Ruijie Reyee RG-RAP and RG-EAP Series Access Points ReyeeOS 1.86

Web-based Configuration Guide

Document Version: V1.0
Date: 2022.03.28

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

Intended 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 features of the RG-EAP and RG-RAP series access points and instructs users to configure the device.

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

Table 1-1 Default Web Configuration

Item	Default
IP address	10.44.77.254
Username/Password	Username and password are not required at your first login and you can configure the access point directly.

1.3 Login to Eweb

1.3.1 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-S***XXXX* (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.

1.3.2 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.

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.

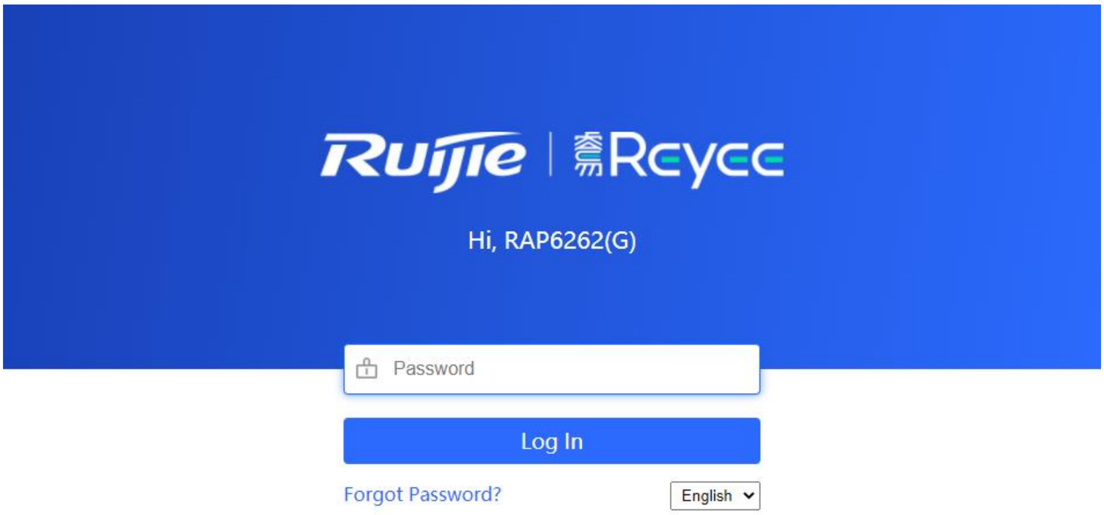
1.3.3 Logging in to the Web Page

(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 web management system.



Username and password are not required at your first login and you can configure the access point directly.

For device security, you are advised to set the management password after your first login to the web management system. After the password is set, you need to enter the password when you log in to the web management system again.

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.

1.4 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/EAP works in the AP mode by default. If you want to switch the work mode, see Switching Work Mode.

1.4.1 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.

1.4.2 Router Mode

The device supports NAT routing and forwarding. The addresses of wireless clients can be assigned by th e 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 will restore to factory settings and its 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.

1.5 Configuration Wizard (Router Mode)

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

1.5.1 Getting Started

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.

1.5.2 Configuration Steps

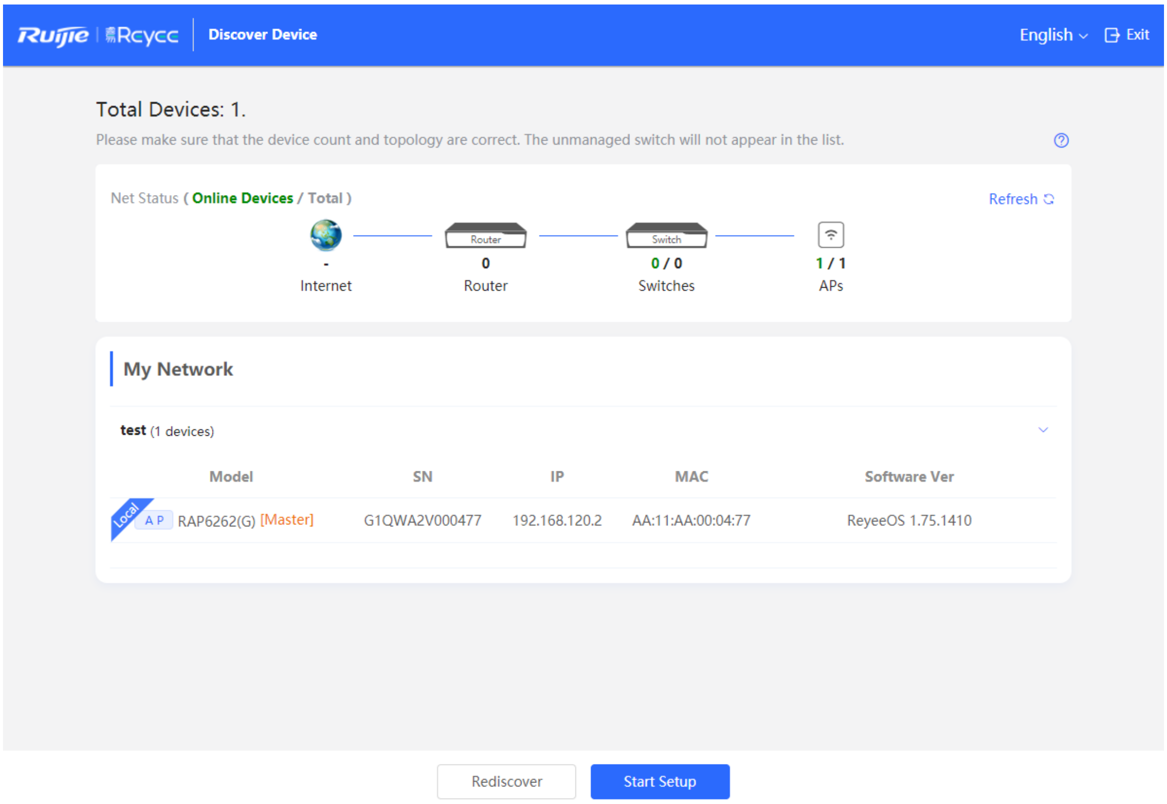
1. Add a Device to Network

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.



Total Devices: 1.

Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.

Net Status (Online Devices / Total)

Internet	Router	Switches	APs
-	0	0 / 0	1 / 1

My Network

test (1 devices)

Model	SN	IP	MAC	Software Ver
Local AP RAP6262(G) [Master]	G1QWA2V000477	192.168.120.2	AA:11:AA:00:04:77	ReyeeOS 1.75.1410

2. 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).

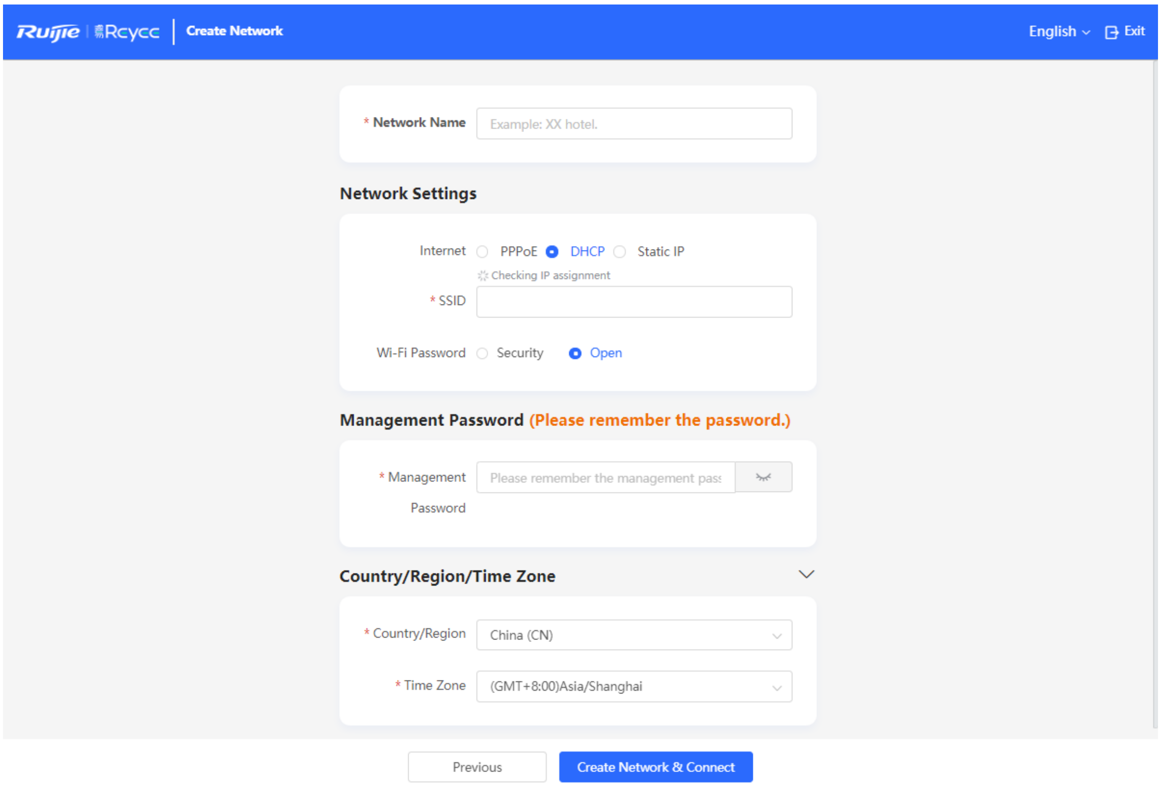
- **DHCP**: The access point detects whether it can obtain an IP address via DHCP by default. If the access point connects to the Internet successfully, you can click **Next** without entering an account.
- **PPPoE**: Click **PPPoE**, and enter the username, password, and service name. Click **Next**.
- **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 complexpassword to enhance the network security.

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

(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 selectthe actual country or region.

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



* Network Name: Example: XX hotel.

Network Settings

Internet ○ PPPoE ● DHCP ○ Static IP

Checking IP assignment

* SSID

Wi-Fi Password ○ Security ● Open

Management Password (Please remember the password.)

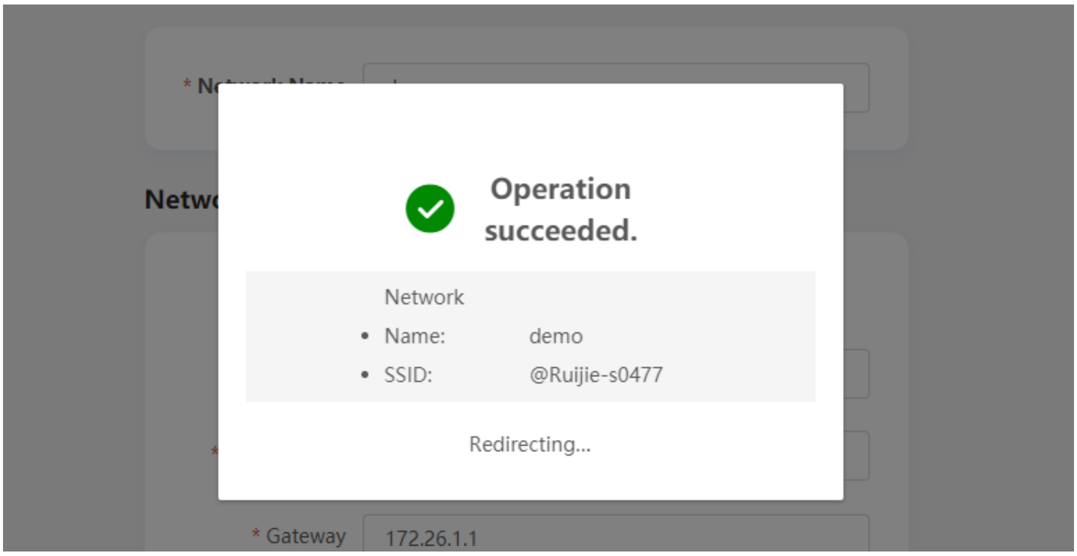
* Management Password: Please remember the management pass

Country/Region/Time Zone

* Country/Region: China (CN)

* Time Zone: (GMT+8:00)Asia/Shanghai

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



Operation succeeded.

Network

- Name: demo
- SSID: @Ruijie-s0477

Redirecting...

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.

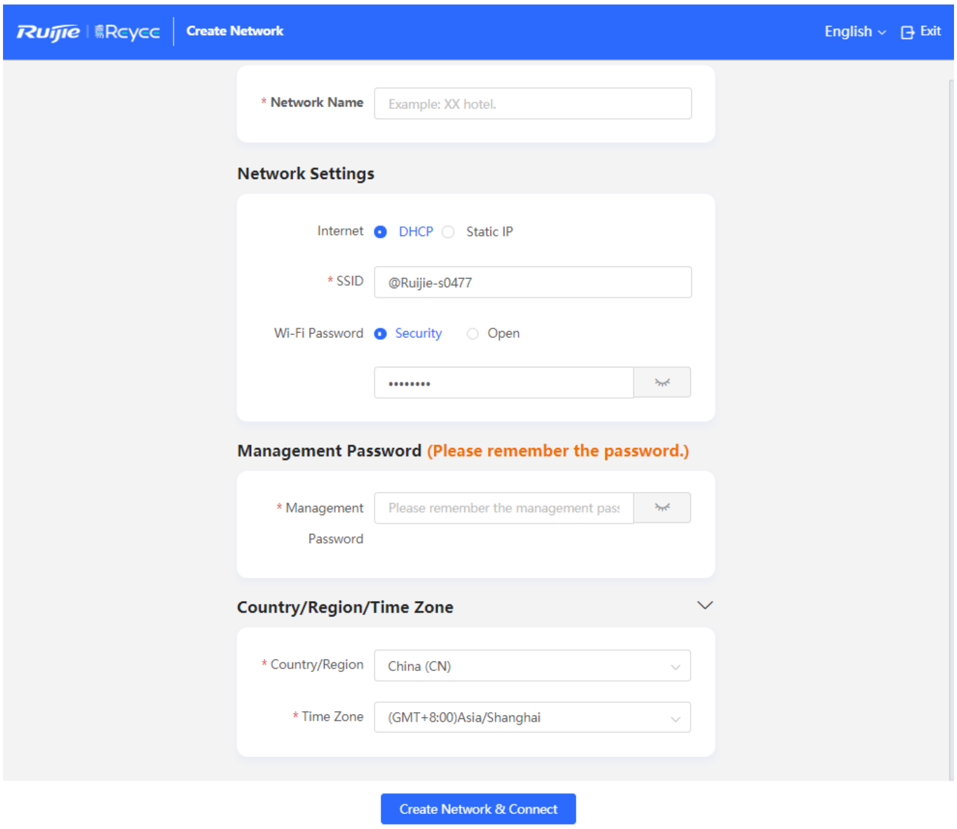
1.6 Configuration Wizard (AP Mode)

1.6.1 Getting Started

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

1.6.2 Configuration Steps

Set the Internet connection type to DHCP. See Creating a New Project for details.



* Network Name: Example: XX hotel.

Network Settings

Internet: ● DHCP ○ Static IP

* SSID: @Ruijie-s0477

Wi-Fi Password: ● Security ○ Open

••••••••

Management Password (Please remember the password.)

* Management Password: Please remember the management pas:

Country/Region/Time Zone

* Country/Region: China (CN)

* Time Zone: (GMT+8:00)Asia/Shanghai

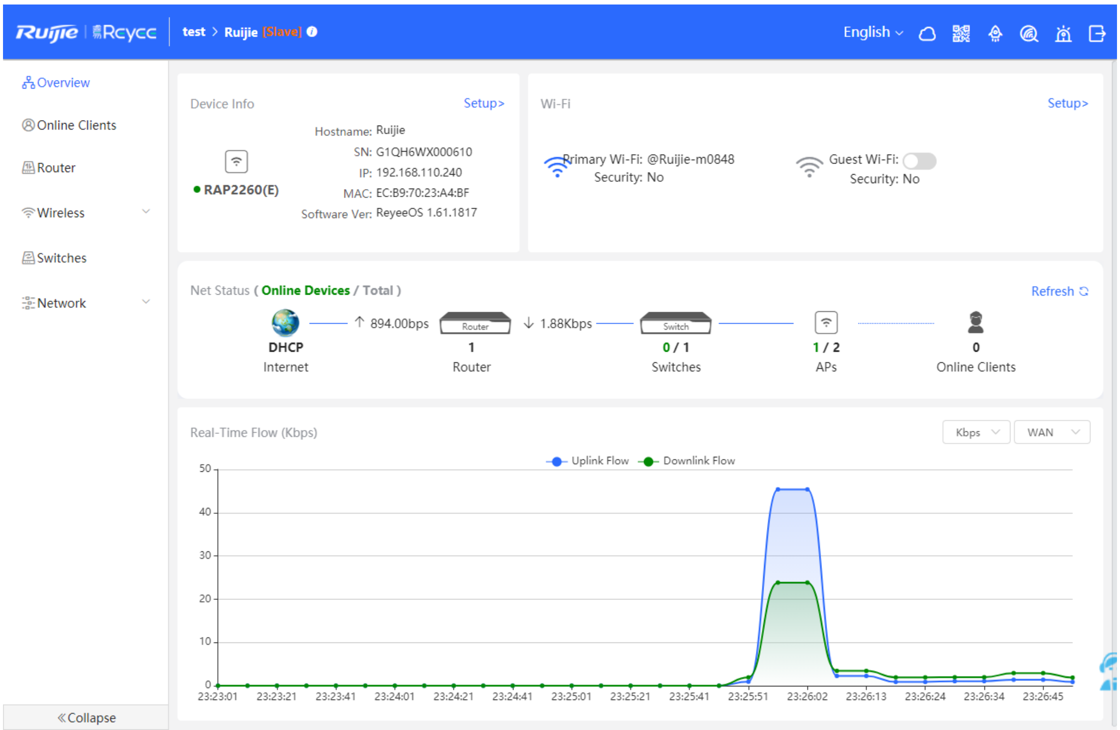
1.7 Configuration Menus

Note

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.

1.7.1 Network-wide Management

The device works in self-organizing network mode by default. The Web page displays the network-wide management menu on the left side, in which you can check the current status of all devices in the network, and modify network-wide configuration, including global Wi-Fi network management configuration (APs and Wi-Fi), routing management configuration (if routers exist in the network), switch management configuration, and network-wide management configuration (time, password, network-wide reboot, and other system settings).



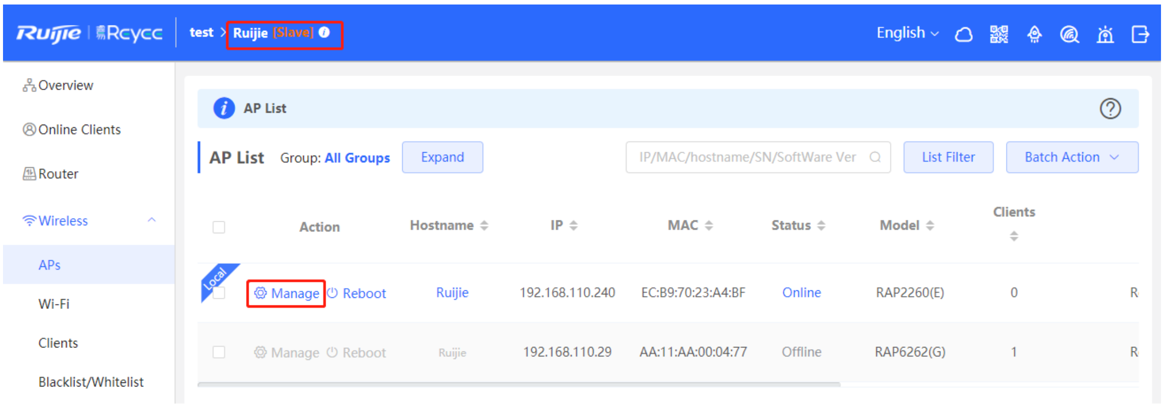
Hostname: Ruijie
SN: G1QH6WX000610
IP: 192.168.110.240
MAC: EC:B9:70:23:A4:BF
Software Ver: ReyeeOS 1.61.1817
● RAP2260(E)

Primary Wi-Fi: @Ruijie-m0848
Security: No
Guest Wi-Fi:
Security: No

↑ 894.00bps ↓ 1.88Kbps
DHCP Internet
1 Router
0 / 1 Switches
1 / 2 APs
0 Online Clients

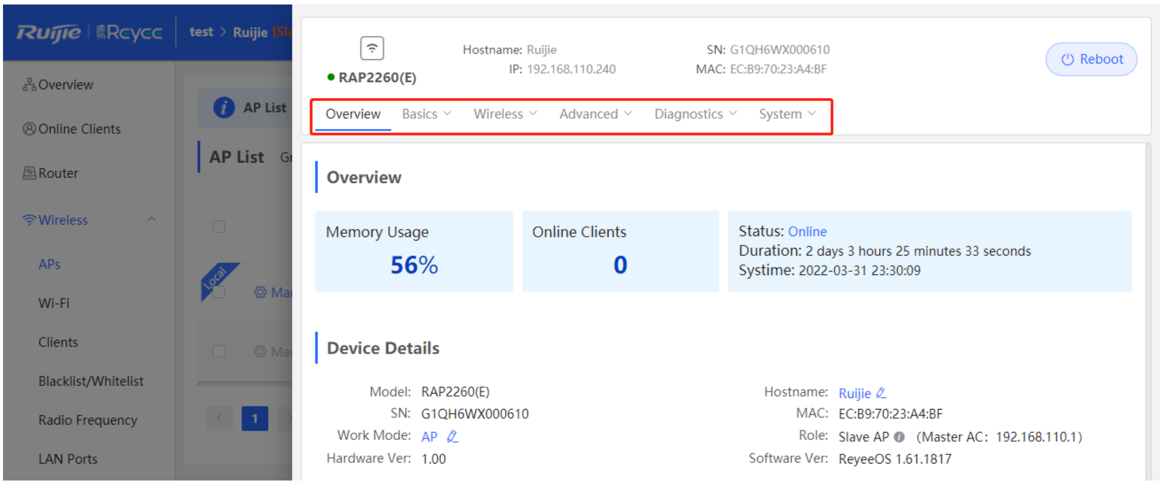
1.7.2 Standalone Management

- If a device is in self-organizing network mode, click the name of the current logged in device or click **Manage** of a specified device in the device list to configure and manage the device.



AP List

	Action	Hostname	IP	MAC	Status	Model	Clients	
□	Manage Reboot	Ruijie	192.168.110.240	EC:B9:70:23:A4:BF	Online	RAP2260(E)	0	R
□	Manage Reboot	Ruijie	192.168.110.29	AA:11:AA:00:04:77	Offline	RAP6262(G)	1	R



● RAP2260(E)

Hostname: Ruijie SN: G1QH6WX000610

IP: 192.168.110.240 MAC: EC:B9:70:23:A4:BF

Overview

Memory Usage 56%

Online Clients 0

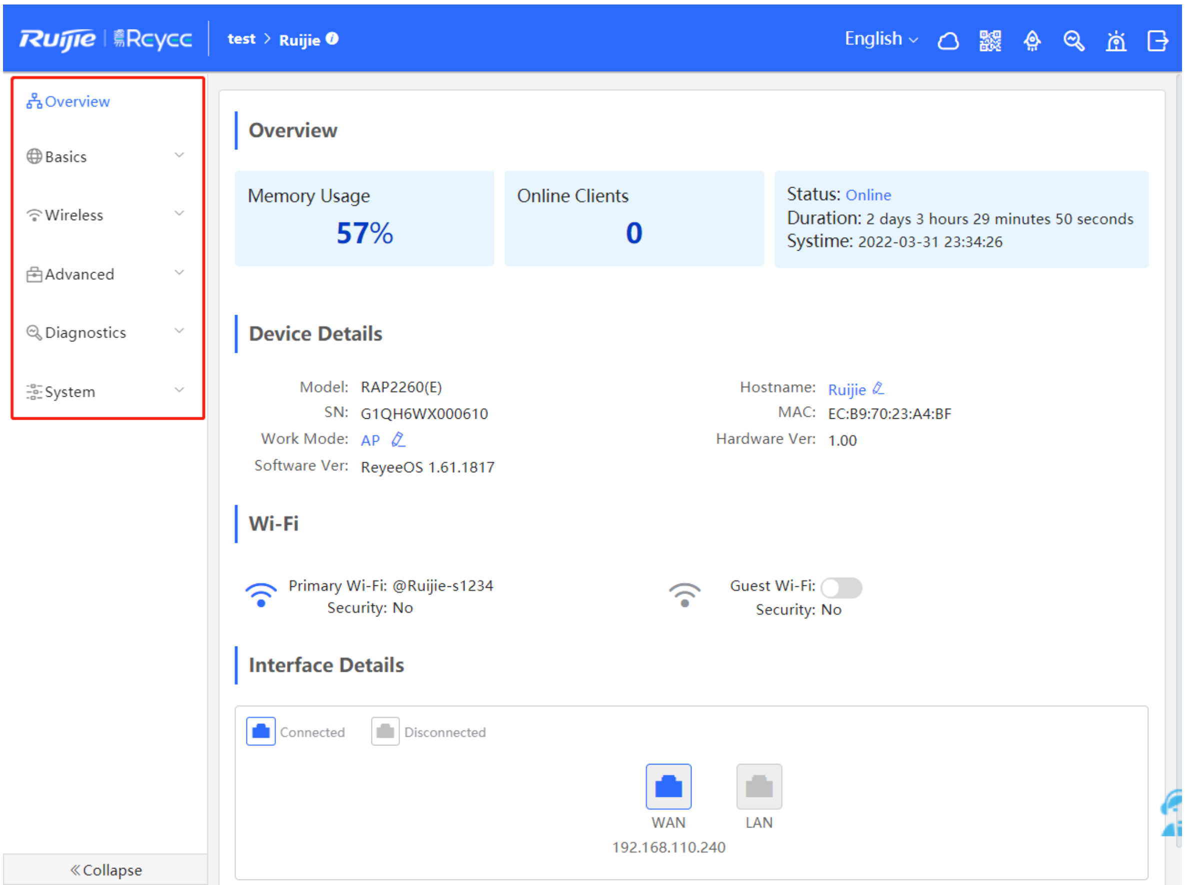
Status: Online
Duration: 2 days 3 hours 25 minutes 33 seconds
Systime: 2022-03-31 23:30:09

Device Details

Model: RAP2260(E)
SN: G1QH6WX000610
Work Mode: AP
Hardware Ver: 1.00

Hostname: Ruijie
MAC: EC:B9:70:23:A4:BF
Role: Slave AP (Master AC: 192.168.110.1)
Software Ver: ReyeeOS 1.61.1817

- If a device is in standalone mode, you can configure and manage only the currently logged in device. The Web page displays the function configuration menu of a single device on the left side.



Overview

Memory Usage 57%

Online Clients 0

Status: Online
Duration: 2 days 3 hours 29 minutes 50 seconds
Systime: 2022-03-31 23:34:26

Device Details

Model: RAP2260(E)
SN: G1QH6WX000610
Work Mode: AP
Software Ver: ReyeeOS 1.61.1817

Hostname: Ruijie
MAC: EC:B9:70:23:A4:BF
Hardware Ver: 1.00

Wi-Fi

Primary Wi-Fi: @Ruijie-s1234
Security: No

Guest Wi-Fi:
Security: No

Interface Details

Connected Disconnected

WAN LAN

192.168.110.240

2 Wi-Fi Network Settings

Caution

By default (the self-organizing network discovery is enabled on devices), slave APs in the network are managed by the master AP/AC in a unified manner. Some Wi-Fi network settings cannot be modified locally but configured globally. Wi-Fi network settings will apply to all APs in the network. If only a specified device needs to be set, go to **Wireless** > **APs** to check and edit an AP group and then configure Wi-Fi settings, or disable the self-organizing network discovery function (see Switching Work Mode) of the device and configure the AP in standalone mode.

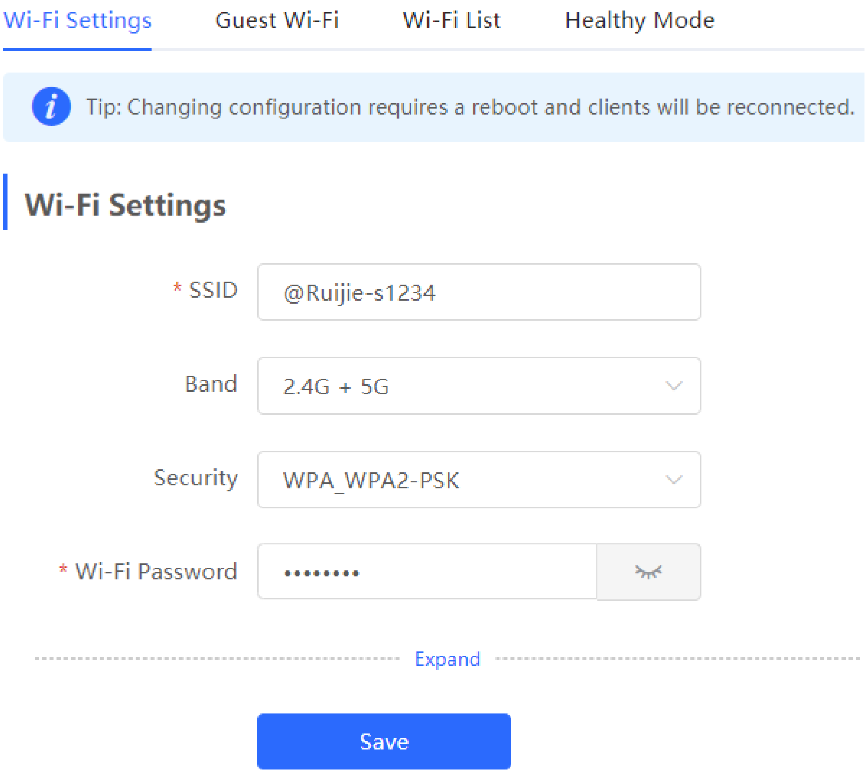
2.1 Configuring SSID and Wi-Fi Password

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Click the target Wi-Fi network, change the SSID and Wi-Fi password of the Wi-Fi network, and click **Save**.

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.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings

* SSID: @Ruijie-s1234

Band: 2.4G + 5G

Security: WPA_WPA2-PSK

* Wi-Fi Password: ••••••••

2.2 Hiding the SSID

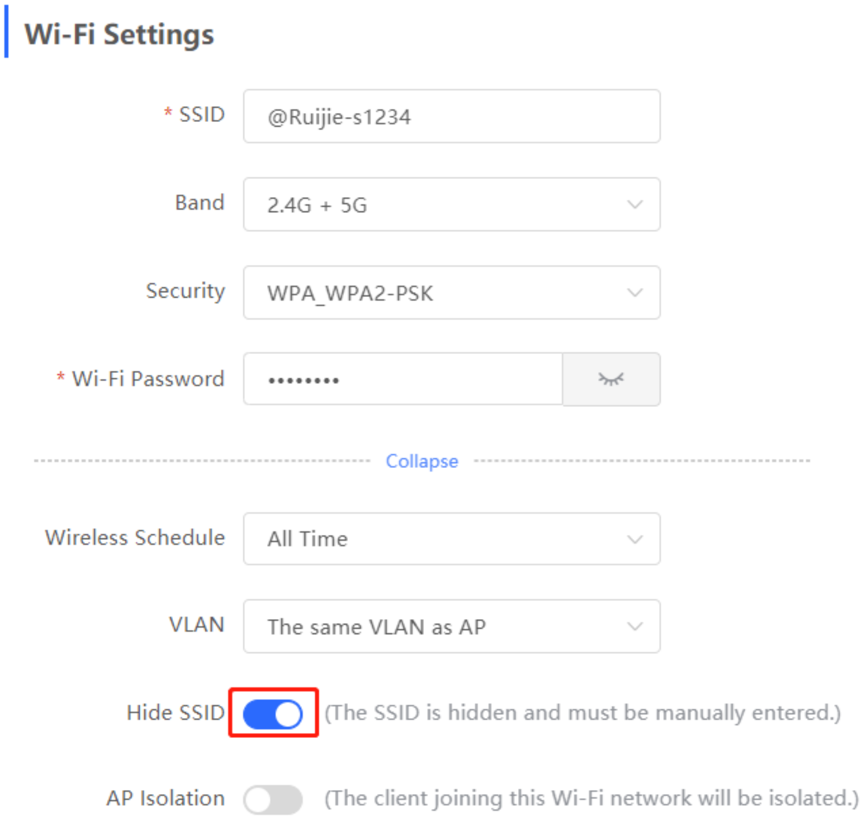
Hiding the SSID can prevent unauthorized clients from accessing the Wi-Fi network and enhance network security. After this function is enabled, the mobile phone or PC cannot search out the SSID. Instead, you have to manually enter the correct SSID and Wi-Fi password. Remember the SSID so that you can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

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

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.



Wi-Fi Settings

* SSID: @Ruijie-s1234

Band: 2.4G + 5G

Security: WPA_WPA2-PSK

* Wi-Fi Password: ••••••••

Wireless Schedule: All Time

VLAN: The same VLAN as AP

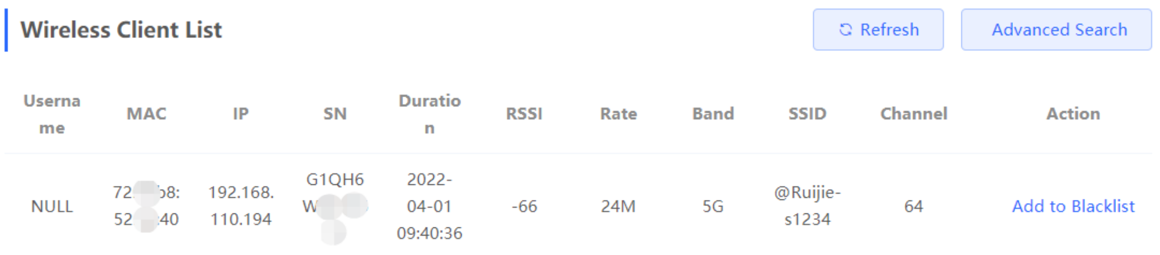
Hide SSID: ● (The SSID is hidden and must be manually entered.)

AP Isolation: ○ (The client joining this Wi-Fi network will be isolated.)

2.3 Checking Wireless Clients

Choose **Wireless** > **Clients**.

Check information about all wireless clients connected to the Wi-Fi network. Click **Add to Blacklist** to disconnect a client and ban the client from accessing the Wi-Fi network.



Wireless Client List

Username	MAC	IP	SN	Duration	RSSI	Rate	Band	SSID	Channel	Action
NULL	72[redacted]8: 52[redacted]40	192.168. 110.194	G1QH6 W[redacted]	2022-04-01 09:40:36	-66	24M	5G	@Ruijie-s1234	64	Add to Blacklist

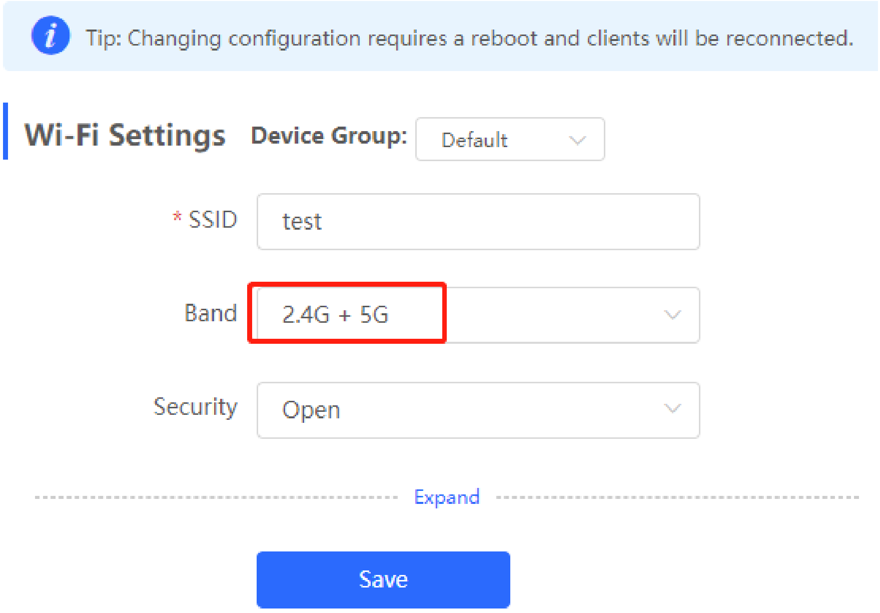
Table 2-1 Description of Wireless Client Information

Item	Description
Username	Name of a client
MAC	MAC address of the client
IP	IPv4 address of the client
SN	SN of the device associated with the client
Duration	Time when the client connects to the Wi-Fi network
RSSI	RSSI of the Wi-Fi network associated with the client
Rate	Association rate of the client and AP
Band	Band type of the Wi-Fi network, to which the client connects
SSID	Name of the Wi-Fi network associated with the client
Channel	Channel of the Wi-Fi network associated with the client

2.4 Configuring Wi-Fi Band

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Set the band of Wi-Fi signals. The device supports the 2.4 GHz and 5 GHz bands. Compared with the 2.4 GHz band, the 5 GHz band supports a higher network transmission rate and is less susceptible to interference, but is inferior in signal coverage and through-wall penetration. You can select an appropriate signal band based on actual requirements. The default Wi-Fi band is **2.4G+5G**, indicating that Wi-Fi signals are emitted in both 2.4 GHz and 5 GHz bands.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

* SSID: test

Band: 2.4G + 5G

Security: Open

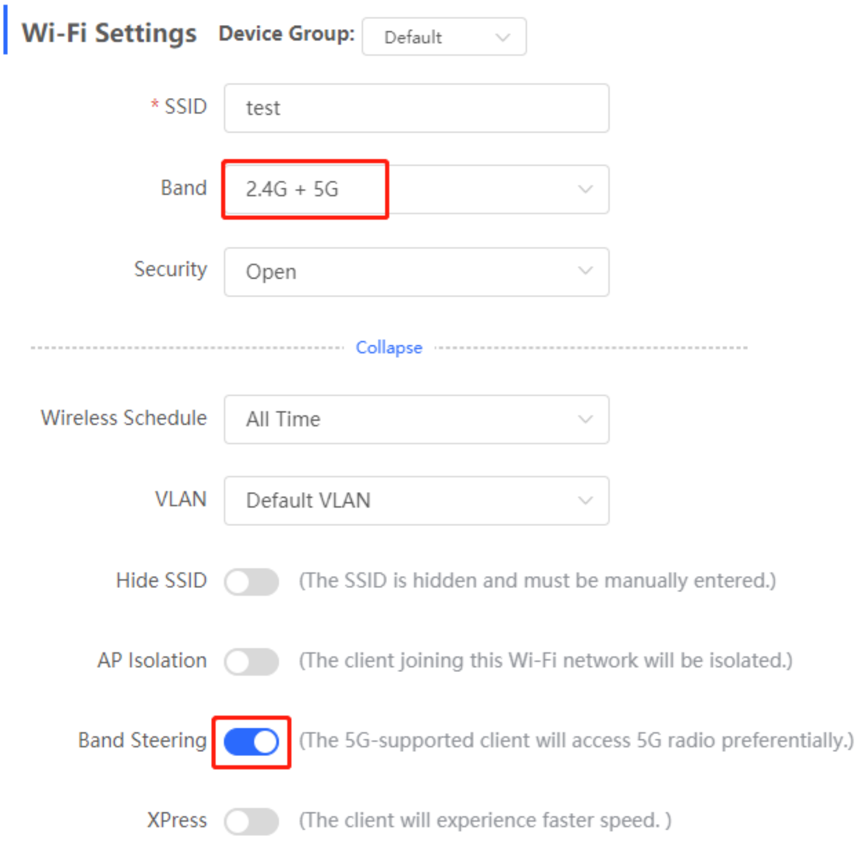
2.5 Configuring Band Steering

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.

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Click **Expand**, 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.



Wi-Fi Settings Device Group: Default

* SSID: test

Band: 2.4G + 5G

Security: Open

Wireless Schedule: All Time

VLAN: Default VLAN

Hide SSID (The SSID is hidden and must be manually entered.)

AP Isolation (The client joining this Wi-Fi network will be isolated.)

Band Steering (The 5G-supported client will access 5G radio preferentially.)

XPress (The client will experience faster speed.)

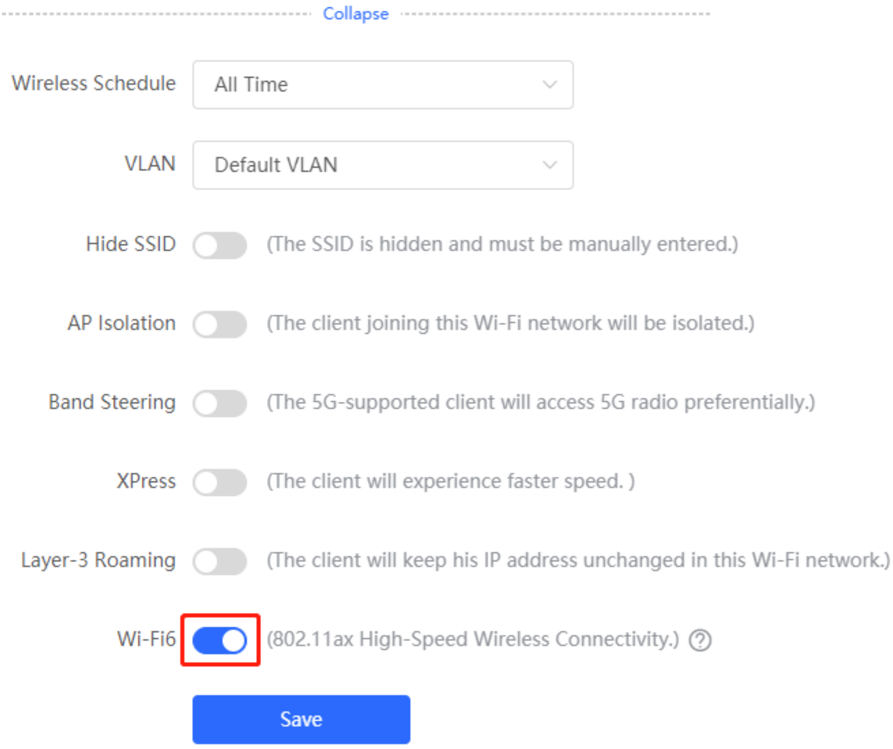
2.6 Configuring Wi-Fi 6

⚠ **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.

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Click **Expand**, turn on **Wi-Fi6** in the expanded settings, and click **Save**. After this function is enabled, wireless clients can enjoy faster Internet access service.



Collapse

Wireless Schedule: All Time

VLAN: Default VLAN

Hide SSID ○ (The SSID is hidden and must be manually entered.)

AP Isolation ○ (The client joining this Wi-Fi network will be isolated.)

Band Steering ○ (The 5G-supported client will access 5G radio preferentially.)

XPress ○ (The client will experience faster speed.)

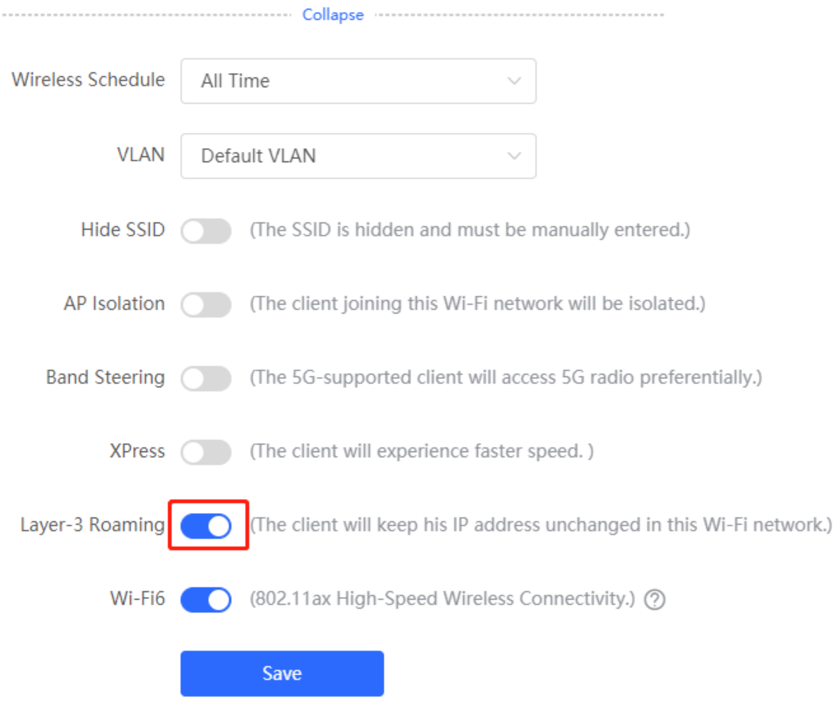
Layer-3 Roaming ○ (The client will keep his IP address unchanged in this Wi-Fi network.)

Wi-Fi6 ● (802.11ax High-Speed Wireless Connectivity.) ?

2.7 Configuring Layer-3 Roaming

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Click **Expand**, 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.



Collapse

Wireless Schedule: All Time

VLAN: Default VLAN

Hide SSID ○ (The SSID is hidden and must be manually entered.)

AP Isolation ○ (The client joining this Wi-Fi network will be isolated.)

Band Steering ○ (The 5G-supported client will access 5G radio preferentially.)

XPress ○ (The client will experience faster speed.)

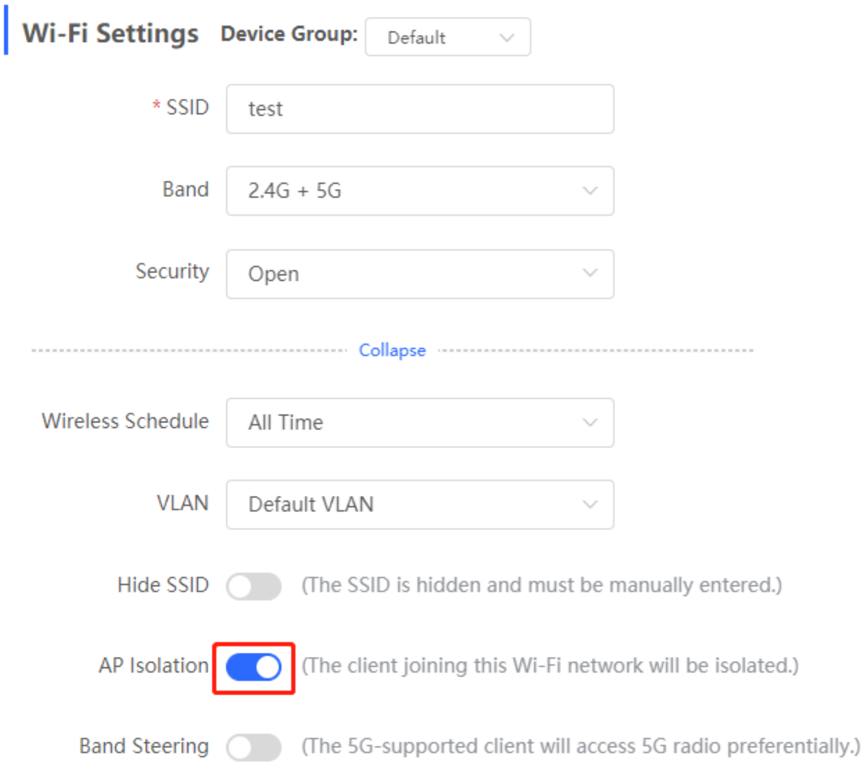
Layer-3 Roaming ● (The client will keep his IP address unchanged in this Wi-Fi network.)

Wi-Fi6 ● (802.11ax High-Speed Wireless Connectivity.) ?

2.8 Configuring AP Isolation

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Click **Expand**, turn on **AP 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.



Wi-Fi Settings Device Group: Default

* SSID: test

Band: 2.4G + 5G

Security: Open

Collapse

Wireless Schedule: All Time

VLAN: Default VLAN

Hide SSID (The SSID is hidden and must be manually entered.)

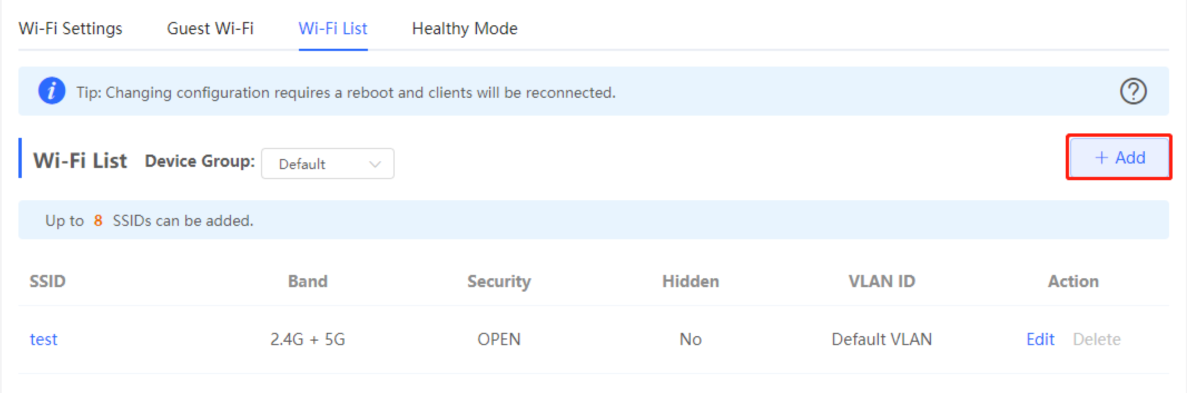
AP Isolation (The client joining this Wi-Fi network will be isolated.)

Band Steering (The 5G-supported client will access 5G radio preferentially.)

2.9 Adding a Wi-Fi Network

Choose **Wireless** > **Wi-Fi** > **Wi-Fi List**.

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.

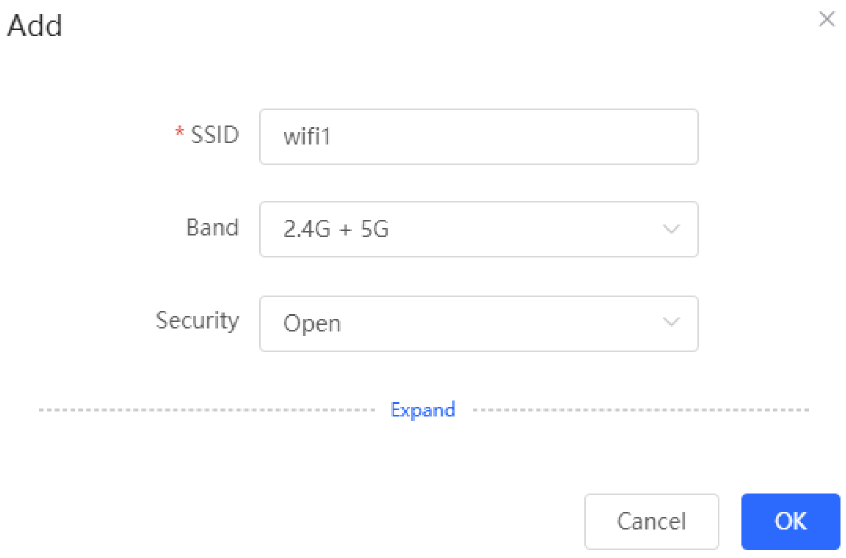


Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
test	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete



Add

* SSID: wifi1

Band: 2.4G + 5G

Security: Open

2.10 Configuring a Guest Wi-Fi

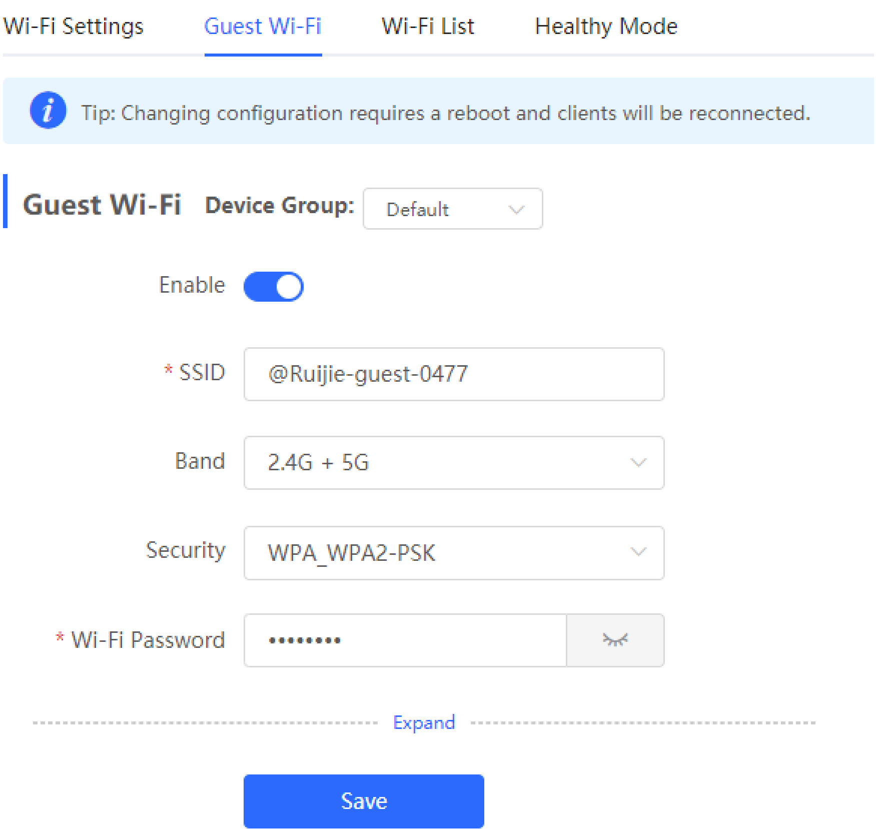
2.10.1 Overview

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.

2.10.2 Configuration Steps

Choose **Wireless** > **Wi-Fi** > **Guest Wi-Fi**.

Turn on **Guest Wi-Fi** and enter the SSID and Wi-Fi password. 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.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi Device Group: Default

Enable: ●

* SSID: @Ruijie-guest-0477

Band: 2.4G + 5G

Security: WPA_WPA2-PSK

* Wi-Fi Password: ••••••••

2.11 Configuring Wi-Fi Blacklist or Whitelist

2.11.1 Overview

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

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

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

Caution

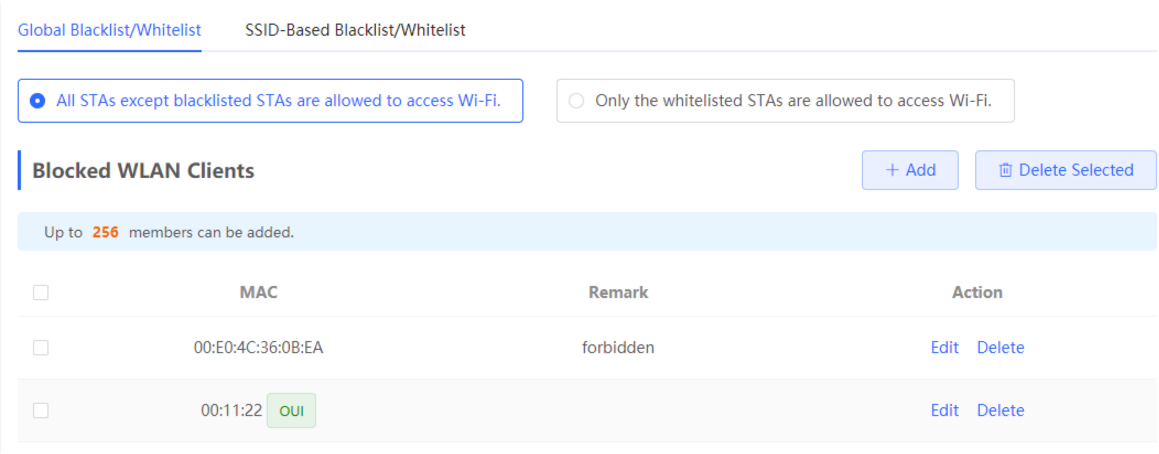
If the whitelist is empty, the whitelist does not take effect. In this case, all clients are allowed to access the Internet.

2.11.2 Configuration Steps

1. Configuring a Global Blacklist/Whitelist

Choose **Wireless** > **Blacklist/Whitelist** > **Global Blacklist/Whitelist**.

Select the blacklist or whitelist mode and click **Add** to configure a blacklist or whitelist 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 blacklist will be forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the access point.



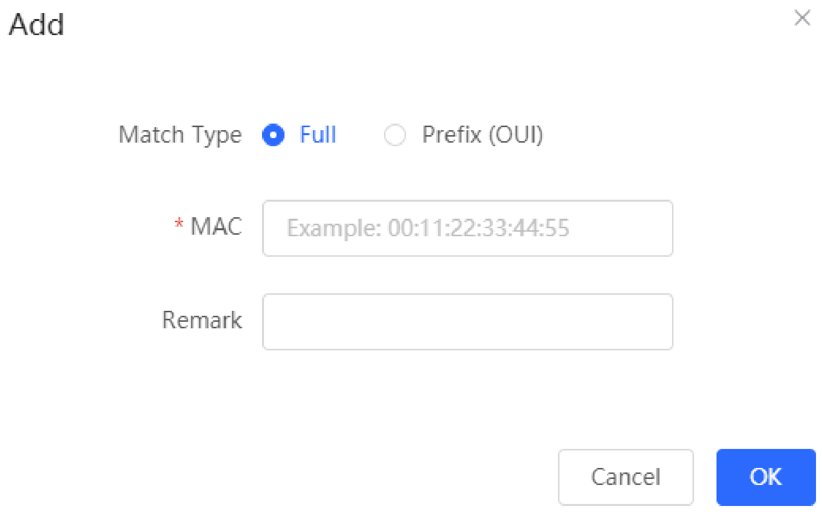
Global Blacklist/Whitelist SSID-Based Blacklist/Whitelist

● All STAs except blacklisted STAs are allowed to access Wi-Fi. ○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients + Add Delete Selected

Up to 256 members can be added.

□	MAC	Remark	Action
□	00:E0:4C:36:0B:EA	forbidden	Edit Delete
□	00:11:22 OUI		Edit Delete



Add ×

Match Type ● Full ○ Prefix (OUI)

* MAC Example: 00:11:22:33:44:55

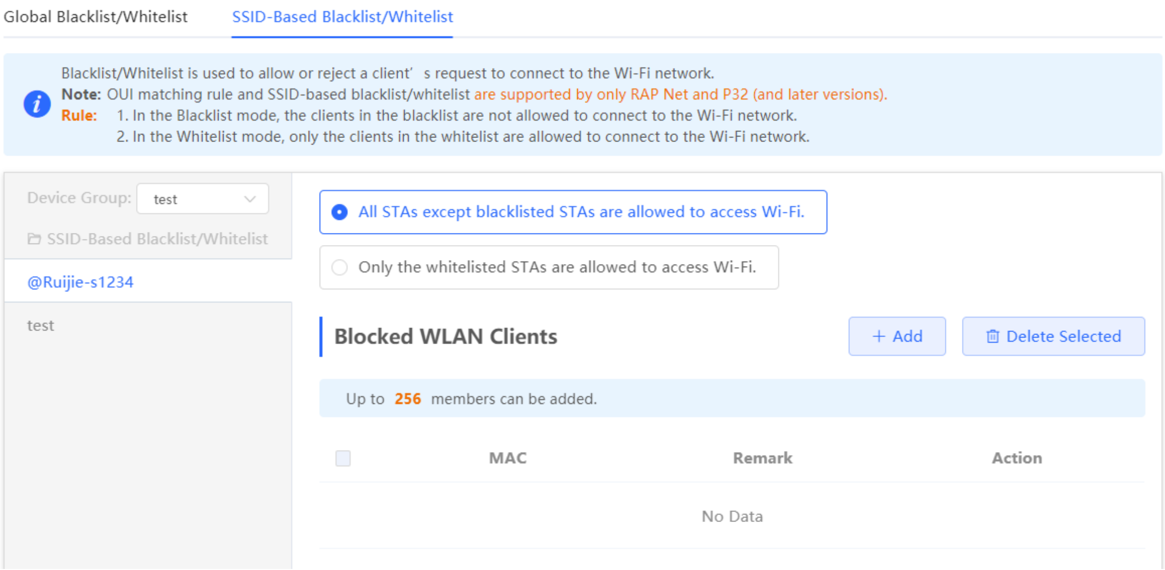
Remark

Cancel OK

2. Configuring an SSID-based Blacklist/Whitelist

Choose **Wireless** > **Blacklist/Whitelist** > **SSID-Based Blacklist/Whitelist**.

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



Blacklist/Whitelist is used to allow or reject a client’ s request to connect to the Wi-Fi network.
Note: OUI matching rule and SSID-based blacklist/whitelist are supported by only RAP Net and P32 (and later versions).
Rule: 1. In the Blacklist mode, the clients in the blacklist are not allowed to connect to the Wi-Fi network.
2. In the Whitelist mode, only the clients in the whitelist are allowed to connect to the Wi-Fi network.

Device Group: test

SSID-Based Blacklist/Whitelist

@Ruijie-s1234

test

● All STAs except blacklisted STAs are allowed to access Wi-Fi.

○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 256 members can be added.

□	MAC	Remark	Action
No Data			

2.12 Optimizing Wi-Fi Network

2.12.1 Overview

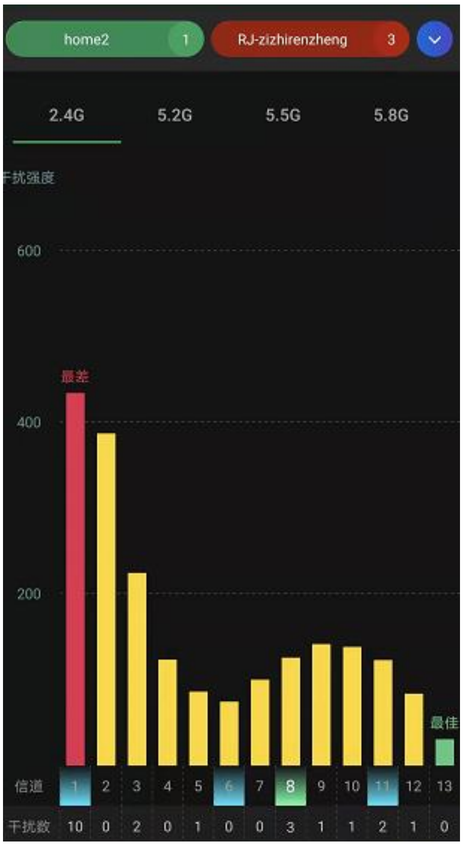
The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point 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.

2.12.2 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.


home2 1
RJ-zizhirenzheng 3
2.4G
5.2G
5.5G
5.8G
干扰强度
600
400
200
最差
最佳
信道 1 2 3 4 5 6 7 8 9 10 11 12 13
干扰数 10 0 2 0 1 0 0 3 1 1 2 1 0

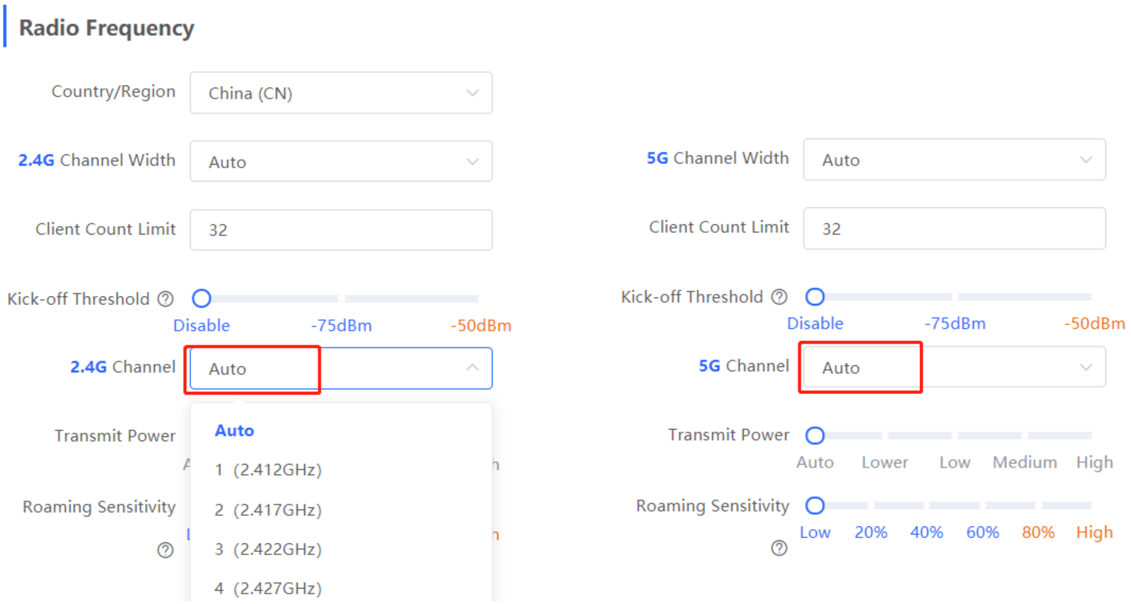
2.12.3 Optimizing the Radio Channel

Choose **Wireless** > **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.



Radio Frequency

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Client Count Limit: 32

Client Count Limit: 32

Kick-off Threshold

Kick-off Threshold

2.4G Channel: Auto

5G Channel: Auto

Transmit Power

Transmit Power

Roaming Sensitivity

Roaming Sensitivity

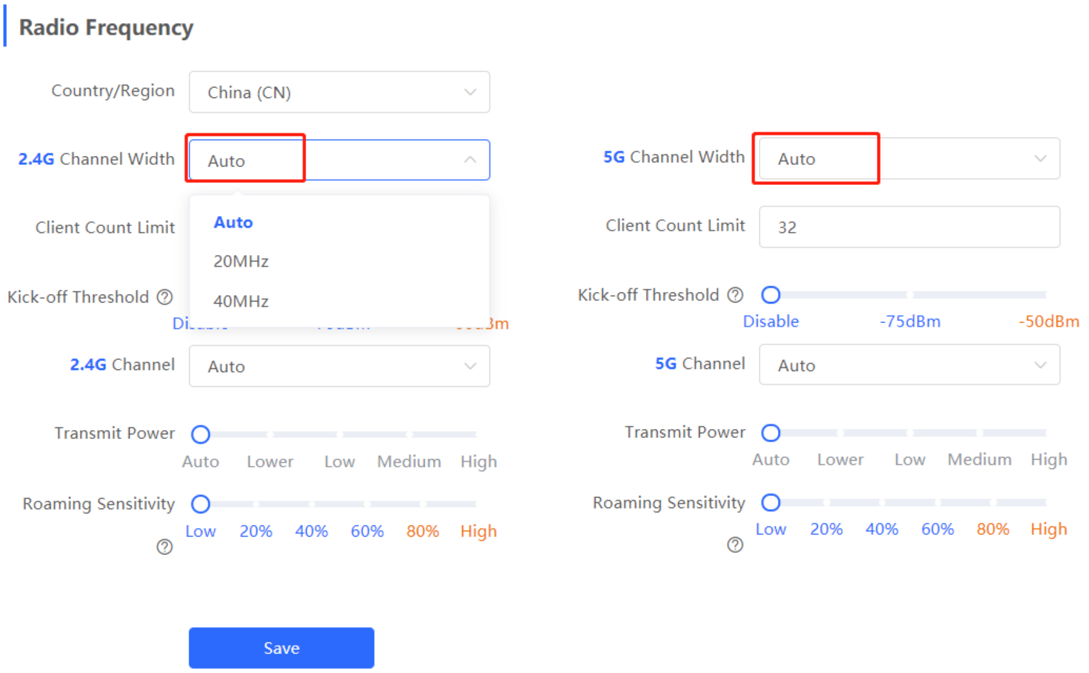
2.12.4 Optimizing the Channel Width

Choose **Wireless** > **Radio Frequency**.

If the interference is severe, choose a lower channel width to avoid network stalling. The access point supports the channel width of 20 MHz and 40 MHz. You are advised to select 20MHz channel width. 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 Frequency

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Client Count Limit

Client Count Limit: 32

Kick-off Threshold

Kick-off Threshold

2.4G Channel: Auto

5G Channel: Auto

Transmit Power

Transmit Power

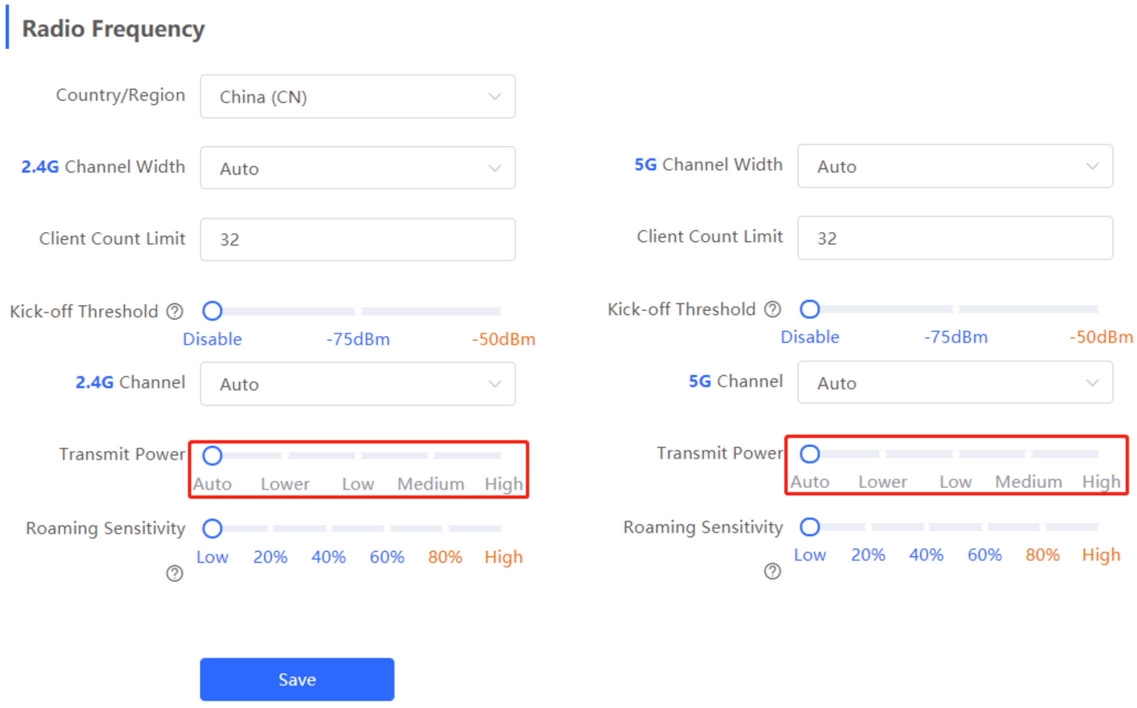
Roaming Sensitivity

Roaming Sensitivity

2.12.5 Optimizing the Transmit Power

Choose **Wireless** > **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.



Radio Frequency

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Client Count Limit: 32

Client Count Limit: 32

Kick-off Threshold: Disable -75dBm -50dBm

Kick-off Threshold: Disable -75dBm -50dBm

2.4G Channel: Auto

5G Channel: Auto

Transmit Power: Auto Lower Low Medium High

Transmit Power: Auto Lower Low Medium High

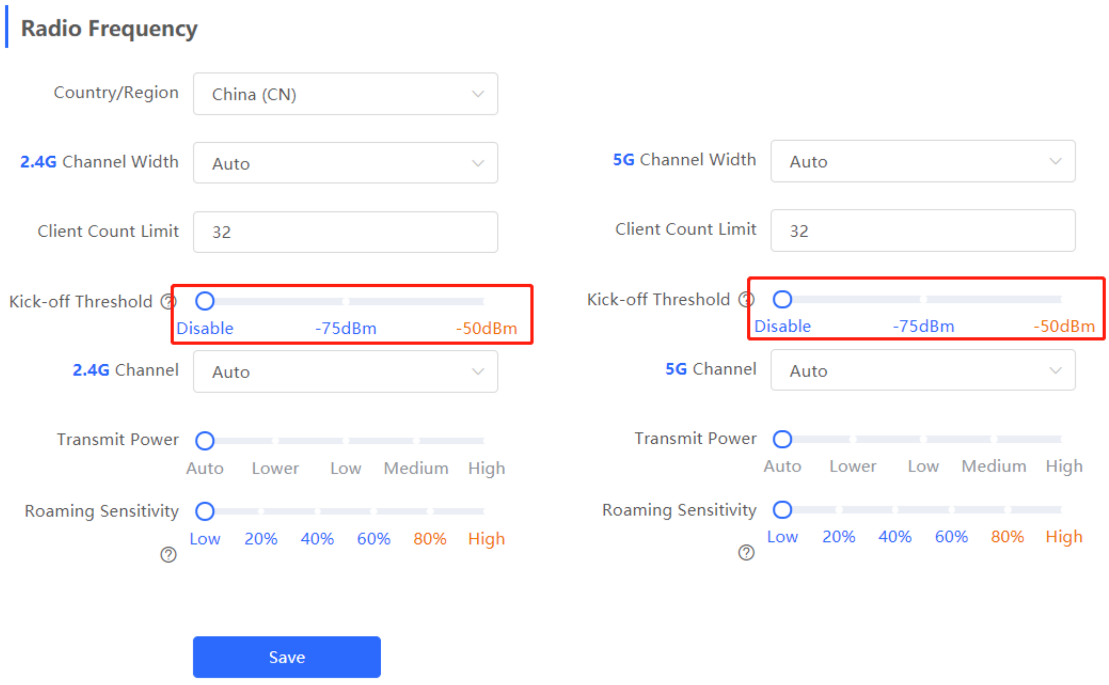
Roaming Sensitivity: Low 20% 40% 60% 80% High

Roaming Sensitivity: Low 20% 40% 60% 80% High

2.12.6 Configuring the Kick-off Threshold

Choose **Wireless** > **Radio Frequency**.

Farther the client is from the access point, lower the signal strength is. When the signal strength is lower than the threshold, the client will be forced offline and select a nearer Wi-Fi signal.



Radio Frequency

Country/Region: China (CN)

2.4G Channel Width: Auto

Client Count Limit: 32

Kick-off Threshold: Disable / -75dBm / -50dBm

2.4G Channel: Auto

Transmit Power: Auto / Lower / Low / Medium / High

Roaming Sensitivity: Low / 20% / 40% / 60% / 80% / High

5G Channel Width: Auto

Client Count Limit: 32

Kick-off Threshold: Disable / -75dBm / -50dBm

5G Channel: Auto

Transmit Power: Auto / Lower / Low / Medium / High

Roaming Sensitivity: Low / 20% / 40% / 60% / 80% / High

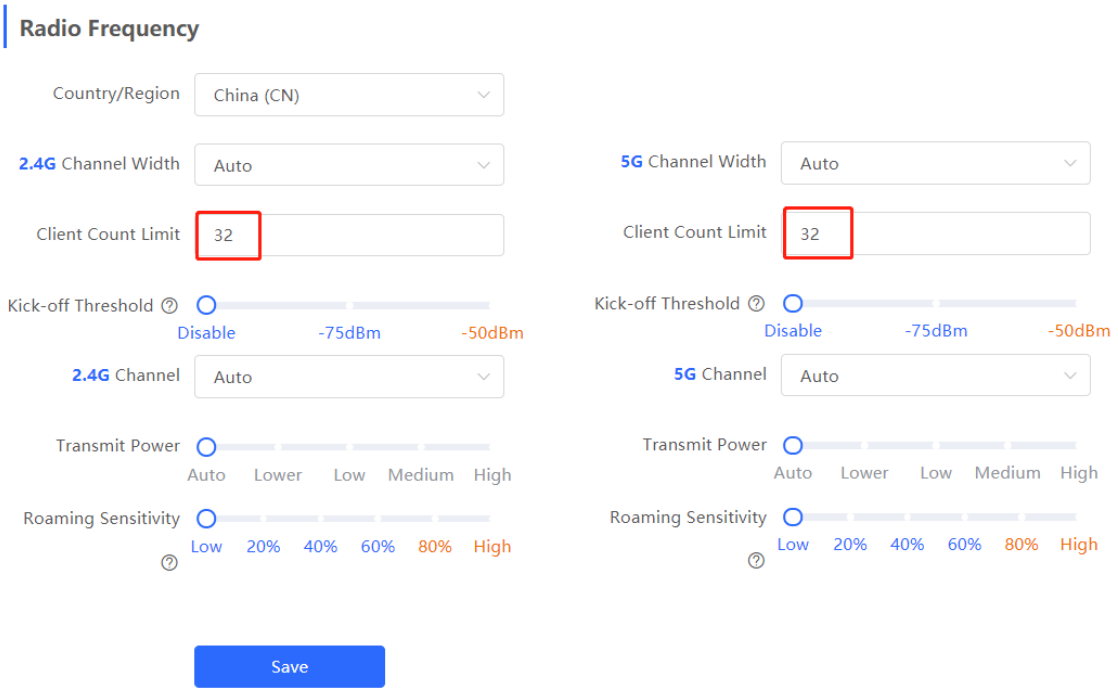
⚠ **Caution**

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

2.12.7 Configuring the Client Limit

Choose **Wireless** > **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.



Radio Frequency

Country/Region: China (CN)

2.4G Channel Width: Auto

Client Count Limit: 32

Kick-off Threshold: Disable

2.4G Channel: Auto

Transmit Power: Auto

Roaming Sensitivity: Low

5G Channel Width: Auto

Client Count Limit: 32

Kick-off Threshold: Disable

5G Channel: Auto

Transmit Power: Auto

Roaming Sensitivity: Low

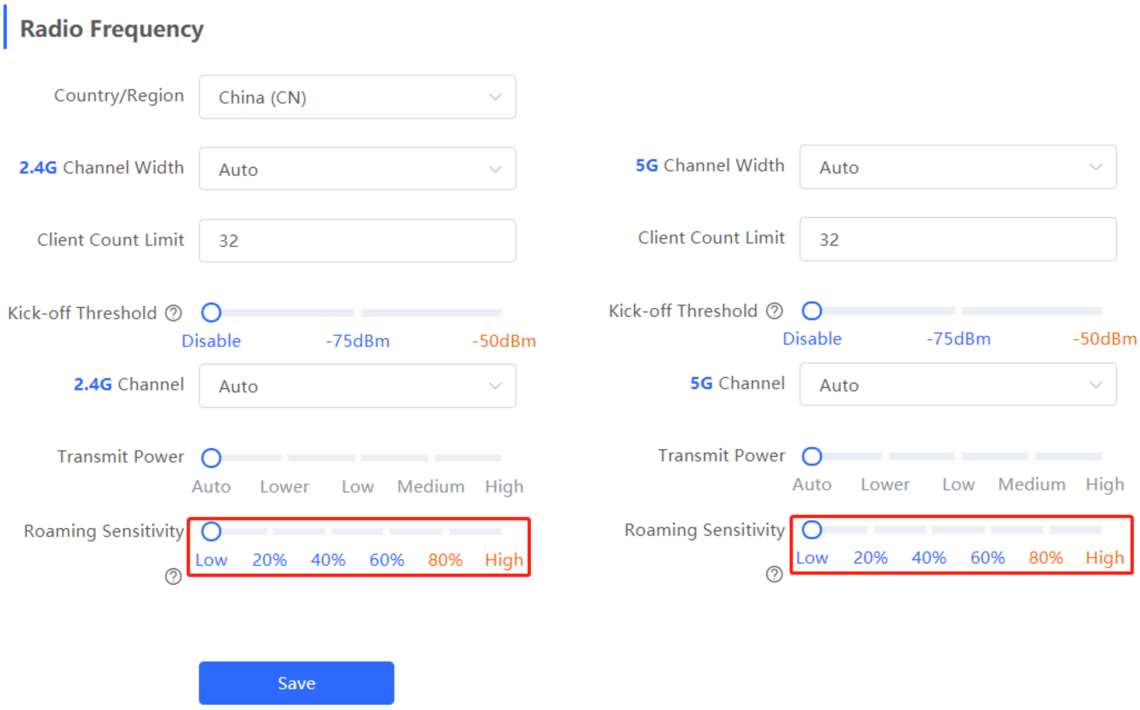
Note

In the self-organizing network mode, the client limit refers to the maximum number of clients accessing all Wi-Fi networks. If you want to specify the client limit for one single access point, group the access point and configure the client limit for this group. Alternatively, proceed with configuration in the standalone mode.

2.12.8 Configuring the Roaming Sensitivity

Choose **Wireless** > **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.



Radio Frequency

Country/Region: China (CN)

2.4G Channel Width: Auto

Client Count Limit: 32

Kick-off Threshold: Disable

2.4G Channel: Auto

Transmit Power: Auto

Roaming Sensitivity: Low

5G Channel Width: Auto

Client Count Limit: 32

Kick-off Threshold: Disable

5G Channel: Auto

Transmit Power: Auto

Roaming Sensitivity: Low

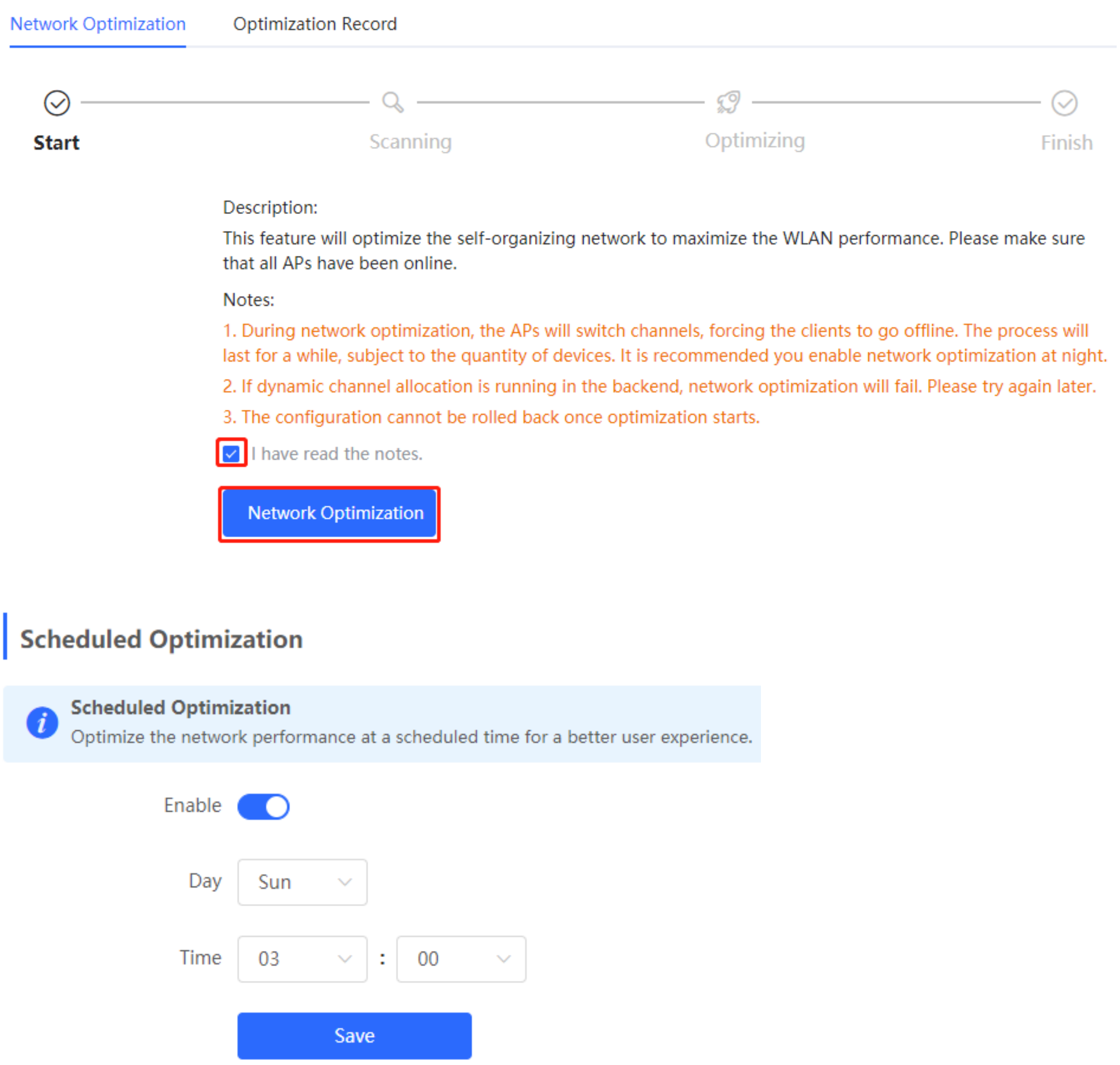
2.12.9 Configuring WIO

Choose **Wireless** > **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.



Description:

This feature will optimize the self-organizing network to maximize the WLAN performance. Please make sure that all APs have been online.

Notes:

1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization at night.

2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.

3. The configuration cannot be rolled back once optimization starts.

☑ I have read the notes.

Scheduled Optimization

Scheduled Optimization

Optimize the network performance at a scheduled time for a better user experience.

Enable: ●

Day: Sun

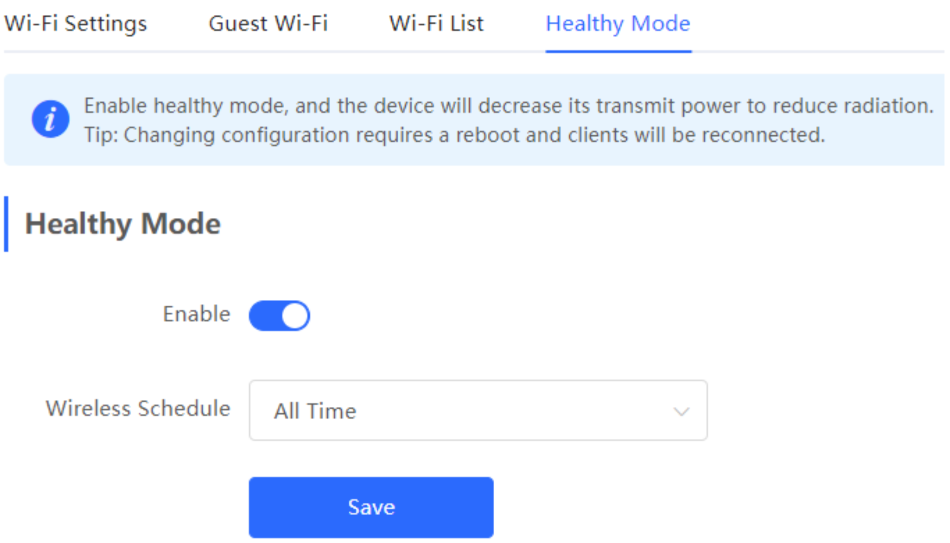
Time: 03 : 00

2.13 Configuring Healthy Mode

Choose **Wireless** > **Wi-Fi** > **Healthy Mode**.

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.



Enable healthy mode, and the device will decrease its transmit power to reduce radiation.
Tip: Changing configuration requires a reboot and clients will be reconnected.

Healthy Mode

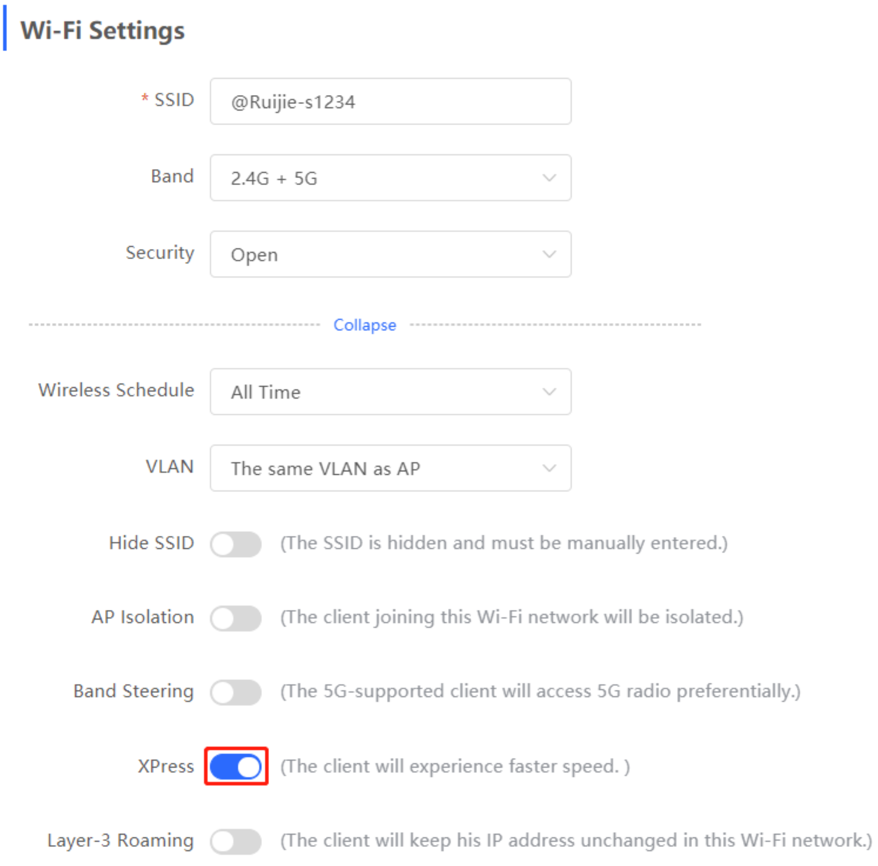
Enable: ●

Wireless Schedule: All Time

2.14 Configuring Xpress

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Click **Expand**, 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.


Wi-Fi Settings

* SSID: @Ruijie-s1234

Band: 2.4G + 5G

Security: Open

Wireless Schedule: All Time

VLAN: The same VLAN as AP

Hide SSID: ○ (The SSID is hidden and must be manually entered.)

AP Isolation: ○ (The client joining this Wi-Fi network will be isolated.)

Band Steering: ○ (The 5G-supported client will access 5G radio preferentially.)

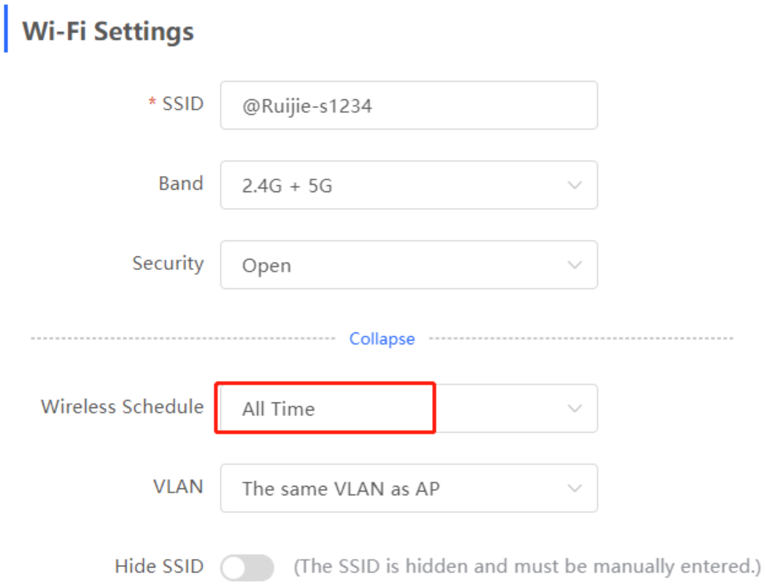
XPress: ● (The client will experience faster speed.)

Layer-3 Roaming: ○ (The client will keep his IP address unchanged in this Wi-Fi network.)

2.15 Configuring Wireless Schedule

Choose **Wireless** > **Wi-Fi** > **Wi-Fi Settings**.

Click **Expand**, 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.



Wi-Fi Settings

* SSID: @Ruijie-s1234

Band: 2.4G + 5G

Security: Open

Wireless Schedule: All Time

VLAN: The same VLAN as AP

Hide SSID: (The SSID is hidden and must be manually entered.)

3 Network Settings

3.1 Switching Work Mode

3.1.1 Work Mode

See Work Mode for details.

3.1.2 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.

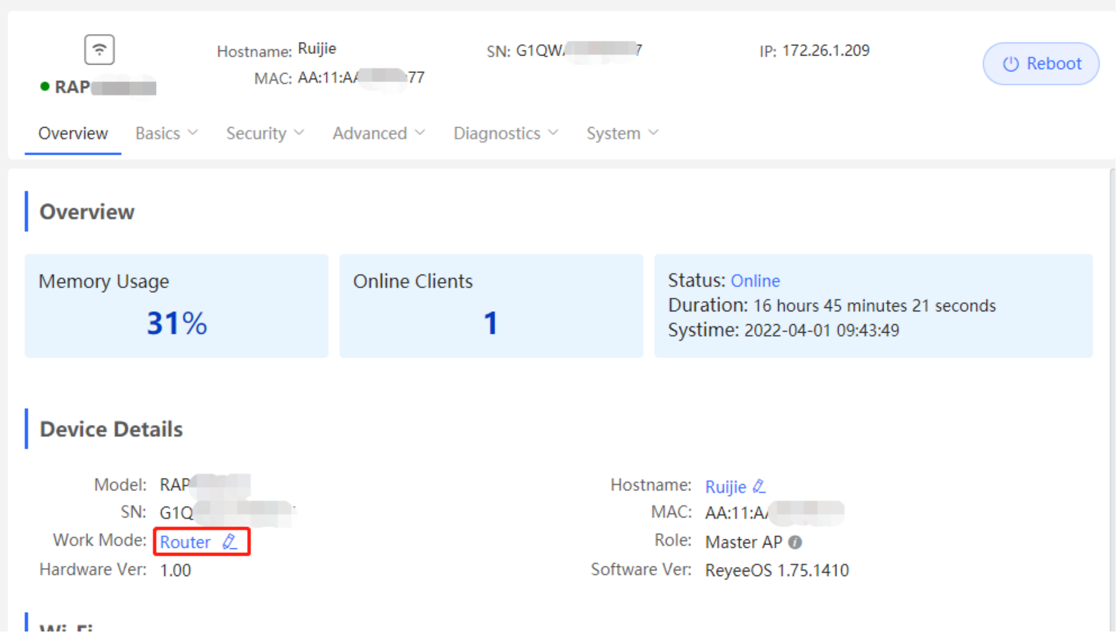
After the self-organizing network discovery function is enabled, the device can be discovered in the network and discover other devices in the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the Web management page of any device 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.

3.1.3 Configuration Steps

Choose **Wireless** > **APs** > **Manage** > **Overview** > **Device Details**.

Click the current work mode to change the work mode.



RAP[redacted]

Hostname: Ruijie

MAC: AA:11:A[redacted]77

SN: G1QW[redacted]7

IP: 172.26.1.209

Overview

Memory Usage 31%

Online Clients 1

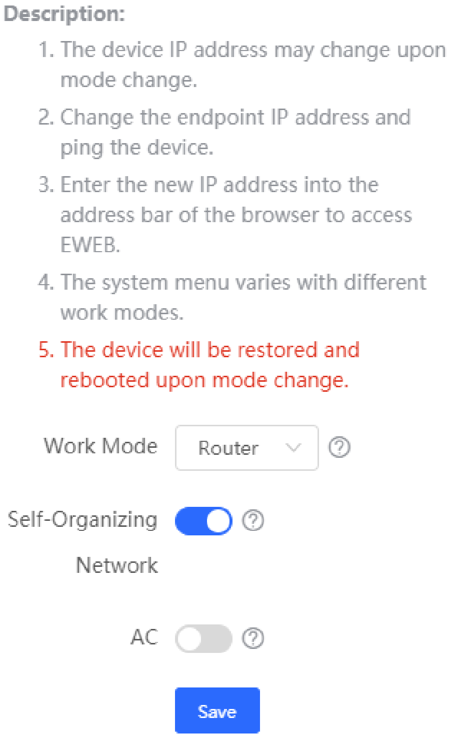
Status: Online
Duration: 16 hours 45 minutes 21 seconds
Systime: 2022-04-01 09:43:49

Device Details

Model: RAP[redacted]
SN: G1Q[redacted]
Work Mode: Router
Hardware Ver: 1.00

Hostname: Ruijie
MAC: AA:11:A[redacted]
Role: Master AP
Software Ver: ReyeeOS 1.75.1410

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.



Description:

1. The device IP address may change upon mode change.
2. Change the endpoint IP address and ping the device.
3. Enter the new IP address into the address bar of the browser to access EWEB.
4. The system menu varies with different work modes.
5. The device will be restored and rebooted upon mode change.

Work Mode: Router

Self-Organizing Network: ●

AC: ○

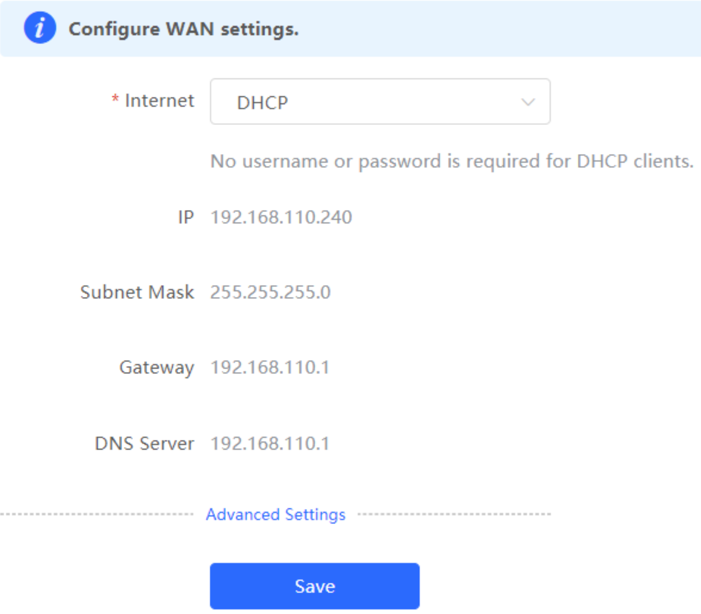
Caution

- Switching the work mode will restore factory settings and restart the device. Therefore, exercise caution when performing this operation.
- After the self-organizing network discovery is enabled, you can check the role of the device in self-organizing network mode.

3.2 Configuring Internet Type

Choose **Wireless** > **APs** > **Manage** > **Basics** > **WAN**.

Select the Internet connection type after confirming with the ISP. For detailed configuration, see Work Mode.



Configure WAN settings.

* Internet	DHCP
	No username or password is required for DHCP clients.
IP	192.168.110.240
Subnet Mask	255.255.255.0
Gateway	192.168.110.1
DNS Server	192.168.110.1

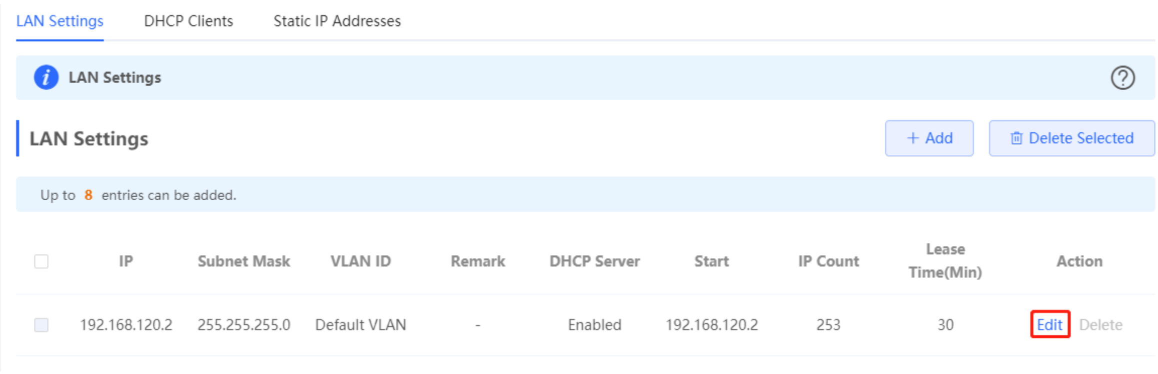
3.3 Configuring LAN Port

Caution

This function is not supported when the device works in AP mode.

Choose **Wireless** > **APs** > **Manage** > **Basics** > **LAN** > **LAN Settings**.

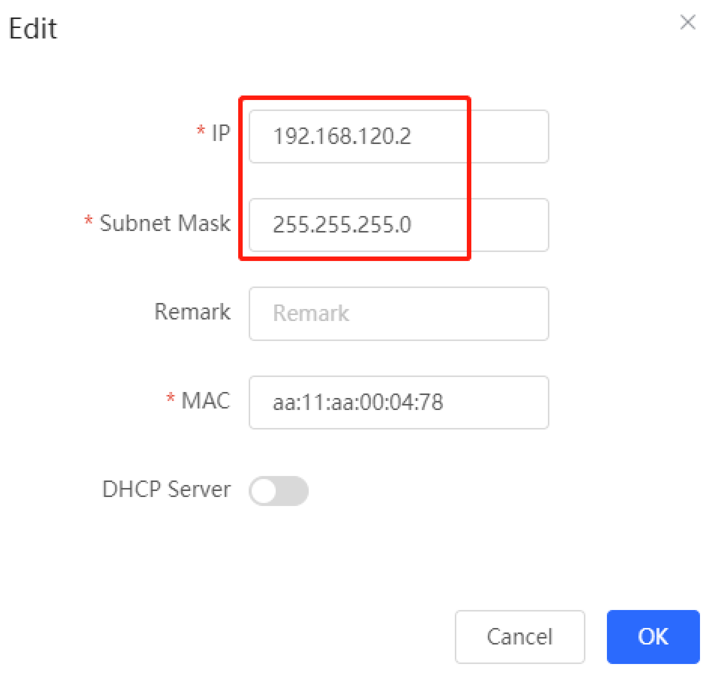
Click **Edit**. In the displayed dialog box, enter the IP address and subnet mask, and click **OK**. Change the IP address of the LAN port. Enter the new IP address in the browser and log in to the device again to configure and manage the device.



LAN Settings

Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	Edit Delete



Edit

* IP: 192.168.120.2

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: aa:11:aa:00:04:78

DHCP Server: ○

3.4 Configuring Repeater Mode

Caution

RG-RAP1200(F) access point does not support this function.

3.4.1 Wired Repeater

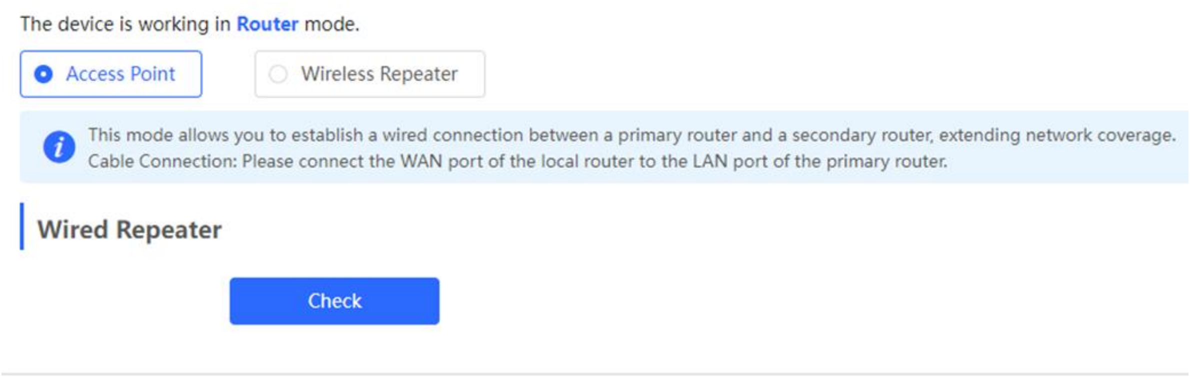
Choose **Wireless** > **APs** > **Manage** > **Basics** > **Repeater Mode**.

Connect a network cable from the WAN port (uplink LAN port) of the device to the upper-layer device.

Select **Access Point**, click **Check**, confirm the Wi-Fi settings of the AP, and then click **Save** to expand the network coverage.

Caution

After the configuration is saved, connected clients will be disconnected from the network for a short period of time. You can reconnect the clients to the Wi-Fi network for restoration.



The device is working in Router mode.

● Access Point ○ Wireless Repeater

This mode allows you to establish a wired connection between a primary router and a secondary router, extending network coverage.
Cable Connection: Please connect the WAN port of the local router to the LAN port of the primary router.

Wired Repeater

3.4.2 Wireless Repeater

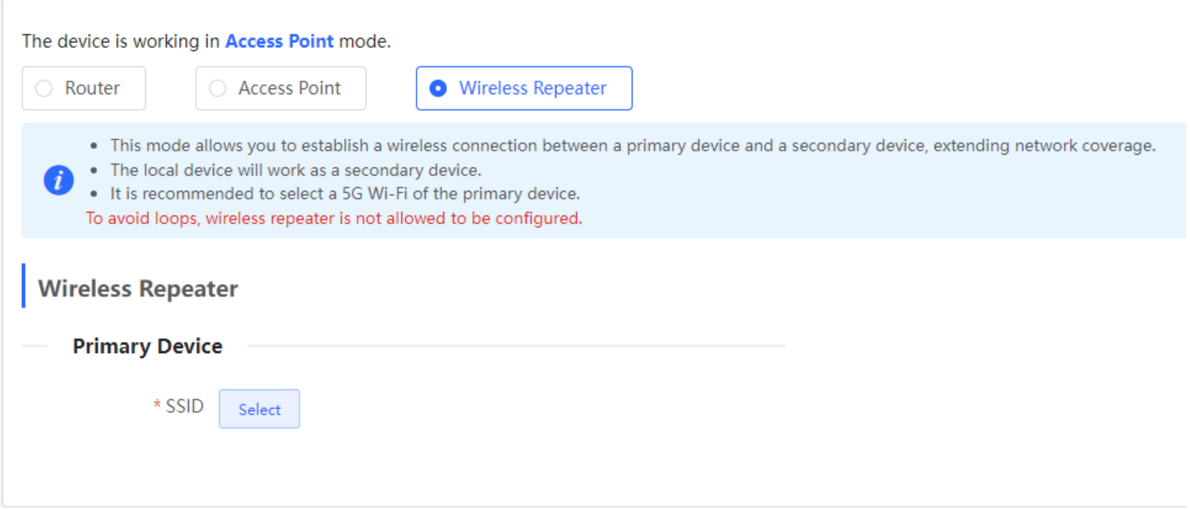
The wireless repeater mode extends the Wi-Fi coverage range of the primary device. The device supports the dual-link wireless repeater mode and can relay both 2.4 GHz and 5 GHz signals of the primary device.

Note

- To avoid loops in wireless repeater mode, remove the network cable from the WAN port.
- Obtain the Wi-Fi name and Wi-Fi password of the upper-layer router.

Choose **Wireless** > **APs** > **Manage** > **Basics** > **Repeater Mode**.

(1) Click **Wireless Repeater** and then click **Select**. A list of surrounding Wi-Fi signals pops up. A list of nearby 5GHz Wi-Fi networks is displayed by default. You can switch from 5 GHz to 2.4 GHz band by selecting **2.4G** from the drop-down list box. You are advised to select a strong 5 GHz Wi-Fi network signal.



The device is working in Access Point mode.

○ Router ○ Access Point ● Wireless Repeater

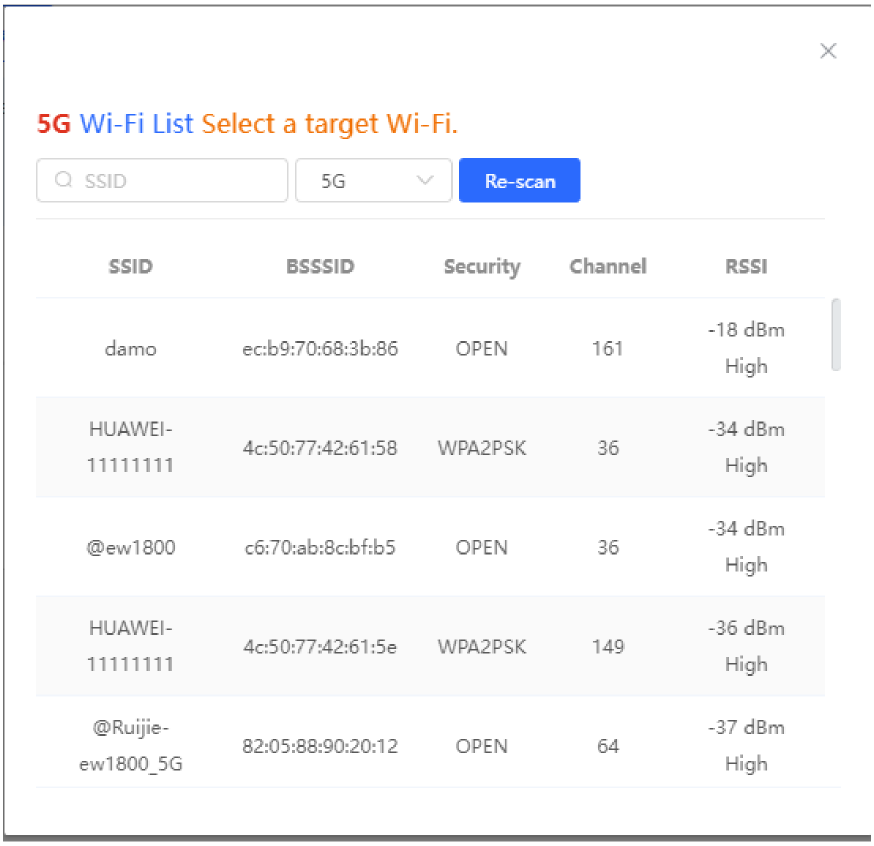
- This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.
- The local device will work as a secondary device.
- It is recommended to select a 5G Wi-Fi of the primary device.

To avoid loops, wireless repeater is not allowed to be configured.

Wireless Repeater

Primary Device

* SSID



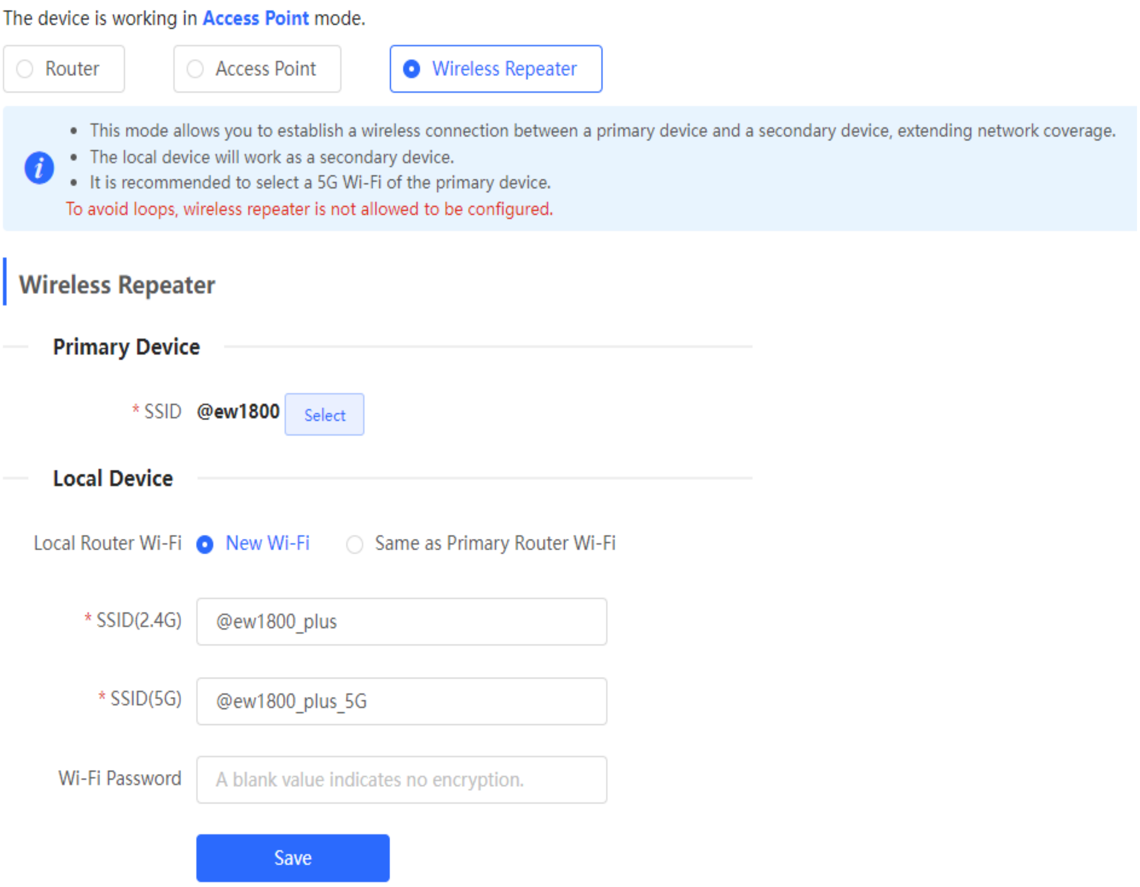
5G Wi-Fi List Select a target Wi-Fi.

SSID	BSSSID	Security	Channel	RSSI
damo	ec:b9:70:68:3b:86	OPEN	161	-18 dBm High
HUAWEI-11111111	4c:50:77:42:61:58	WPA2PSK	36	-34 dBm High
@ew1800	c6:70:ab:8c:bf:b5	OPEN	36	-34 dBm High
HUAWEI-11111111	4c:50:77:42:61:5e	WPA2PSK	149	-36 dBm High
@Ruijie-ew1800_5G	82:05:88:90:20:12	OPEN	64	-37 dBm High

(2) Select the Wi-Fi signal of the upper-layer device that you want to relay. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.

(3) Configure **Local Router Wi-Fi**. You can select **New Wi-Fi** or **Same as Primary Router Wi-Fi**.

- If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the router are automatically synchronized with those on the primary router. Generally, clients merge Wi-Fi signals with the same name into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.
- If **New Wi-Fi** is selected, you can set a local Wi-Fi name and password. Clients will search out different Wi-Fi signals.



The device is working in **Access Point** mode.

○ Router ○ Access Point ● Wireless Repeater

- This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.
- The local device will work as a secondary device.
- It is recommended to select a 5G Wi-Fi of the primary device.

To avoid loops, wireless repeater is not allowed to be configured.

Wireless Repeater

Primary Device

* SSID @ew1800 Select

Local Device

Local Router Wi-Fi ● New Wi-Fi ○ Same as Primary Router Wi-Fi

* SSID(2.4G) @ew1800_plus

* SSID(5G) @ew1800_plus_5G

Wi-Fi Password A blank value indicates no encryption.

Save

Caution

- After the configuration is saved, the AP will be disconnected from the Wi-Fi network and needs to connect to the new Wi-Fi network. Exercise caution when performing this operation. Record the new Wi-Fi name and password.
- You are advised to install the AP in a position where the RSSI is greater than two bars of signal to prevent signal loss. If the signal at the installation position is too weak, the relay may fail or the signal quality after amplification may be poor.

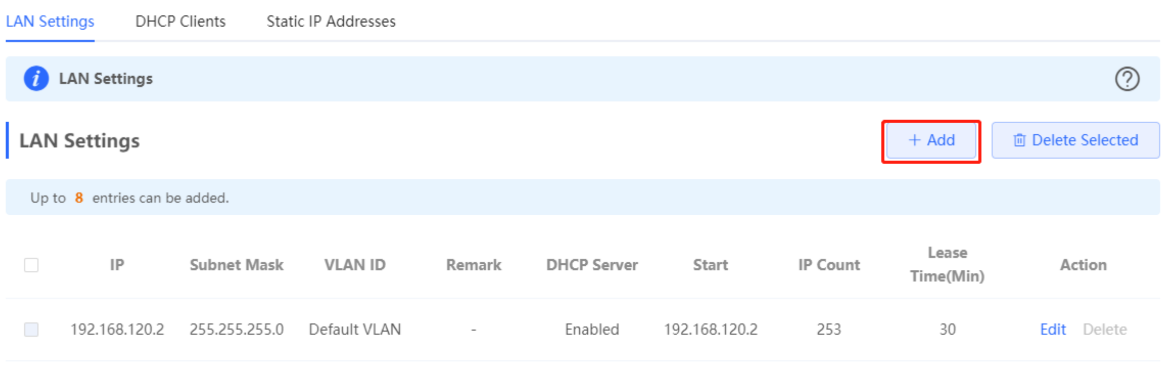
3.5 Creating a VLAN

Caution

This function is not supported when the device works in AP mode.

Choose **Wireless** > **APs** > **Manage** > **Basics** > **LAN** > **LAN Settings**.

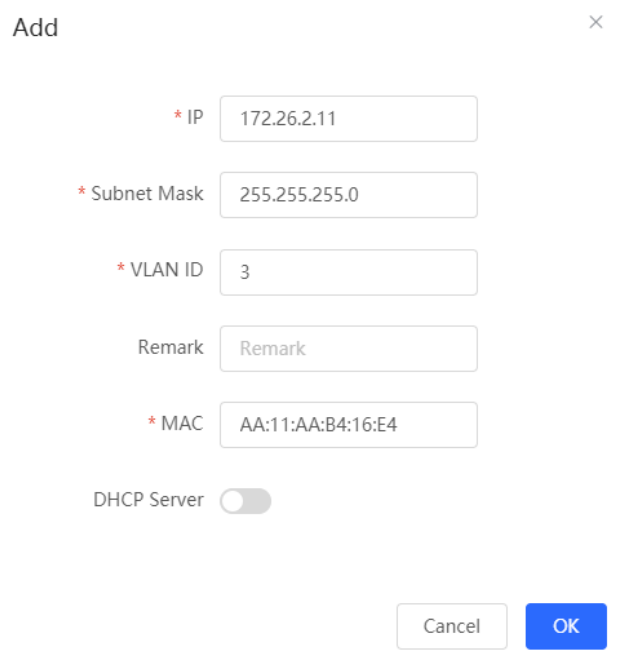
A LAN can be classified into multiple VLANs. Click **Add** to create a VLAN.



LAN Settings

Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	Edit Delete



* IP: 172.26.2.11

* Subnet Mask: 255.255.255.0

* VLAN ID: 3

Remark: Remark

* MAC: AA:11:AA:B4:16:E4

DHCP Server: ○

Table 3-1 VLAN Configuration

Parameter	Description
IP	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.
Remark	VLAN description.
MAC	MAC address of the VLAN interface.

Parameter	Description
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 3.9 Configuring the 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.

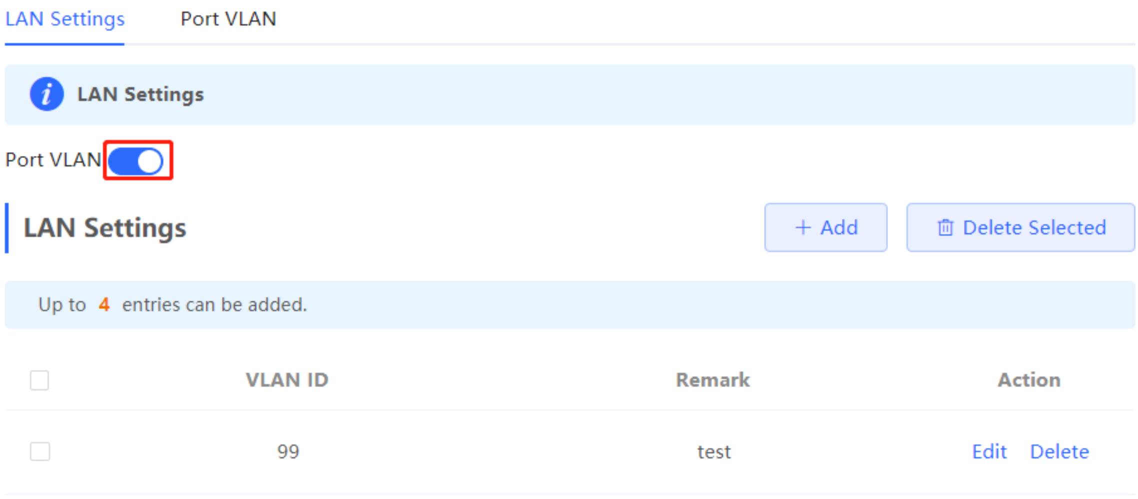
3.6 Configuring Port VLAN

Caution

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

Choose **Wireless** > **APs** > **Manage** > **Basics** > **LAN**.

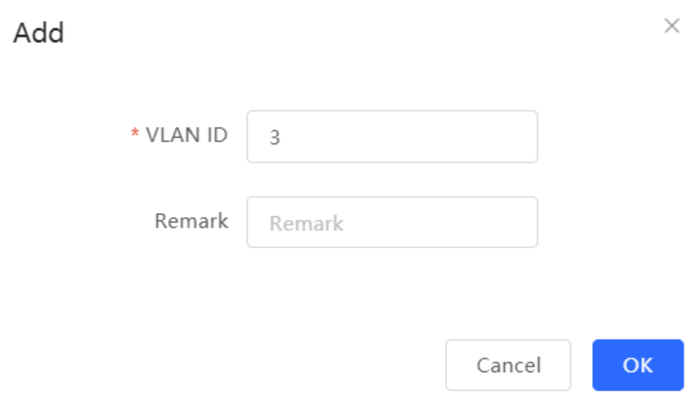
(1) On the **LAN Settings** tab page, turn on **Port VLAN**, and click **OK** in the confirmation dialog box.



Up to 4 entries can be added.

□	VLAN ID	Remark	Action
□	99	test	Edit Delete

(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.

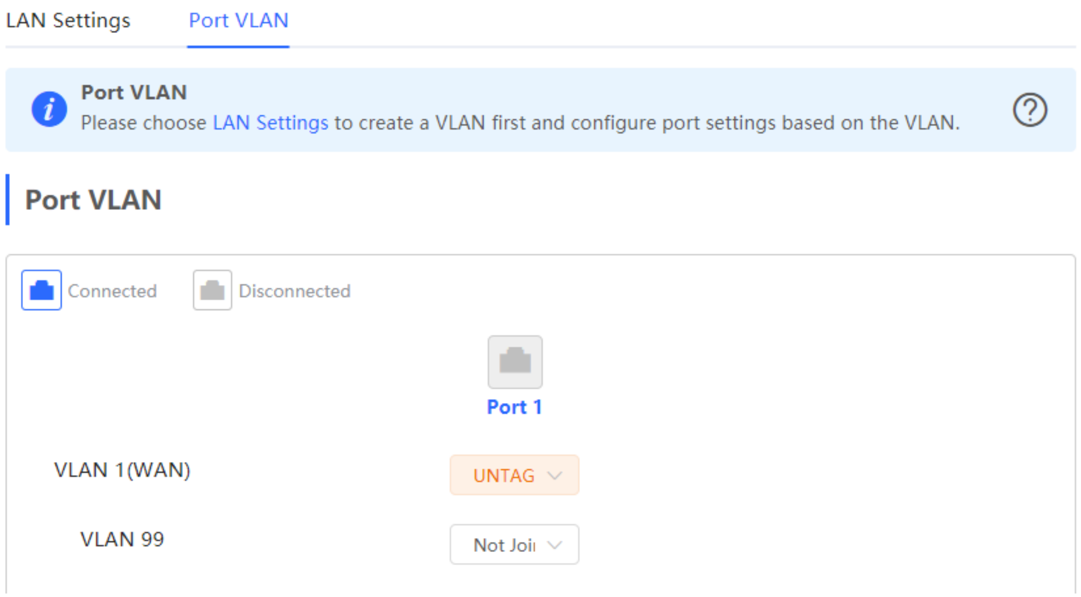


* VLAN ID: 3

Remark: Remark

(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.



Port VLAN

Please choose LAN Settings to create a VLAN first and configure port settings based on the VLAN.

Port VLAN

	Port 1
VLAN 1(WAN)	UNTAG
VLAN 99	Not Joi

3.7 Changing MAC Address

Choose **Wireless** > **APs** > **Manage** > **Basics** > **WAN**.

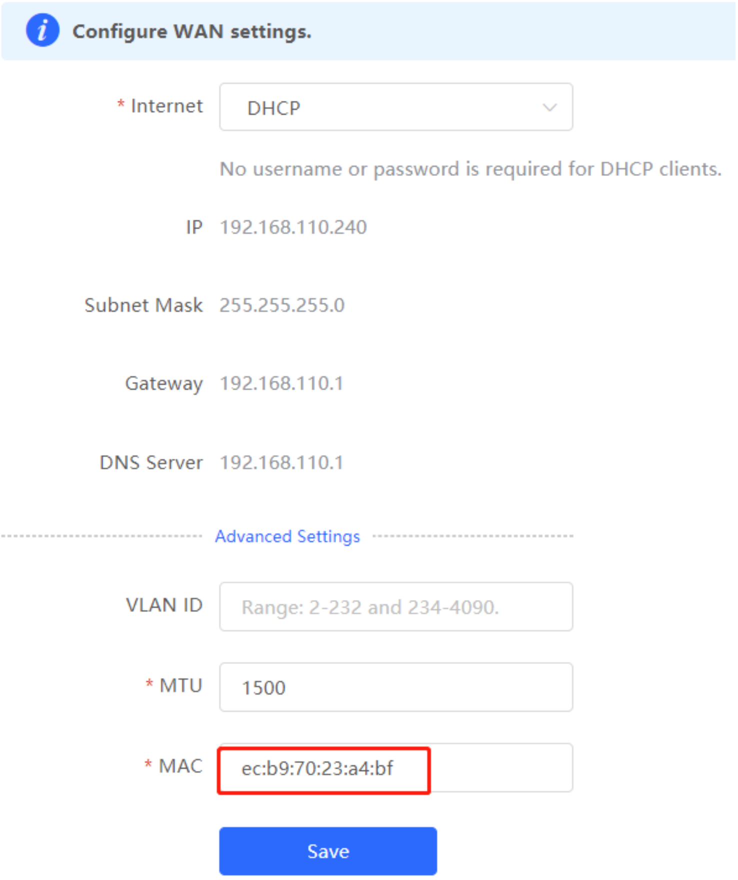
ISPs may restrict the access of devices with unknown MAC addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port.

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 **Basics** > **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.



Configure WAN settings.

* Internet: DHCP

No username or password is required for DHCP clients.

IP: 192.168.110.240

Subnet Mask: 255.255.255.0

Gateway: 192.168.110.1

DNS Server: 192.168.110.1

VLAN ID: Range: 2-232 and 234-4090.

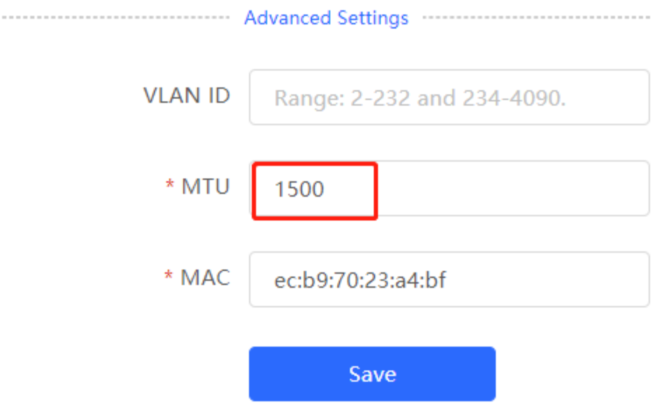
* MTU: 1500

* MAC: ec:b9:70:23:a4:bf

3.8 Changing MTU

Choose **Wireless** > **APs** > **Manage** > **Basics** > **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.



* MTU: 1500

* MAC: ec:b9:70:23:a4:bf

3.9 Configuring DHCP Server

⚠ **Caution**

This function is not supported when the device works in AP mode.

3.9.1 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.

3.9.2 Configuring the DHCP Server Function

Choose **Wireless** > **APs** > **Manage** > **Basics** > **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.

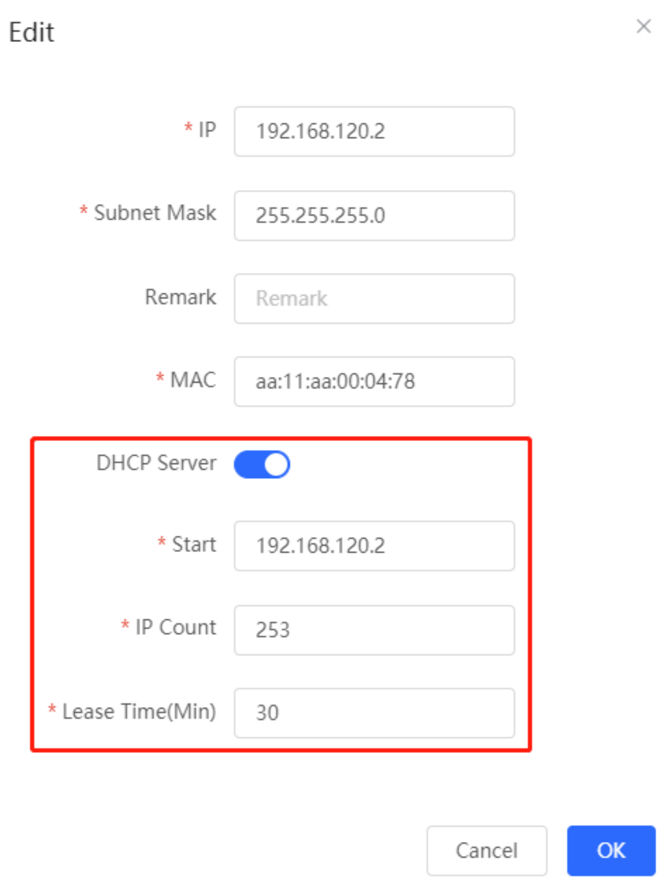
⚠ **Caution**

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. Aclient 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.



Edit ×

* IP: 192.168.120.2

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: aa:11:aa:00:04:78

DHCP Server: ●

* Start: 192.168.120.2

* IP Count: 253

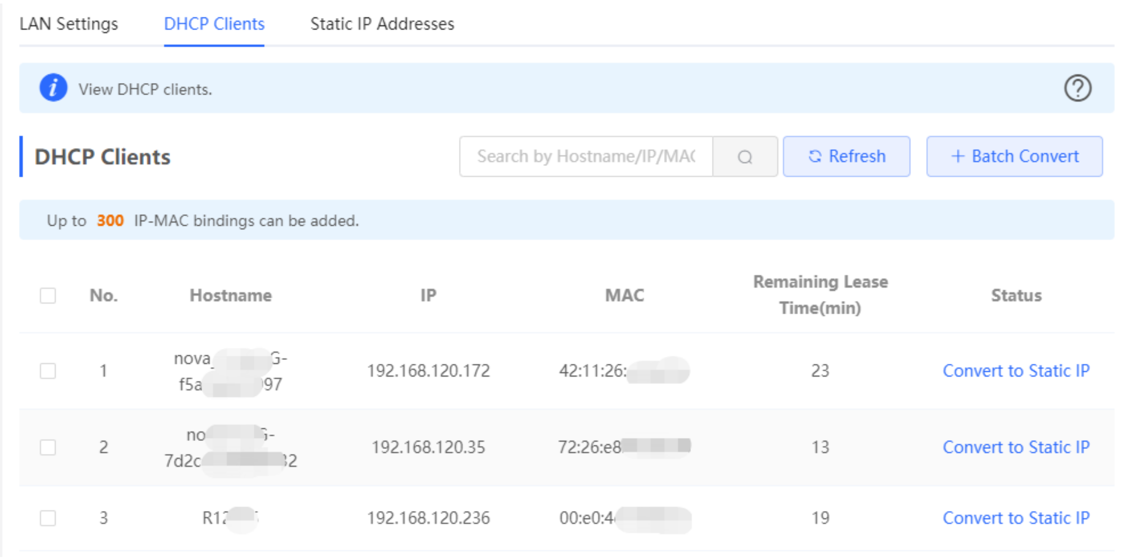
* Lease Time(Min): 30

Cancel OK

3.9.3 Displaying Online DHCP Clients

Choose **Wireless** > **APs** > **Manage** > **Basics** > **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.



LAN Settings | DHCP Clients | Static IP Addresses

View DHCP clients.

DHCP Clients

Search by Hostname/IP/MAC | Refresh | + Batch Convert

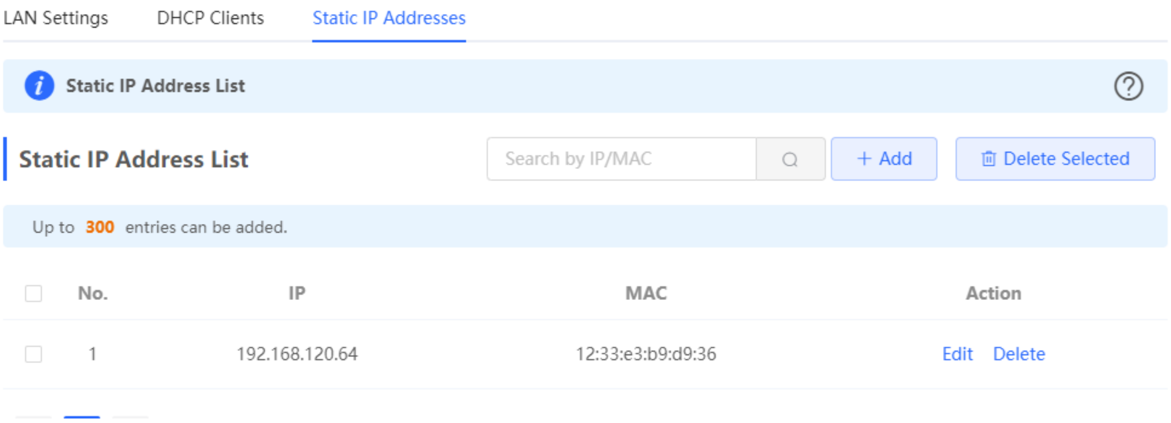
Up to 300 IP-MAC bindings can be added.

□	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
□	1	nova[redacted]G-f5a[redacted]97	192.168.120.172	42:11:26:[redacted]	23	Convert to Static IP
□	2	no[redacted]-7d2c[redacted]2	192.168.120.35	72:26:e8[redacted]	13	Convert to Static IP
□	3	R1[redacted]	192.168.120.236	00:e0:4[redacted]	19	Convert to Static IP

3.9.4 Displaying the DHCP Static IP Address List

Choose **Wireless** > **APs** > **Manage** > **Basics** > **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.



Static IP Address List

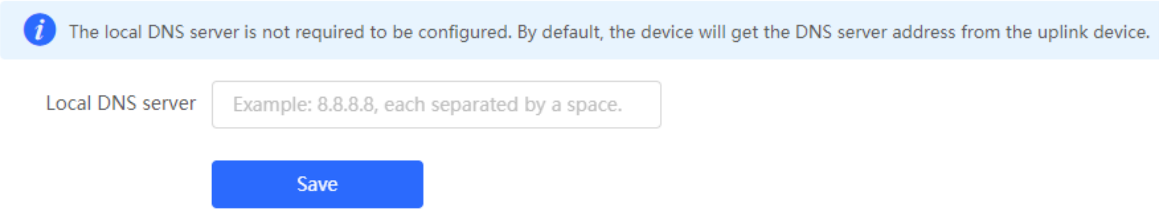
Up to 300 entries can be added.

□	No.	IP	MAC	Action
□	1	192.168.120.64	12:33:e3:b9:d9:36	Edit Delete

3.10 Configuring DNS

Choose **Wireless** > **APs** > **Manage** > **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.

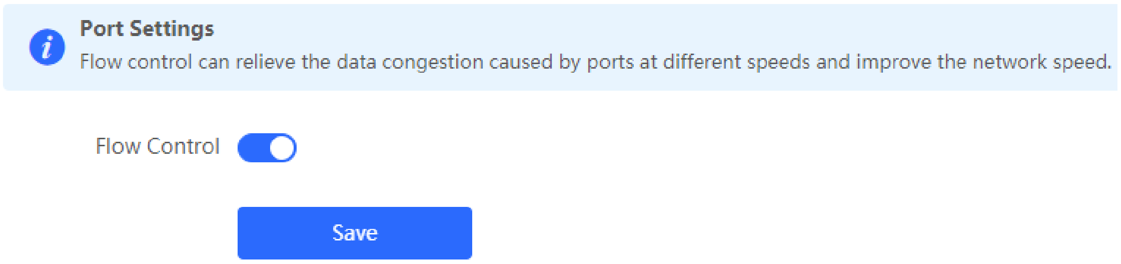


The local DNS server is not required to be configured. By default, the device will get the DNS server address from the uplink device.

3.11 Configuring Port Flow Control

Choose **Wireless** > **APs** > **Manage** > **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.



Port Settings

Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.

Flow Control ●

3.12 Configuring ARP Binding

Caution

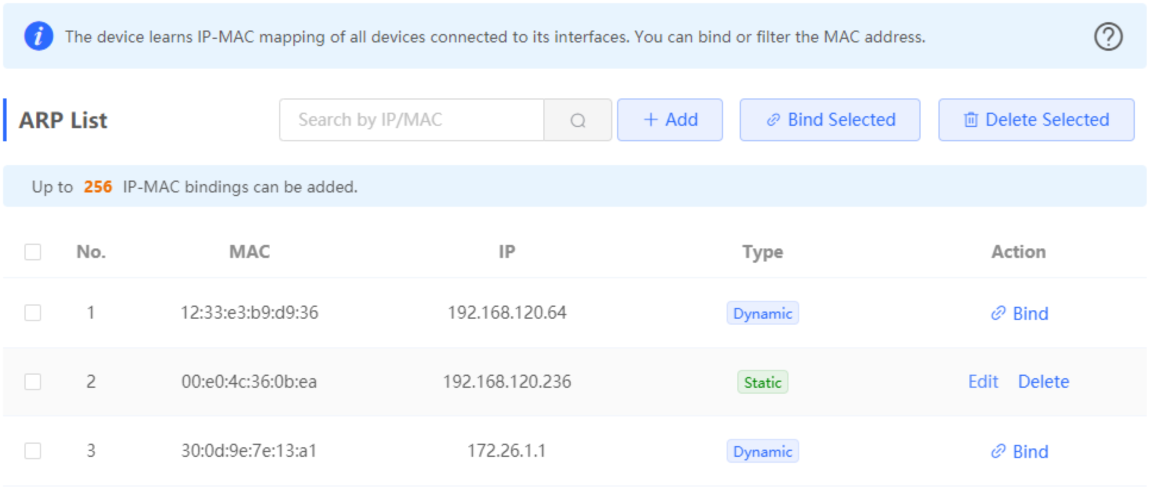
This function is not supported when the device works in AP mode.

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.

Choose **Wireless** > **APs** > **Manage** > **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.



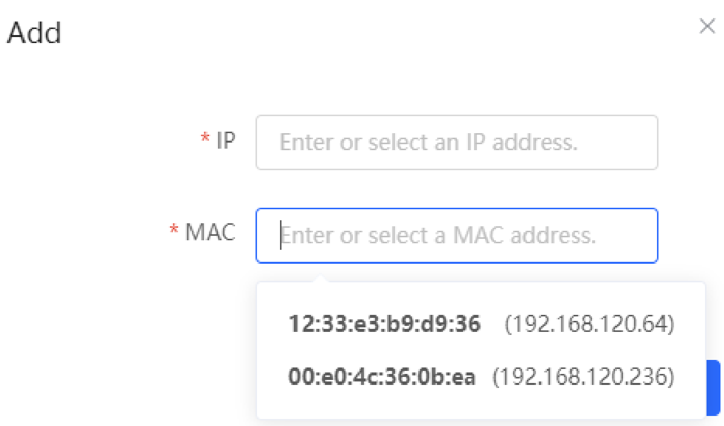
The device learns IP-MAC mapping of all devices connected to its interfaces. You can bind or filter the MAC address.

ARP List

Up to 256 IP-MAC bindings can be added.

□	No.	MAC	IP	Type	Action
□	1	12:33:e3:b9:d9:36	192.168.120.64	Dynamic	Bind
□	2	00:e0:4c:36:0b:ea	192.168.120.236	Static	Edit Delete
□	3	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	Bind

(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.



Add

* IP Enter or select an IP address.

* MAC Enter or select a MAC address.

12:33:e3:b9:d9:36 (192.168.120.64)

00:e0:4c:36:0b:ea (192.168.120.236)

3.13 Configuring LAN Ports

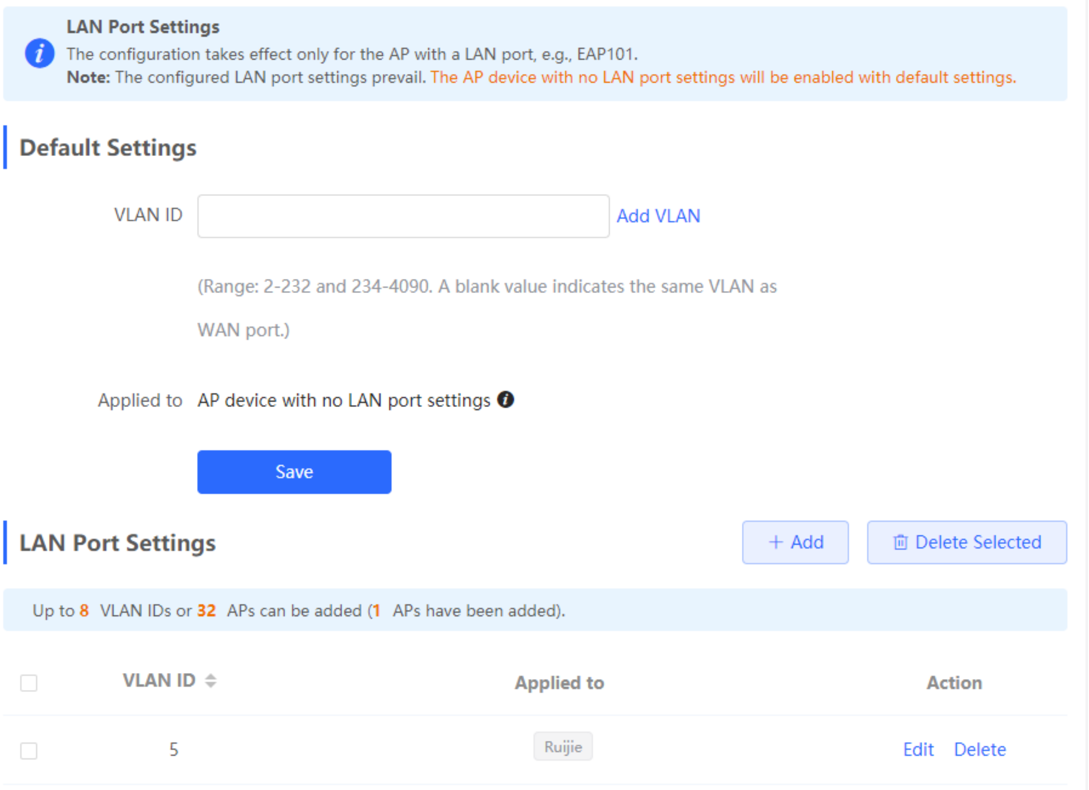
Caution

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

Choose **Wireless** > **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.



LAN Port Settings

The configuration takes effect only for the AP with a LAN port, e.g., EAP101.

Note: The configured LAN port settings prevail. The AP device with no LAN port settings will be enabled with default settings.

Default Settings

VLAN ID [ ] Add VLAN

(Range: 2-232 and 234-4090. A blank value indicates the same VLAN as WAN port.)

Applied to AP device with no LAN port settings

Save

LAN Port Settings + Add | Delete Selected

Up to 8 VLAN IDs or 32 APs can be added (1 APs have been added).

□	VLAN ID	Applied to	Action
□	5	Ruijie	Edit Delete

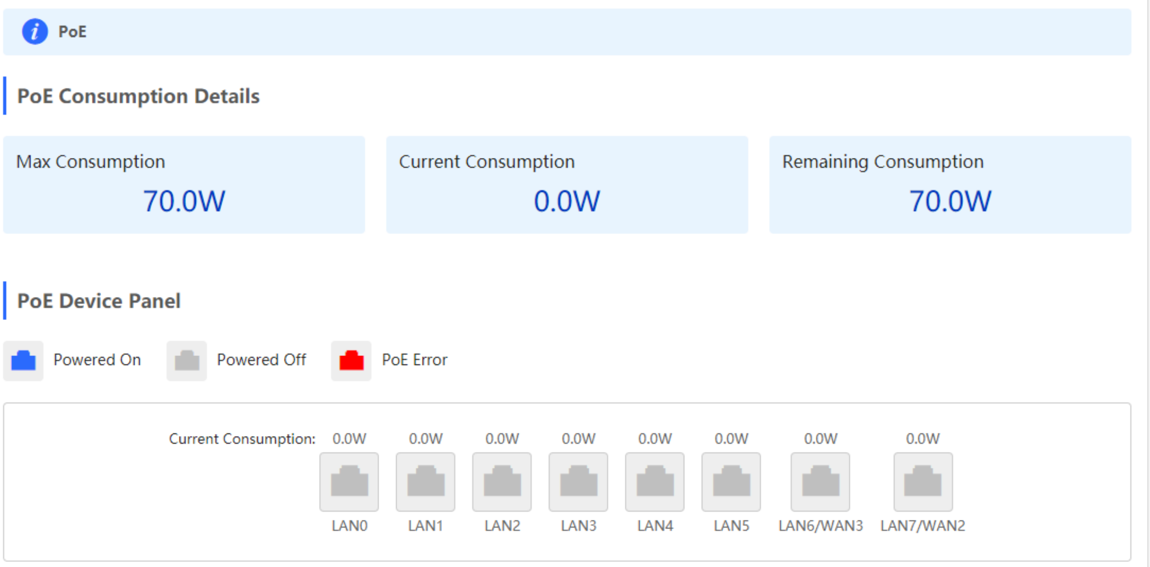
4 System Settings

4.1 PoE

Caution

Only RG-RAP1200(P) supports this function.

The device supplies power to PoE powered devices through ports. You can check the total power, current consumption, remaining consumption, and whether PoE power supply status is normal. Move the cursor over a port. The power switch icon ● appears. You can click it to control whether to enable PoE on the port.



PoE

PoE Consumption Details

Max Consumption 70.0W

Current Consumption 0.0W

Remaining Consumption 70.0W

PoE Device Panel

Powered On Powered Off PoE Error

Current Consumption:	0.0W	0.0W	0.0W	0.0W	0.0W	0.0W	0.0W	0.0W
	LAN0	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6/WAN3	LAN7/WAN2

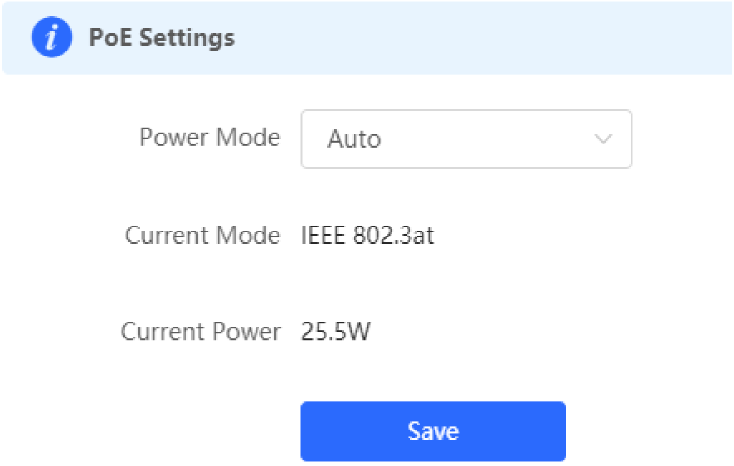
4.2 PoE Settings

Caution

Only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G) and RG-RAP6262(G) support this function.

Choose **Wireless** > **APs** > **Manage** > **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. By default, the device automatically negotiates with the power sourcing equipment (PSE) about the power mode. The default configuration is recommended.



PoE Settings

Power Mode: Auto

Current Mode: IEEE 802.3at

Current Power: 25.5W

4.3 Setting the Login Password

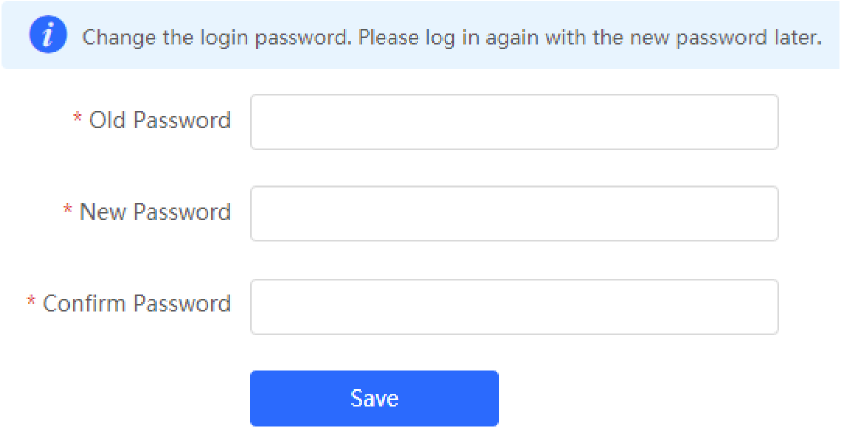
In standalone mode: Choose **System** > **Login** > **Login Password**.

In self-organizing network mode: Choose **Network** > **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.



Change the login password. Please log in again with the new password later.

* Old Password

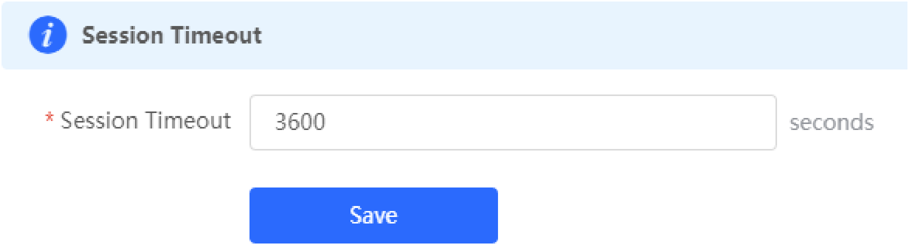
* New Password

* Confirm Password

4.4 Setting the Session Timeout Duration

Choose **Wireless** > **APs** > **Manage** > **System** > **Login** > **Session Timeout**.

If no operation is performed on the Web 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.



Session Timeout

* Session Timeout 3600 seconds

4.5 Setting and Displaying System Time

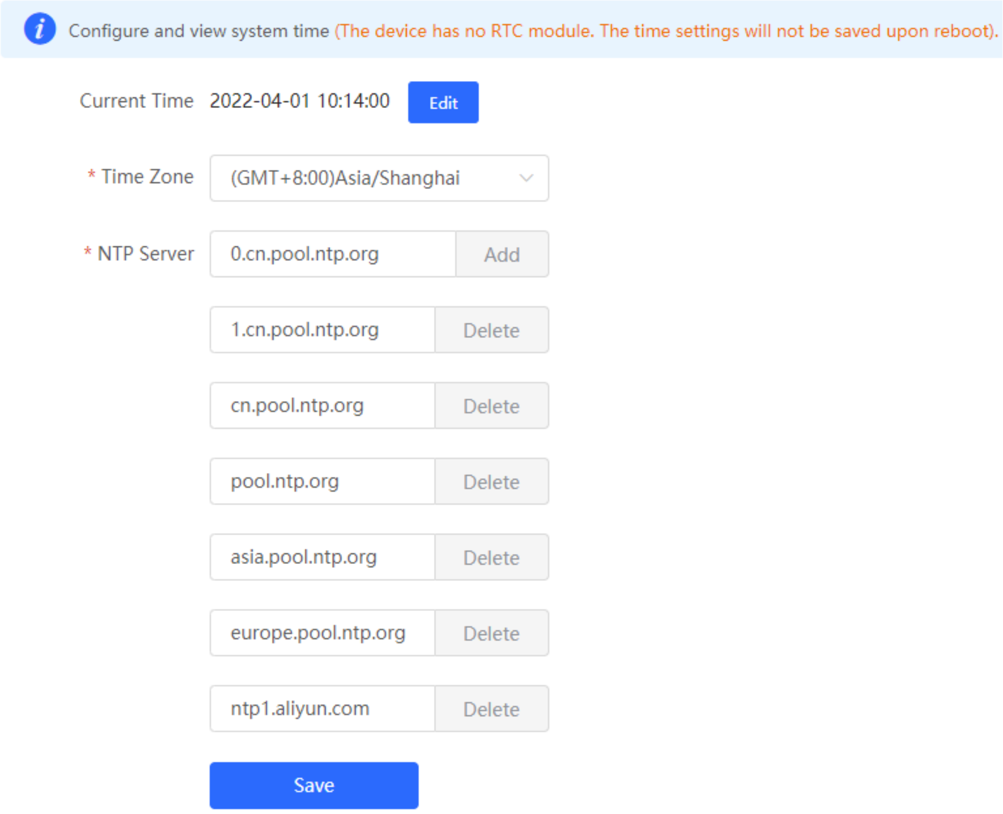
In standalone mode: Choose **System** > **System Time**.

In self-organizing network mode: Choose **Network** > **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 as required.

⚠ **Caution**

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



Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot).

Current Time 2022-04-01 10:14:00

* Time Zone (GMT+8:00)Asia/Shanghai

* NTP Server 0.cn.pool.ntp.org

1.cn.pool.ntp.org

cn.pool.ntp.org

pool.ntp.org

asia.pool.ntp.org

europe.pool.ntp.org

ntp1.aliyun.com

4.6 Configuring Reboot

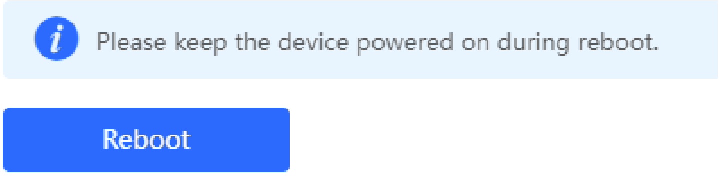
⚠ **Caution**

- 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.

4.6.1 Rebooting the Current Device

Choose **Wireless** > **APs** > **Manage** > **System** > **Reboot** > **Reboot**.

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



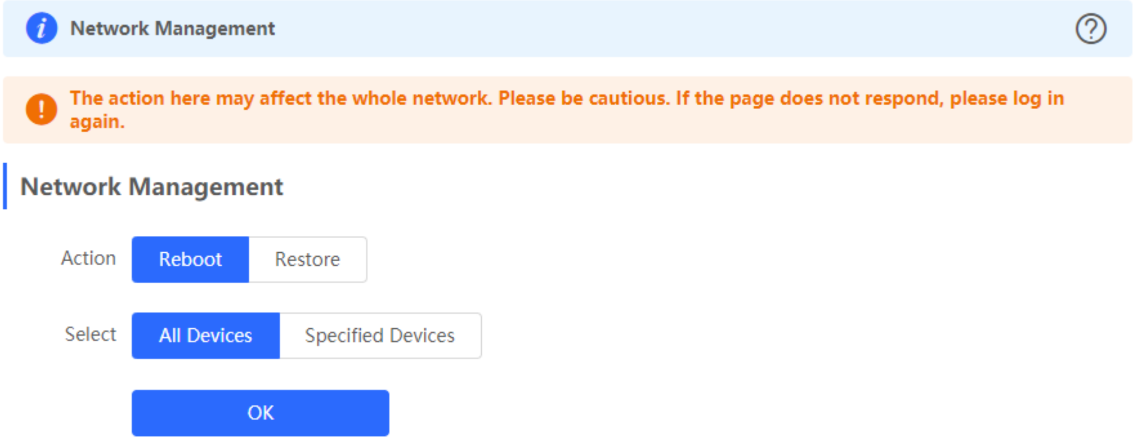
Please keep the device powered on during reboot.

4.6.2 Rebooting All Devices in the Network

In self-organizing network mode, you can reboot all devices in the network in batches.

Choose **Network** > **Reboot & Reset**.

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



Network Management

The action here may affect the whole network. Please be cautious. If the page does not respond, please log in again.

Network Management

Action: Reboot | Restore

Select: All Devices | Specified Devices

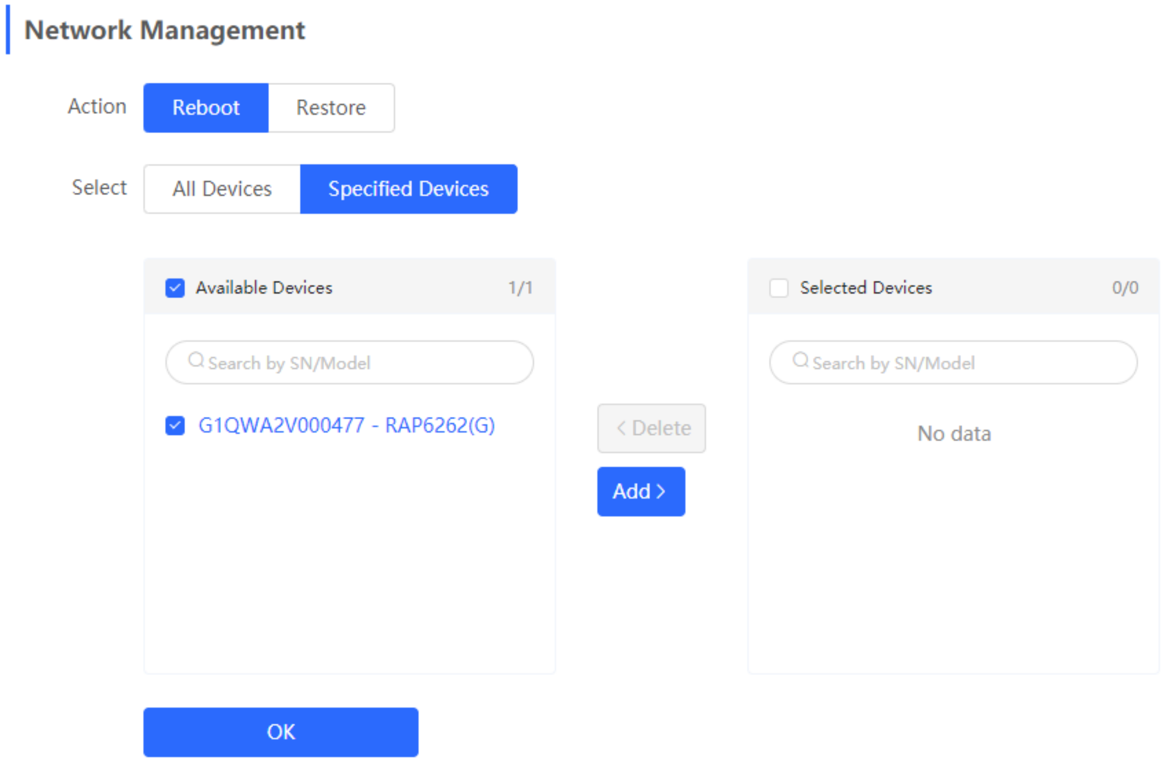
OK

4.6.3 Rebooting the Specified Device

In self-organizing network mode, you can reboot specified devices in the network in batches.

Choose **Network** > **Reboot & Reset**.

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 **OK**. Specified devices in the **Selected Devices** list will be rebooted.



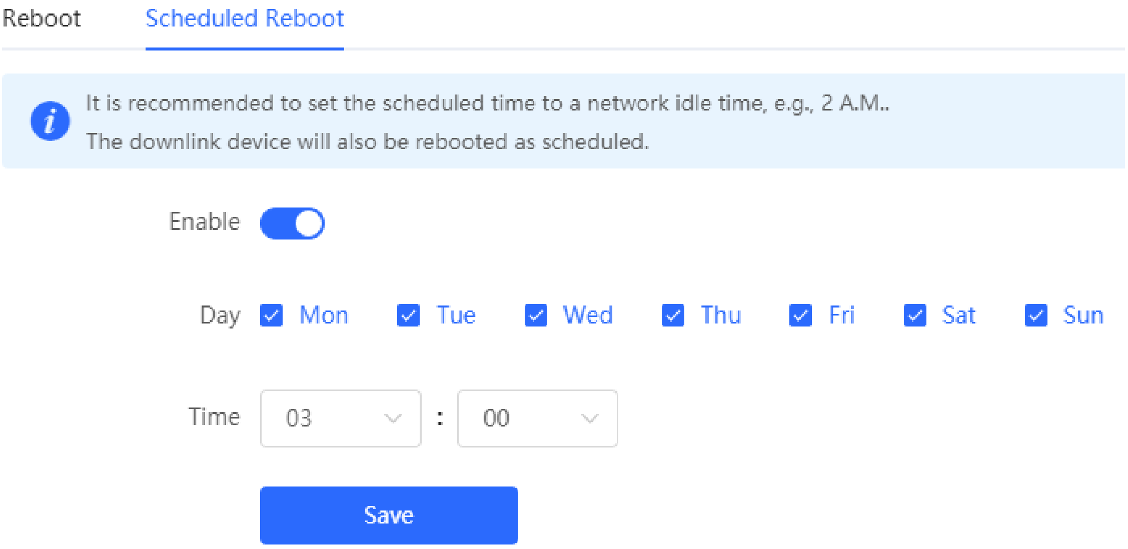
4.7 Configuring Scheduled Reboot

4.7.1 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 4.4.

Choose **Wireless** > **APs** > **Manage** > **System** > **Reboot** > **Scheduled Reboot**.

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



Reboot Scheduled Reboot

It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..
The downlink device will also be rebooted as scheduled.

Enable: On

Day: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Time: 03 : 00

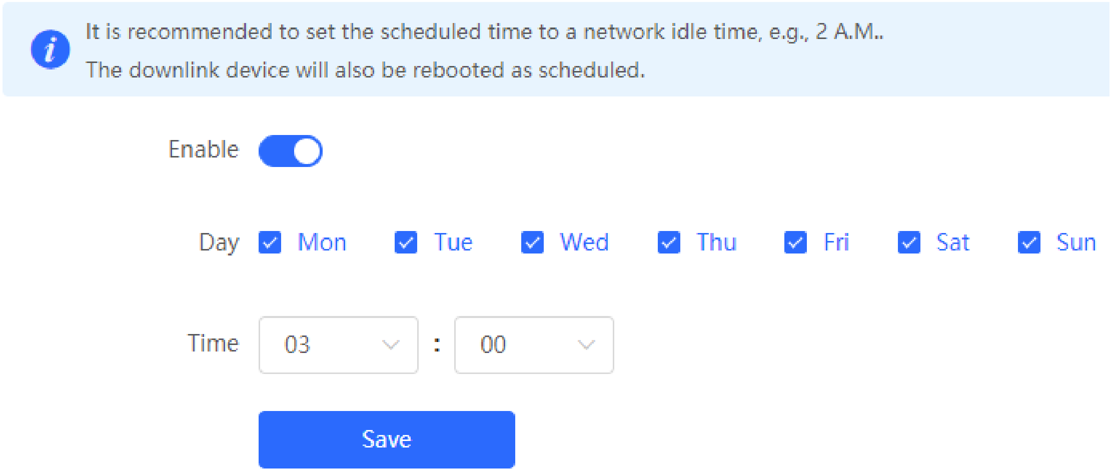
Save

4.7.2 Configuring Scheduled Reboot for All Devices in the Network

In self-organizing network mode, you can reboot all devices in the network in batches as scheduled. 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 4.4.

Choose **Network** > **Scheduled Reboot**.

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches the scheduled reboot time, all devices in the network will reboot.



It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..
The downlink device will also be rebooted as scheduled.

Enable: On

Day: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Time: 03 : 00

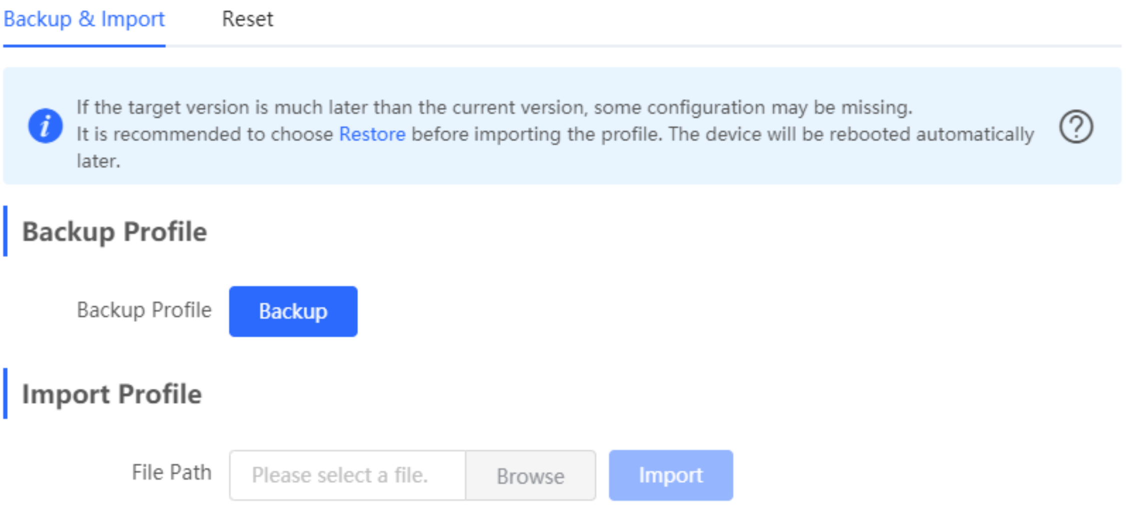
Save

4.8 Configuring Backup and Import

Choose **Wireless** > **APs** >**Manage** > **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.



If the target version is much later than the current version, some configuration may be missing. It is recommended to choose Restore before importing the profile. The device will be rebooted automatically later.

Backup Profile

Backup Profile

Import Profile

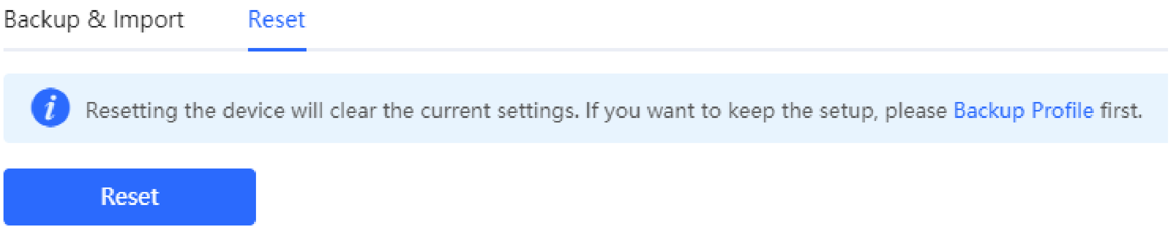
File Path: Please select a file.

4.9 Restoring Factory Settings

4.9.1 Restoring the Current Device to Factory Settings

Choose **Wireless** > **APs** > **Manage** > **System** > **Management** > **Reset**.

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



Resetting the device will clear the current settings. If you want to keep the setup, please Backup Profile first.

Caution

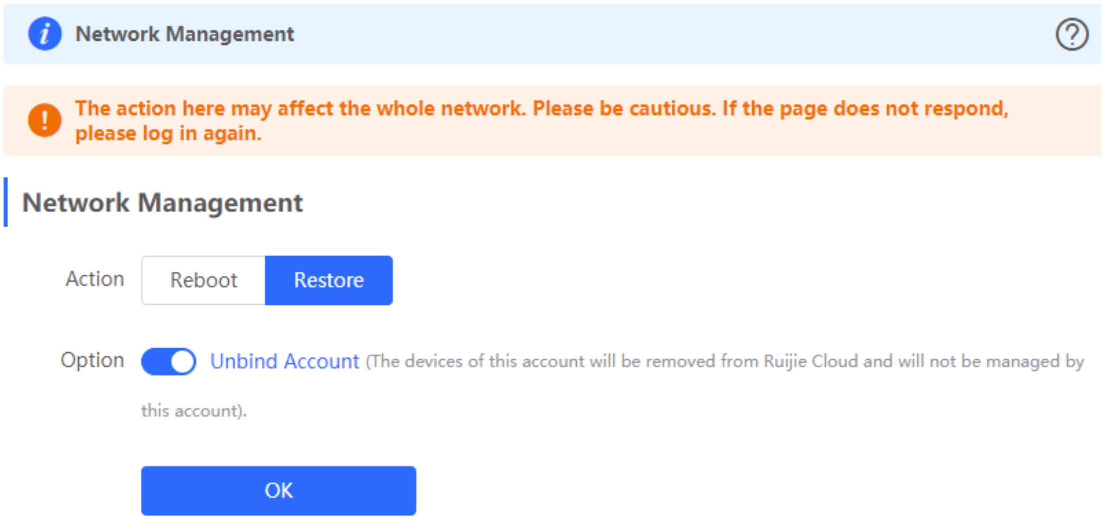
The operation will clear all configuration of the current device. If you want to retain the current configuration, back up the configuration first (See Configuring Backup and Import). Therefore, exercise caution when performing this operation.

4.9.2 Restoring All Devices to Factory Settings

In the self-organizing network mode, all devices in the network will be restored to factory settings.

Choose **Network** > **Reboot & Reset**

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



Network Management

The action here may affect the whole network. Please be cautious. If the page does not respond, please log in again.

Network Management

Action: Reboot | Restore

Option: Unbind Account (The devices of this account will be removed from Ruijie Cloud and will not be managed by this account).

OK

Caution

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

4.10 Performing Upgrade and Checking System Version

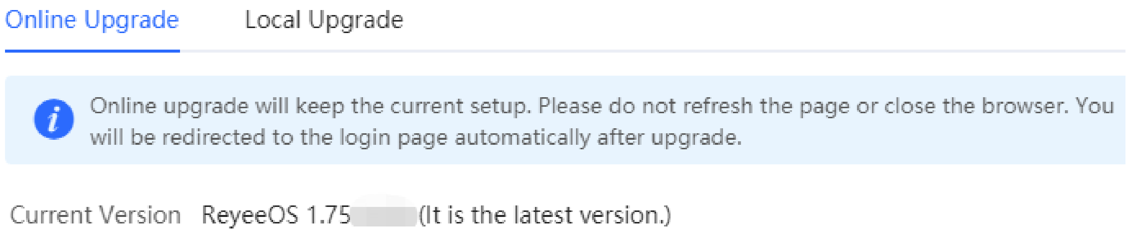
Caution

- 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.

4.10.1 Online Upgrade

Choose **Wireless** > **APs** > **Manage** > **System** > **Upgrade** > **Online Upgrade**.

You can view the current system version. If there is a new version available, you can click it for an update.



Online Upgrade | Local Upgrade

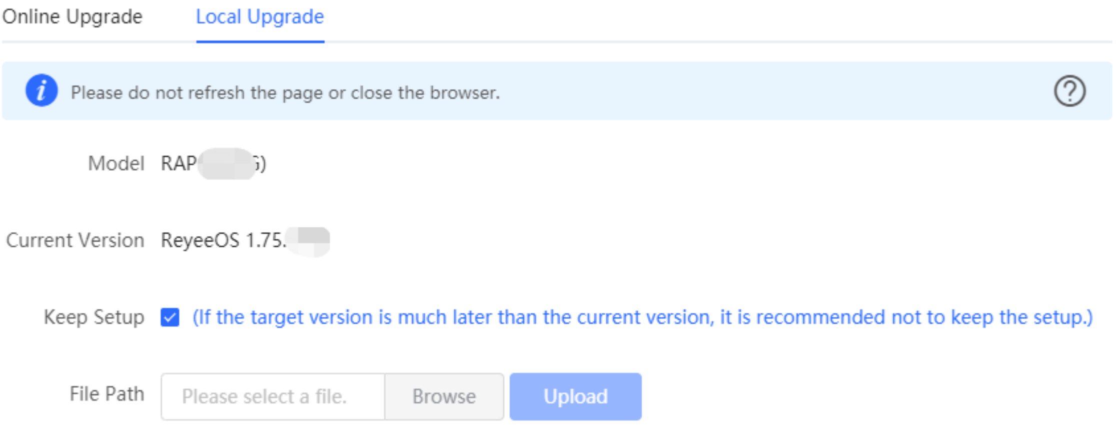
Online upgrade will keep the current setup. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrade.

Current Version ReyeeOS 1.75[redacted](It is the latest version.)

4.10.2 Local Upgrade

Choose **Wireless** > **APs** > **Manage** > **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 **Keep** Setup. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.



Please do not refresh the page or close the browser.

Model RAP[redacted]5)

Current Version ReyeeOS 1.75.[redacted]

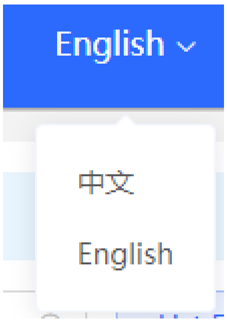
Keep Setup ☑ (If the target version is much later than the current version, it is recommended not to keep the setup.)

File Path Please select a file.

4.11 Switching System Language

Choose in the upper right corner of the Web page.

Click a required language to switch the system language.



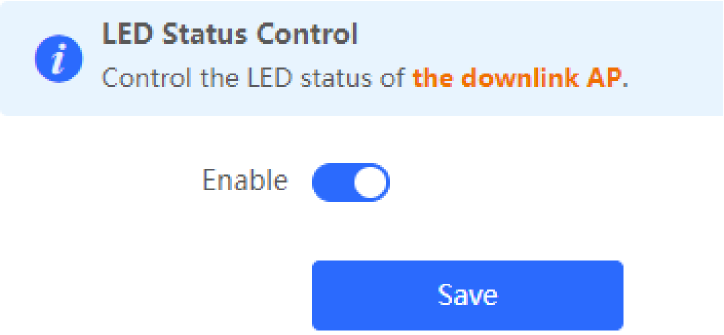
4.12 Configuring LED Status Control

⚠ **Caution**

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

Choose **Wireless** > **LED**.

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



LED Status Control

Control the LED status of **the downlink AP**.

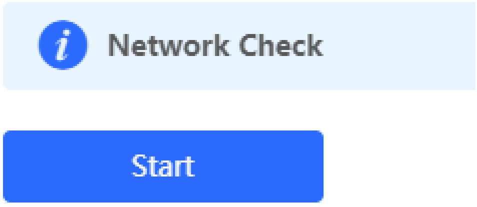
5 Network Diagnosis Tools

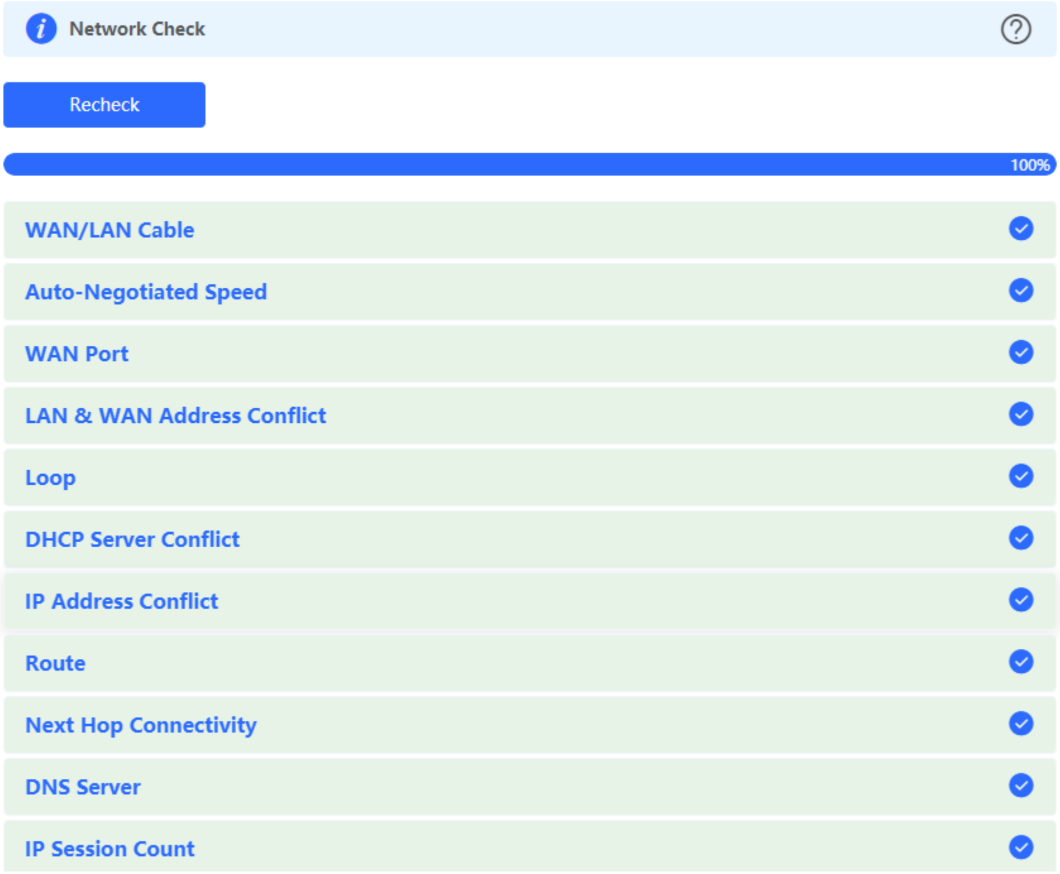
5.1 Network Check

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

Choose **Wireless** > **APs** > **Manage** > **Diagnostics** > **Network Check**.

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





WAN/LAN Cable ✓

Auto-Negotiated Speed ✓

WAN Port ✓

LAN & WAN Address Conflict ✓

Loop ✓

DHCP Server Conflict ✓

IP Address Conflict ✓

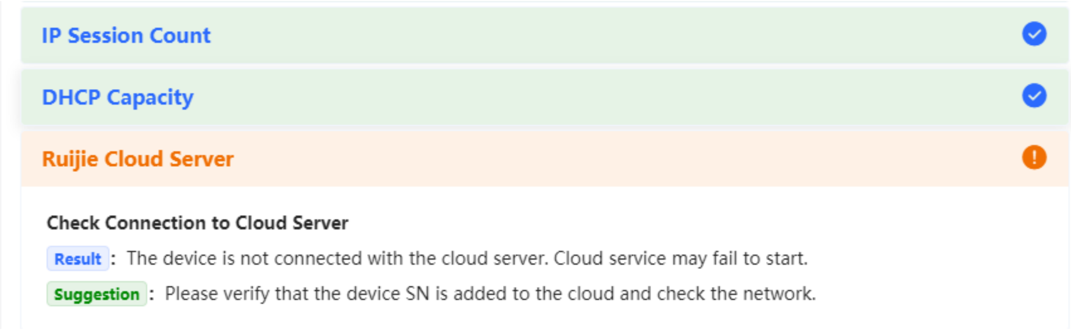
Route ✓

Next Hop Connectivity ✓

DNS Server ✓

IP Session Count ✓

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



IP Session Count ✓

DHCP Capacity ✓

Ruijie Cloud Server !

Check Connection to Cloud Server

Result : The device is not connected with the cloud server. Cloud service may fail to start.

Suggestion : Please verify that the device SN is added to the cloud and check the network.

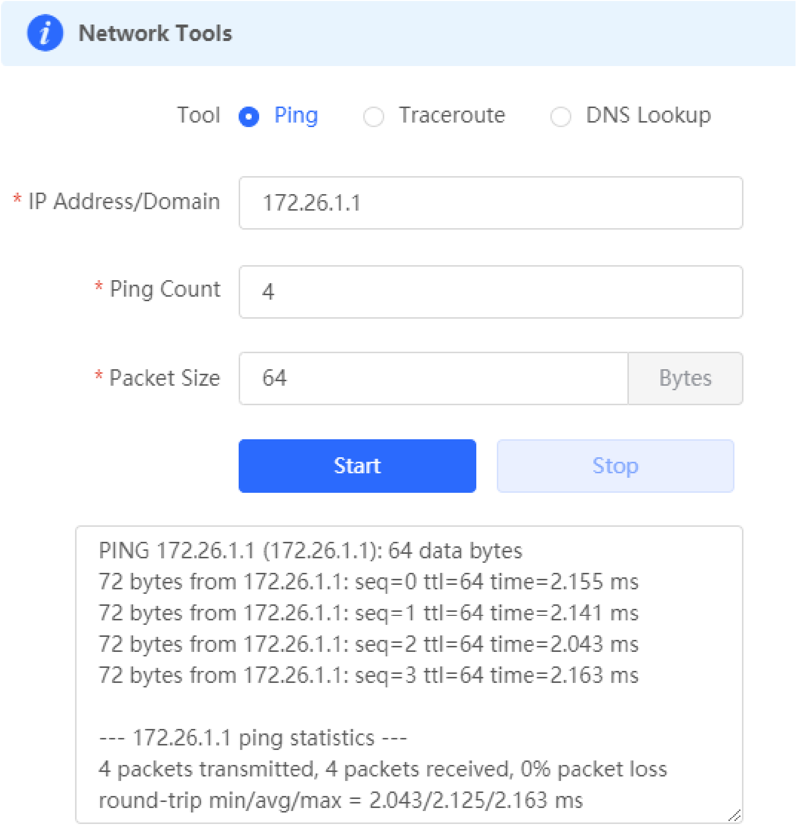
5.2 Network Tools

Choose **Wireless** > **APs** > **Manage** > **Diagnostics** > **Network Tools**.

When you select the ping tool, you can enter the IP address or URL and click **Start** to test 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.



Network Tools

Tool ● Ping ○ Traceroute ○ DNS Lookup

* IP Address/Domain: 172.26.1.1

* Ping Count: 4

* Packet Size: 64 Bytes

```
PING 172.26.1.1 (172.26.1.1): 64 data bytes
72 bytes from 172.26.1.1: seq=0 ttl=64 time=2.155 ms
72 bytes from 172.26.1.1: seq=1 ttl=64 time=2.141 ms
72 bytes from 172.26.1.1: seq=2 ttl=64 time=2.043 ms
72 bytes from 172.26.1.1: seq=3 ttl=64 time=2.163 ms

--- 172.26.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.043/2.125/2.163 ms
```

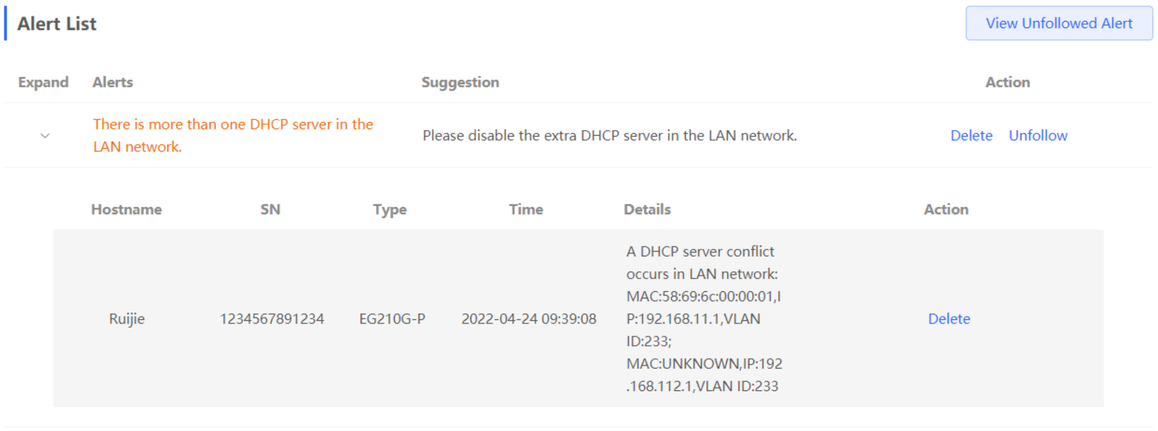
5.3 Alarms

Choose **Wireless** > **APs** > **Manage** > **Diagnostics** > **Alarms**.

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

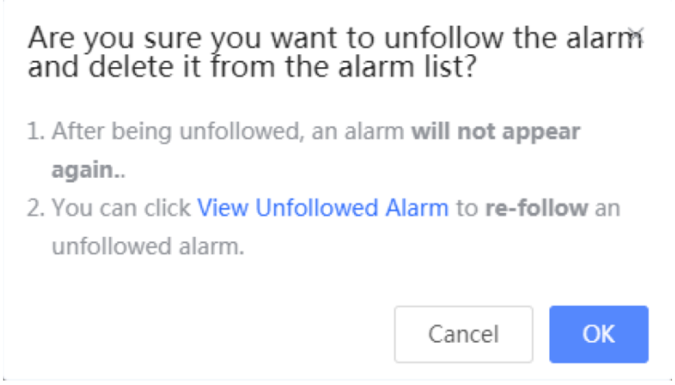
After unfollowing a type of alarm, you will not discover and process all alarms of this type promptly. Therefore, exercise caution when performing this operation.



Alert List

Expand	Alerts	Suggestion	Action
⌄	There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.	Delete Unfollow

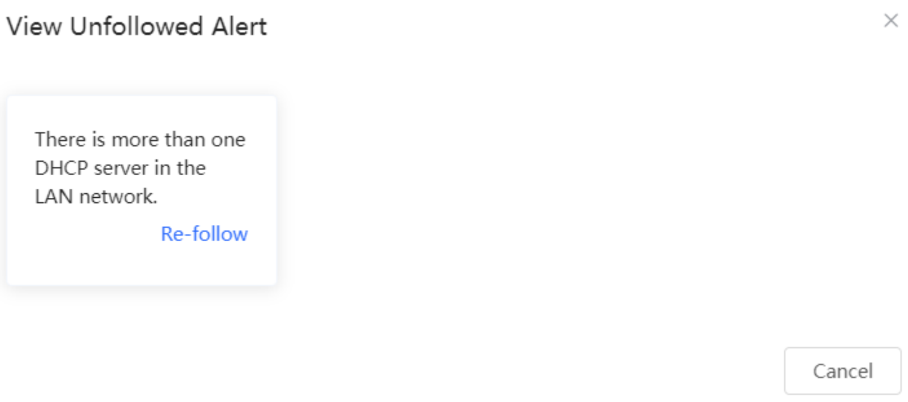
Hostname	SN	Type	Time	Details	Action
Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,IP:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192.168.112.1,VLAN ID:233	Delete



Are you sure you want to unfollow the alarm and delete it from the alarm list?

1. After being unfollowed, an alarm **will not appear again.**.
2. You can click View Unfollowed Alarm to **re-follow** an unfollowed alarm.

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



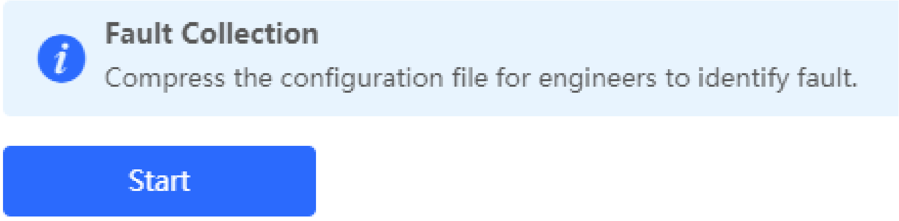
View Unfollowed Alert

There is more than one DHCP server in the LAN network.

5.4 Fault Collection

Choose **Wireless** > **APs** > **Manage** > **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.



Fault Collection

Compress the configuration file for engineers to identify fault.