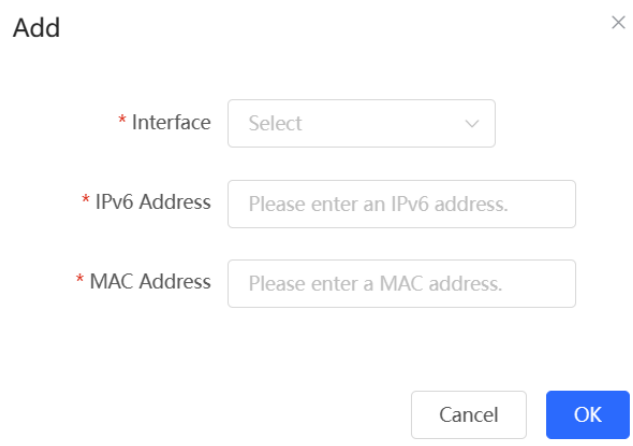
4.16.8 Configuring the IPv6 Neighbor List

In IPv6, Neighbor Discovery Protocol (NDP) is an important basic protocol. NDP replaces the ARP and ICMP route discovery protocols of IPv4, and supports the following functions: address resolution, neighbor status tracking, duplicate address detection, router discovery, and redirection.

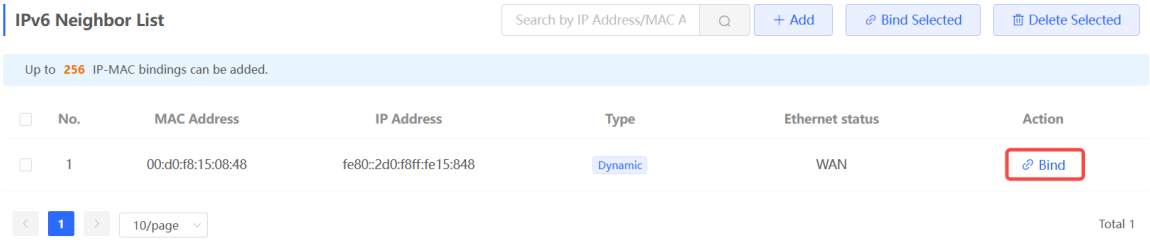
In **Local Device** mode, choose **Security>> IPv6 Neighbor List**



(1) Click **Add** and add the interface, IPv6 address and MAC address of the neighbor



(2) Select the IPv6 neighbor list to be bound, and click **Bind** in the **Action** column to bind the IPv6 address and MAC address.

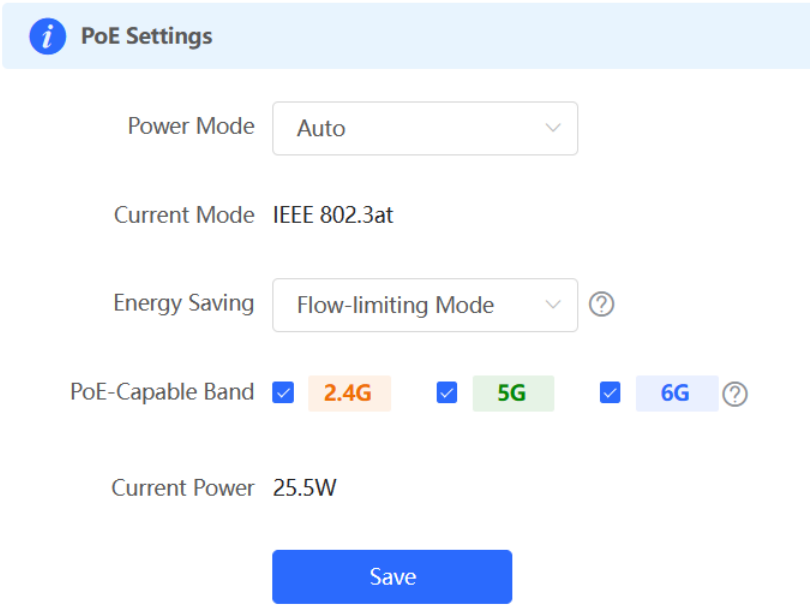

IPv6 Neighbor List
Search by IP Address/MAC A
+ Add
Bind Selected
Delete Selected
Up to 256 IP-MAC bindings can be added.
No.
MAC Address
IP Address
Type
Ethernet status
Action
1
00:d0:f8:15:08:48
fe80::2d0:f8ff:fe15:848
Dynamic
WAN
Bind
1
10/page
Total 1

5 System Settings

5.1 PoE Settings

In **Local Device** mode, choose **Advanced** >> **PoE Settings**

Set the power mode for the AP to accept power over PoE. In AF mode, the maximum power supported by the device is 15.4 W. In AT mode, the maximum power is 30 W according to the IEEE 802.3at standard. In BT mode, the maximum power is 51 W according to the IEEE 802.3bt standard. By default, the device automatically negotiates with the power sourcing equipment (PSE) about the power mode. The default configuration is recommended.



5.2 Setting the Login Password

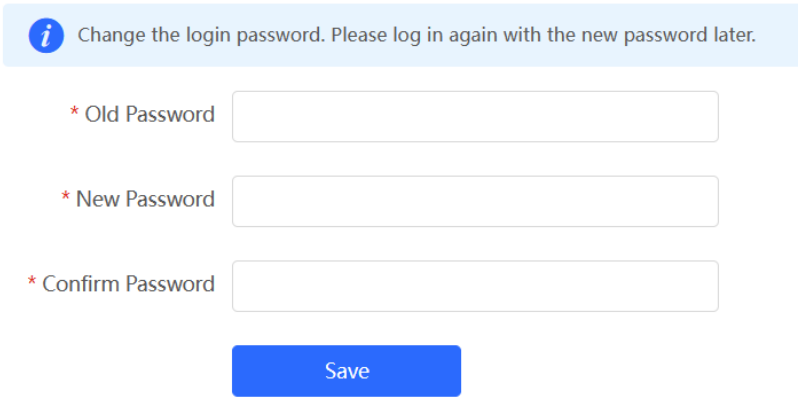
If the device works in self-organizing network mode, and **Network** mode webpage is displayed, choose **System** >> **Login Password**

In standalone mode, choose **System** >> **Login** >> **Login Password**

Enter the old password and new password. After saving the configuration, use the new password to log in.

Caution

In self-organizing network mode, the login password of all devices in the network will be changed synchronously.

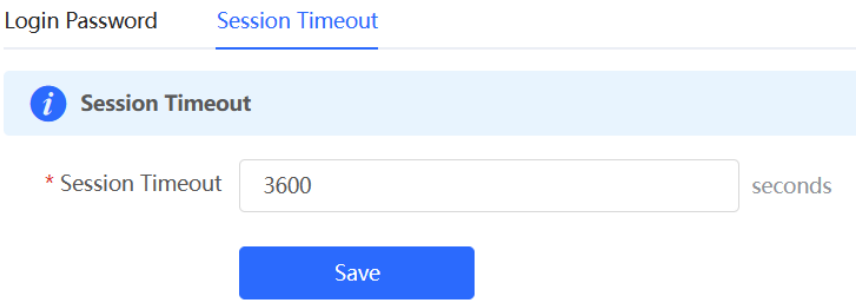


5.3 Setting the Session Timeout Duration

If the device works in self-organizing network mode, and **Local Device** mode webpage is displayed, choose **System** >> **Login**

In standalone mode, choose **System** >> **Login** >> **Session Timeout**

If no operation is performed on the eWeb page within a period of time, the session is automatically disconnected. When you need to perform operations again, enter the password to log in again. The default timeout duration is 3600 seconds, that is, 1 hour.



5.4 Setting and Displaying System Time

If the device works in self-organizing network mode, and **Network** mode webpage is displayed, choose **System** >> **System Time**

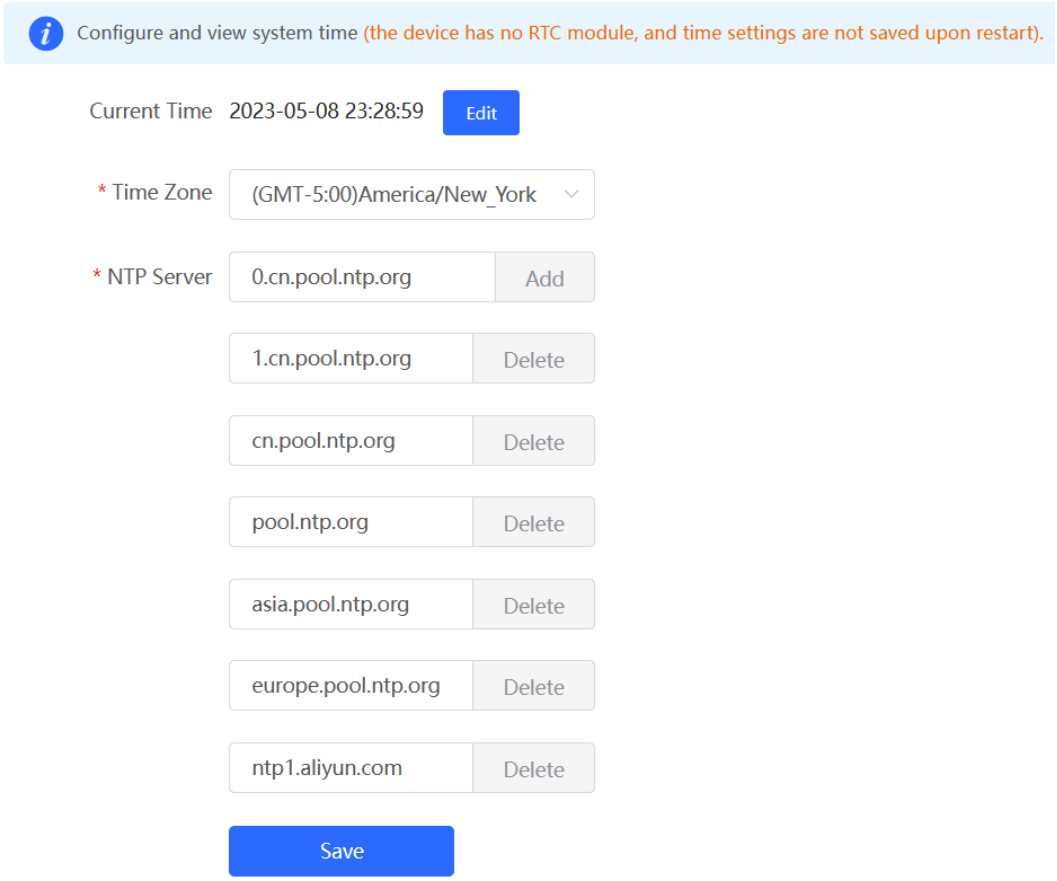
In standalone mode, choose **System** >> **System Time**

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the device supports

Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server.

Caution

In self-organizing network mode, the system time of all devices in the network will be changed synchronously.



5.5 Configuring Reboot

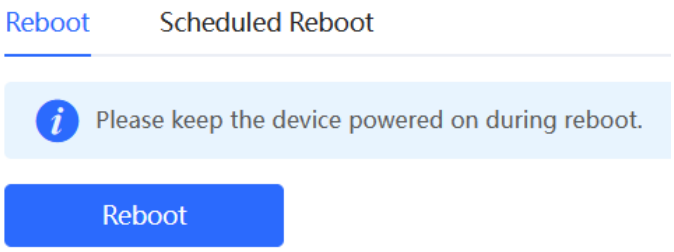
Caution

- Do not cut off power during system reboot to avoid device damage.
- Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.
- Rebooting the device affects the network. Therefore, exercise caution when performing this operation.

5.5.1 Rebooting the Current Device

In **Local Device** mode, choose **System** >> **Reboot** >> **Reboot**

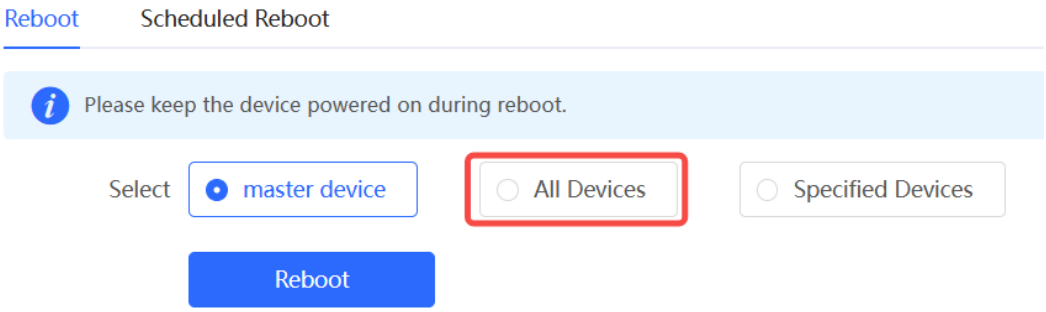
Click **Reboot**. The device will restart.



5.5.2 Rebooting All Devices in the Network

In **Network** mode, choose **System** >> **Reboot** >> **Reboot**

Click **Reboot**, select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.



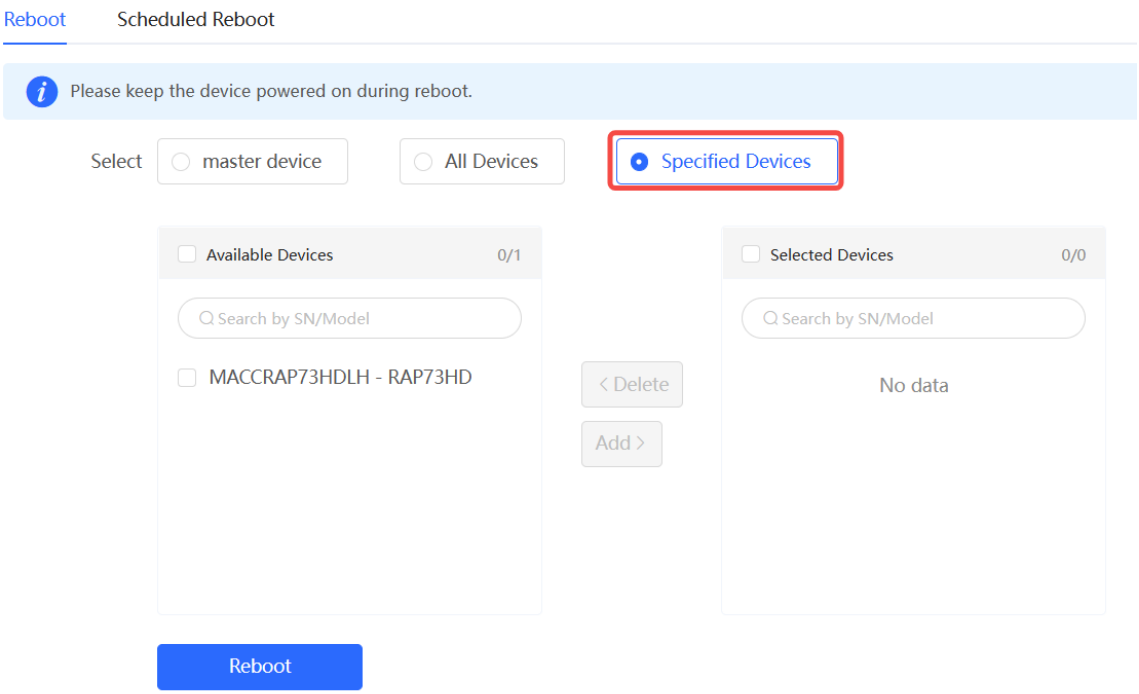
Caution

It takes time to reboot all devices in the current network. The action may affect the whole network. Please be cautious.

5.5.3 Rebooting the Specified Device

In **Network** mode, choose **System** >> **Reboot** >> **Reboot**

Click **Reboot**, click **Specified Devices**, select required devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.



5.6 Configuring Scheduled Reboot

5.6.1 Configuring Scheduled Reboot for the Current Device

Confirm that the system time is accurate to avoid network interruption caused by device reboot at wrong time. For details about how to configure the system time, see Setting the Session Timeout Duration.

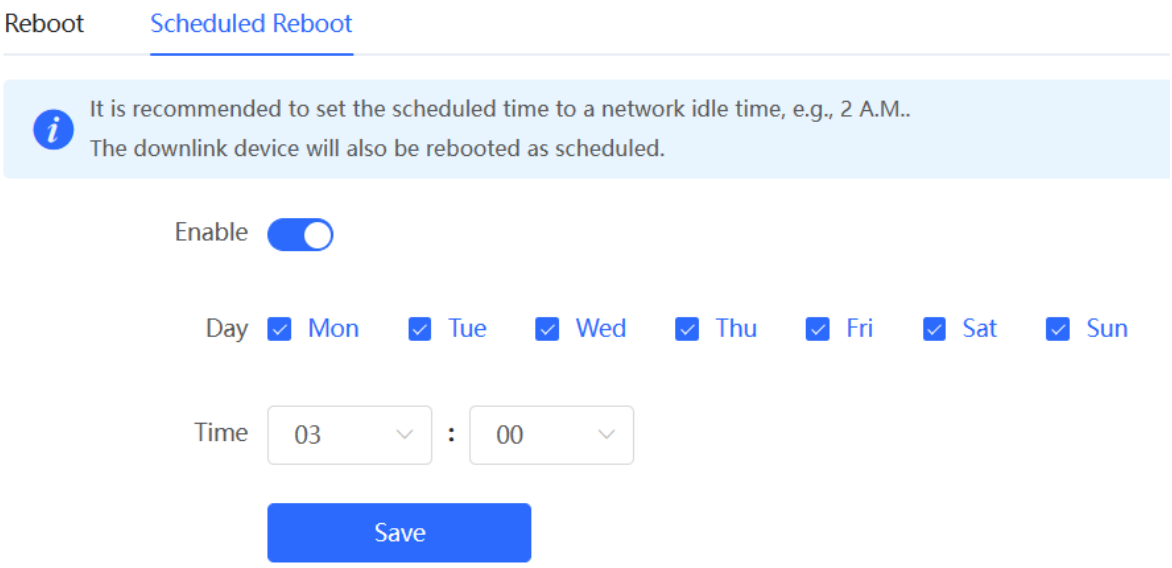
Choose **System** >> **Reboot** >> **Scheduled Reboot**

To configure scheduled reboot for all devices in the network, choose **Network**>> **Scheduled Reboot**

Caution

If you configure scheduled reboot on the management webpage, all devices will restart when the system time matches with the scheduled reboot time. Please be cautious.

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches with the scheduled reboot time, the device will restart. You are recommended to set scheduled reboot time to off-peak hours.

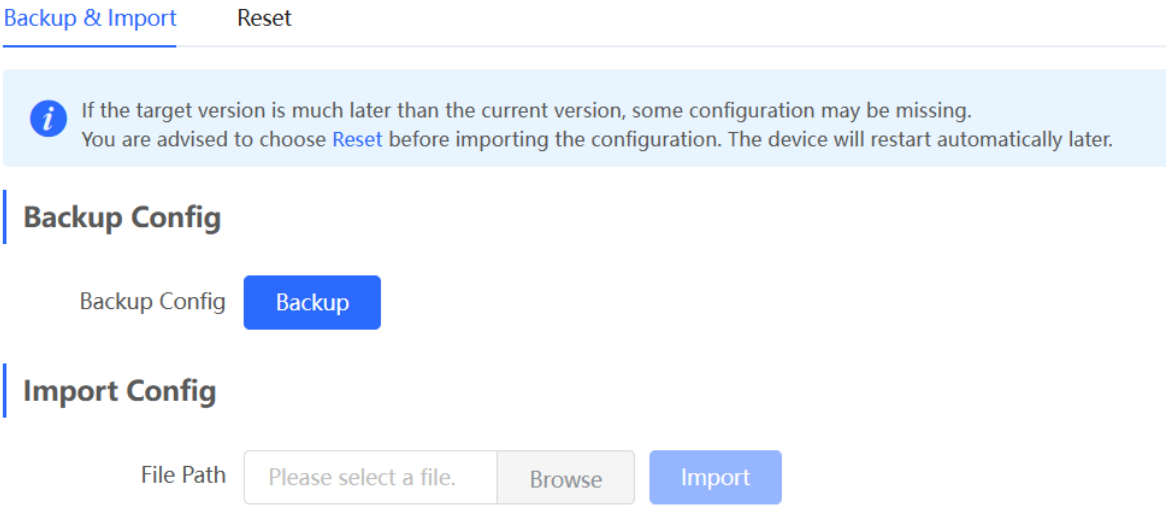


5.7 Configuring Backup and Import

Choose **System** >> **Management** >> **Backup & Import**

Configuration backup: Click **Backup** to download a configuration file locally.

Configuration import: Click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The device will restart.

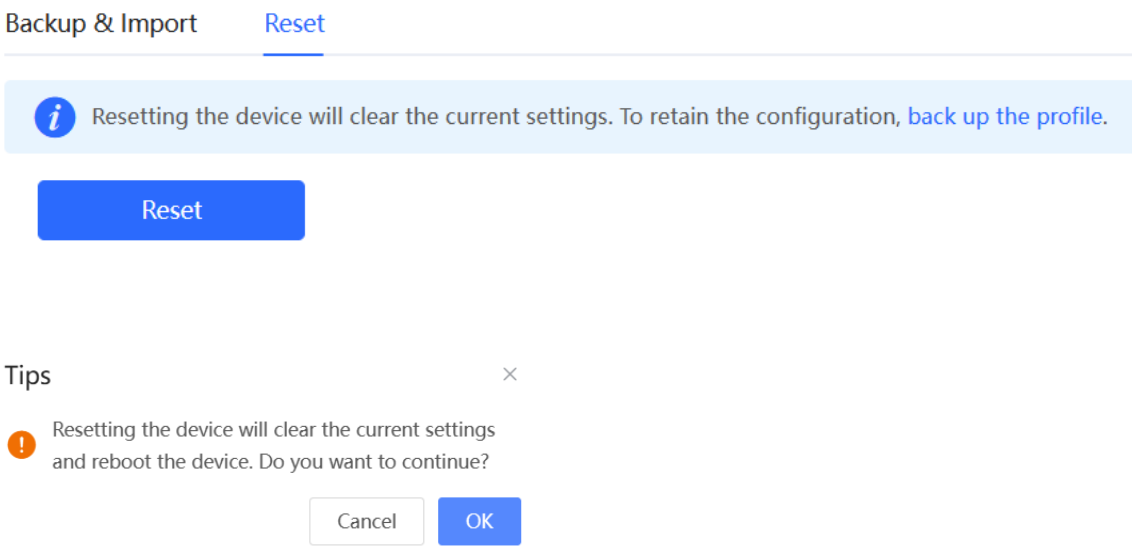


5.8 Restoring Factory Settings

5.8.1 Restoring the Current Device to Factory Settings

In **Local Device** mode, choose **System** >> **Management** >> **Reset**

Click **Reset** to restore the current device to the factory settings.



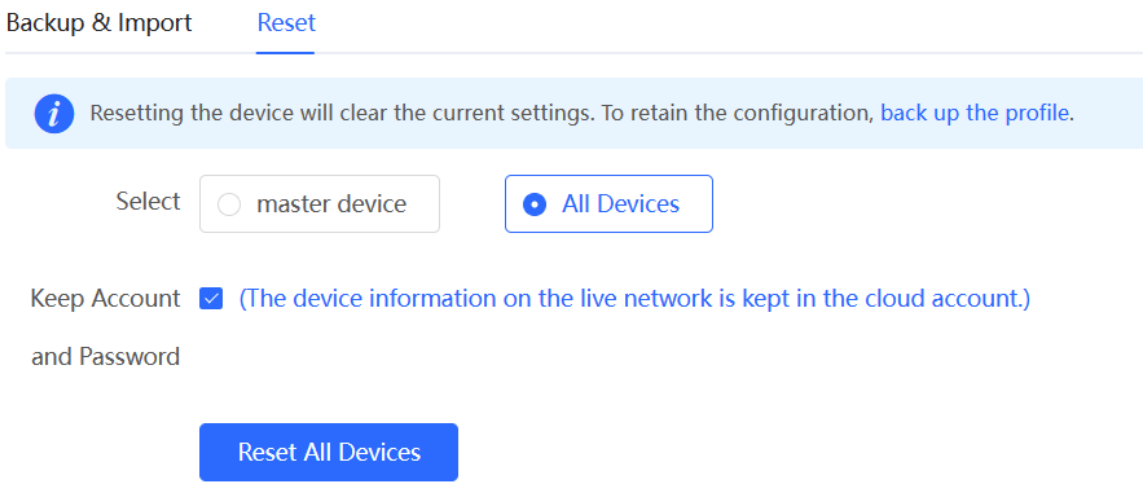
Caution

The operation will clear all configuration of the current device. If you want to retain the current configuration, back up the configuration first (See Configuring Backup and Import). Therefore, exercise caution when performing this operation.

5.8.2 Restoring All Devices to Factory Settings

In **Network** mode, choose **System** >> **Management** >> **Reset**

Click **All Devices**, select whether to enable **Unbind Account** and Click **Reset All Devices**. All devices in the network will be restored to factory settings.



Caution

The operation will clear all configuration of all devices in the network. Therefore, exercise caution when performing this operation.

5.9 Performing Upgrade and Checking System Version

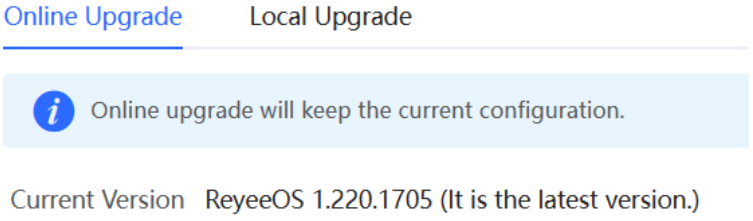
Caution

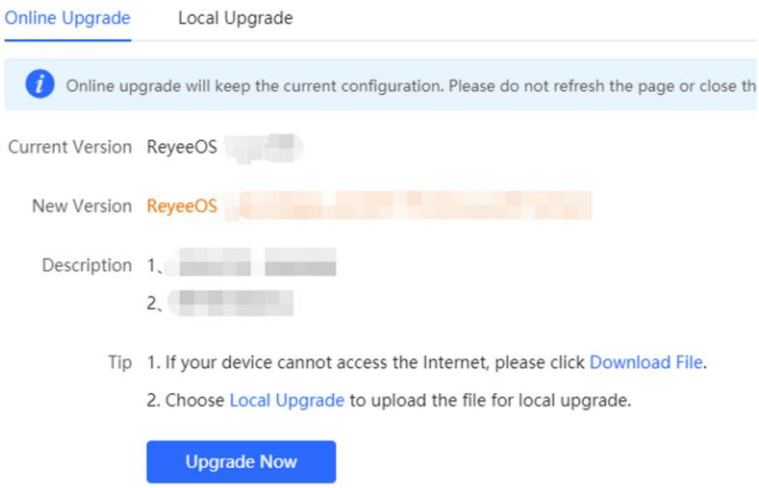
- You are advised to back up the configuration before upgrading the access point.
- After being upgraded, the access point will reboot. Therefore, exercise caution when performing this operation.

5.9.1 Online Upgrade

In **Local Device** mode, choose **System** >> **Upgrade** >> **Online Upgrade**

The current version is displayed, and the system will check if there is a new version available. If an available version is detected, you can click **Upgrade Now** to upgrade online. If the network environment for online upgrade is unavailable, you can click **Download File** to save the upgrade package locally. You can then perform a local upgrade using the downloaded file.

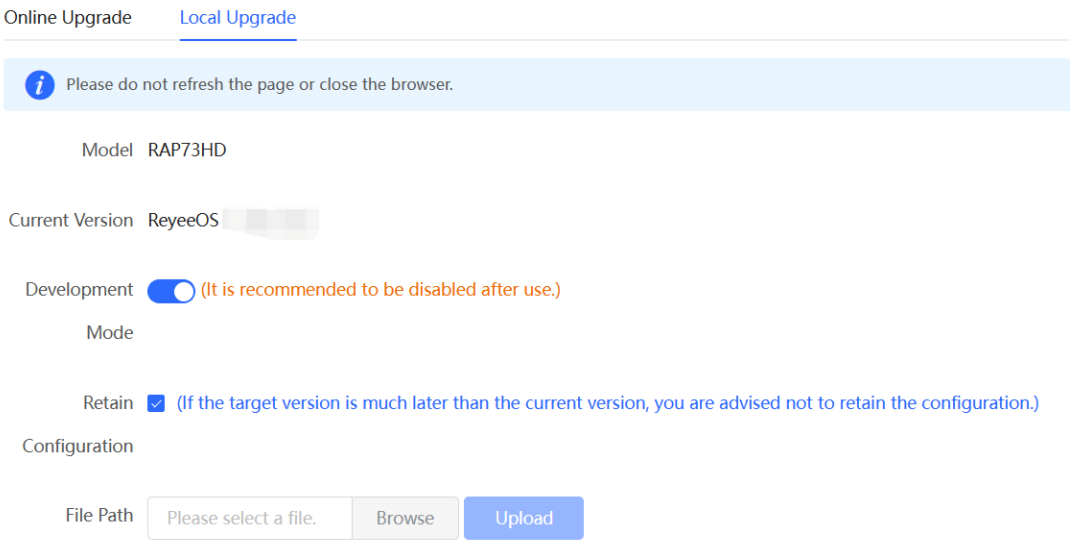




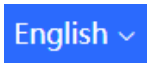
5.9.2 Local Upgrade

In **Local Device** mode, choose **System** >> **Upgrade** >> **Local Upgrade**

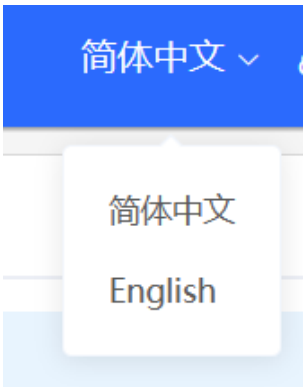
You can view the current software version, hardware version and device model. If you want to upgrade the device with the configuration retained, check **Retain Configuration** Setup. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.



5.10 Switching System Language

Choose  in the upper right corner of the eWeb page.

Click a required language to switch the system language.



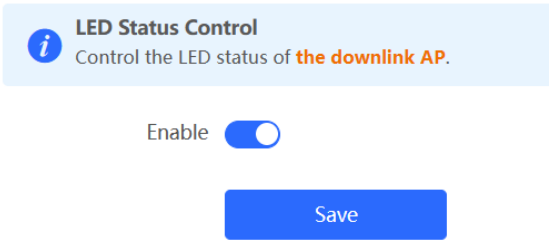
5.11 Configuring LED Status Control

Caution

The LED Status Control function is not supported in the standalone mode (self-organizing network is not enabled).

In **Network** mode, choose **Network**>> **LED**

Turn on the LED of all downlink access points in the network.

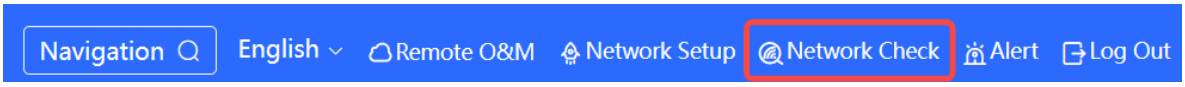


6 Network Diagnosis Tools

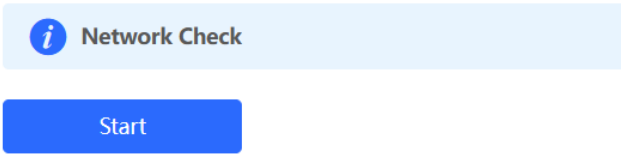
6.1 Network Check

When a network error occurs, perform **Network Check** to identify the fault and take the suggested action.

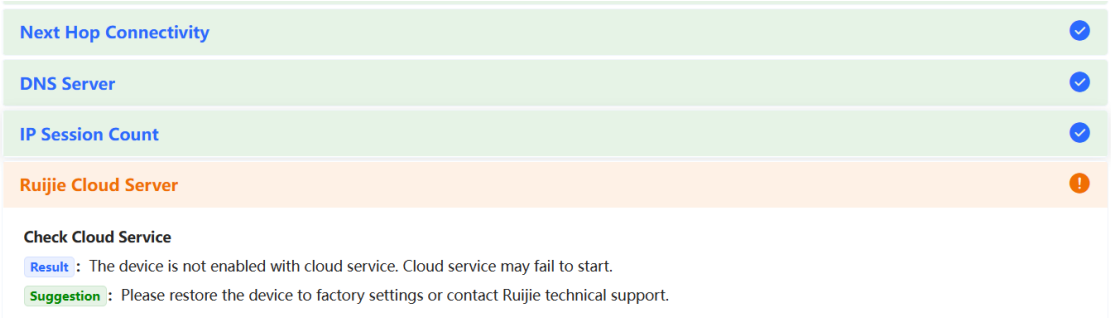
(1) Click  in the navigation bar, or choose **Diagnostics**>> **Network Check** and go to the **Network Check** page.



(2) Click **Start** to perform the network check and show the result.



(3) After performing the network check, you will find the check result and suggested action.

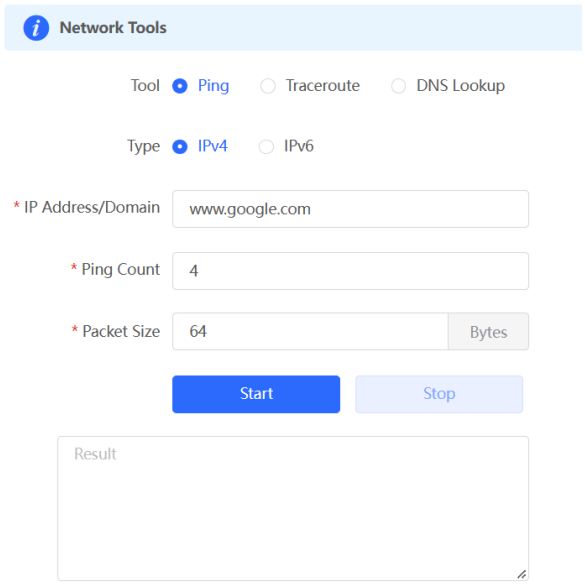


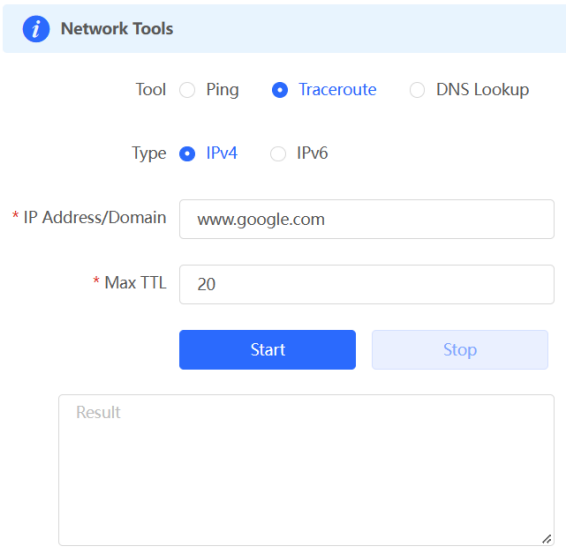
6.2 Network Tools

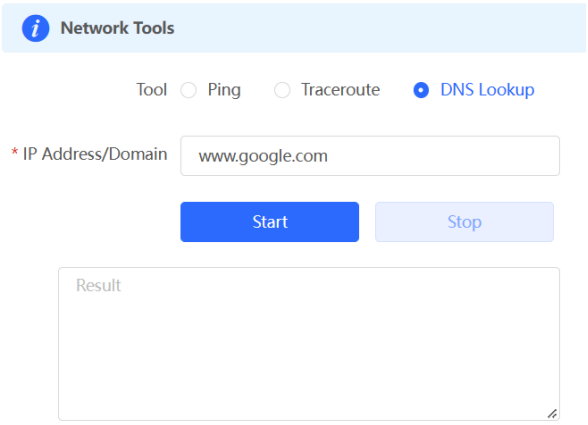
In **Local Device** mode, choose **Diagnostics** >> **Network Tools**

- The Ping tool tests the connectivity between the access point and the IP address or URL. The message "Ping failed" indicates that the access point cannot reach the IP address or URL.
- The Traceroute tool displays the network path to a specific IP address or URL.
- The DNS Lookup tool displays the DNS server address used to resolve a URL.

Enter an IP address or a URL, and click **Start**. If you need to perform the ping or Traceroute operation, configure other parameters as required.







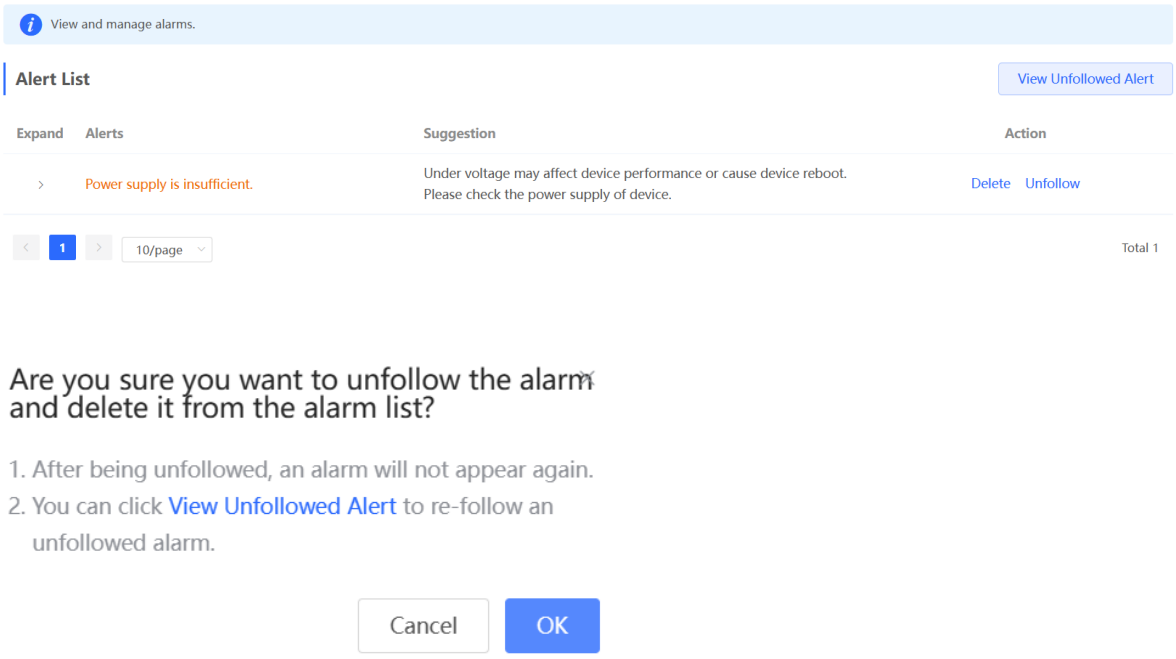
6.3 Alarms

In **Network** mode, choose **Network**>> **Alerts**

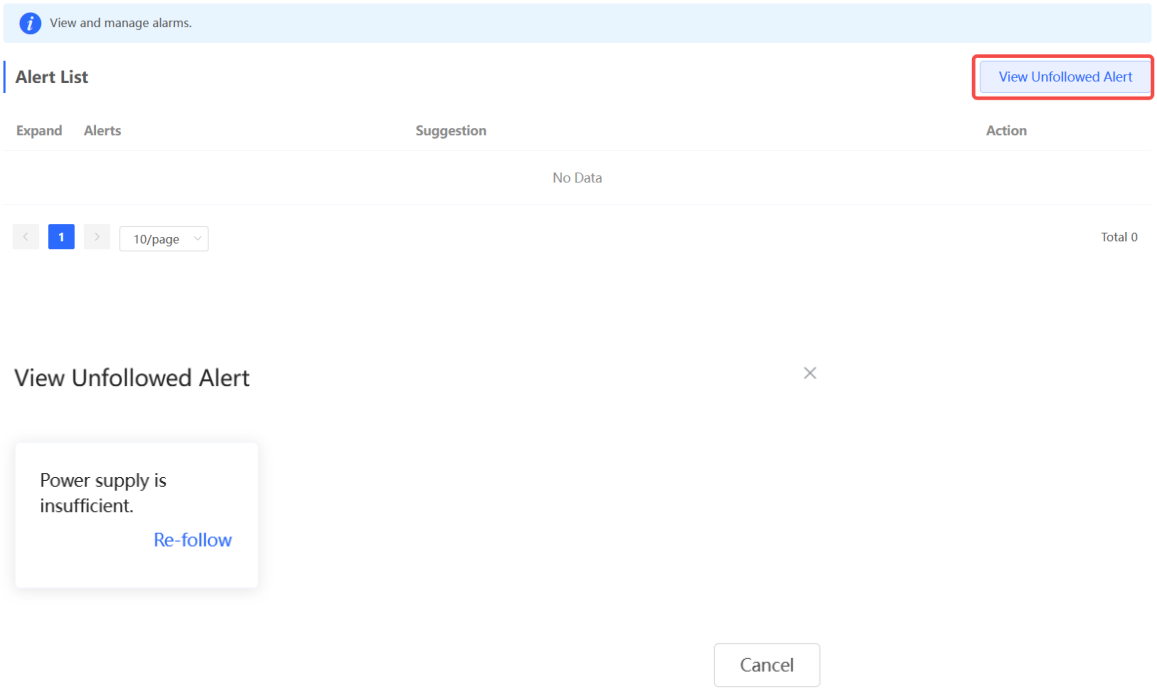
The Alarms page displays possible problems on the network environment and device. All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarm.

Caution

After unfollowing a type of alarm, you will not discover and process all alarms of this type promptly. Therefore, exercise caution when performing this operation.



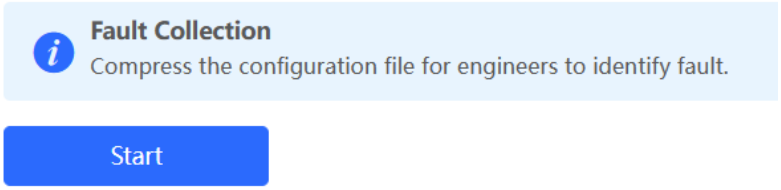
Click **View Unfollowed Alarm** to view the unfollowed alarm. You can follow the alarm again in the pop-up window.



6.4 Fault Collection

In **Local Device** mode, choose **Diagnostics**>> **Fault Collection**

When an unknown fault occurs on the device, you can collect fault information on this page. Click **Start** to collect fault information and compress it into a file for engineers to identify fault.



7 FAQs

7.1 Login Failure

➢ **What can I do when I failed to log in to the eWeb management system?**

Perform the following steps:

(1) Check that the Ethernet cable is properly connected to the LAN port of the device.

(2) Before accessing the setup page, you are advised to choose **Auto** for the device enabled with DHCP service to assign an IP address to the PC. If you want to configure a static IP address for the PC, please make sure the IP address of the PC and the LAN port are in the same IP range. The default IP address of the LAN port is 10.44.77.254, and the subnet mask is 255.255.255.0. The IP address of the PC should be set to 10.44.77.X (X is an integer between 2 and 254), and the subnet mask is 255.255.255.0.()

(3) Run the **Ping** command to check the connectivity between the PC and the device. If the ping fails, please check the network settings.

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

7.2 Factory Setting Restoration

➢ **How can I restore the device to factory settings?**

Power on the device and press the **Reset** button for more than 5 seconds. The device is restored to factory settings after it is restarted. Then, you can log in to the eWeb management system using the default IP address (10.44.77.254) and default password (**admin**).

7.3 Password Loss

➢ **What can I do when I forget the password?**

- Webpage management password loss: Please enter the Wi-Fi password. If it is still incorrect, please restore the device to factory settings.
- Wi-Fi password loss: When the access point expands the Wi-Fi coverage, its Wi-Fi password is consistent with that of the master router. Please check the configuration of the master router and enter its Wi-Fi password. If the password is still incorrect, please restore the device to factory settings and reconfigure the Wi-Fi password.