Ruijie Reyee
RG-APF1250 Access Point

Implementation Cookbook

Document Version: V1.0
Date: 2024-07-05
Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.


and other Ruijie networks logos are trademarks of Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- The official website of Ruijie Reyee: https://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

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

This document also uses signs to indicate some important points during the operation. The meanings of these signs are 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.

Note

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

Instruction

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. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

- The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

RG-APF1250 Access Point Implementation Cookbook

This cookbook consists of multiple independent volumes, introducing the installation, deployment, and web-based configuration of the RG-APF1250 access point, including:

01- Installation Guide

02- ReyeeOS 2.290 Configuration Guide

Ruijie Reyee RG-APF1250 Access Point

Installation Guide

Document version: V1.0
Date: 2024-07-01
Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.

, and other Ruijie networks logos are trademarks of Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

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://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

Conventions

The signs used in this document are described as follows:

1. Signs

Danger

An alert that contains important safety instructions. Before you work on any equipment, be aware of the hazards involved and be familiar with standard practices in case of accidents.

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.

2. Notes

This manual presents installation instructions, troubleshooting techniques, technical specifications, cable and connector requirements, and usage guidelines. It is intended for users who want to gain insight into the above content and have some experience in installing and maintaining network hardware. It is assumed that users are already familiar with relevant terms and concepts.

Contents

Preface I

1 Overview 1

1.1 About the RG-APF1250 1

1.2 Terms 1

1.3 Package Contents 2

1.4 Product Appearance 3

1.4.2 Front Panel 3

1.4.3 Rear Panel 5

1.5 Technical Specifications 6

1.6 Technical Specifications of Power Supply 8

1.7 Cooling 8

2 Preparing for Installation 9

2.1 Safety Guidelines 9

2.2 Site Requirements 9

2.2.1 Temperature and Humidity 9

2.2.2 Cleanliness 9

2.2.3 ESD Damage Prevention 10

2.2.4 Anti-Interference 10

2.2.5 Installation Site 10

2.3 Tools 11

3 Installing the AP 12

3.1 Before You Begin 12

3.2 Safety Precautions During Installation 12

3.3 Installing the AP 12
3.4 Bundling Cables 14
3.5 Verifying Installation 15
4 Commissioning 16
4.1 Setting Up the Configuration Environment 16
4.2 Powering on the AP 16
4.2.1 Checklist Before Power-on 16
4.2.2 Checklist After Power-on 16
4.3 Rectifying Power Supply Failures 16
5 Monitoring and Maintenance 17
5.1 Monitoring 17
5.2 Maintenance 17
6 Troubleshooting 18
6.1 General Troubleshooting Flowchart 18
6.2 Common Faults 18
6.2.1 System Status LED Is Off After the AP Is Powered On 18
6.2.2 After an Ethernet Cable is Connected, the Ethernet Port Cannot Be Used 18
6.2.3 A Client Cannot Discover the AP 18
7 Appendix 19
7.1 Connectors and Media 19

1 Overview

1.1 About the RG-APF1250

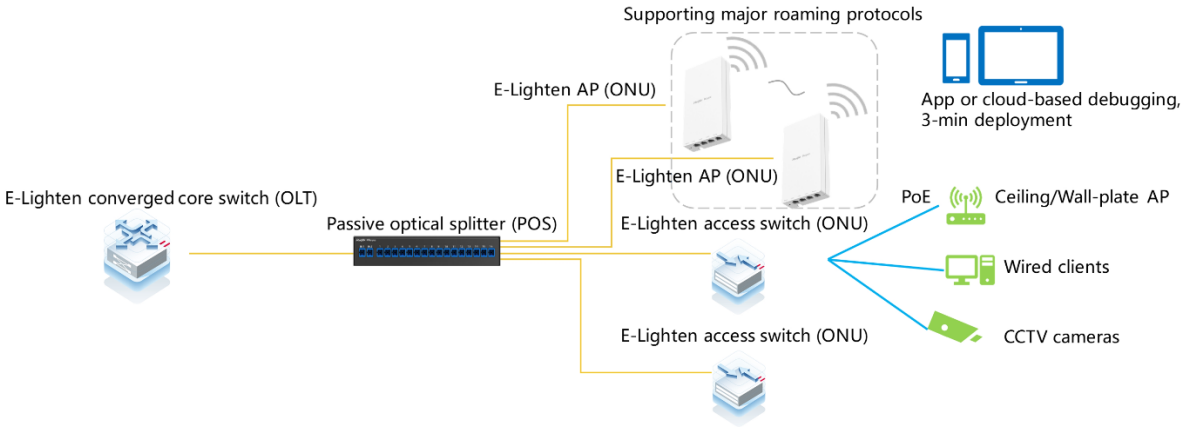
Passive Optical Local Area Network (POL) is a new networking mode that utilizes point-to-multipoint (P2MP) technology. Compared with the traditional Ethernet solution that relies on the point-to-point (P2P) technology, this mode features fewer nodes to be maintained, a simplified Layer 2 network architecture, and seamless upgrades.

Ruijie Reyee has developed a new series of products for Ethernet optical splitting to form the Reyee e-Lighten Solution. This solution supports both POL (P2MP) and traditional Ethernet (P2P) networking modes. In this way, contractors can complete the networking and commissioning of POLs without training.

The Reyee e-Lighten Solution includes e-Lighten converged switches (OLTs), e-Lighten APs (ONUs), e-Lighten access switches (ONUs), optical transceivers, and passive optical splitters. The RG-APF1250 is a multi-service wall-mounted e-Lighten AP (ONU) launched by Ruijie Reyee for the POL. With an attractive design, the RG-APF1250 can be directly installed on a wall using a mounting bracket to smoothly blend into the environment. In compliance with the IEEE 802.11a/b/g/n/ac Wave 1 and IEEE 802.11ac Wave 2 standards, the RG-APF1250 can work on both 2.4 GHz and 5 GHz frequency bands. The RG-APF1250 provides a combined data rate of 1167 Mbps, eliminating the performance bottleneck.

In hotel scenarios, based on multi-service integration of the RG-APF1250, one fiber-to-the-home (FTTH) cable can meet the access requirements of five services in hotel rooms, including wireless network, wired network, guest control, IPTV, and VoIP services. This reduces traditional Ethernet cables and saves significant labor costs, thereby providing contractors with a cost-effective POL solution for hotels.

1.2 Terms



- Passive optical network (PON): A PON uses optical fibers to transmit data. On a PON, no external power supply or electronic amplifier is required. Instead, a PON uses passive optical splitters to transmit optical signals from an OLT to multiple ONUs.
- Optical line terminal (OLT): An OLT is a device on the equipment room side of a PON and is responsible for sending and receiving optical signals.

- Optical network unit (ONU): An ONU is a device on the access side of a PON. It connects to clients and communicates with the OLT. It is responsible for converting optical signals and transmitting data.
- PON port: A PON port is a downlink port of an OLT for connecting to an ONU.

1.3 Package Contents

Table 1-1 Package Contents

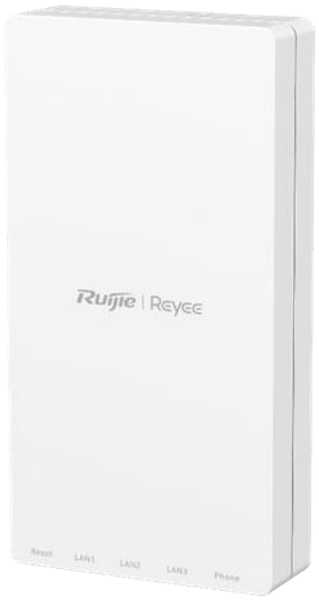
No.	Item	Quantity
1	RG-APF1250 access point	1
2	Mounting bracket (pre-installed on the AP)	1
3	M4 x 20 mm Phillips pan head screws	2
4	Nuts	2
5	DC power adapter	1
6	User Manual	1
7	Warranty card	1

Note

The package contents are subject to the purchase contract, and actual delivery may vary. Please check the items carefully against the package contents or purchase contract. If you have any questions, please contact your distributor.

1.4 Product Appearance

Figure 1-1 Appearance



1.4.2 Front Panel

Figure 1-2 Front Panel



Table 1-2 Components on the Front Panel

No.	Component	Description
1	Reset button	Press the button for shorter than 2s: Restart the AP. Press the button for longer than 2s and shorter than 5s: No operation. Press the button for longer than 5s: Restore to factory settings.
2	3 x LAN ports (RJ45)	10/100/1000Base-T Ethernet ports for connecting wired terminals
3	VoIP port (RJ11)	VoIP port for connecting a VoIP cable

Figure 1-3 LEDs



Table 1-3 LEDs

No.	LED	Description
1	System status LED	Off: The AP is not powered on.
		Solid blue: The AP is working properly without alarms.
		Fast blinking blue (8 Hz). The possible causes are as follows: ● The AP start fails. ● The AP restart fails.
		Blinking blue twice. The possible causes are as follows: ● Factory settings are restored. ● Version upgrade is performed. **Note** In this LED state, do not power off the AP.
		Solid blue (one long blink and three short blinks): The main program is lost.
		Blinking blue (long on and short off): The AP is not added on the cloud.
		Fast blinking blue for 3s (8 Hz) and off for 3s: The AP is being searched for on Ruijie Reyee App.
2	Optical port LED	Off: The AP is not powered on.

No.	LED	Description
		Blinking yellow: The ONU is registering.
		Blinking red: The ONU registration fails.
		Blinking green: The optical port is connected and data is being transmitted.
		Solid green: The optical port is connected but no data is being transmitted.

1.4.3 Rear Panel

Figure 1-4 Rear Panel



Table 1-4 Ports on the Rear Panel

No.	Port	Description
1	SC port	1000Base-X SC optical port for connecting an optical cable
2	DC power connector	Power connector for DC power supply of 12 V/1.5 A
3	Label	The label is located on the back of the device

1.5 Technical Specifications

Table 1-5 Technical Specifications

Radio Design	2.4 GHz and 5 GHz: dual-radio dual-stream
Wi-Fi Standards	IEEE 802.11ac Wave 2 and Wave 1 and IEEE 802.11a/b/g/n
Operating Frequency Bands	IEEE 802.11b/g/n: 2.4 GHz to 2.4835 GHz IEEE 802.11a/n/ac: 5 GHz: 5.150 GHz to 5.350 GHz, 5.470 GHz to 5.725 GHz, 5.725 GHz to 5.850 GHz **Note** The operating bands vary in different countries.
Antenna Type	Built-in omnidirectional onboard antenna (basic gain: 2.0 dBi)
Spatial Streams	2.4 GHz: 2x2 MIMO 5 GHz: 2x2 MIMO
Max. Wi-Fi Speed	2.4 GHz: 300 Mbps 5 GHz: 866.7 Mbps Combined: 1166.7 Mbps
Modulation	DBPSK/DQPSK/CCK(DSSS)/BPSK/QPSK/16QAM/64QAM/256QAM
Receiver Sensitivity	IEEE 11b: –91 dBm (1 Mbps), –88 dBm (5 Mbps), –85 dBm (11 Mbps) IEEE 11a/g: –89 dBm (6 Mbps), –80 dBm (24 Mbps), –76 dBm (36 Mbps), –71 dBm (54 Mbps) IEEE 11n: –83 dBm (MCS0), –65 dBm (MCS7), –83 dBm (MCS8), –65 dBm (MCS15) IEEE 11ac HT20: –83 dBm (MCS0), –57 dBm (MCS9) IEEE 11ac HT40: –79 dBm (MCS0), –57 dBm (MCS9) IEEE 11ac HT80: –76 dBm (MCS0), –51 dBm (MCS9)
Transmit Power	Frequency bands using and the max EIRP. **Note** Country specific restrictions apply. ● European Union & United Kingdom: ○ 2400 to 2483.5 MHz, EIRP ≤ 20 dBm ○ 5150 to 5350 MHz, EIRP ≤ 23 dBm ○ 5470 to 5725 MHZ, EIRP ≤ 30 dBm ● United States: ○ 2400 to 2483.5 MHz, max output power ≤ 30 dBm & EIRP ≤ 36 dBm

	○ 5150 to 5250 MHz, max output power ≤ 30 dBm & EIRP ≤ 36 dBm ○ 5250 to 5350 MHz, max output power ≤ 24 dBm & EIRP ≤ 30 dBm ○ 5470 to 5725 MHz, max output power ≤ 24 dBm & EIRP ≤ 30 dBm ○ 5725 to 5825 MHz, max output power ≤ 30 dBm & EIRP ≤ 36 dBm ● Myanmar: ○ 2400 to 2483.5 MHz, EIRP ≤ 23 dBm ○ 5725 to 5825 MHz, EIRP ≤ 30 dBm ● Thailand: ○ 2400 to 2483.5 MHz, EIRP ≤ 20 dBm ○ 5150 to 5350 MHz, EIRP ≤ 23 dBm ○ 5470 to 5725 MHz, EIRP ≤ 30 dBm ○ 5725 to 5825 MHz, EIRP ≤ 30 dBm ● Indonesia: ○ 2400 to 2483.5 MHz, EIRP ≤ 27 dBm ○ 5150 to 5350 MHz, EIRP ≤ 23 dBm ○ 5725 to 5825 MHz, EIRP ≤ 23 dBm ● Egypt: ○ 2400 to 2483.5 MHz, EIRP ≤ 20 dBm ○ 5150 to 5350 MHz, EIRP ≤ 23 dBm
Power Step	1 dBm
ONU Power Range	The power range of the SC optical port of the ONU is from –8 dBm to –28 dBm. If the power is beyond this range, the AP may be abnormal or damaged. **Caution** The SC optical port of the ONU should not be directly connected to the PON port of the OLT. According to the power indicator, when short-distance single-mode fibers are used, a linear optical attenuator or optical splitter should be added on the link to avoid damage to the AP.
Dimensions (W x D x H)	165 mm x 86 mm x 29 mm (6.50 in. x 3.39 in. x 1.14 in.) The height is the edge height of the AP, excluding the mounting bracket and SMA connectors.
Weight	AP: 0.236 kg (0.520 lbs.)
Service Ports	Bottom: 3 x 10/100/1000Base-T Ethernet downlink ports 1 x VoIP port for connecting a VoIP cable Rear: 1 x 1000Base-X SC optical port for connecting an optical cable 1 x DC power connector for connecting the power supply

Management Port	N/A
Status LED	1 x system status LED, 1 x optical port LED
Power Supply Options	12 V/1.5 A DC power adapter (normal operation)
Max. Power Consumption	≤ 12.95 W
Bluetooth 5.0	Not supported.
Environment	Operating temperature: 0°C to 40°C (32°F to 104°F)
	Storage temperature: –40°C to +70°C (–40°F to +158°F)
	Operating humidity: 5% RH to 95% RH (non-condensing)
	Storage humidity: 5% RH to 95% RH (non-condensing)
Installation Method	Wall mounting using screws
Certification	CE
MTBF	> 400,000 hours

1.6 Technical Specifications of Power Supply

The RG-APF1250 supports DC power supply of 12 V/1.5 A using a DC power adapter. The following table lists the adapter specifications.

Inner Diameter	Outer Diameter	Depth	Conductor Resistance	Insulation Resistance	Voltage Resistance (Insulation and Conductor)	Polarity
2.00+/– 0.05 mm	6.30+/– 0.20 mm	9 mm	30 mΩ	100 MΩ	500 V	Center positive (reverse not supported)

1.7 Cooling

The RG-APF1250 adopts a fanless design and can be installed on a wall.

2 Preparing for Installation

2.1 Safety Guidelines

The wall-mounted RG-APF1250 functions as an important intermediate node for network connection and determines whether the connected subnet can operate properly.

The following safety guidelines must be followed during installation and use:

- Do not place the AP in a wet position and keep the AP away from liquid.
- Keep the AP away from heat sources.
- Wear an anti-ESD wrist strap during installation and maintenance.
- Do not wear loose clothing. Tighten your belt, scarf, and sleeves to prevent clothing from snagging on components and causing damage.
- Keep tools and components away from walking areas.
- You are advised to use an uninterrupted power supply (UPS) to avoid interference caused by power failures.

2.2 Site Requirements

The wall-mounted RG-APF1250 must be installed indoors for normal operation and prolonged service life. The installation site must meet the following requirements.

2.2.1 Temperature and Humidity

To ensure normal operation and prolonged service life of the AP, maintain appropriate temperature and humidity conditions at the installation site. In an environment with a high relative humidity, insulating materials are prone to poor insulation or even electricity leakage. In an environment with a low relative humidity, insulating gaskets may shrink, resulting in screw loosening. In a dry environment, static electricity is more likely to occur, posing a risk to the internal circuits of the AP. A high temperature can accelerate the aging process of insulation materials, greatly reducing the availability of the AP and severely affecting its service life. The following table lists the temperature and humidity requirements.

Operating Temperature	Operating Humidity
0°C to 40°C (32°F to 104°F)	5% RH to 95% RH (non-condensing)

2.2.2 Cleanliness

Dust poses a major threat to the AP. The indoor dust can cause electrostatic adhesion when falling on the AP, causing poor contact. Such electrostatic adhesion occurs more easily when the indoor relative humidity is low, not only affecting the service life of the AP, but also causing communication failure easily.

The following table lists the requirements for dust concentration and particle size indoors.

Max. Diameter (μm)	0.5	1	3	5
Max. Concentration (Number of Particles/m^3)	1.4 x 10^7	7 x 10^5	2.4 x 10^5	1.3 x 10^5

Apart from dust, harmful gases such as the salt, acid, and sulfide in the air at the installation site must meet strict requirements. These gases accelerate metal corrosion and component aging. The following table lists the limits for harmful gases including SO_2, H_2S, NO_2, NH_3, and Cl_2 at the installation site.

Gas	**Average (mg/m^3)**	**Maximum (mg/m^3)**
Sulfur dioxide (SO_2)	0.2	1.5
Hydrogen sulfide (H_2S)	0.006	0.03
Nitrogen dioxide (NO_2)	0.04	0.15
Ammonia gas (NH_3)	0.05	0.15
Chlorine gas (Cl_2)	0.01	0.3

2.2.3 ESD Damage Prevention

The wall-mounted RG-APF1250 applies ESD damage prevention in the circuit design. However, excessive static electricity may still damage the PCB. ESD on the communication network connected to the AP mainly originates from two sources:

- Outdoor high-voltage power lines, lightning, and other external electric fields
- Internal systems such as indoor flooring materials and the structure of the AP

To prevent damage caused by static electricity, pay attention to the following:

- Keep the site as dust-free as possible.
- Maintain appropriate temperature and humidity conditions.

2.2.4 Anti-Interference

Electromagnetic and current interferences should be prevented. The following anti-interference requirements must be met:

- Take interference prevention measures for the power supply system.
- Keep the AP far away from the grounding system or lightning protection grounding system of the power facility.
- Keep the AP far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers.

2.2.5 Installation Site

When the AP is installed on the wall, the following conditions must be met:

- The wall surface must be smooth and clean.

- Ethernet cable connectivity is normal.

2.3 Tools

Common Tools	Phillips screwdriver, cables, fastening bolts, diagonal pliers, and cable ties
Special Tools	Wire stripper, crimper, RJ45 connector crimping plier, wire cutter, and anti-ESD gloves
Meters	Multimeter and bit error rate tester (BERT)

Note

The RG-APF1250 is delivered without a toolkit. Prepare the preceding tools by yourself.

3 Installing the AP

Caution

Before installing the AP, ensure that the guidelines and requirements in Chapter 2 have been met.

3.1 Before You Begin

Before installing the RG-APF1250, carefully plan and arrange the installation location, networking mode, power supply, and cabling. Confirm the following requirements before installation:

- The installation site meets the temperature and humidity requirements of the AP.
- The power supply and required current are available at the installation site.
- The selected power supply modules meet the system power requirements.
- The installation site meets the cabling requirements of the AP.
- The installation site meets the site requirements of the AP.
- The customized AP meets the client-specific requirements.

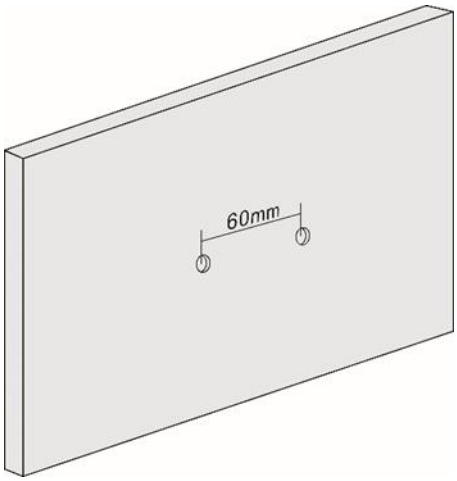
3.2 Safety Precautions During Installation

To ensure the normal operation and prolonged service life of the AP, observe the following safety precautions:

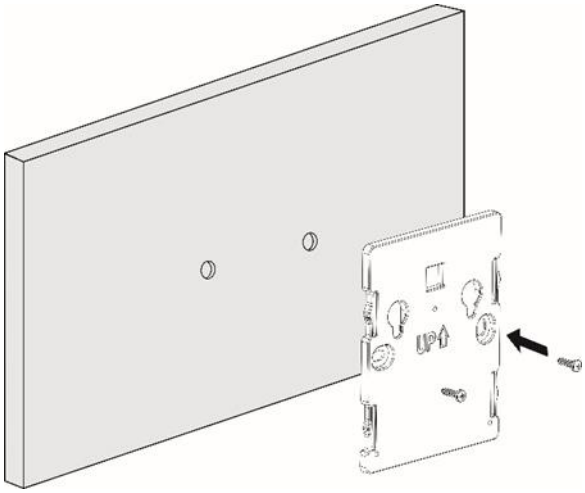
- Do not power on the AP during installation.
- Place the AP in a well-ventilated environment.
- Do not expose the AP to high temperatures.
- Keep the AP away from high-voltage power cables.
- Install the AP indoors.
- Do not expose the AP to a thunderstorm or strong electric field.
- Keep the AP clean and dust-free.
- Cut off the power supply before cleaning the AP.
- Do not wipe the AP with a damp cloth.
- Do not wash the AP with liquid.
- Do not open the enclosure when the AP is working.
- Secure the AP properly.

3.3 Installing the AP

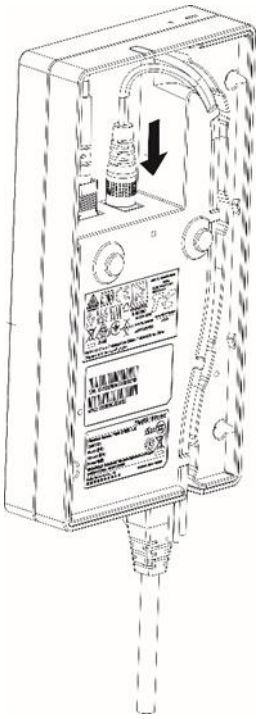
(1) Drill two screw holes on the wall and leave 60 mm (2.36 in.) between the two holes.



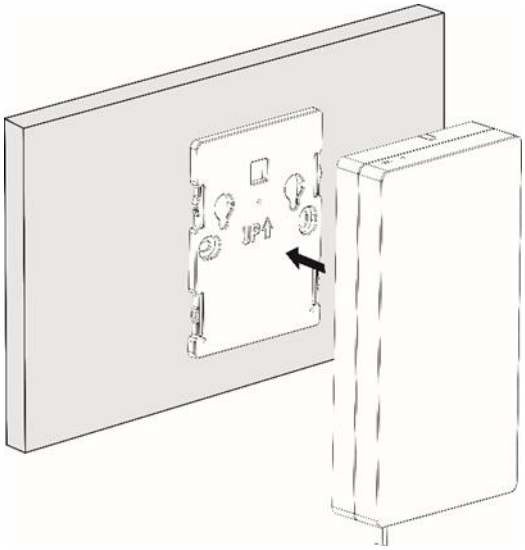
(2) Adjust the position of the mounting bracket on the wall, and then fix it to the wall using M4 x 20 mm Phillips pan head screws.



(3) Connect the optical cable to the 1000M SC optical port on the rear panel of the AP, and connect the DC power cord to the DC power connector on the rear panel of the AP.



(4) Align the hangers at the rear panel of the AP with the mounting holes on the mounting bracket, and push the hangers downward along the guide rails to secure the AP.



3.4 Bundling Cables

Precautions

- Bundle the cable in a visually pleasing way.
- Make sure that the twisted pairs at the connectors have natural bends or bends of large radius.
- Do not bundle the twisted pairs too tightly, as this may reduce the cable service life and transmission performance.

Bundling Procedure

(1) Bundle the drooping part of the twisted pairs and place the bundle as near the WAN/PoE ports as possible.

(2) Fasten the twisted pairs to the cable trough of the mounting bracket.

(3) Route the twisted pairs under the AP and run them in a straight line.

3.5 Verifying Installation

- Verify that the AP is securely fastened.
- Verify that the twisted pair type matches the port type.
- Verify that the cables are properly bundled.

4 Commissioning

4.1 Setting Up the Configuration Environment

Power the AP using an adapter. After setting up the environment, ensure that the adapter is in good contact and meets safety requirements.

4.2 Powering on the AP

4.2.1 Checklist Before Power-on

- The power supply capability of the adapter is normal.
- The optical cable, Ethernet cable, and VoIP cable are properly connected.

4.2.2 Checklist After Power-on

- Verify the LED status.
- After the AP is powered on, check whether the SSID can be searched by a mobile phone or other wireless clients.

4.3 Rectifying Power Supply Failures

For the wall-mounted RG-APF1250, you can determine whether the power system is faulty based on the status of the LEDs on the front panel. For details about LED status, see Table 1-3. If an exception occurs, check the following items:

- Check whether the AP is properly powered.
- Check whether the Ethernet cable is properly connected.

Note

If the AP cannot start after all the preceding items are verified, contact local distributors or technical support.

5 Monitoring and Maintenance

5.1 Monitoring

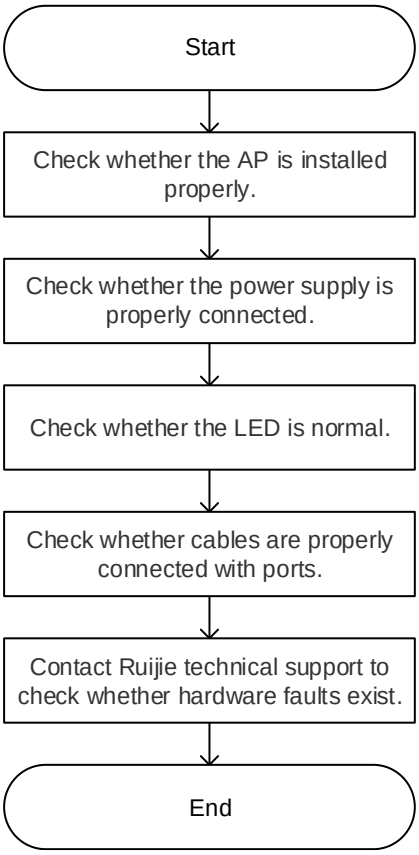
When the RG-APF1250 is operating, you can monitor the AP running status by observing the LED.

5.2 Maintenance

If a fault occurs, contact Ruijie technical support.

6 Troubleshooting

6.1 General Troubleshooting Flowchart



6.2 Common Faults

6.2.1 System Status LED Is Off After the AP Is Powered On

Verify that the adapter connected to the DC power connector is working properly, and check whether the Ethernet cable is connected properly.

6.2.2 After an Ethernet Cable is Connected, the Ethernet Port Cannot Be Used

Verify that the adapter connected to the DC power connector is working properly. Then verify that the Ethernet cable is capable of providing the required data rate and is properly connected.

6.2.3 A Client Cannot Discover the AP

(1) Verify that the AP is properly powered.

(2) Verify that the Ethernet port is correctly connected.

(3) Verify that the AP is correctly configured.

(4) Move the client closer to the AP.

7 Appendix

7.1 Connectors and Media

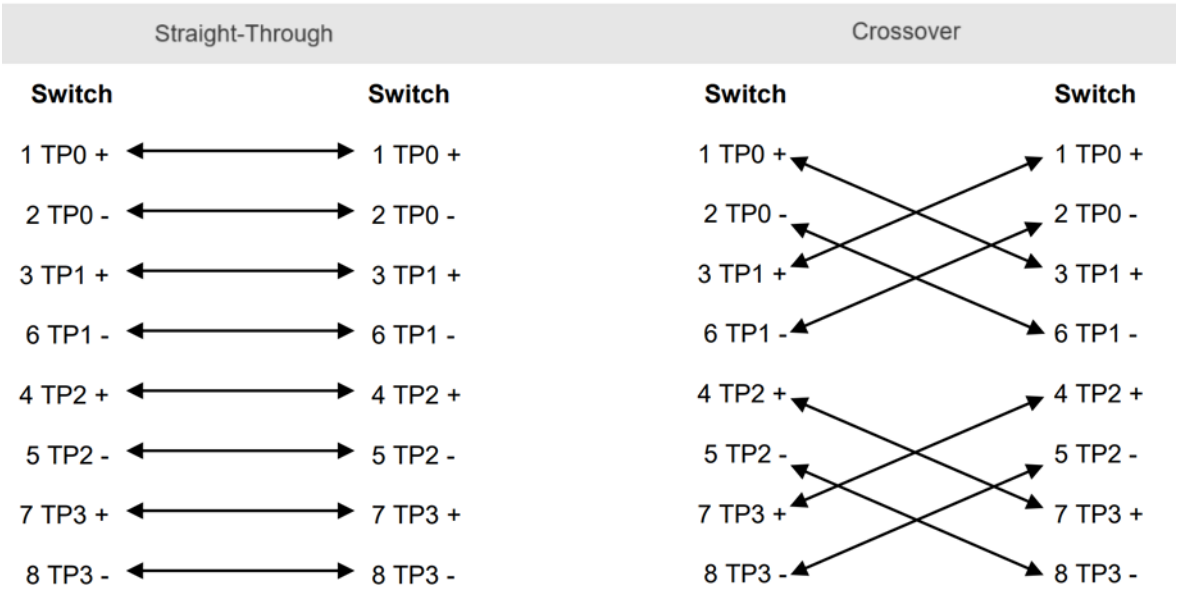
1000BASE-T/100BASE-TX/10BASE-T Port

The 1000BASE-T/100BASE-TX/10BASE-T port is a 10/100/1000 Mbps auto-negotiation port that supports auto MDI/MDIX crossover.

Compliant with IEEE 802.3ab, 1000BASE-T requires Category 5e 100-ohm UTP or STP (STP is recommended) with a maximum connection distance of 100 meters (328 ft.).

The 1000BASE-T port requires all four pairs of wires to be connected for data transmission. Figure 7-1 shows the four pairs of wires for the 1000BASE-T port.

Figure 7-1 1000BASE-T Twisted Pair Connections



100BASE-TX/10BASE-T can be interconnected using cables of the preceding specifications. For 10 Mbps, the 100BASE-TX/10BASE-T port can be connected using 100-ohm Category 3, Category 4, and Category 5 cables. For 100 Mbps, the 100BASE-TX/10BASE-T port can be connected using 100-ohm Category 5 cables with a maximum connection distance of 100 meters. Table 7-1 lists 100BASE-TX/10BASE-T pin assignments.

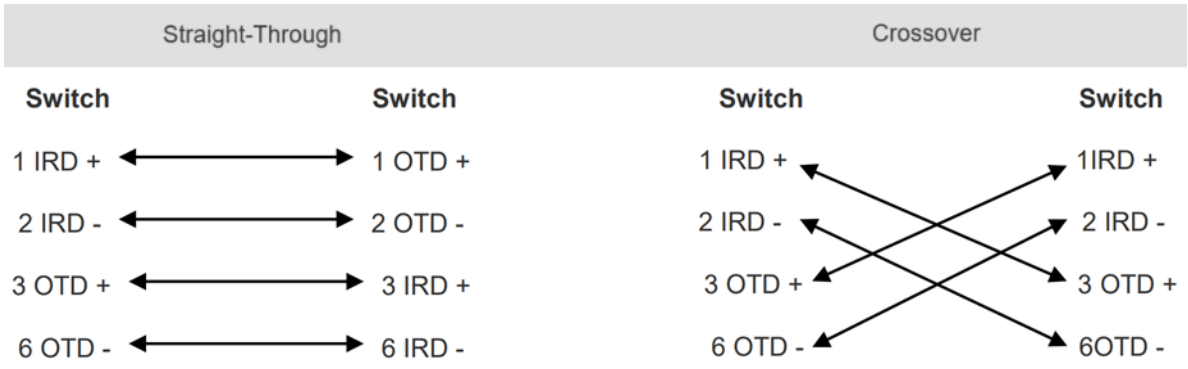
Table 7-1 100BASE-TX/10BASE-T Pin Assignments

Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-

Pin	Socket	Plug
4, 5, 7, 8	Not Used	Not Used

Figure 7-2 shows the wiring of straight-through and crossover cables for 100BASE-TX/10BASE-T.

Figure 7-2 100BASE-TX/10BASE-T Twisted Pair Connections



Ruijie Reyee RG-APF1250 Access Point ReyeeOS 2.290

Configuration Guide

Document Version: V1.0
Date: 2024-05-14
Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.


and other Ruijie networks logos are trademarks of Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

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://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

GUI 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. Notes

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

Preface I

1 Fast Internet Access 1

1.1 Configuration Environment Requirements 1

1.1.1 PC 1

1.2 Logging In to the Web Interface 1

1.2.1 Connecting to the Device 1

1.2.2 Configuring the IP Address of the Management Client 1

1.2.3 Logging in to the Web Interface 2

1.3 Work Modes 3

1.4 Configuration Wizard (AP Mode) 3

1.4.1 Getting Started 3

1.4.2 Configuration Steps 3

1.5 Web Interface 5

1.5.1 Single-mode Management Page 5

1.5.2 Dual-Mode Management Page 7

2 Wi-Fi Network Settings 9

2.1 Configuring AP Groups 9

2.1.1 Overview 9

2.1.2 Configuration Steps 9

2.2 Adding a Wi-Fi Network 10

2.3 Configuring SSID and Wi-Fi Password 12

2.4 Hiding the SSID 13

2.4.1 Overview 13

2.4.2 Configuration Steps 13
2.5 Checking Wireless Clients 14
2.6 Configuring the Wi-Fi Band 15
2.7 Configuring Band Steering 15
2.8 Configuring Wi-Fi 6 16
2.9 Configuring Wi-Fi 7 17
2.10 Enable Layer-3 Roaming 18
2.11 Configuring Client Isolation 19
2.12 Configuring a Guest Wi-Fi 19
2.12.1 Overview 19
2.12.2 Configuration Steps 19
2.13 Configuring Wi-Fi Blocklist/Allowlist 20
2.13.1 Overview 20
2.13.2 Configuration Steps 20
2.14 Optimizing Wi-Fi Network 21
2.14.1 Overview 21
2.14.2 Getting Started 21
2.14.3 Optimizing the Radio Channel 22
2.14.4 Optimizing the Channel Width 23
2.14.5 Optimizing the Transmit Power 23
2.14.6 Configuring the Multicast Rate 24
2.14.7 Configuring the Client Limit 24
2.14.8 Configuring Client Disconnection Threshold 25
2.14.9 Configuring the Roaming Sensitivity 26

2.14.10 Configuring the Access Threshold 27
2.14.11 Configuring the Response RSSI Threshold 27
2.14.12 Configuring WIO 28
2.14.13 Configuring K/V Roaming Optimization 29
2.15 Configuring Healthy Mode 30
2.16 Configuring XPress 31
2.17 Configuring Wireless Schedule 31
3 Network Settings 33
3.1 Switching Work Mode 33
3.1.1 Work Mode 33
3.1.2 Self-Organizing Network Discovery 33
3.1.3 Configuration Steps 33
3.1.4 Viewing Device Role 34
3.2 Configuring the Internet Connection Type (IPv4) 34
3.3 Configuring Port VLAN 35
3.4 Changing the MAC Address 36
3.5 Changing the MTU 37
3.6 Configuring DNS 37
3.7 Configuring Port Flow Control 38
3.8 Configuring the AP LAN Port 38
3.9 Configuring the Optical Transceiver 39
3.10 Configuring VoIP 40
3.10.1 Overview 40
3.10.2 Prerequisites 41

3.10.3 Configuration Steps 41
4 System Settings 44
4.1 Setting the Login Password 44
4.2 Setting the Session Timeout Duration 44
4.3 Setting and Displaying System Time 45
4.4 Configuring Reboot 46
4.4.1 Rebooting the Current Device 46
4.4.2 Rebooting All Devices on the Network 47
4.4.3 Rebooting the Specified Device 47
4.5 Configuring Scheduled Reboot 48
4.6 Configuring Backup and Import 49
4.7 Restoring Factory Settings 49
4.7.1 Restoring the Current Device to Factory Settings 49
4.7.2 Restoring All Devices to Factory Settings 50
4.8 Checking the System Version and Performing System Upgrade 51
4.8.1 Online Upgrade 51
4.8.2 Local Upgrade 51
4.9 Switching System Language 52
4.10 Configuring LED Status Control 52
5 Network Diagnosis Tools 53
5.1 Network Check 53
5.2 Network Tools 54
5.3 Alerts 55
5.4 Fault Collection 56

6 FAQs.....58

6.1 Fail to Log In to the Web Interface 58

6.2 Restore Factory Settings 58

6.3 Forgot Password.....58

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 characters 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 Logging In to the Web Interface

1.2.1 Connecting to the Device

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

- Wired connection

Connect a local area network (LAN) port of the device to the network port of the PC, and configure the IP address for the PC. See 1.2.2 Configuring the IP Address of the Management Client.

- Wireless connection

On a mobile phone or laptop, search for a wireless network whose Wi-Fi name is @Ruijie-bXXXX. (XXXX is the last four digits of the MAC address of the device). In this mode, you do not need to set the IP address of the management client, and can skip the steps in 1.2.2 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 on the same network segment as the default IP address of the device (default IP address: 10.44.77.254, subnet mask: 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 Web Configuration

Item	Default Value
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 management client can access the web interface of the device.

- 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.

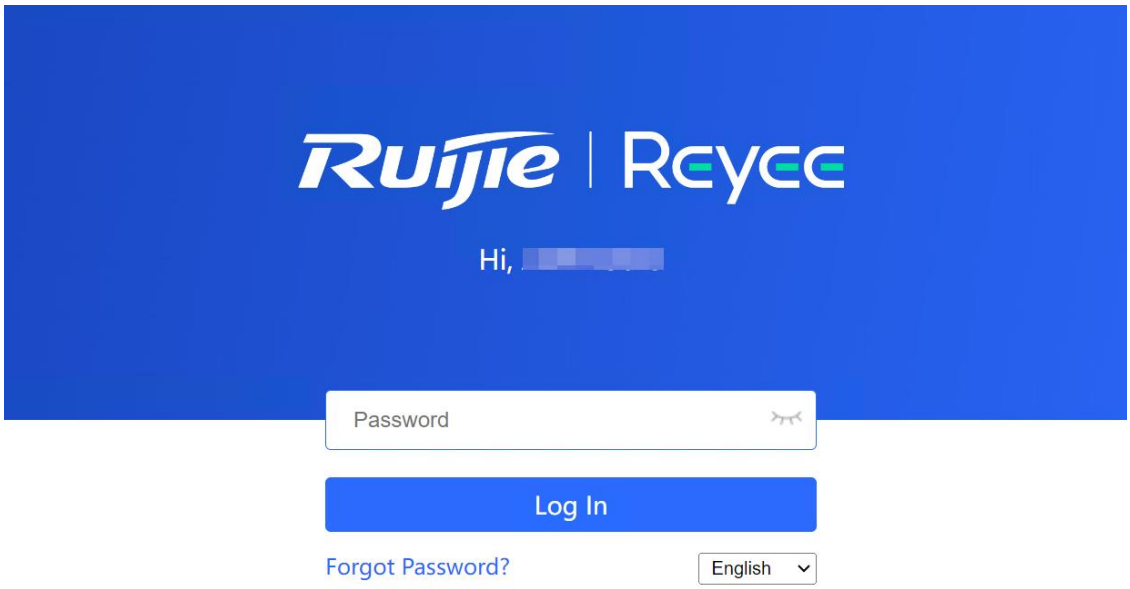
1.2.3 Logging in to the Web Interface

(1) Enter the IP address (10.44.77.254 by default) of the device 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 interface of the device as long as the management client and the device are on the same network segment of a LAN.

(2) On the web page that is displayed, enter the password and click **Log In** to enter the web interface



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.

If you forget the IP address or password, you can press and hold the **Reset** button on the device for more than 5 seconds when the device is connected to the power supply to restore factory settings. After reset, 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. Exercise caution when performing this operation.

1.3 Work Modes

The device works in AP mode.

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

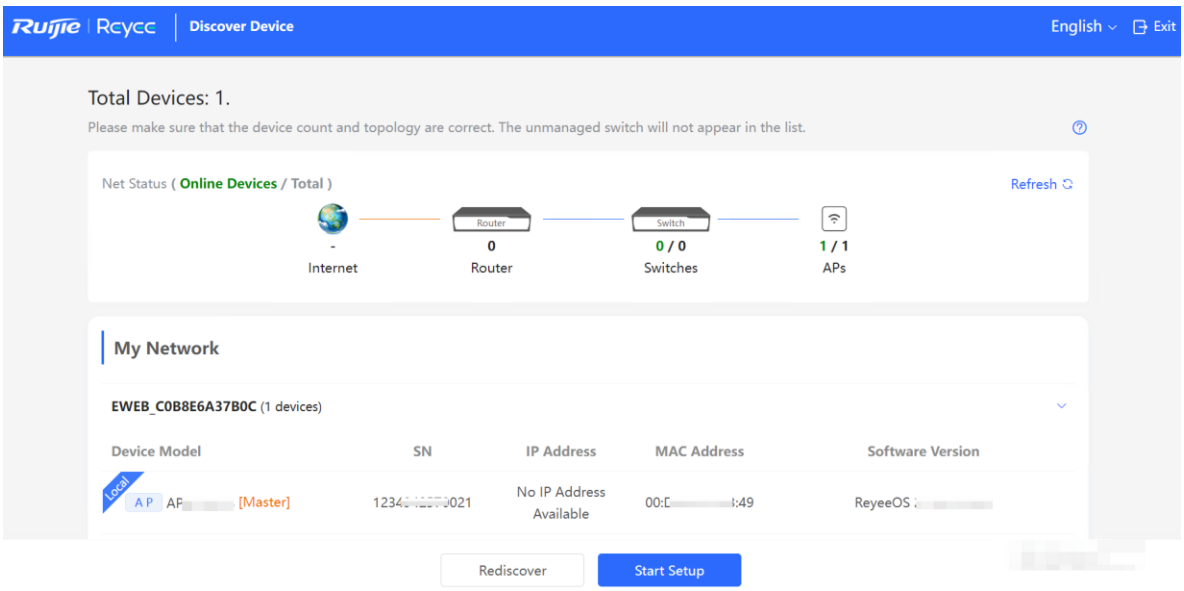
1.4 Configuration Wizard (AP Mode)

1.4.1 Getting Started

- Connect the device to a power supply and connect the LAN port of the device to an uplink device with an Ethernet cable.
- Check whether the uplink device can access the Internet, and that the current network is connected to the Internet.

1.4.2 Configuration Steps

By default, you can perform batch settings and centralized management for all devices on the network. Therefore, before starting the configuration, you need to check and confirm the number of online devices and network status. After confirmation, click **Start Setup**.



Configure the Internet connection type, and Wi-Fi settings.

(1) **Internet:** Select the Internet connection type confirmed by the ISP.

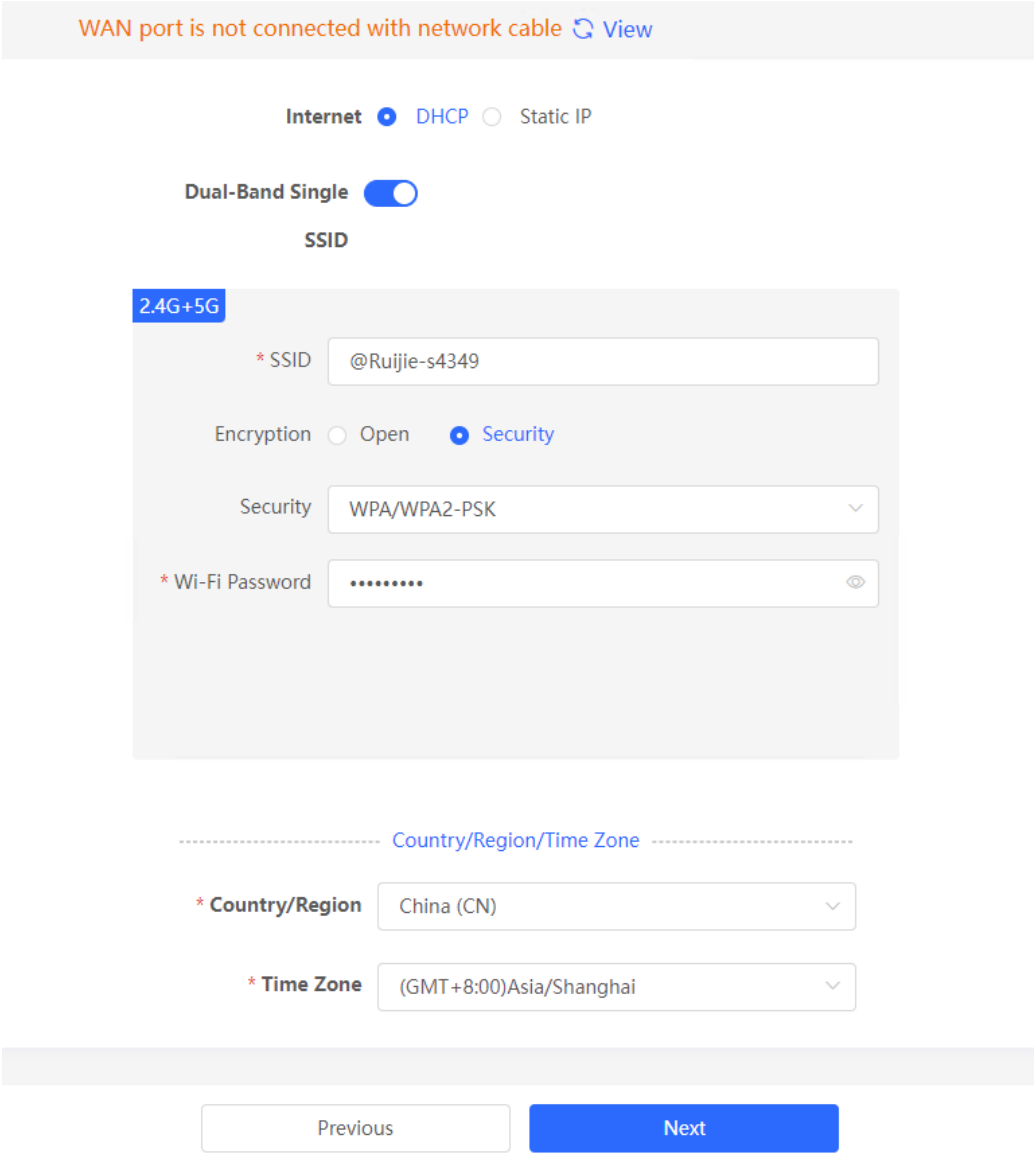
- **DHCP**: The device detects whether it can obtain an IP address via DHCP by default. If it connects to the Internet successfully, you can click **Next** without entering an account.
- **Static IP**: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.

(2) **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.

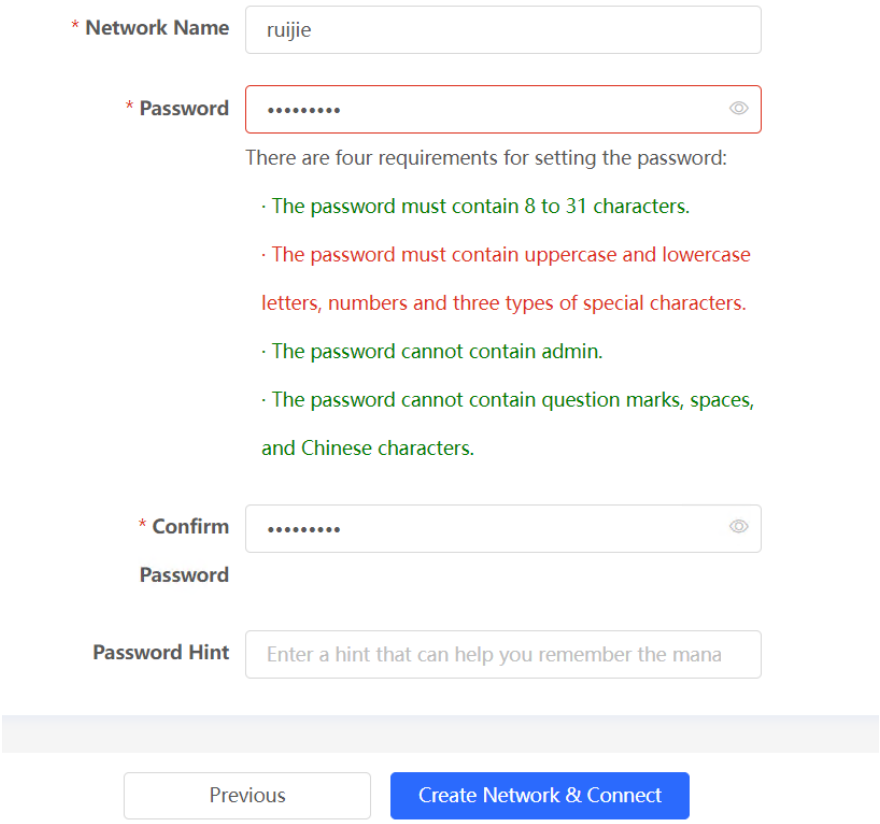
(3) **Country/Region:** The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.

(4) **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 **Next**.



Set the project name and password for the login page. After the configuration is complete, click **Create Network & Connect**. The device will deliver the initialization configuration and detect the network.



1.5 Web Interface

To facilitate flexible device management, the web interface displays different system configuration menus in different work modes. For details about the device work mode, see 3.1 Switching Work Mode.

For RG-APF1250, see 1.5.1 Single-mode Management Page.

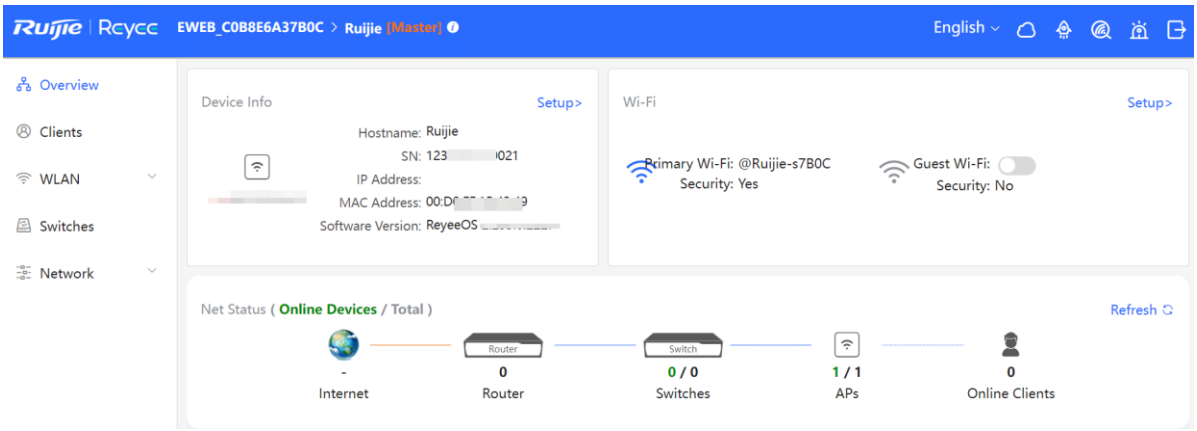
Note

When the self-organizing network is enabled, the web interface is subject to the primary device on the network. If the primary device supports the dual-mode management, the dual-mode management page is also displayed for the secondary devices.

1.5.1 Single-mode Management Page

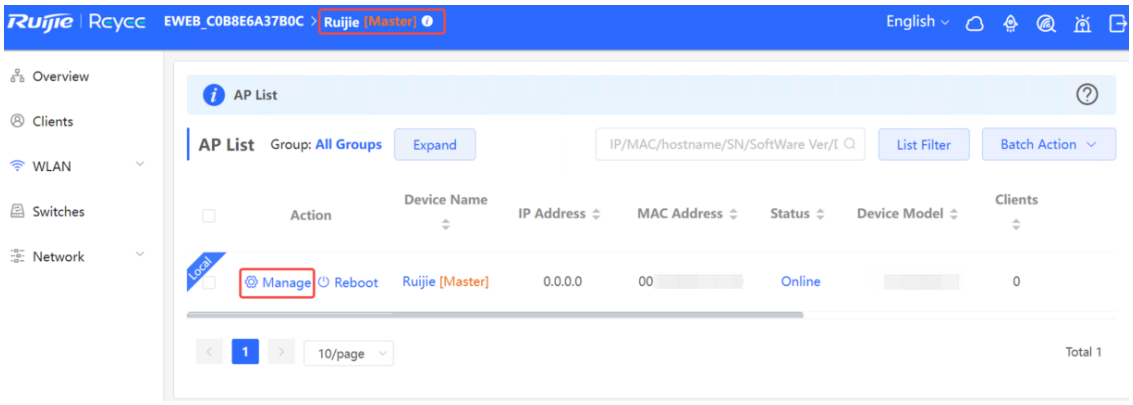
1. Network-wide Management

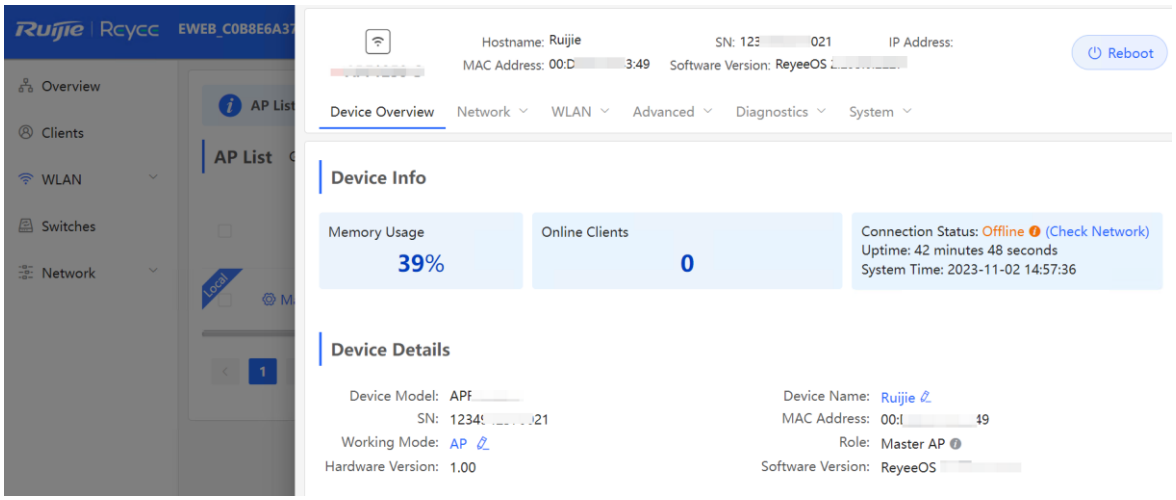
The device works in self-organizing network mode by default. The web interface displays the network-wide management menu on the left side, in which you can perform global wireless management (APs and Wi-Fi), routing management (if there is one on the network), switching management, and network-wide management (time, password, network-wide reboot, and other system settings). You can also view the status of all devices on the current network and modify network-wide settings.



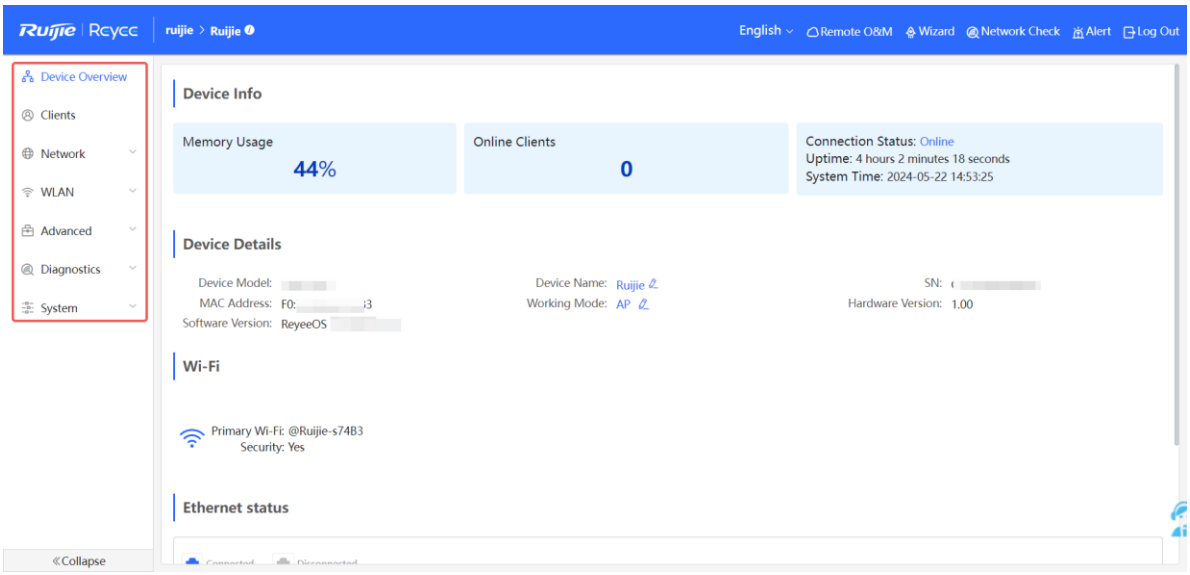
2. Standalone Management

- If the device is in self-organizing network mode, click the name of the currently logged-in device or click **Manage** of a specified device in the APs by choosing **WLAN** > **APs** to configure and manage the device.





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



1.5.2 Dual-Mode Management Page

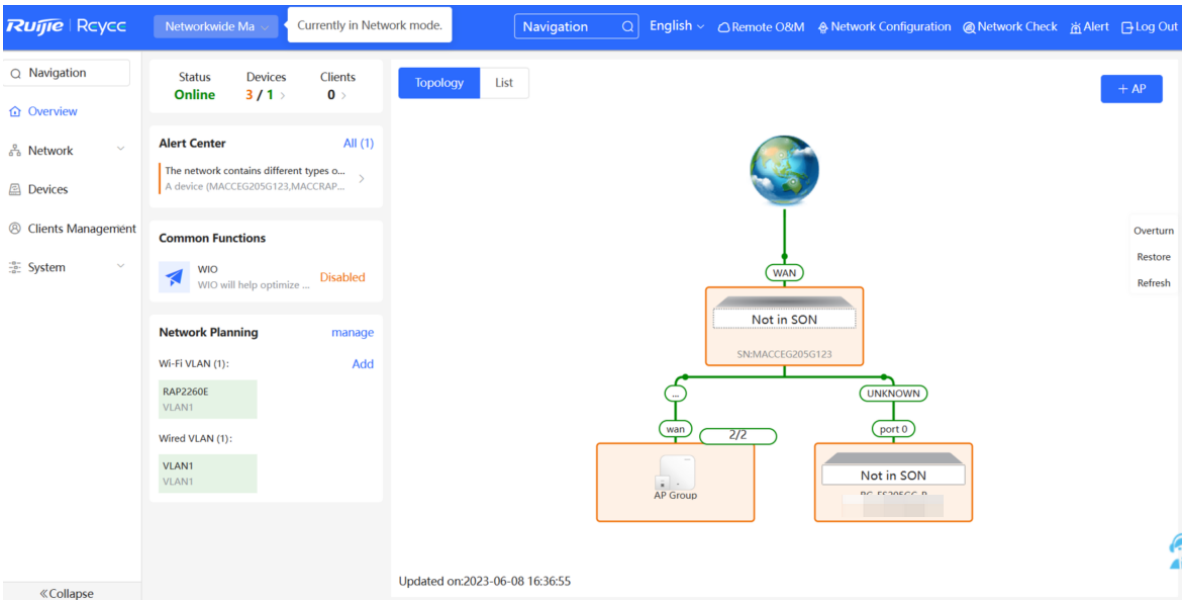
1. Management Mode

The self-organizing network is enabled by default. You can disable it manually. If the self-organizing network is disabled, the device works in the local device mode.

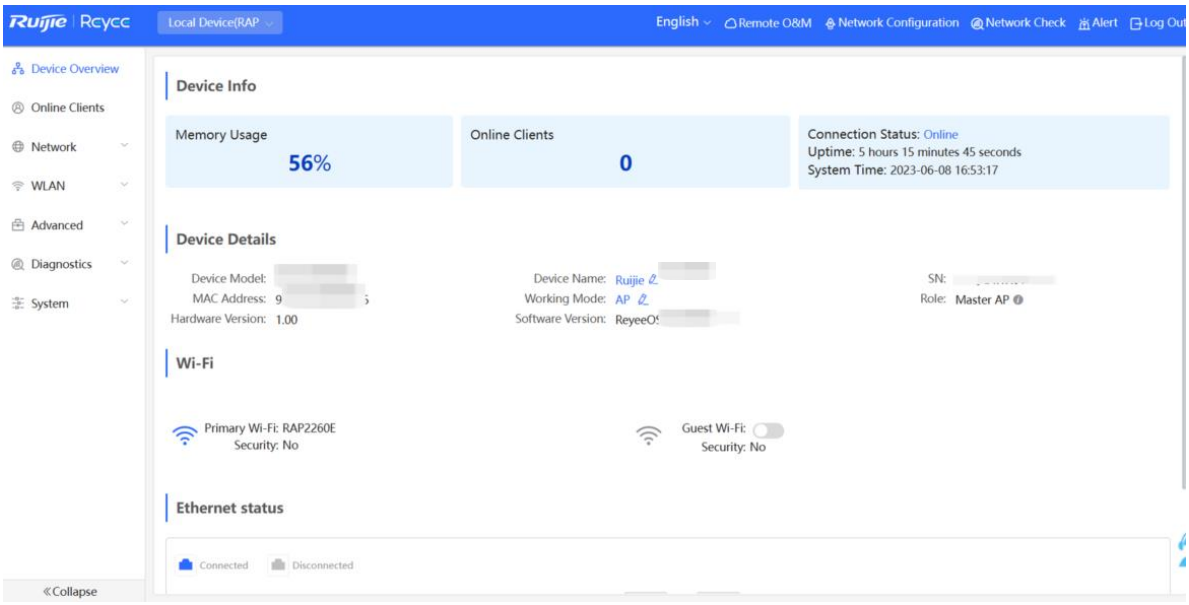
If the self-organizing network is enabled, the device can work in the SON mode and the local device mode. You can switch between the two modes on the web interface. The configuration menu varies by the management mode.

- SON mode: You can view the management information of all devices on the network, and configure all devices from a network point of view.
- Local Device mode: Only the currently logged in device can be configured.

SON mode web interface:

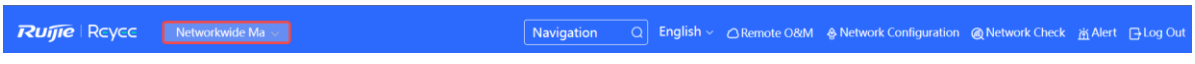


Local Device mode web interface:



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.





2 Wi-Fi Network Settings

Note

Wi-Fi network settings cover the Wi-Fi settings of the currently logged in device and the management of all wireless devices on the network. If the self-organizing network feature is enabled, the Wi-Fi network settings will be synchronized to all wireless devices on the network. You can configure device groups to limit the synchronization range. For details, see 2.1 Configuring AP Groups.

2.1 Configuring AP Groups

2.1.1 Overview

After the self-organizing network feature is enabled, the device can function as the primary AP/AC to batch configure and manage its downlink APs by group. Group the APs before the delivering the configurations.

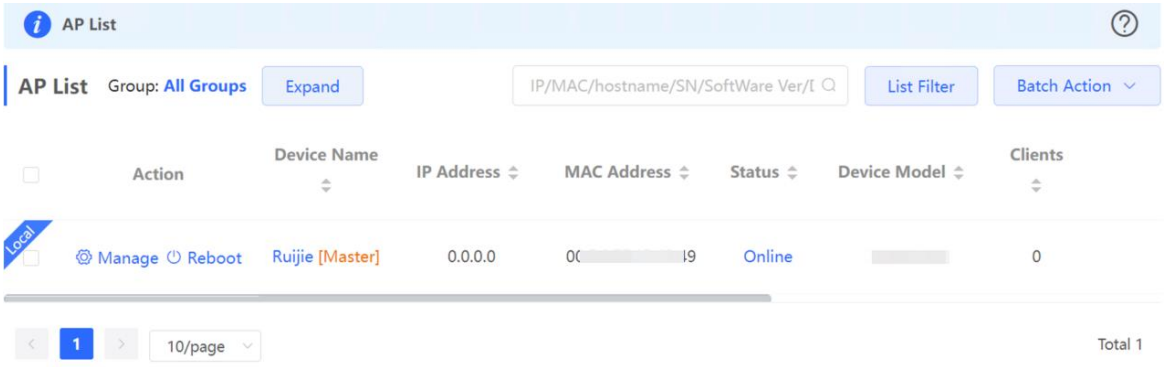
Note

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.

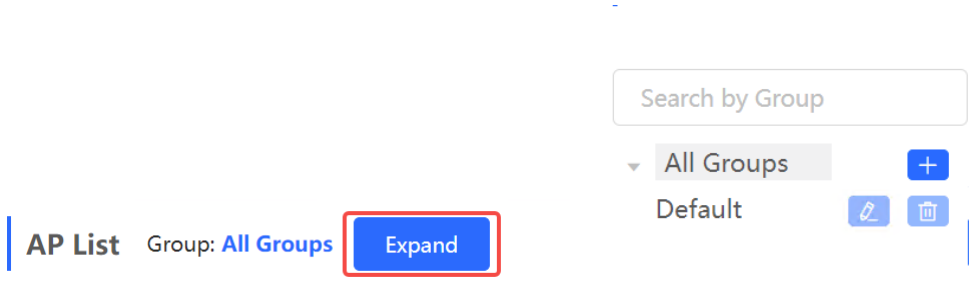
2.1.2 Configuration Steps

Go to the configuration page: Choose **WLAN** > **APs**.

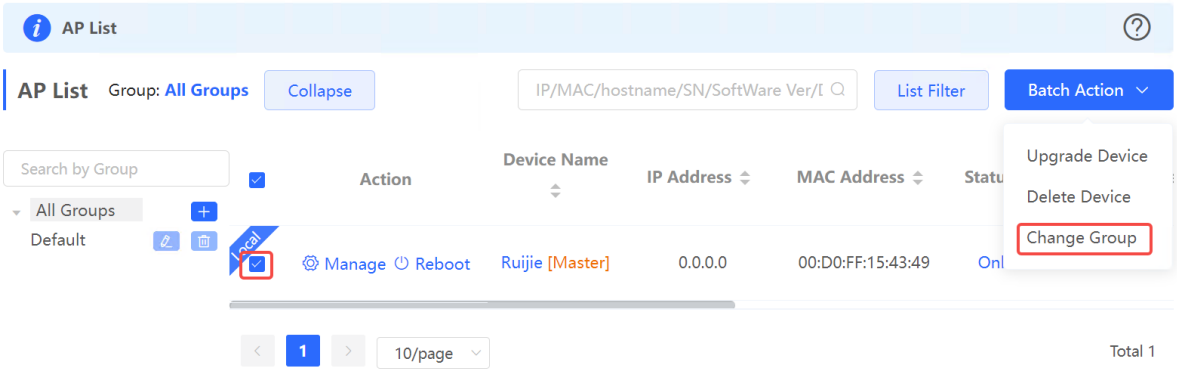
(1) View the information of all APs on the current network, including the basic information, RF information, and model. Click the serial number in the APs or **Manage** to configure a single device.

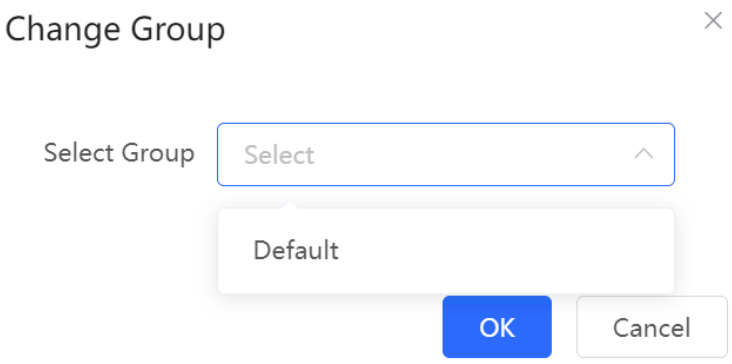


(2) Click **Expand** to view all groups on the left pane of the **APs** page. Click  to create a new group. Up to 8 groups can be added. You can click  to edit the group name and click  to delete the group. The default group cannot be deleted and its name cannot be edited.



(3) Click the group name on the left pane to view all devices in the group. A device can only belong to one 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. As a result, the configurations of this group will apply to this device. Click **Delete Offline Devices** to remove any offline device from the list.





2.2 Adding a Wi-Fi Network

(1) Go to the configuration page:

- 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.

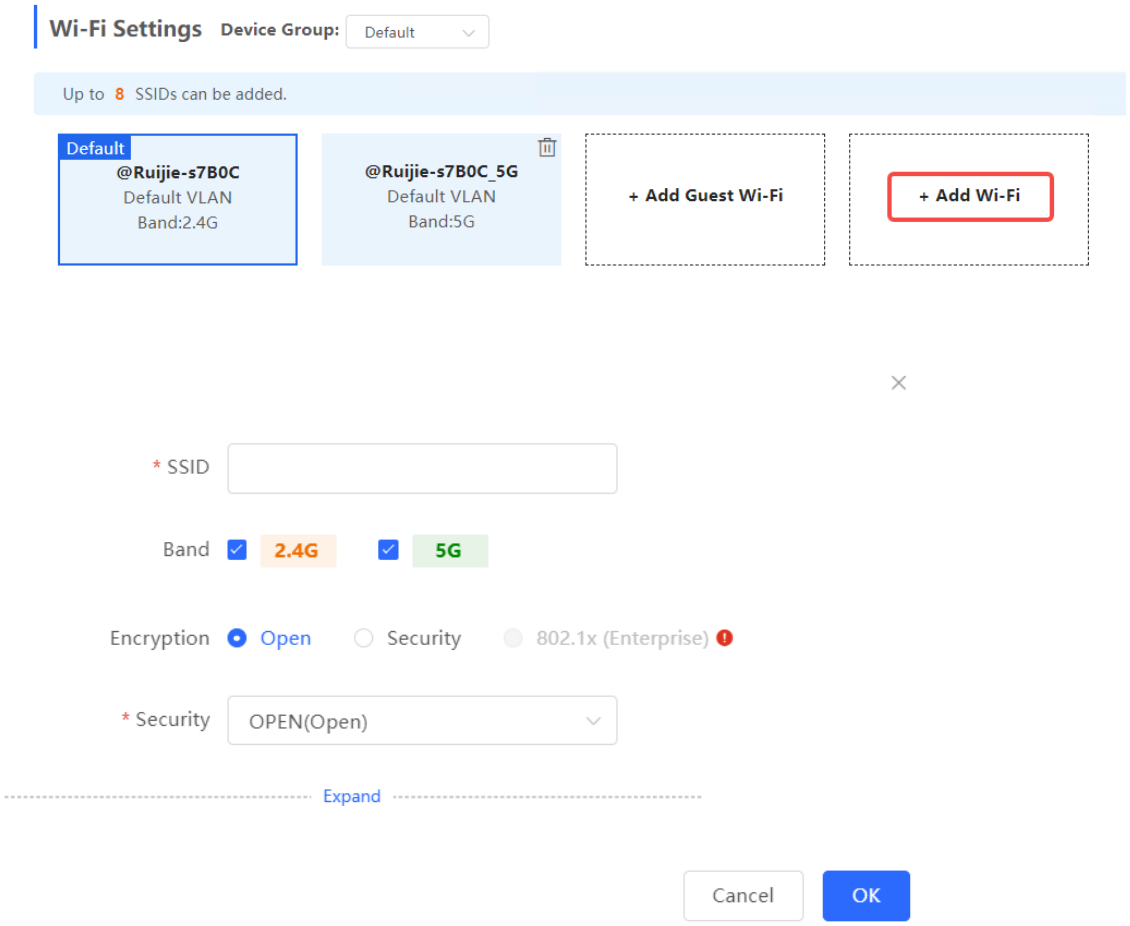


Table 2-1 Wireless Network Parameters

Parameter	Description
SSID	The name displayed when a wireless client searches for a wireless network.
SSID Encoding	The SSID encoding standard is set to "UTF-8" by default when Chinese characters are included in the SSID. If the Chinese characters are garbled, you can choose "GBK" as the SSID encoding standard.
Band	The frequency band used for wireless data transmission. 2.4 GHz and 5 GHz frequency bands are supported. The 5 GHz frequency band offers a faster transmission rate and less interference compared to the 2.4 GHz frequency band, but it has weaker signal coverage and wall penetration. The frequency band can be selected according to actual needs. The default band is 2.4 GHz+5 GHz, on which Wi-Fi transmits on both the 2.4 GHz and 5 GHz bands.
Encryption	Select an encryption mode for the wireless network connection. The options are as follows: Open, Security and 802.1x(Enterprise).
Wi-Fi Password	When the encryption mode is set to WPA-PSK, a Wi-Fi password needs to be entered. The password for connecting to the wireless network, consisting of 8-16 characters.

Parameter	Description
Wi-Fi Standard	Wireless mode, including 802.11be (Wi-Fi 7), 802.11ax (Wi-Fi 6), and compatible mode 802.11be (Wi-Fi 7): This parameter takes effect only on APs that support the IEEE 802.11be protocol. In addition, the connected terminals must support the IEEE 802.11be protocol to experience the high-speed Internet access experience brought by Wi-Fi 7. 802.11ax (Wi-Fi 6): This parameter takes effect only on APs that support the IEEE 802.11ax protocol. In addition, access clients must support IEEE 802.11ax so that users can enjoy high-speed Internet access experience brought by Wi-Fi 6. Compatibility mode: The AP supports 802.11n (Wi-Fi 4) in the 2.4 GHz band and 802.11ac (Wi-Fi 5) in the 5 GHz band. The AP has good compatibility with STAs that do not support Wi-Fi 6 and above.
Wireless Schedule	Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.
VLAN	Set the VLAN to which the Wi-Fi signal belongs. You can select User and AP in the same VLAN or Other VLAN and enter the VLAN ID.
Hide SSID	Enabling the Hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the Wi-Fi name after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current Wi-Fi name before you enable this function.
Client Isolation	After this function is enabled, clients associated with the Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.
Band Steering	After this function is enabled, the client supporting 5 GHz selects the 5G Wi-Fi network preferentially. You can enable this function only when Band is set to 2.4 GHz + 5 GHz.
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for gaming.
Layer 3 Roaming	After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.

2.3 Configuring SSID and Wi-Fi Password

(1) Go to the configuration page:

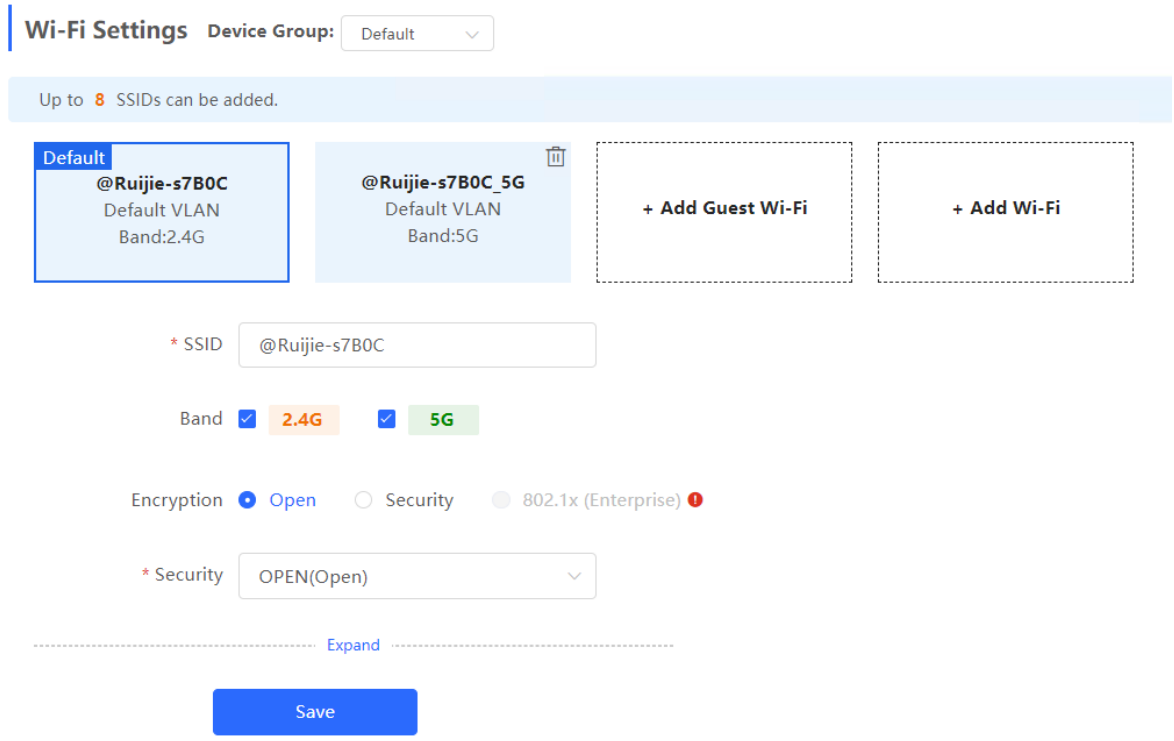
- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Enter the SSID, select the encryption type, enter the Wi-Fi password of the Wi-Fi network, and click **Save**. If the encryption type is set to **Open**, the Wi-Fi network is an open network, and clients can connect to the

Internet without a password. The Wi-Fi password must be a string of 8 to 16 characters, which can contain letters, digits, and special characters (<=>[]!@#$*()).

Caution

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



2.4 Hiding the SSID

2.4.1 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.

2.4.2 Configuration Steps

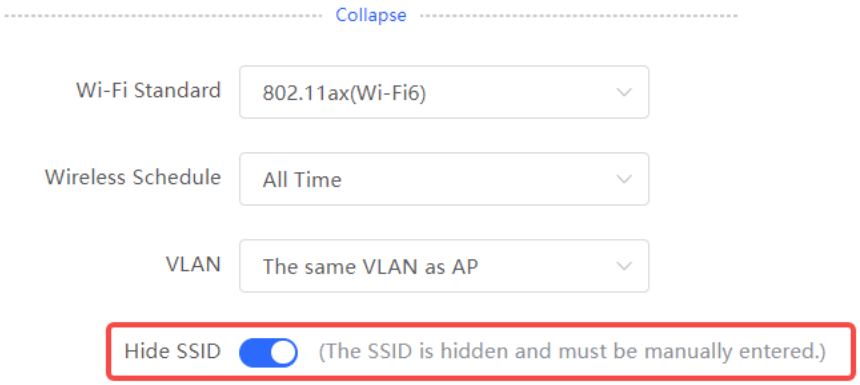
(1) Go to the configuration page:

- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **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. Exercise caution when performing this operation.



2.5 Checking Wireless Clients

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

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

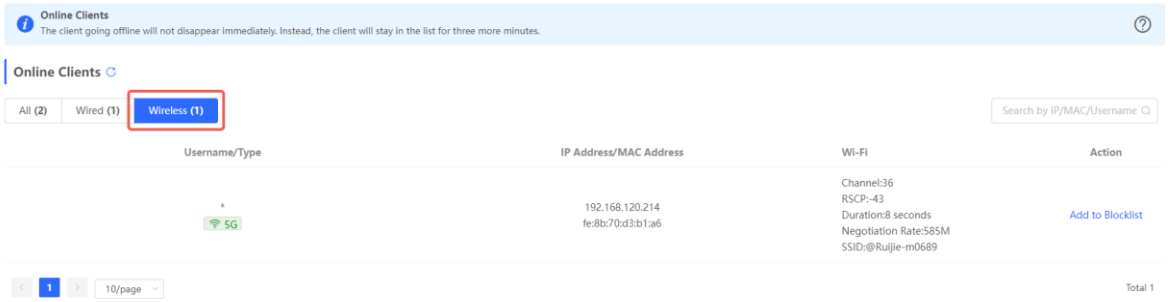


Table 2-2 Wireless Client Parameters

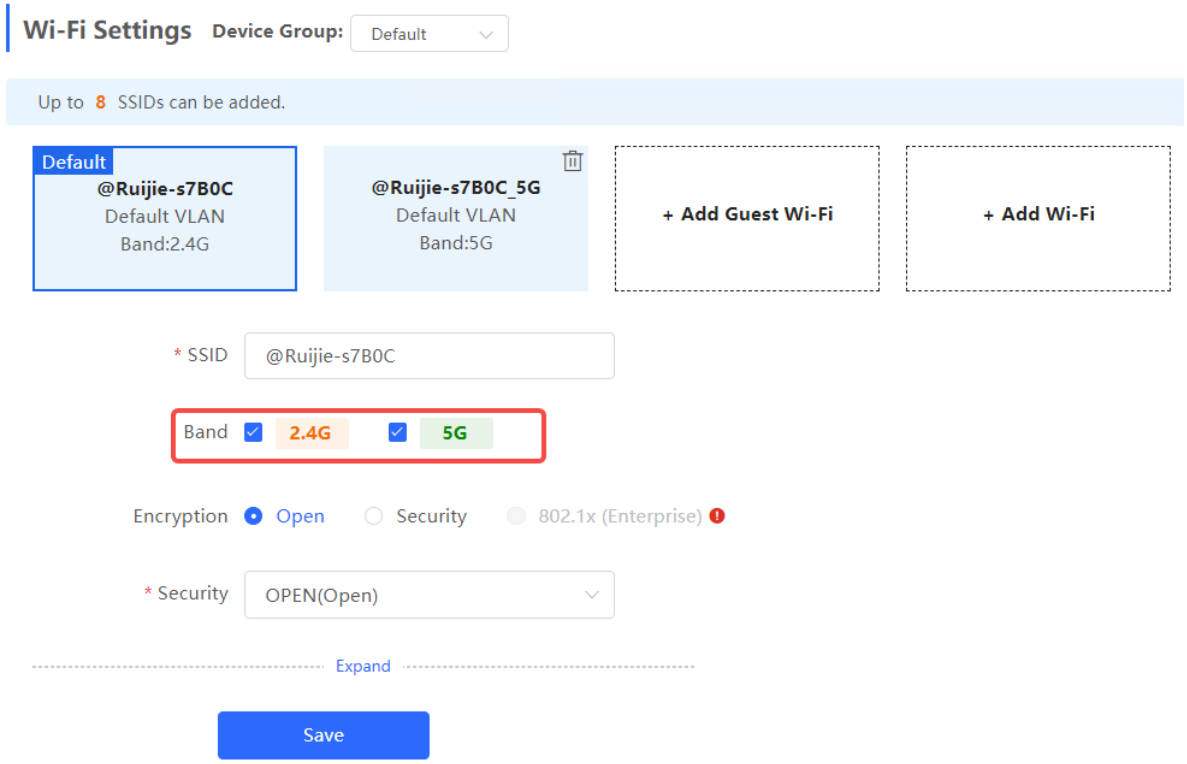
Item	Description
Username/Type	Name of a client and the band.
IP Address/MAC Address	IPv4 address/MAC address of the client.
Wi-Fi	● Channel of the Wi-Fi network associated with the client. ● RSCP of the Wi-Fi network associated with the client. ● Duration of the Wi-Fi network associated with the client. ● Negotiation rate of the Wi-Fi network associated with the client. ● Name of the Wi-Fi network associated with the client.

2.6 Configuring the Wi-Fi Band

(1) Go to the configuration page:

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

(2) 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.



2.7 Configuring Band Steering

Caution

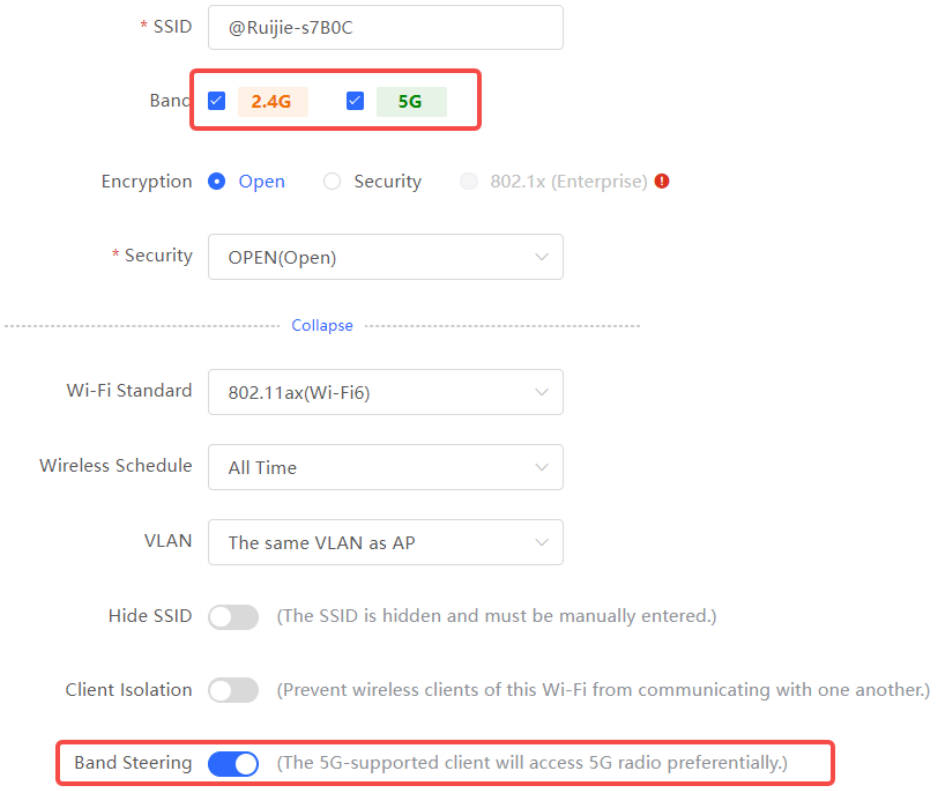
This function can be enabled only after the dual-band integration (**Band** is set to **2.4G+5G**) is enabled on the Wi-Fi network. A client automatically selects a band only when the SSIDs of the 2.4 GHz and 5 GHz bands are the same.

(1) Go to the configuration page:

- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **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 **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.



2.8 Configuring Wi-Fi 6

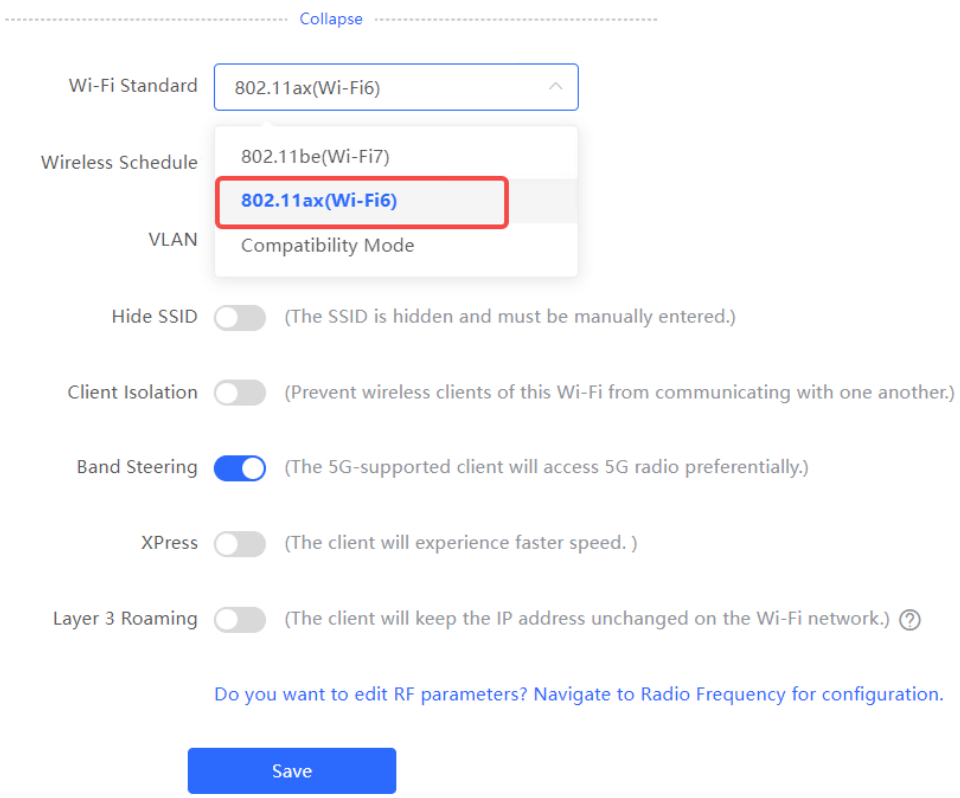
Caution

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 configuration page:

- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **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 **Wi-Fi6** in the expanded settings, and click **Save**. After this function is enabled, wireless clients can enjoy faster Internet access service.



2.9 Configuring Wi-Fi 7

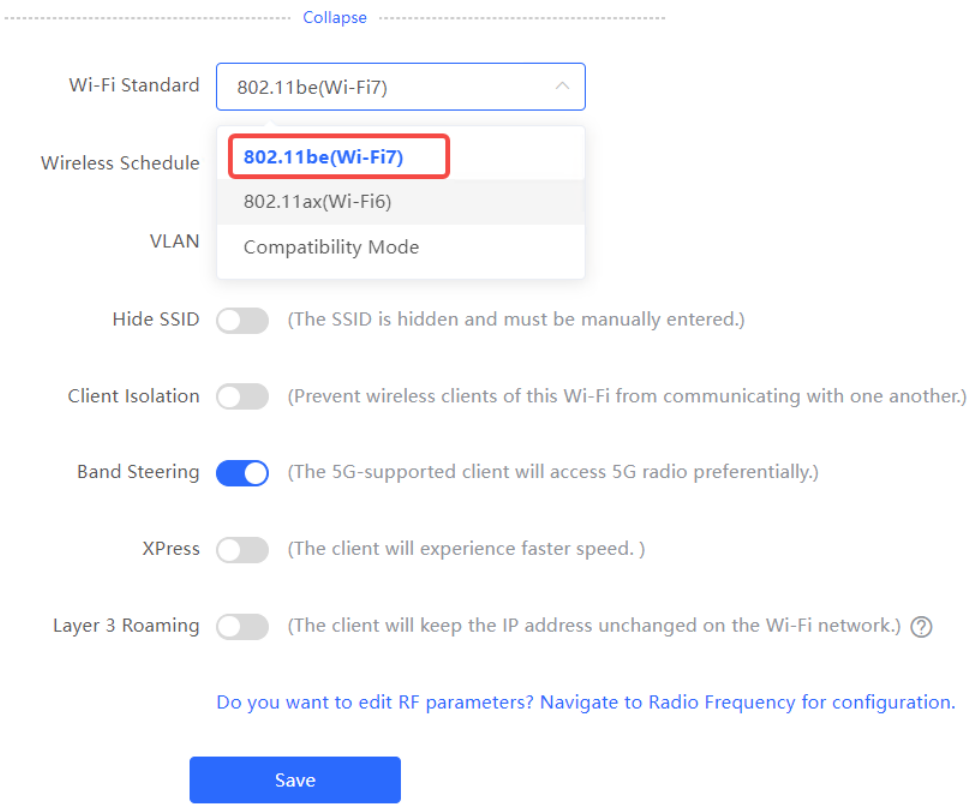
Caution

This configuration takes effect only on APs that support the IEEE 802.11be protocol. In addition, the connected clients must support the IEEE 802.11be protocol to experience the high-speed Internet access brought by Wi-Fi 7. If the client does not support Wi-Fi 7, you can disable this feature.

(1) Go to the configuration page:

- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **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 **Wi-Fi7** in the expanded settings, and click **Save**. After this function is enabled, wireless clients can enjoy faster Internet access service.

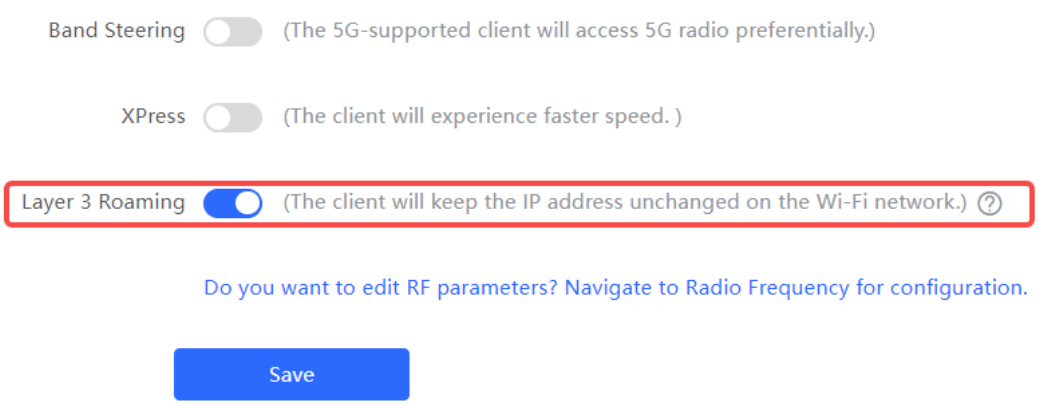


2.10 Enable Layer-3 Roaming

(1) Go to the configuration page:

- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **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 **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.

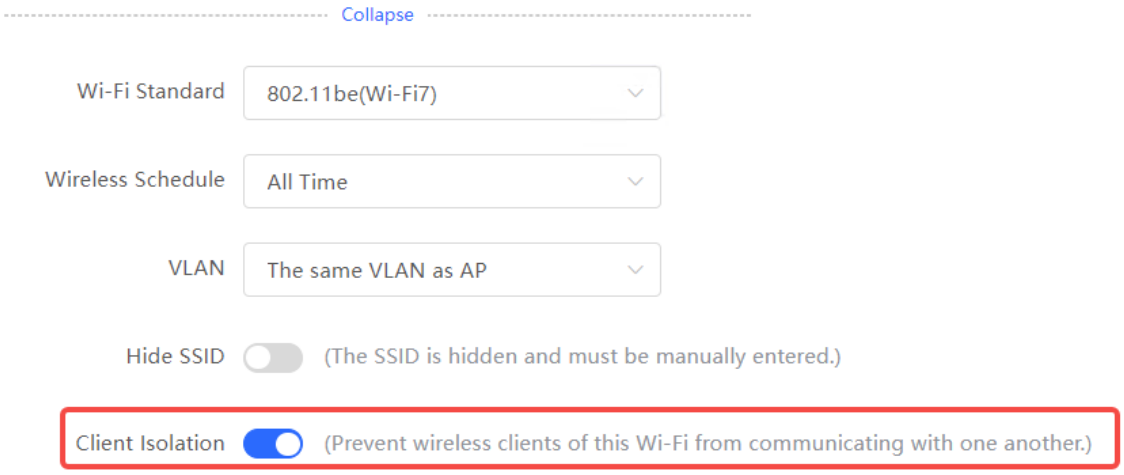


2.11 Configuring Client Isolation

(1) Go to the configuration page:

- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **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 **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.



2.12 Configuring a Guest Wi-Fi

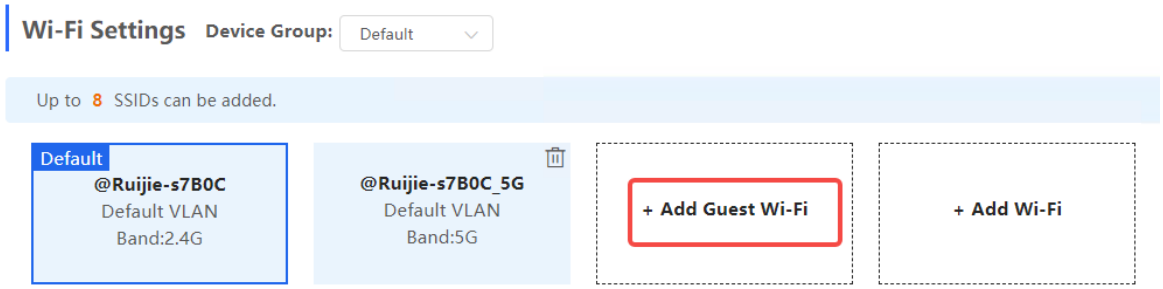
2.12.1 Overview

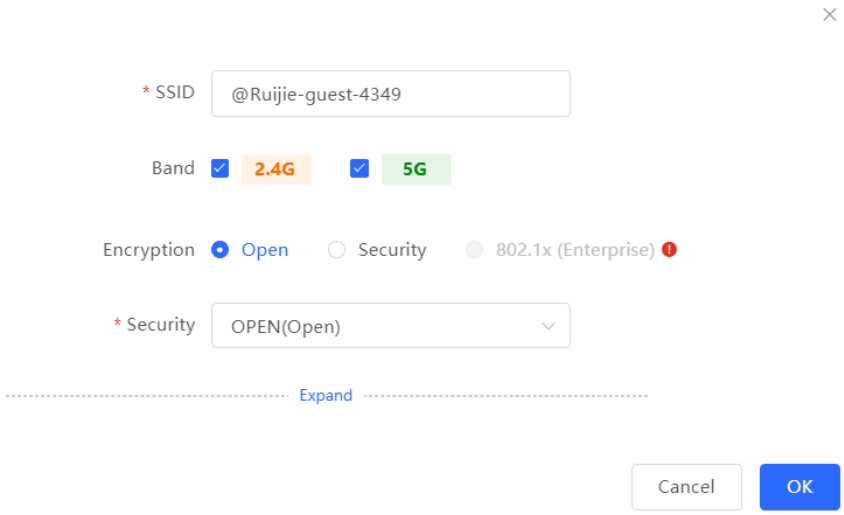
The guest Wi-Fi is disabled by default. By default, user isolation is enabled for guest Wi-Fi. That is, connected users are isolated from each other and can only access the Internet through the Wi-Fi. They cannot access each other to improve security. The guest Wi-Fi can be automatically turned off at a scheduled time.

2.12.2 Configuration Steps

Choose **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.





2.13 Configuring Wi-Fi Blocklist/Allowlist

2.13.1 Overview

You can configure a global Wi-Fi blocklist/allowlist.

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

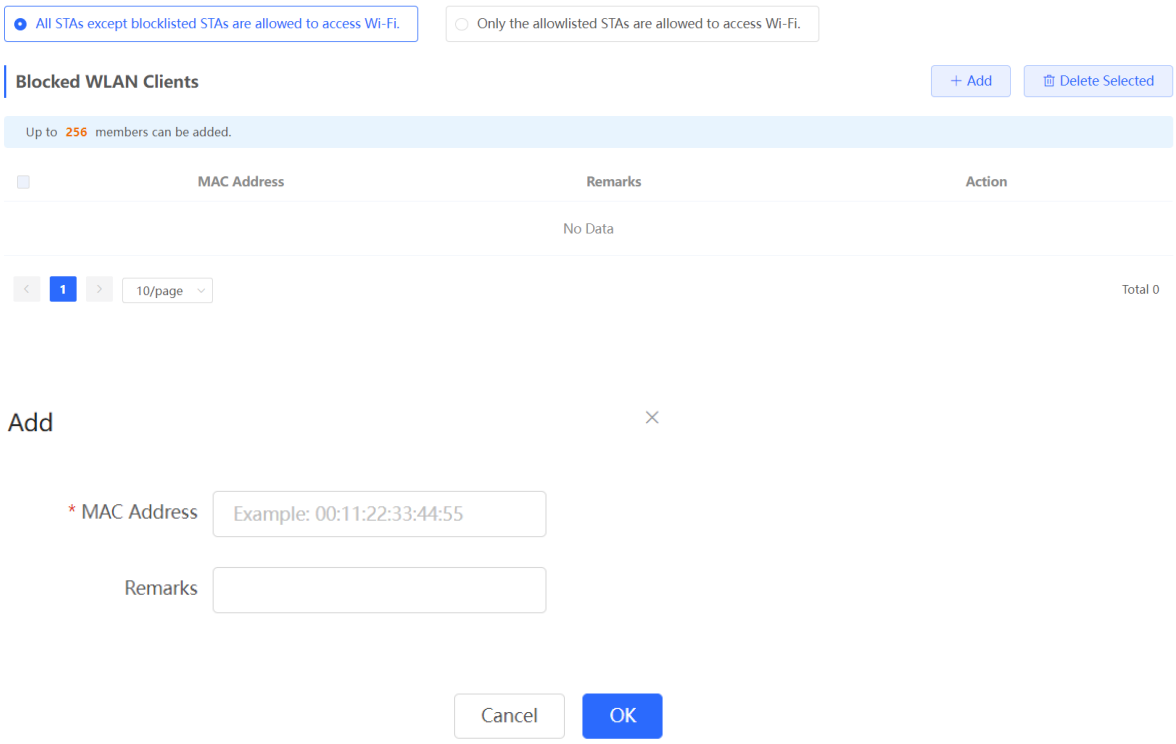
If the allowlist is empty, the allowlist does not take effect. In this case, all clients are allowed to access the Internet.

2.13.2 Configuration Steps

1. Configuring a Global Allowlist/Blocklist

Choose **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.



2.14 Optimizing Wi-Fi Network

2.14.1 Overview

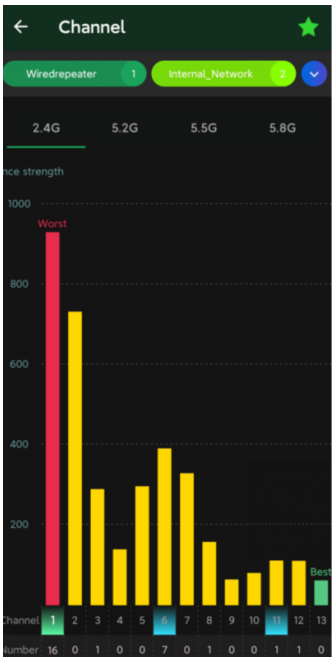
The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point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

Caution

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

2.14.2 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.



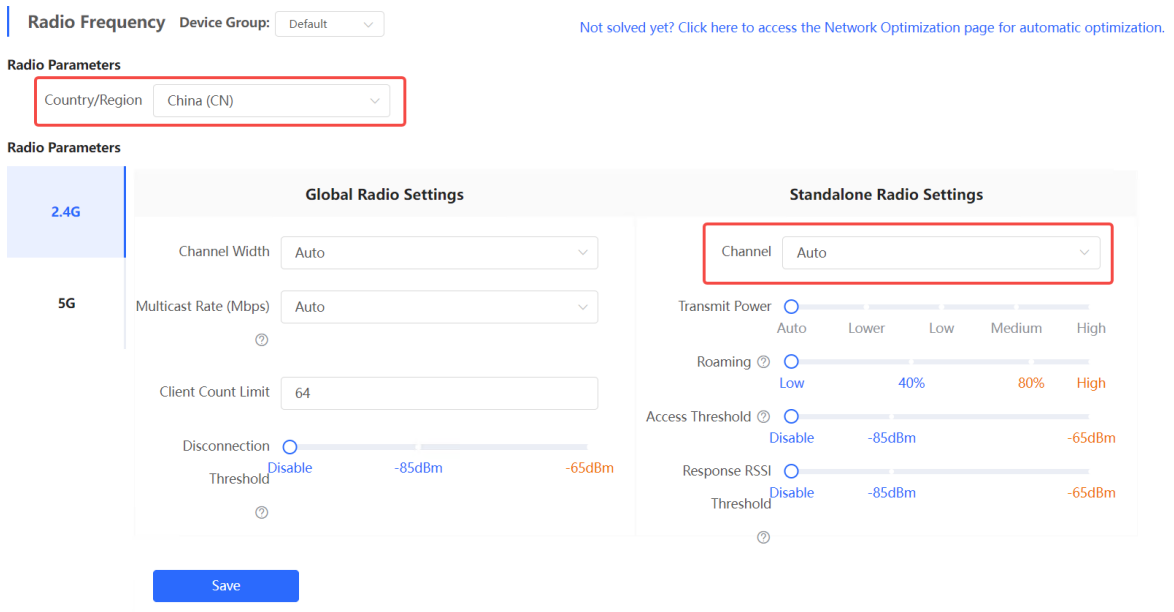
2.14.3 Optimizing the Radio Channel

- Primary device: Choose **WLAN** > **Radio Frequency**
- Secondary device: Choose **WLAN** > **APs**. Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**.

Choose the best channel identified by a Wi-Fi test tool. Click **Save** to make the configuration take effect immediately. The more devices in a channel, the greater the interference.

Note

The available channels and the VoIP feature are dependent on the country/region code. Please correctly set the country/region code corresponding to your location.



2.14.4 Optimizing the Channel Width

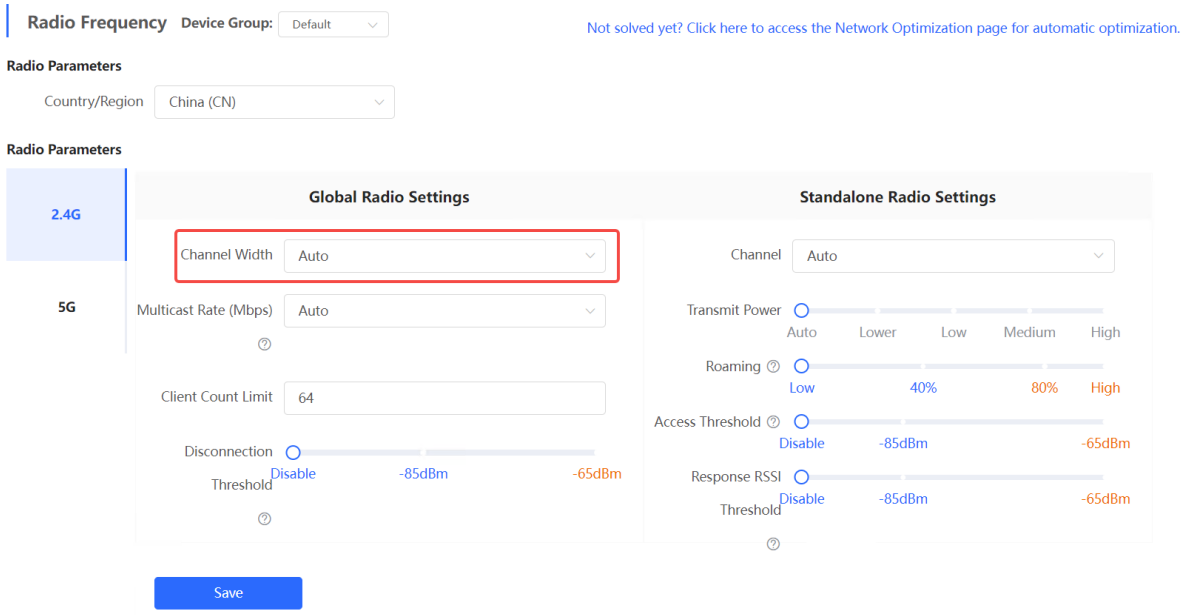
Choose **WLAN** > **Radio Frequency**.

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 access point supports the channel width of 20 MHz and 40 MHz in the 2.4 GHz channel, and the channel width of 20 MHz and 40 MHz and 80 MHz and 160 MHz in the 5 GHz channel.

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

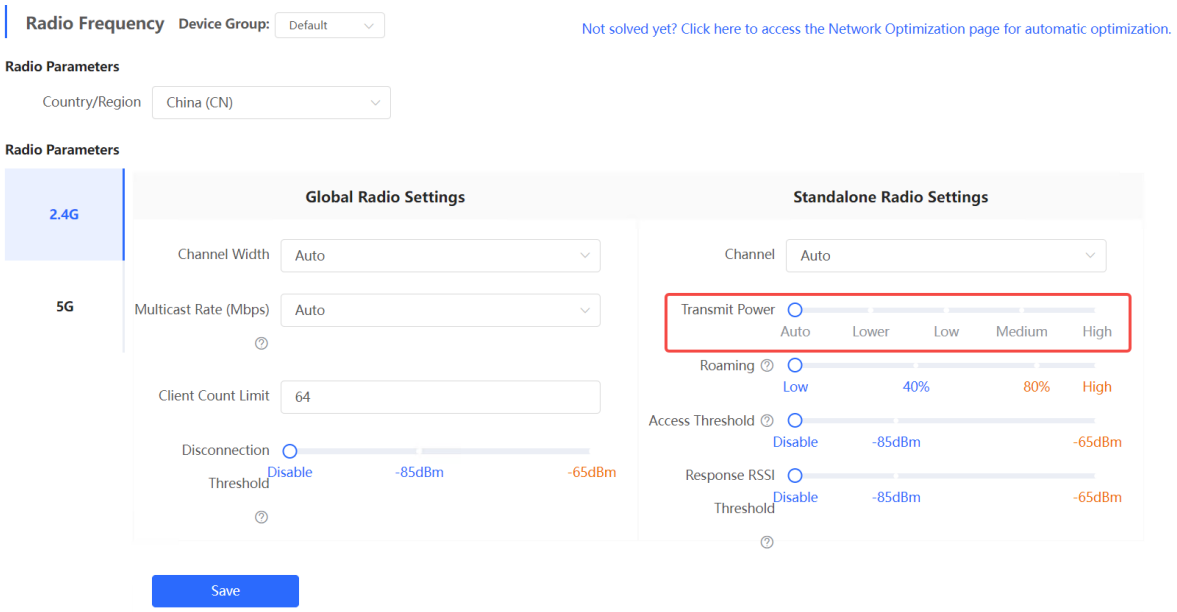
In the self-organizing network mode, the channel width settings will be synchronized to all devices in the network.



2.14.5 Optimizing the Transmit Power

- Primary device: Choose **WLAN** > **Radio Frequency**
- Secondary device: Choose **WLAN** > **APs.** Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**.

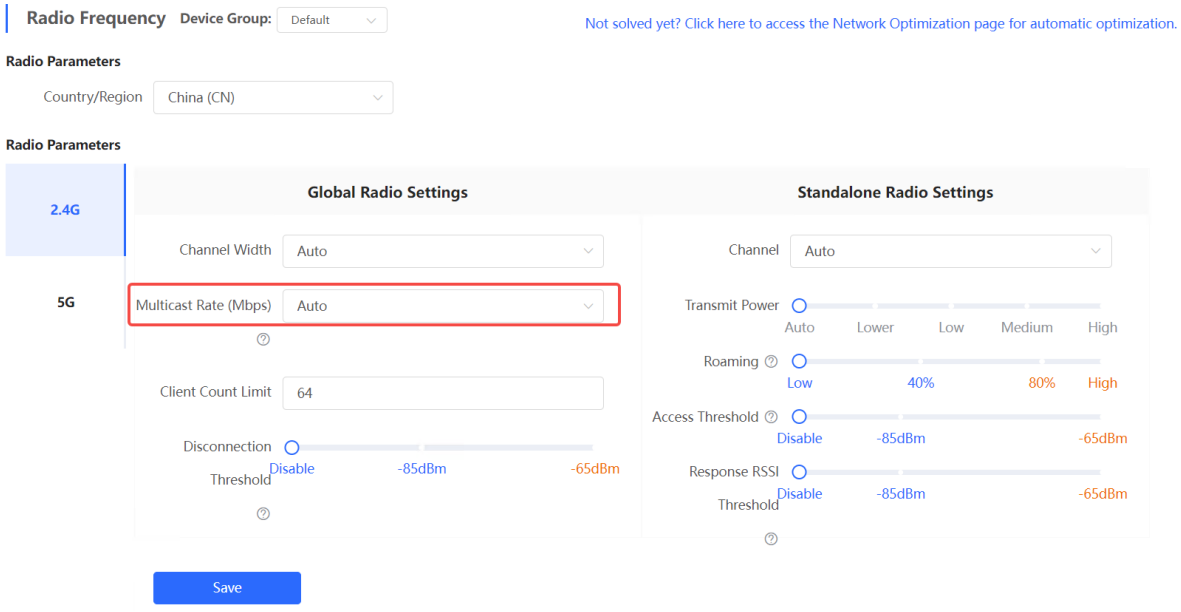
A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. In a high-density scenario, you are advised to set the transmit power to a small value. The **Auto** mode is recommended, indicating automatic adjustment of the transmit power. After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



2.14.6 Configuring the Multicast Rate

Choose **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**.

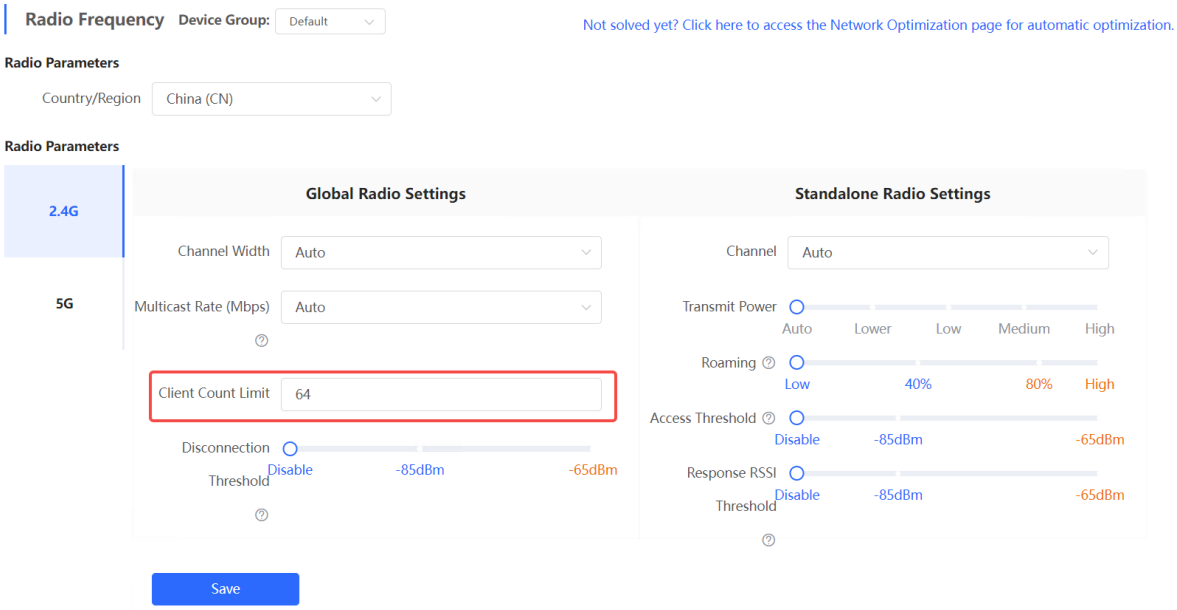


2.14.7 Configuring the Client Limit

Choose **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

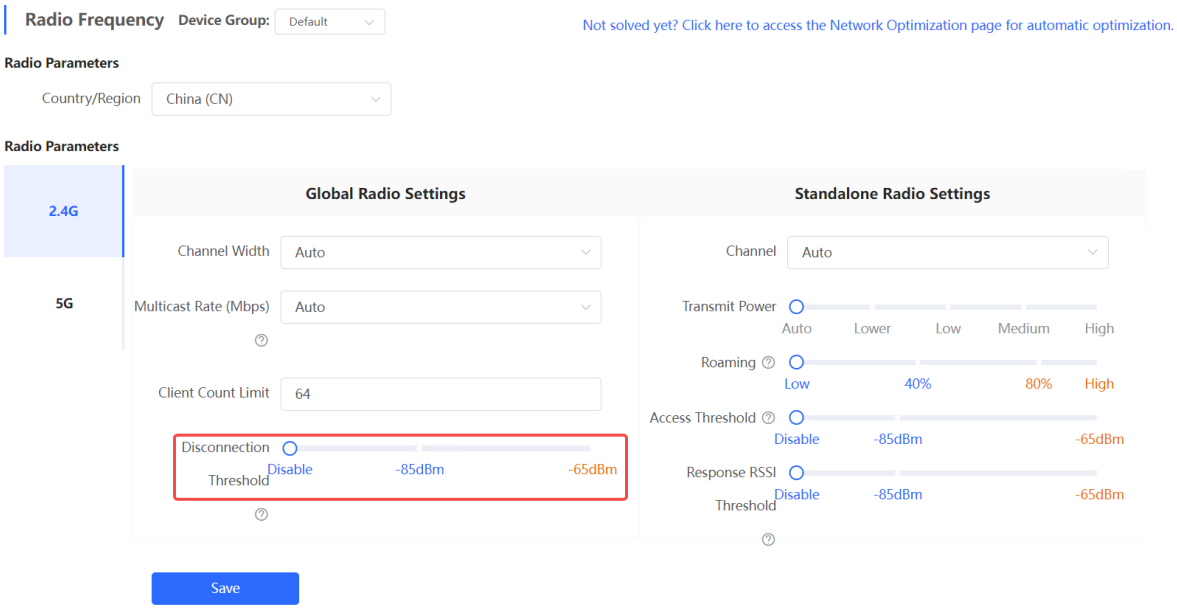
The **Client Count Limit** refers to the maximum number of clients that can be connected to a single access point.

2.14.8 Configuring Client Disconnection Threshold

Choose **WLAN** > **Radio Frequency**.

In the case of multiple Wi-Fi signals, setting the disconnection 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 disconnection 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 disconnection threshold is, the easier it is for the client to be kicked offline. To ensure normal Internet access, you are advised to disable the disconnection threshold or set the value to less than –75 dBm. After adjusting the configuration, click **Save**.



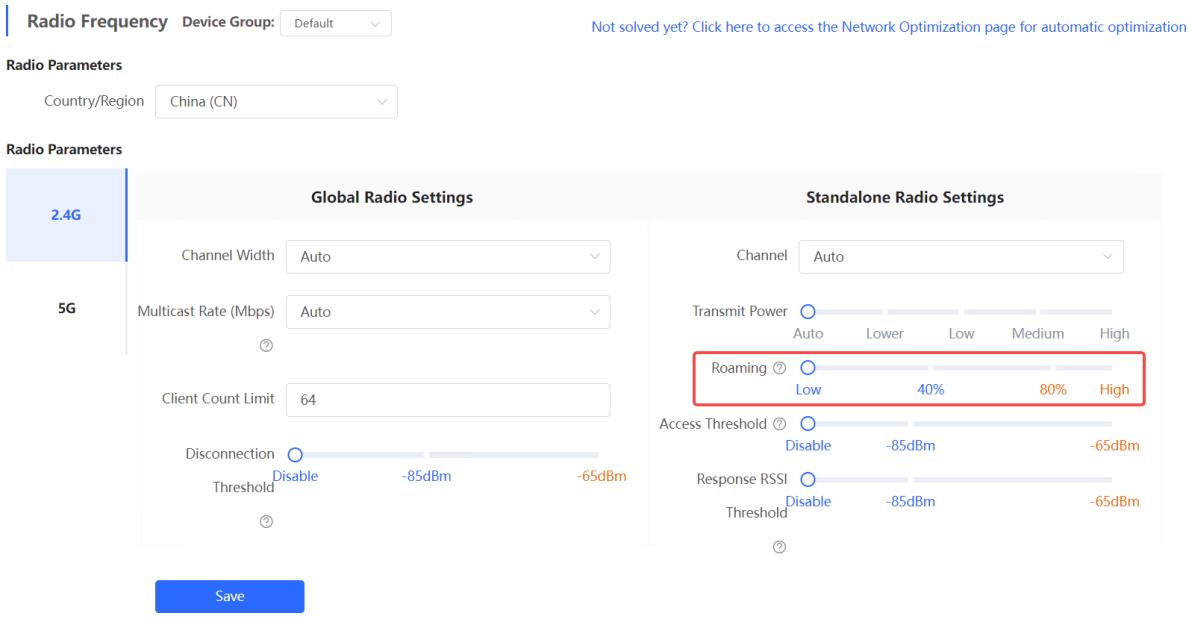
Caution

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

2.14.9 Configuring the Roaming Sensitivity

- Primary device: Choose **WLAN** > **Radio Frequency**.
- Secondary device: Choose **WLAN** > **APs**. Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**.

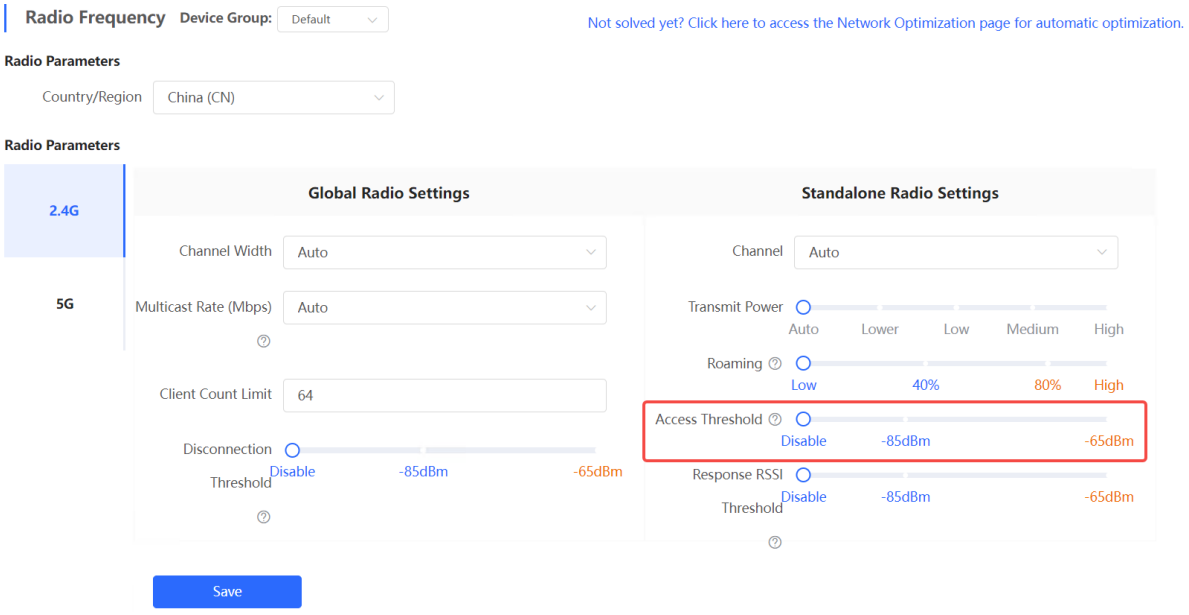
The roaming sensitivity enables the device to actively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving the sensitivity of wireless roaming. Higher the roaming sensitivity level, smaller the wireless signal coverage. 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**.



2.14.10 Configuring the Access Threshold

- Primary device: Choose **WLAN** > **Radio Frequency**.
- Secondary device: Choose **WLAN** > **APs**. Select the target device in the device list and click **Manage** > **WLAN** > **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**.

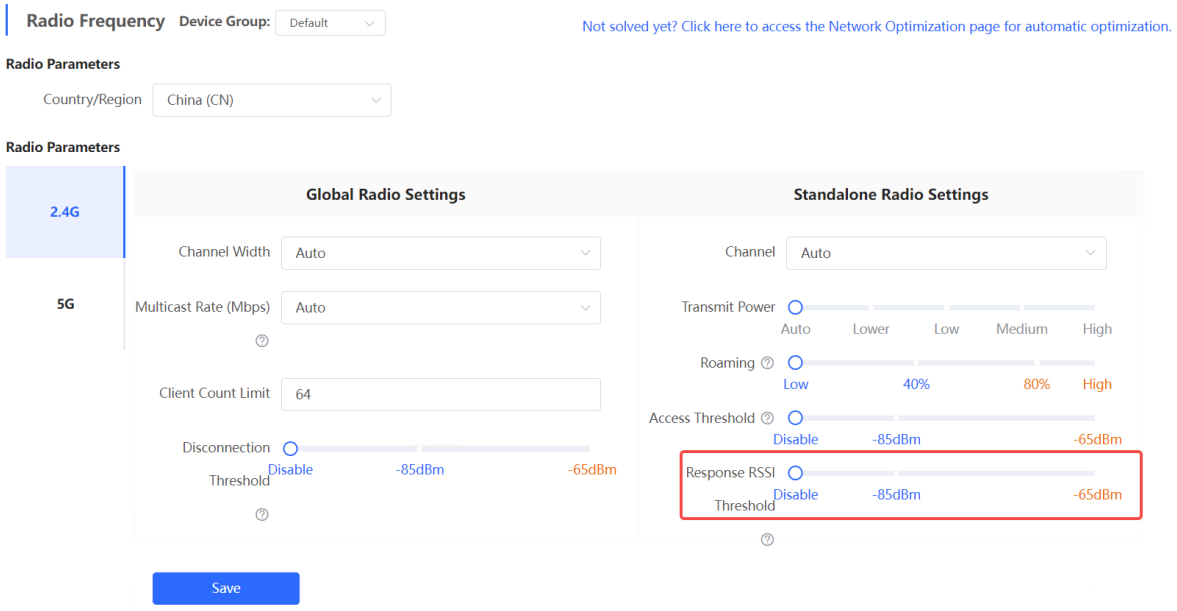


2.14.11 Configuring the Response RSSI Threshold

- Primary device: Choose **WLAN** > **Radio Frequency**.
- Secondary device: Choose **WLAN** > **APs.** Select the target device in the device list and click **Manage** >

WLAN > **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**.



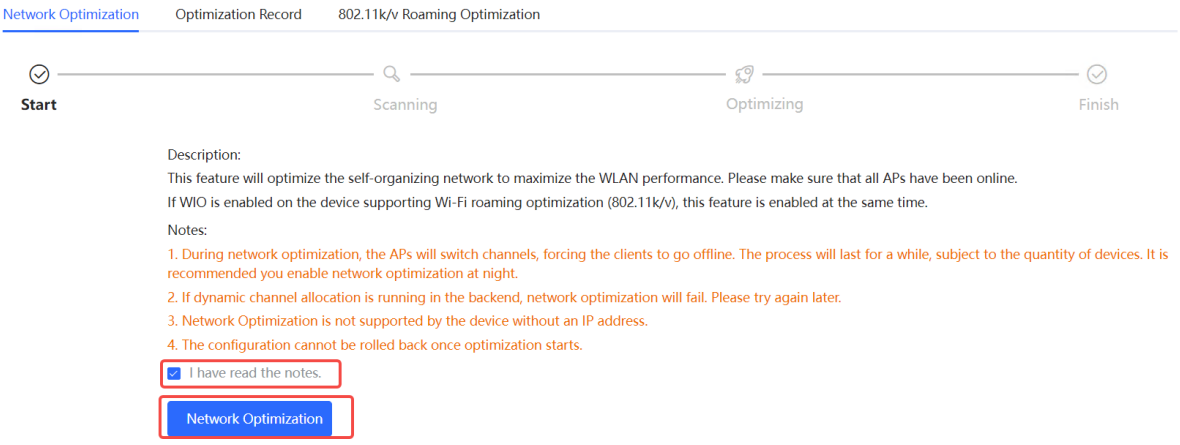
2.14.12 Configuring WIO

Choose **WLAN** > **WIO**.

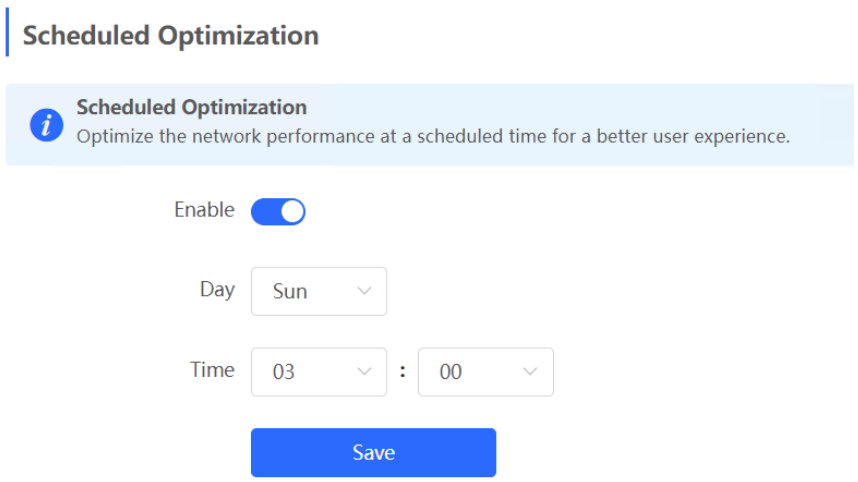
Click **I have read the notes.** And then click **Network Optimization** to optimize the wireless network.

Caution

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



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.



2.14.13 Configuring K/V Roaming Optimization

Go to the configuration page: Choose **Network** > **WIO** > **802.11k/v Roaming Optimization**.

Select the optimization mode, and then click **Enable**. The Wi-Fi roaming is further optimized using the 802.11k/v protocol. 802.11k/v-compliant smart clients can switch to 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 automatically scanned when this function is enabled for the first time.

Caution

- This function is only supported in SON mode.
- During the WLAN environment scanning, APs on the WLAN will switch channels, forcing the clients to go offline. The process may last for about 2 minutes.

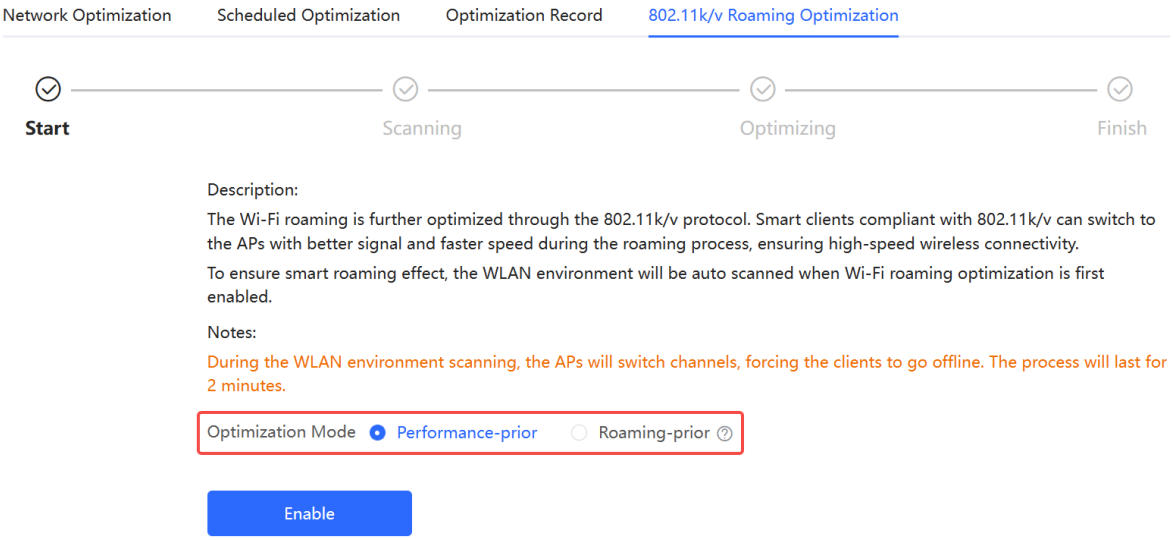
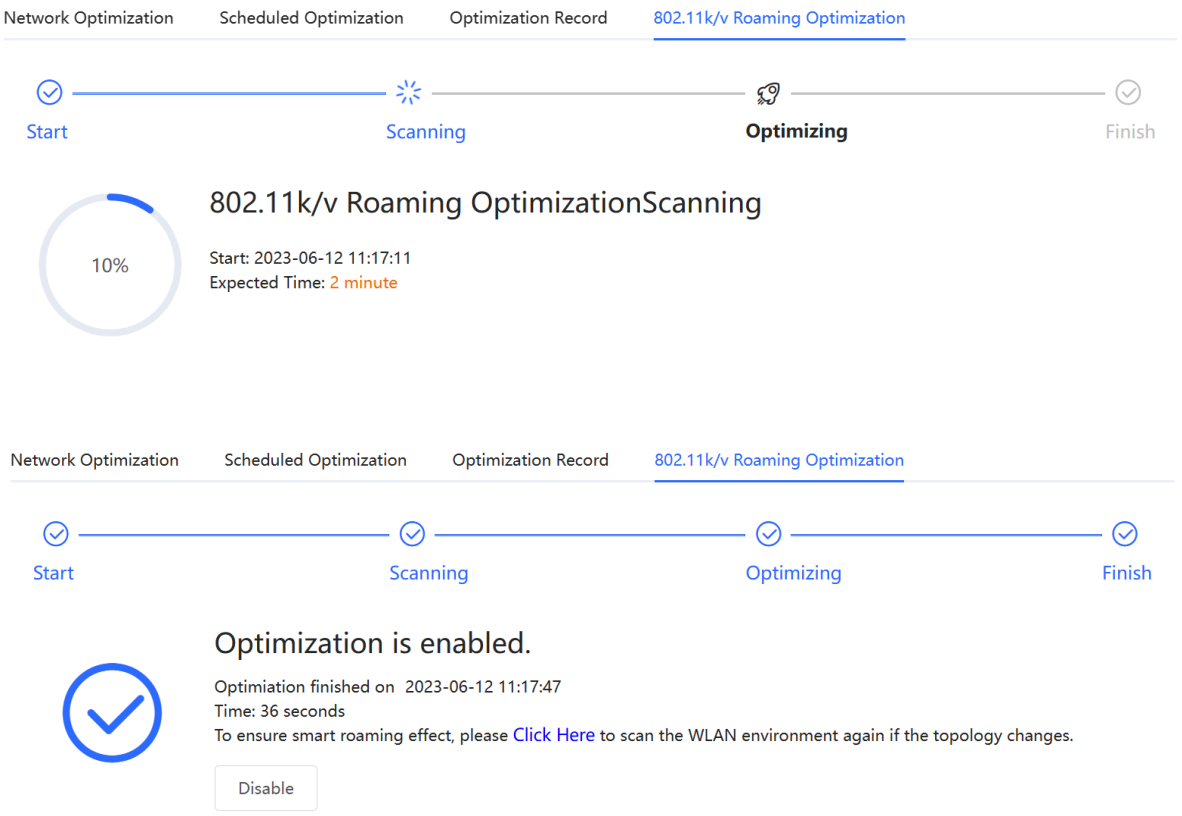


Table 2-3 Optimization Mode Parameters

Parameter	Description
Performance-prior	Maximum negotiation speed is guaranteed, but connection stability may be compromised.
Roaming-prior	Connection stability is guaranteed, but maximum negotiation speed may be reduced.

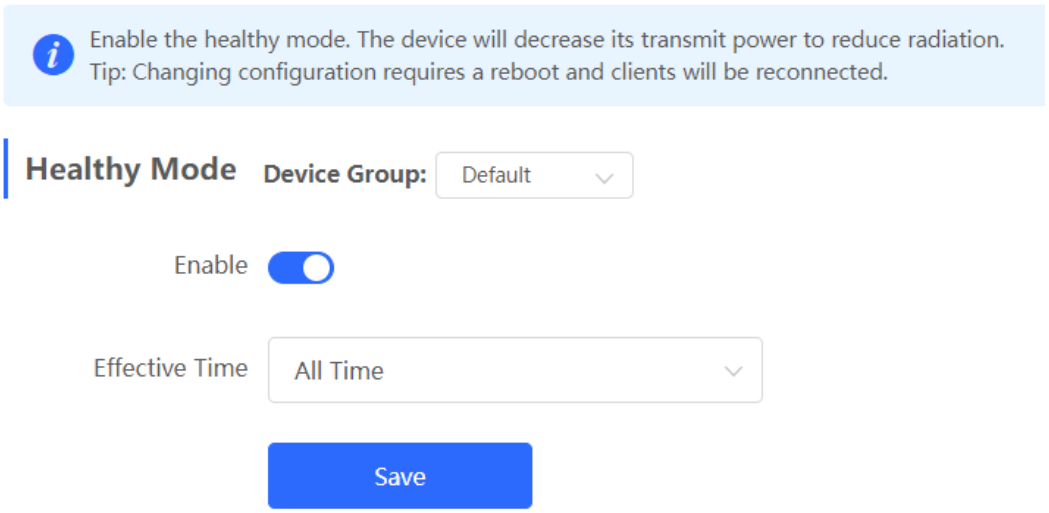


2.15 Configuring Healthy Mode

Choose **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.

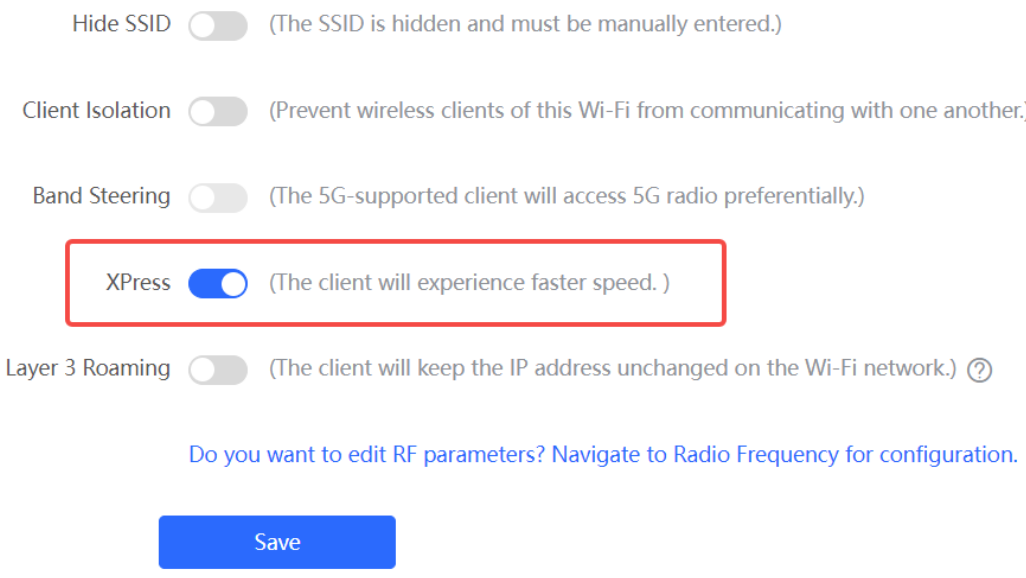


2.16 Configuring XPress

(1) Go to the configuration page:

- Method 1: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **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 **XPress** in the expanded settings and click **Save**. After XPress is enabled, the gaming traffic will be prioritized, ensuring a more stable gaming experience.



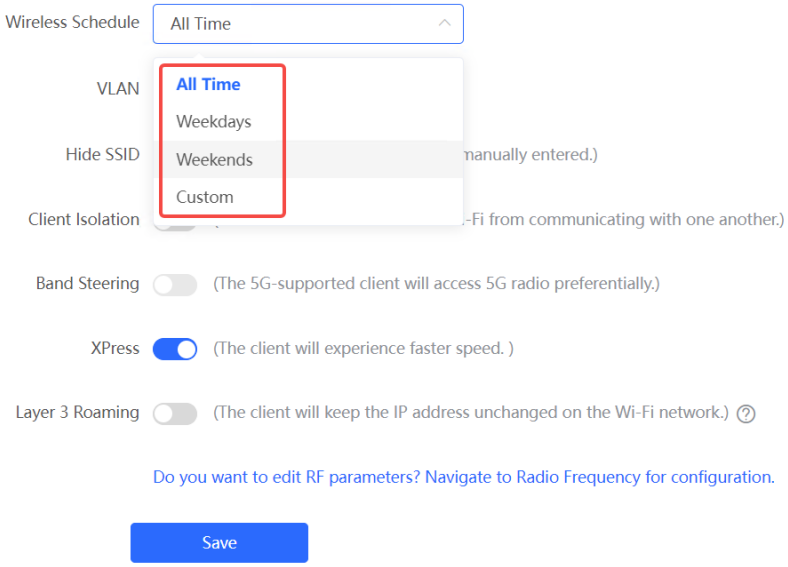
2.17 Configuring Wireless Schedule

(1) Go to the configuration page:

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

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

(2) 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.



3 Network Settings

Note

This chapter takes the currently logged in device as an example to describe the entry of each function setting page. If you need to configure other devices in the network, please refer to the following path to enter the configuration page of the corresponding device, and then configure the function. Choose **WLAN** > **APs.** Select the target device in the device list and click **Manage**.

3.1 Switching Work Mode

3.1.1 Work Mode

See 1.3 Work Modes for details.

3.1.2 Self-Organizing Network Discovery

You can set whether to enable the self-organizing network discovery function. This function is enabled by default.

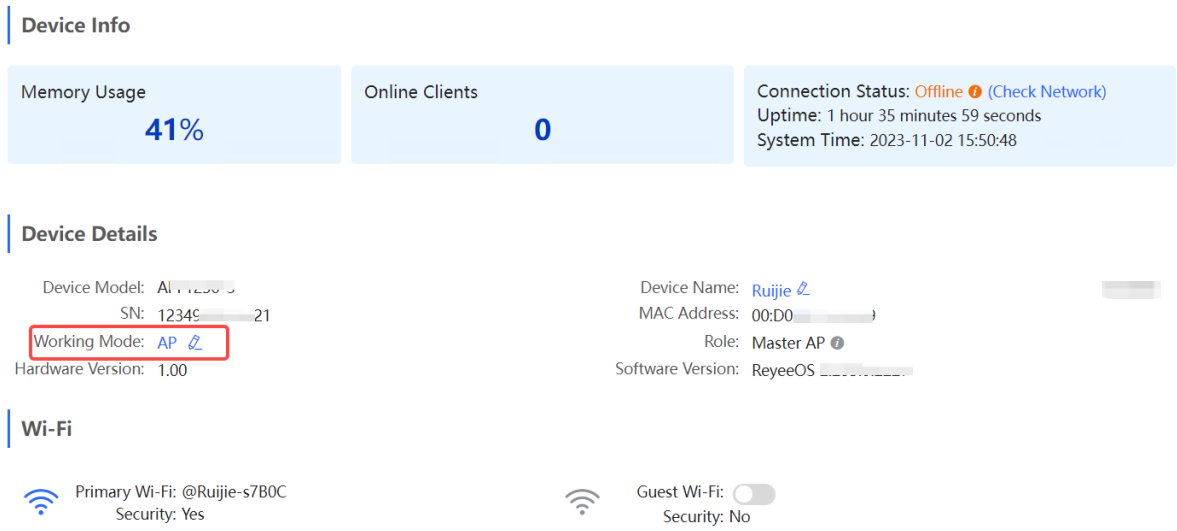
After the self-organizing network discovery function is enabled, the device can be discovered in the network and discover other devices in the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the web interface of any device in 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 **WLAN** > **APs** > **Manage > Device Overview** > **Device Info.**

Click the current work mode to change the work mode.



3.1.4 Viewing Device Role

Choose **WLAN** > **APs** > **Manage > Device Overview** > **Device Info**.

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

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

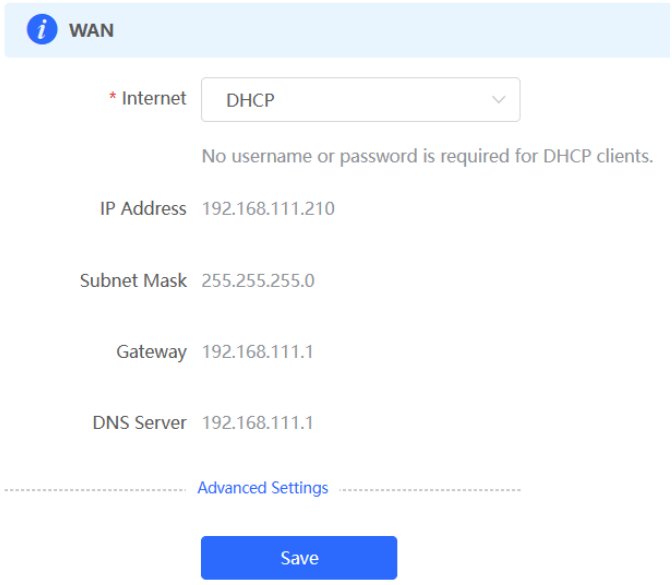
Secondary AP/Device: The device has been managed by an AC. The secondary APs are managed by the primary AP/AC in a unified manner. Some wireless network settings cannot be edited alone, and thus the primary AP/AC delivers configurations to edit the network settings in a unified manner.



3.2 Configuring the Internet Connection Type (IPv4)

Choose **WLAN** > **APs** > **Manage > Network** > **WAN** > **WAN**.

Select the Internet connection type after confirming with the ISP. After completing the configuration, click **Save**.



The device supports the following Internet connection types:

- 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.

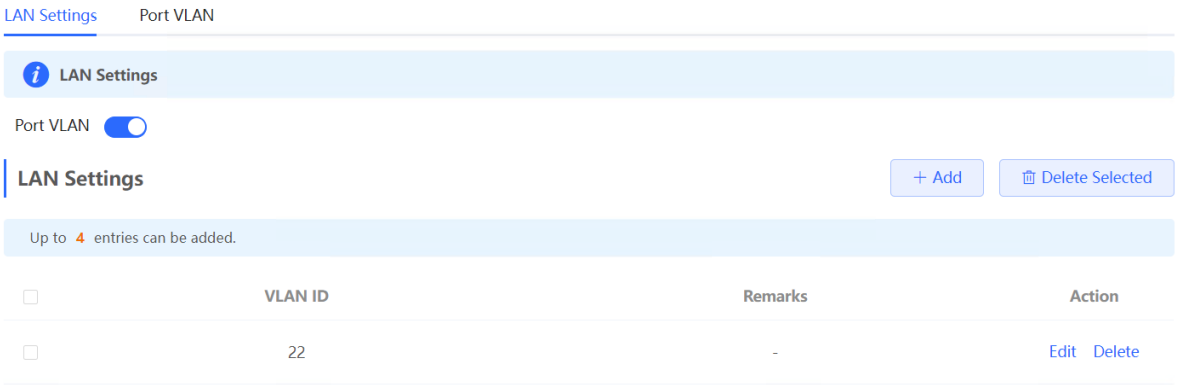
3.3 Configuring Port VLAN

Caution

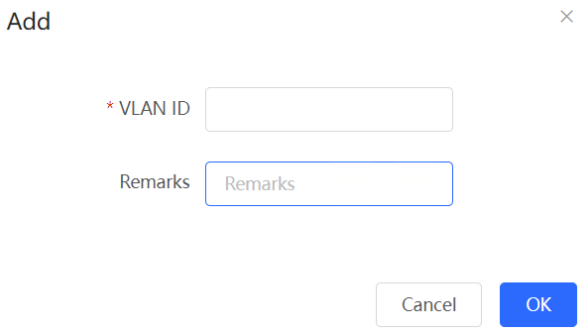
The port VLAN can be configured only when the device works in AP mode.

Choose **WLAN** > **APs** > **Manage > Network** > **LAN**.

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

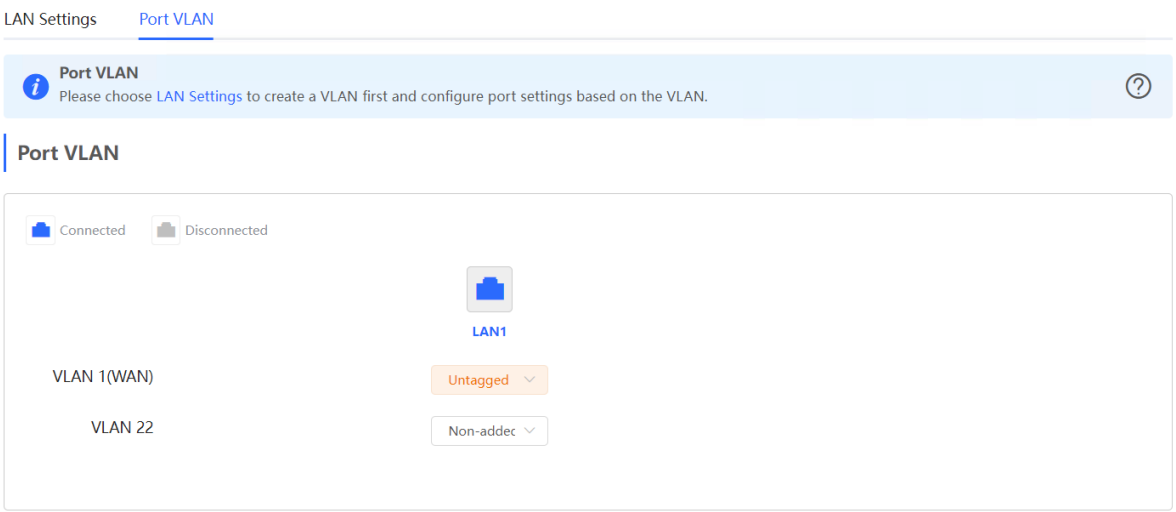


(2) Click Add. Enter the VLAN ID and description, and click OK to create a VLAN. The added VLAN is used to set the VLAN, to which a port belongs.



(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.



3.4 Changing the MAC Address

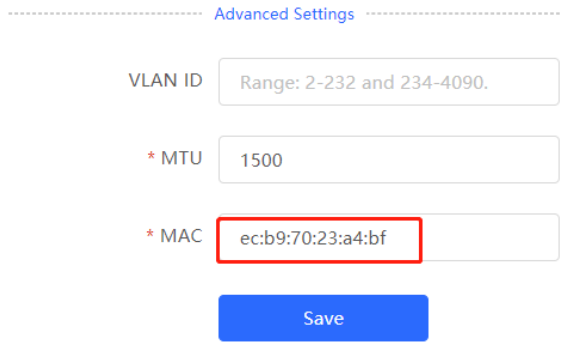
Choose **WLAN** > **APs** > **Manage > Network** > **WAN** > **WAN**.

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.

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. Exercise caution when performing this operation.

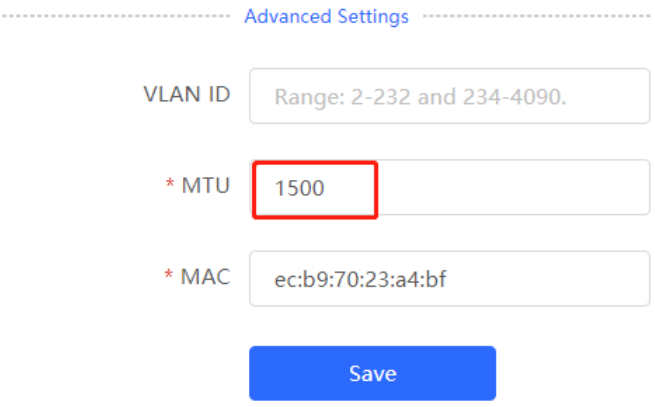


3.5 Changing the MTU

Choose **WLAN** > **APs** > **Manage > Network** > **WAN** > **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.

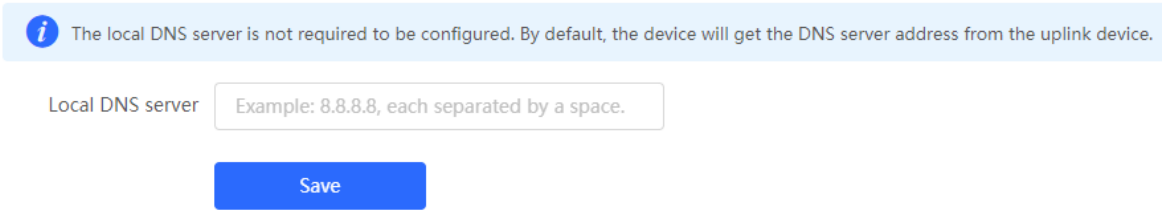
Click **Advanced Settings** to expand the configuration items, enter the MTU value, and click **Save**.



3.6 Configuring DNS

Choose **WLAN** > **APs** > **Manage** > **Advanced** > **Local DNS**.

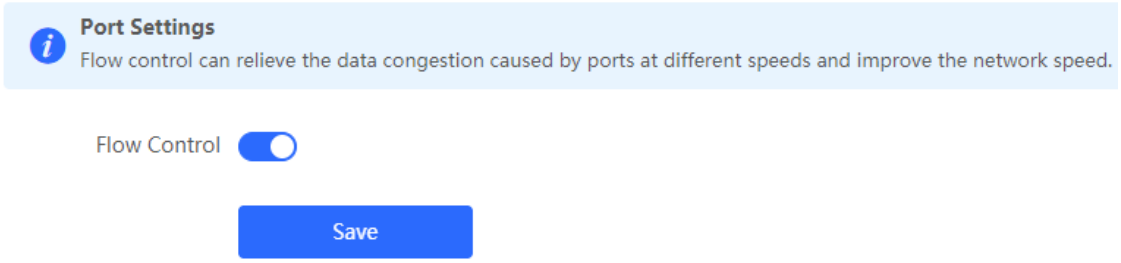
Enter the IP address of the DNS server and click Save. The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default. The default configuration is recommended. The available DNS service varies from region to region. You can consult the local ISP.



3.7 Configuring Port Flow Control

Choose **WLAN** > **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.



3.8 Configuring the AP LAN Port

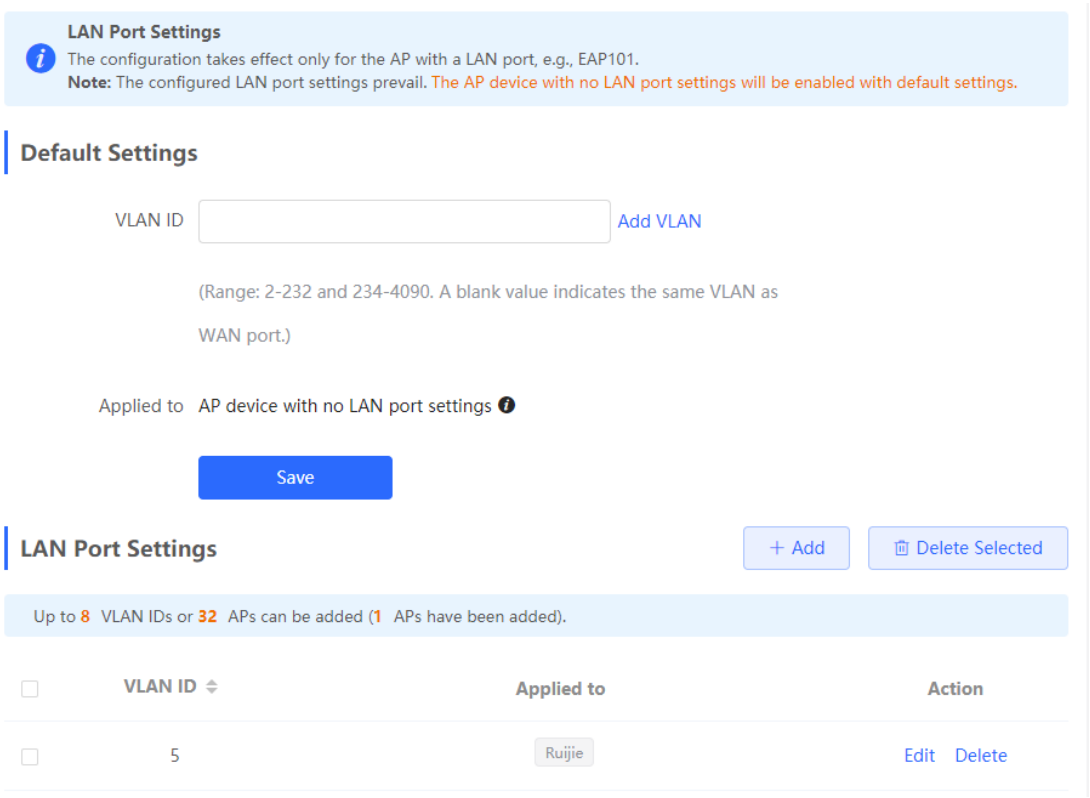
Caution

This configuration takes effect only on APs with a LAN port.

Choose **WLAN** > **LAN Port** (**LAN Port Settings**).

Enter the VLAN ID and click **Save** to set the VLAN to which the wired port of the AP belongs. If the VLAN ID is empty, it indicates the wired port 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 default configuration of the AP wired port will take effect if the configuration is not applied to the AP in the AP wired port configuration list. You can click **Add** to add a configuration to the AP wired port configuration list.



3.9 Configuring the Optical Transceiver

Choose **WLAN** > **APs** > **Manage** > **Network** > **Optical Transceiver Info**.

The **Optical Transceiver Info** page displays the optical port connection status of the device.

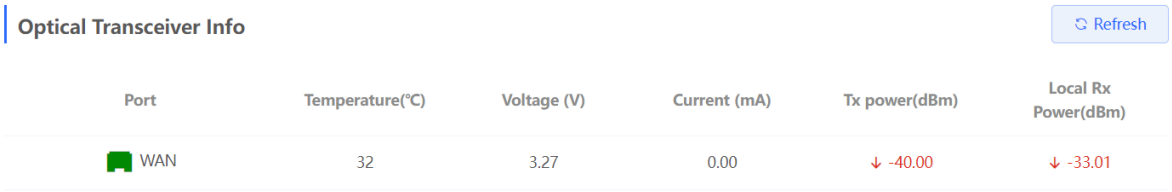


Table 3-1 Optical Transceiver Parameters

Parameter	Description
Temperature (°C)	Current working temperature of the optical transceiver.
Voltage (V)	Current working voltage of the optical transceiver.
Current (mA)	Current of the optical transceiver.
Tx Power (dBm)	Power of the optical signal sent by the optical transceiver.
Local Rx Power (dBm)	Power of the optical signal received by the optical transceiver, which indicates the quality of the optical signal

Parameter	Description
	sent to the device.

3.10 Configuring VoIP

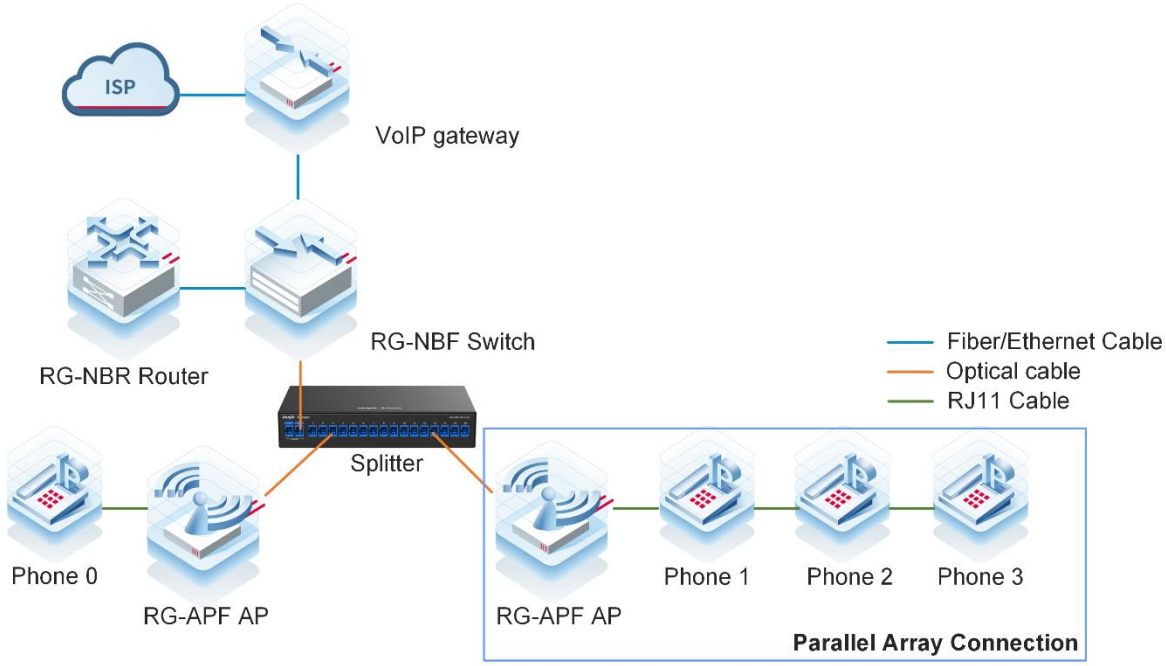
3.10.1 Overview

Traditional hotel room phone systems usually require dedicated phone lines and devices, which need regular maintenance and are costly. When adding rooms or functions, the traditional guest room telephone system requires additional telephone lines and devices to meet the new demand, which increases the complexity of deployment and costs, and cannot meet the needs of modern hotels for diversified communication functions, scalability, and cost-effectiveness.

Voice over Internet Protocol (VoIP) compresses voice signals using compression algorithms and packages them into IP packets for transmission on the Internet. VoIP reduces communication costs and provides rich functions, such as call forwarding, voice mail, and multimedia communication, to enhance the customer experience.

With Reyee VoIP gateway and Ruijie Reyee App or Ruijie Cloud, VoIP system construction and quick deployment and acceptance can be achieved in hotels and apartments.

Figure 3-1 VoIP Network Architecture



Parallel Array Connection

On a VoIP network, the RG-APF series supports parallel array connection for connecting VoIP phones. This means that multiple VoIP phones (up to three) can be connected to the SC port of an RG-APF access point. The parallel array connection is shown in Figure 3-1.

A user can use a VoIP phone connected to the same RG-APF access point in parallel array connection to make voice calls to another VoIP phone connected to another RG-APF access point. For example, phones 1, 2, and

3 can receive calls from phone 0 at the same time. The phones connected in parallel arrays can also communicate with each other during a voice call. That is, phones 1, 2, and 3 can communicate with each other during a voice call to voice phone 0.

3.10.2 Prerequisites

Caution

- On a VoIP network, an SIP-compliant VoIP gateway must be used as the SIP server.
- An RG-APF access point supports the SIP protocol, which is compatible with most VoIP gateways.
- The name of the RG-APF access point must be used as the extension number.

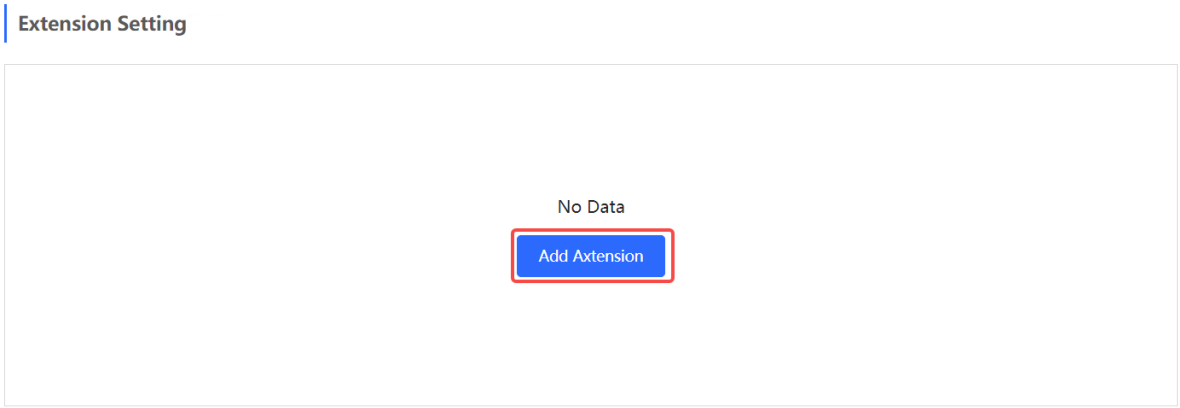
You can connect a VoIP phone to the phone port of the RG-APF access point. Each RG-APF access point is registered with the VoIP gateway through the network using the SIP protocol for interconnection of internal phones. A VoIP gateway connects a public switched telephone network (PSTN) to an IP network to implement VoIP communication. A Reyee VoIP gateway can be automatically connected to the cloud management platform for VoIP configuration.

Before configuring the VoIP service, ensure that each AP in the hotel is named uniquely. Otherwise, automatic registration of the extension number will be affected. You are advised to name the APs according to the room number. For example, the AP in room 303 is named '303'. When multiple APs exist in a room, a suffix should be added. For example, if there are two APs in room 101, they are named 101_1 and 101_2.

3.10.3 Configuration Steps

Choose **WLAN** > **APs** > **Manage** > **Network** > **Extension Setting**.

Click **Add Extension** on the **Extension Setting** page, enter the phone information, and click **OK**.



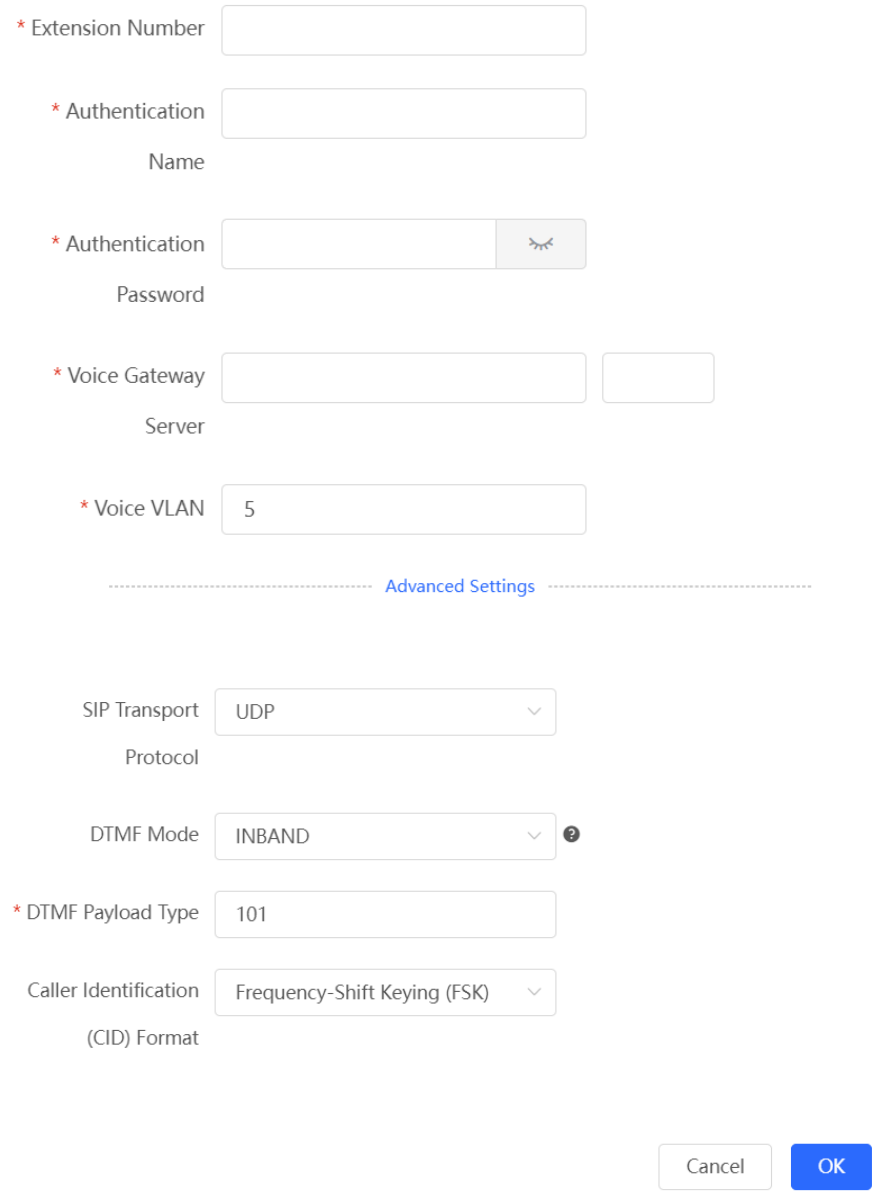


Table 3-2 Extension Configuration Parameters

Parameter	Description
Extension Number	Extension number. Each extension is assigned a unique extension number.
Authentication Name	Authentication ID. The authentication name can be the same as the extension number or set in a project.
Authentication Password	Authentication password. The password must contain at least six characters and cannot be the same as the authentication name.

Parameter	Description
Voice Gateway Server	IP address (or domain name) and port number of the voice gateway server
Voice VLAN	VLAN ID for voice service (Range: 2–4094)
SIP Transport Protocol	Ensure that SIP messages are transmitted correctly across the network by choosing the right transmission protocol, either UDP or TCP: ● UDP: Suitable for most real-time interactive communications, such as voice calls. ● TCP: Suitable for transmitting SIP control messages in unstable network environments or when higher reliability is required.
DTMF Mode	Different modes for transmitting DTMF signals. ● INBAND: DTMF signals are mixed with the audio stream for transmission. ● RFC2833: DTMF signals are separately transmitted as special RTP event packets. ● SIP INFO: DTMF signals are separately transmitted in SIP INFO messages.
DTMF Payload Type	The encapsulation method for transmitting special data packets in VoIP. The default value is 101, with a value range of 96 to 127.
Caller Identification (CID) Format	The transmission method for call identification information on the phone. ● Frequency-Shift Keying (FSK): Transmit information in the ASCII character set. ● Dual-Tone Multi-Frequency (DTMF): Transmit numbers from 0 to 9 and a few characters, including #, *, A, B, C, and D.

After an extension is added, you can view the extension information on the **Extension Setting** page.

4 System Settings

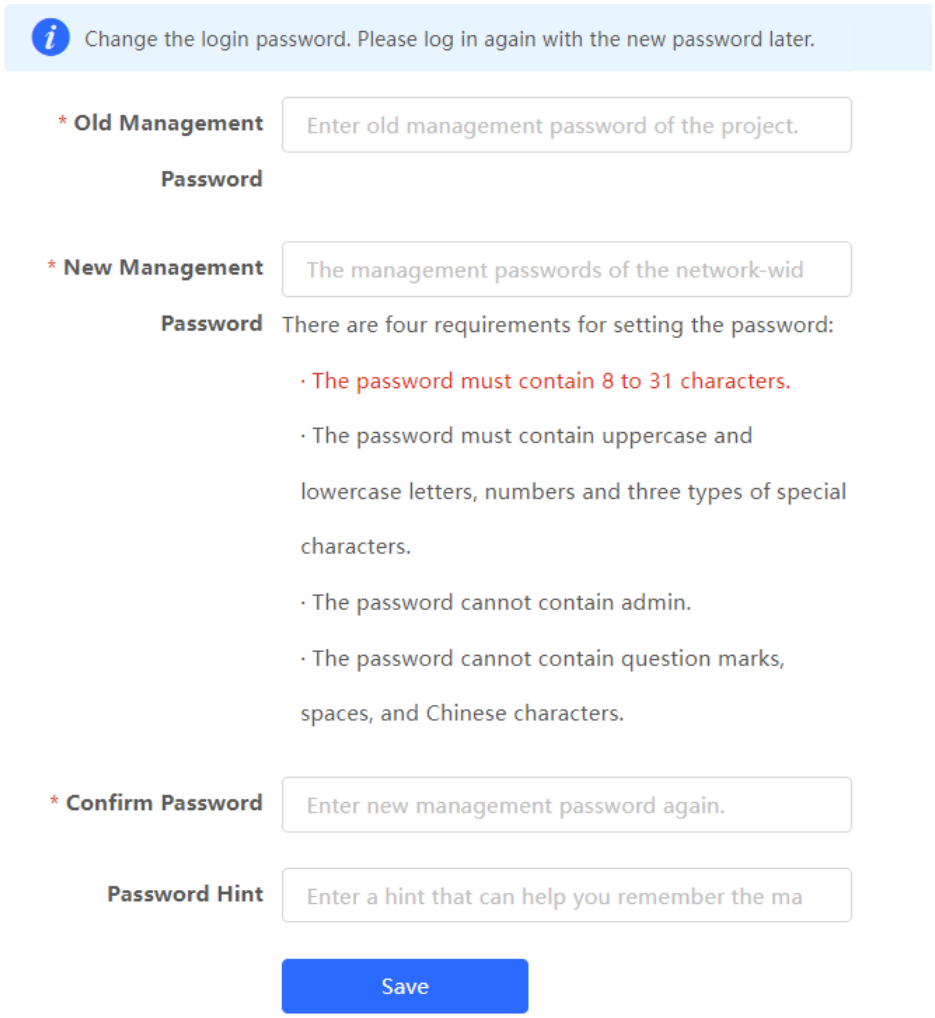
4.1 Setting the Login Password

- SON mode: Choose **Network** > **Password**.
- 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.

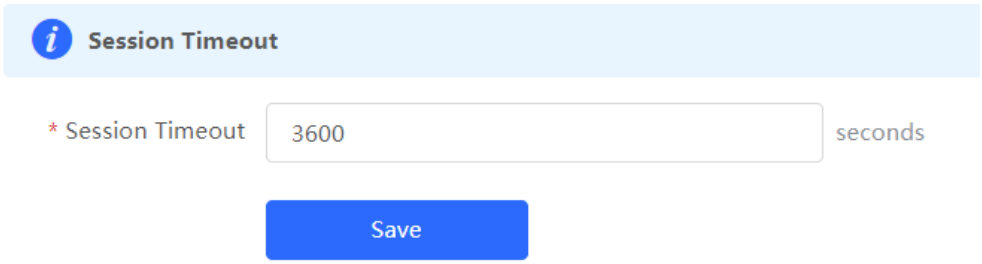


4.2 Setting the Session Timeout Duration

- SON mode: Choose **WLAN** > **APs** > **Manage** > **System** > **Login** > **Session Timeout**.

- Standalone mode: Choose **System** > **Login** > **Session Timeout**.

If no operation is performed on the Web interface 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.



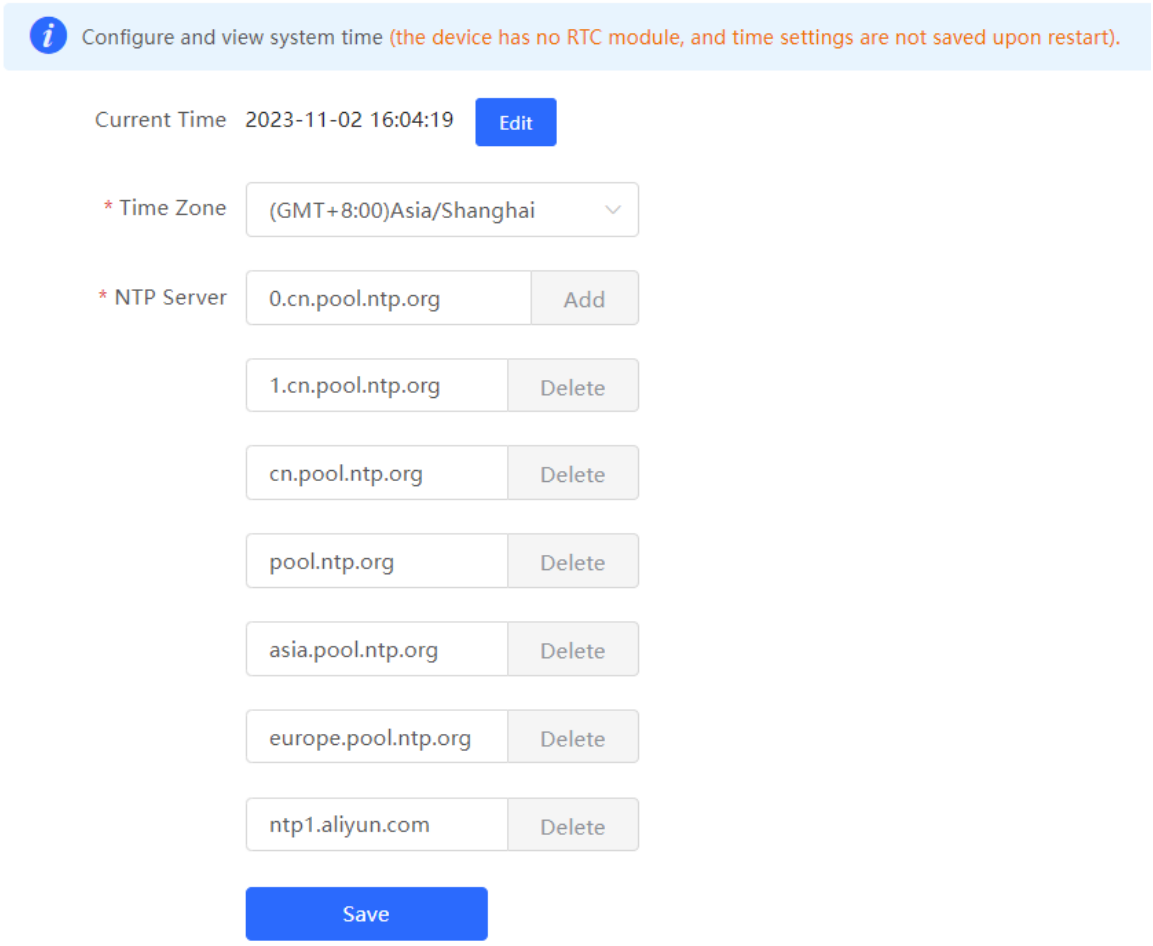
4.3 Setting and Displaying System Time

- SON mode: Choose **Network** > **Time**.
- 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.



4.4 Configuring Reboot

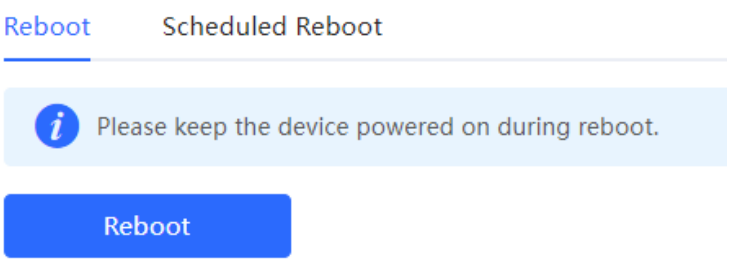
Caution

- 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. Exercise caution when performing this operation.

4.4.1 Rebooting the Current Device

SON mode: Choose **WLAN** > **APs** > **Manage** > **System** > **Reboot.**

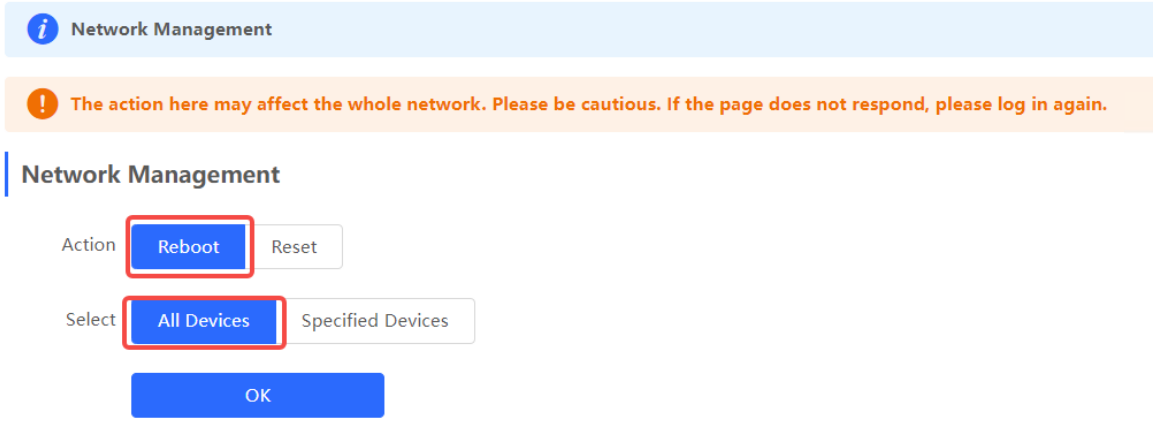
Standalone mode: Choose **System** > **Reboot** > **Reboot.** Click **Reboot**. The device will restart.



4.4.2 Rebooting All Devices on the Network

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

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



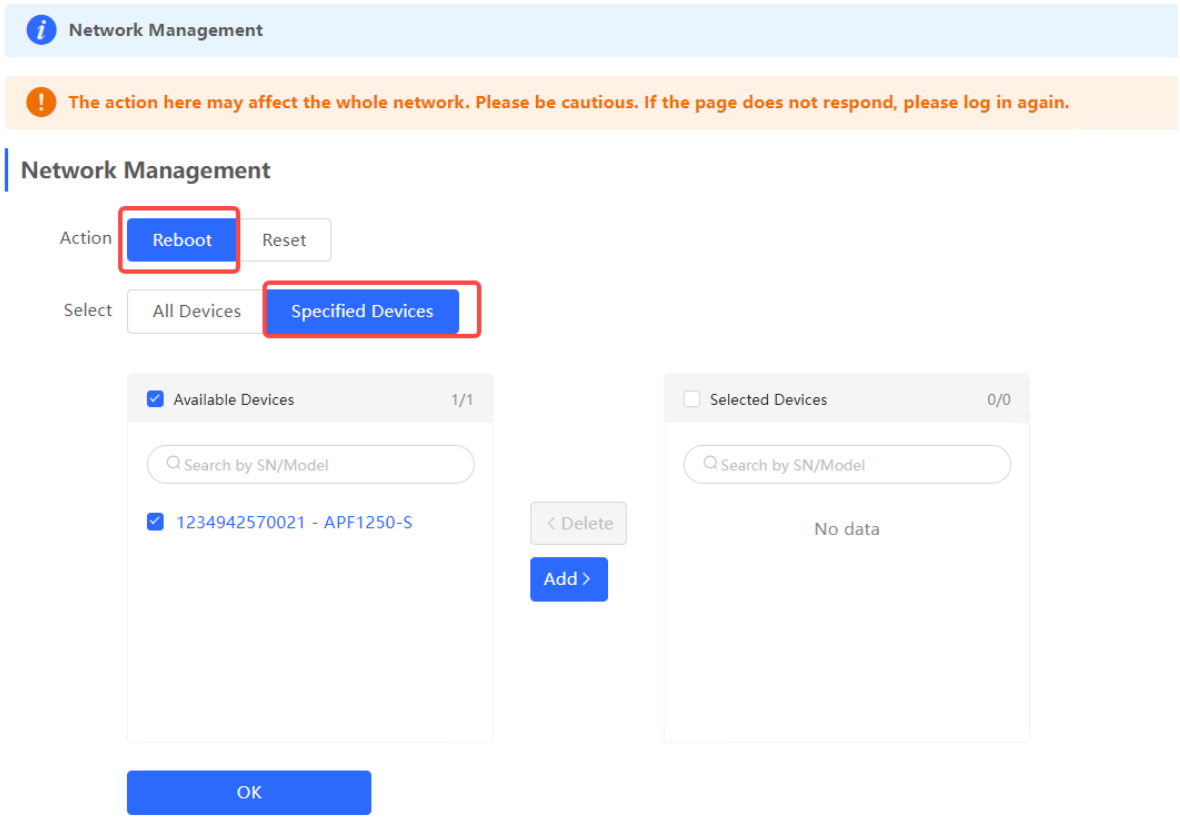
Caution

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

4.4.3 Rebooting the Specified Device

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

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.



4.5 Configuring Scheduled Reboot

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 4.3 Setting and Displaying System Time.

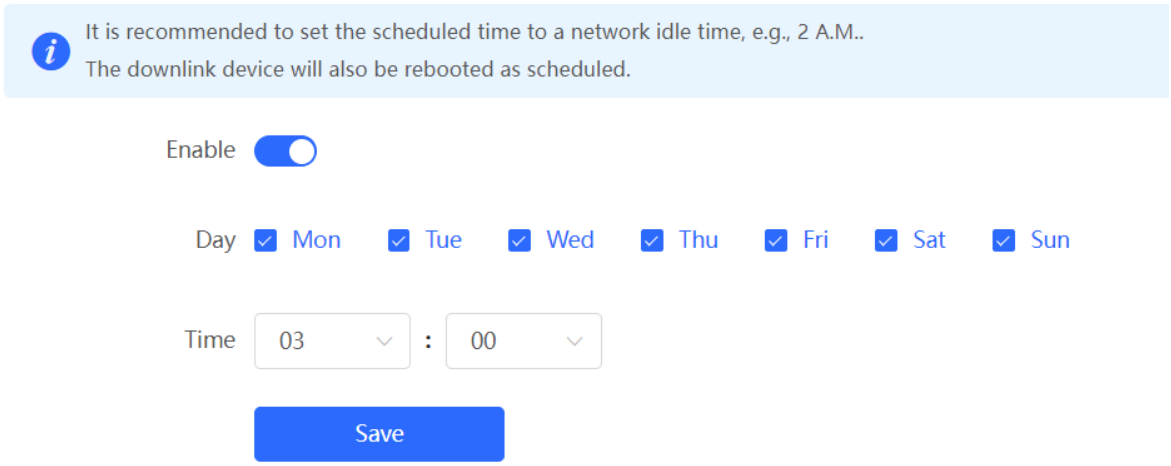
To configure scheduled reboot for the current device, choose **Network** > **Scheduled Reboot**.

To configure scheduled reboot for all devices in the network, choose **System** > **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.

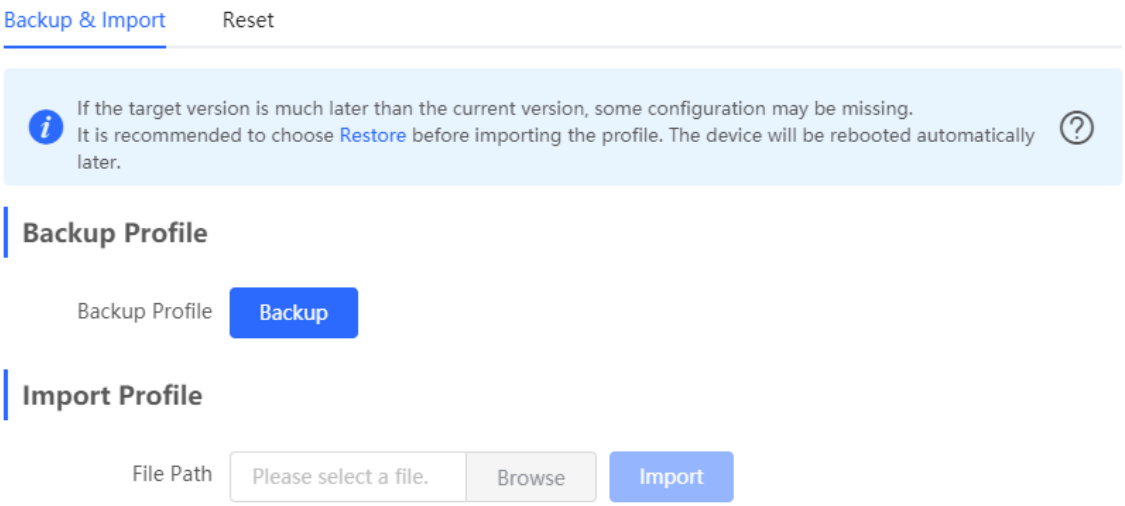


4.6 Configuring Backup and Import

Choose **WLAN** > **APs** > **Manage** > **System** > **Backup** > **Backup & Import**.

Configuration backup: Click **Backup** to generate a backup configuration and download the configuration file to the local device.

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

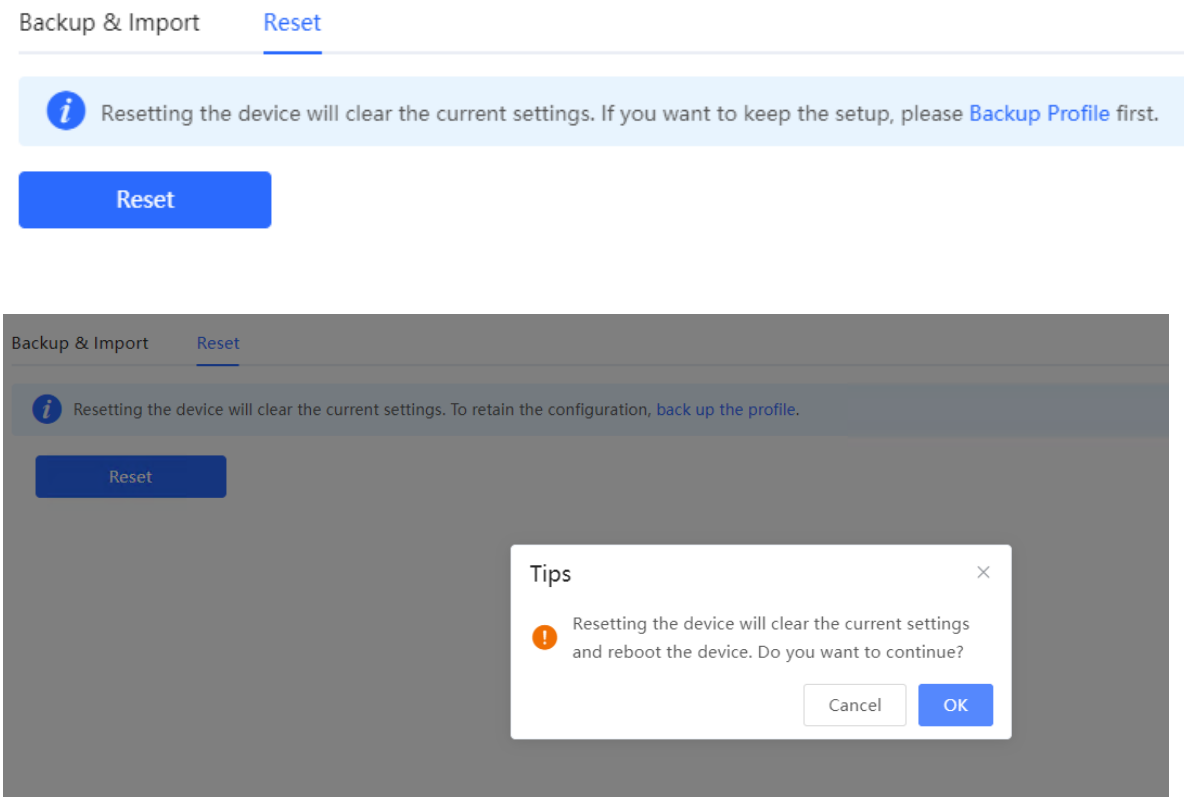


4.7 Restoring Factory Settings

4.7.1 Restoring the Current Device to Factory Settings

Choose **WLAN** > **APs** > **Manage** > **System** > **Backup** > **Reset**.

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



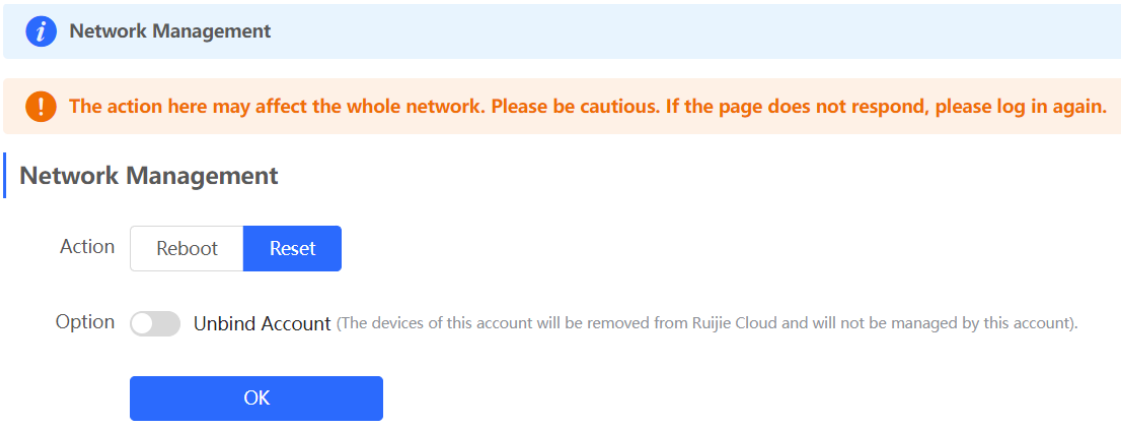
Caution

This operation will all configuration of the current device and restart the device. If you want to retain the current configuration, back up the configuration first (see 4.6 Configuring Backup and Import). Exercise caution when performing this operation.

4.7.2 Restoring All Devices to Factory Settings

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

Select **Reset** and click **OK**. All devices on the current network will be restored to factory settings.



Caution

This operation will clear all existing settings of all devices on the network and restart the devices. Exercise caution when performing this operation.

4.8 Checking the System Version and Performing System Upgrade

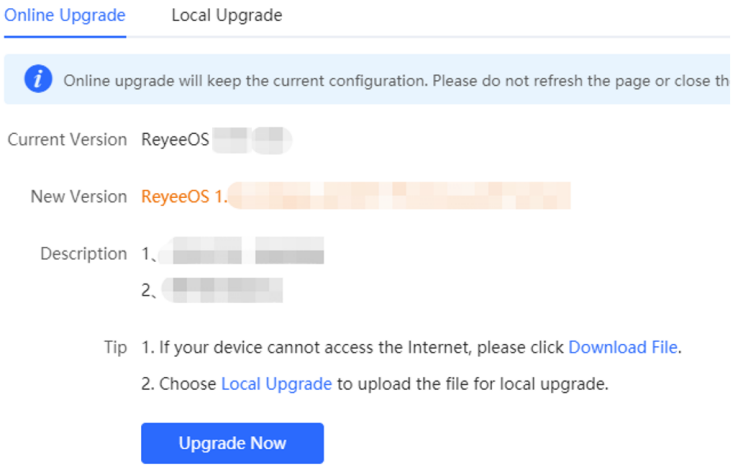
Caution

- You are advised to back up the configuration before performing software upgrade.
- Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.

4.8.1 Online Upgrade

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

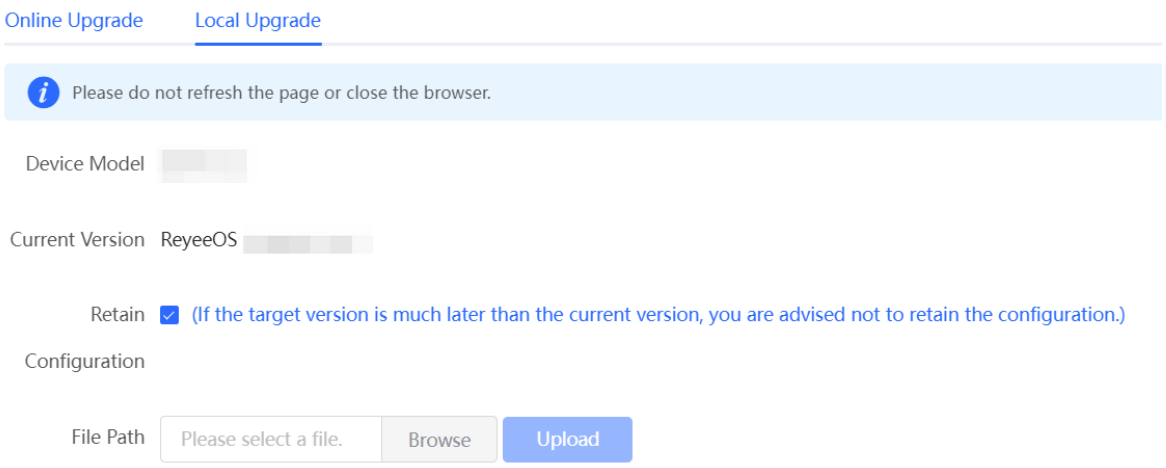
The current page displays the current system version and allows you to detect whether a later version is available. If a version update is detected, click **Upgrade Now** to perform online update. If the network environment does not support online upgrade, click **Download File** to download the upgrade package locally and then perform local upgrade.



4.8.2 Local Upgrade

Choose **WLAN** > **APs** > **Manage** > **System** > **Upgrade** > **Local Upgrade**.

The device model and current software version are displayed. You can choose whether to retain the configuration for upgrade. Click **Browse** to select a local software package, and click **Upload** to upload the package.



4.9 Switching System Language

Choose English in the upper right corner of the Web page.

Click a language in the drop-down list as the language of the web interface.



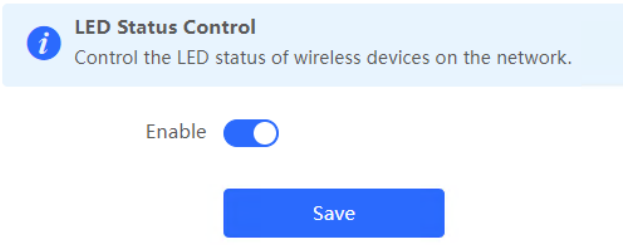
4.10 Configuring LED Status Control

Caution

In standalone mode (when the self-organizing network discovery function is disabled), the LED Status Control function cannot be enabled.

Choose **WLAN** > **LED**.

Enable or disable the system status LED of all downlink APs on the current network.



5 Network Diagnosis Tools

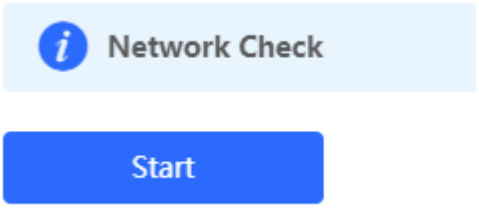
5.1 Network Check

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

(1) Click the icon on the right of the navigation bar or choose **Diagnostics** > **Network Check** and go to the **Network Check** page.

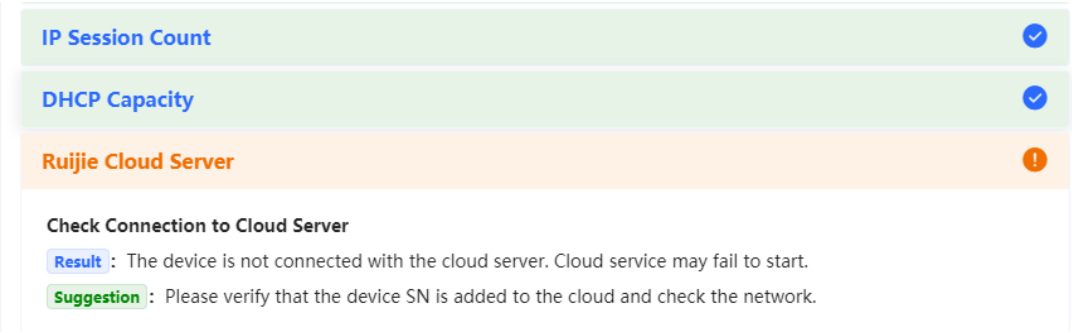


(2) Click **Start** to run the network check. The test result will be displayed.





(3) If a network problem is detected, the detection result and handling suggestions are displayed. You can refer to the suggestions to troubleshoot the fault.

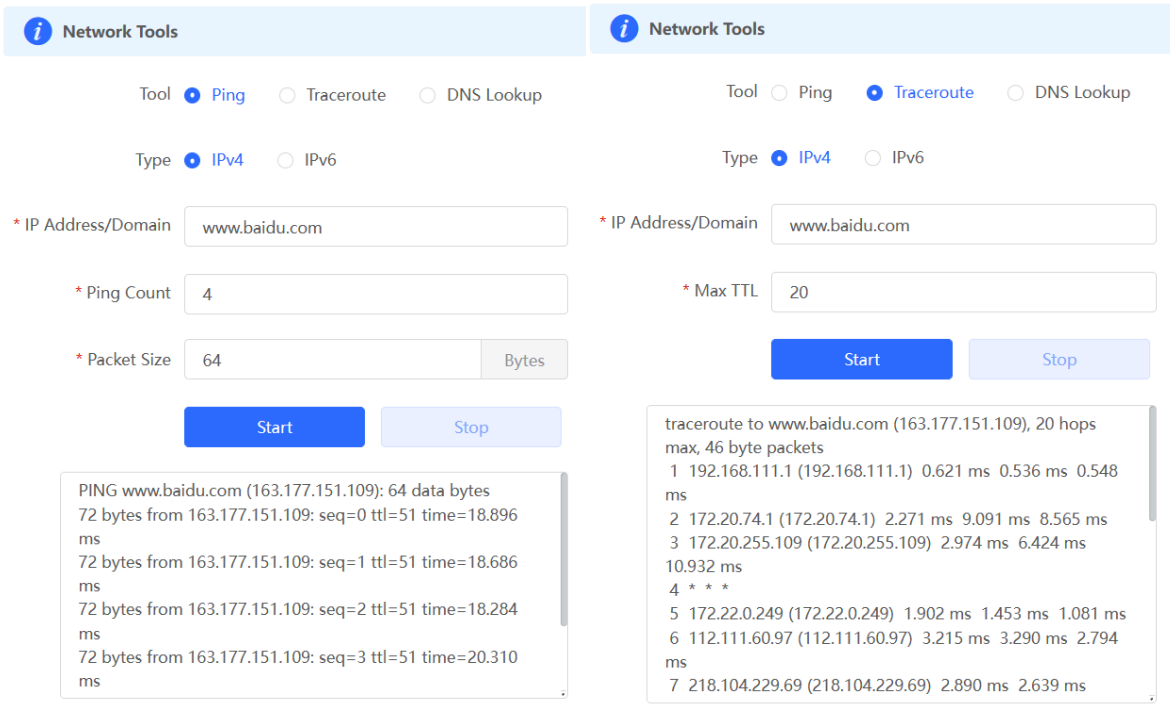


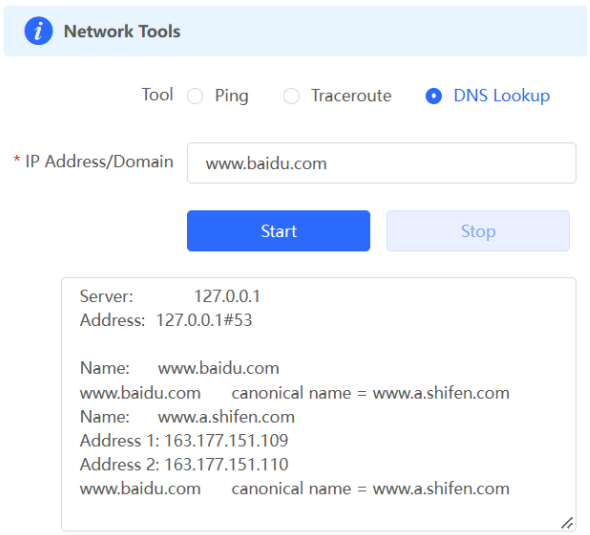
5.2 Network Tools

Choose **WLAN** > **APs** > **Manage** > **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.





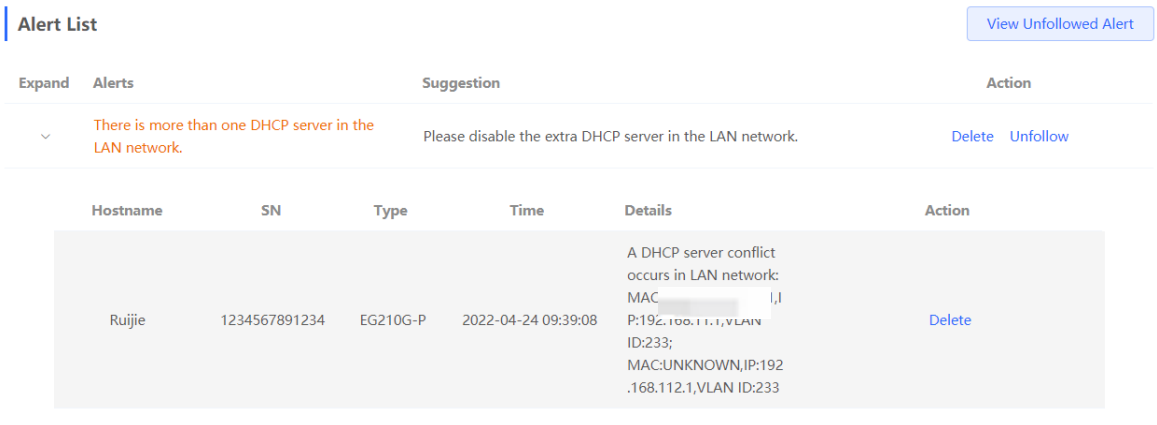
5.3 Alerts

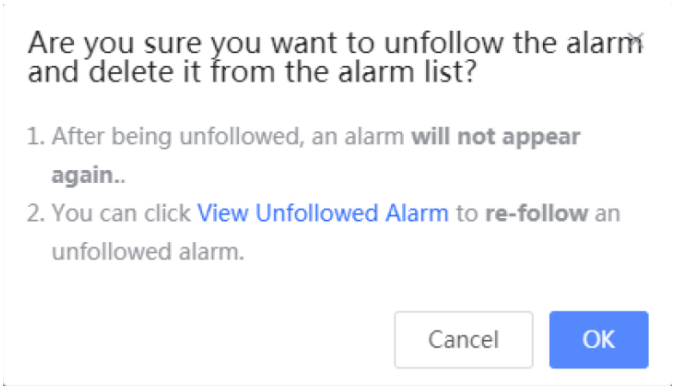
Choose **WLAN** > **APs** > **Manage** > **Diagnostics** > **Alarms**.

The **Alert List** 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 a type of alarm.

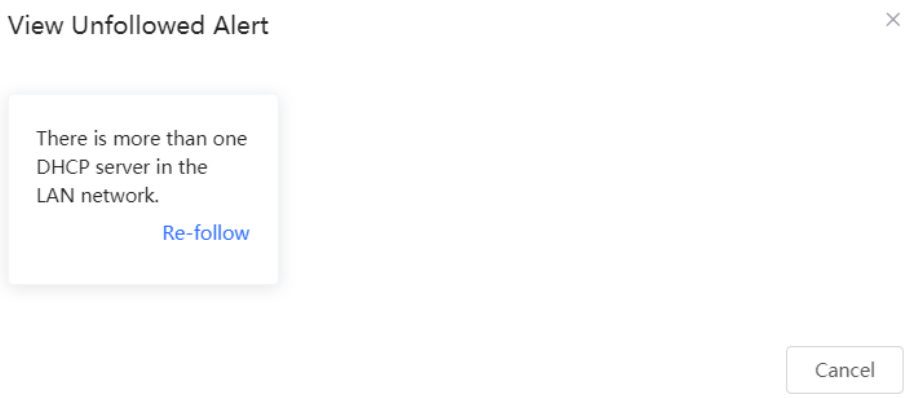
Caution

After a type of alarm is unfollowed, all alarms of this type will not be displayed. Exercise caution when performing this operation.





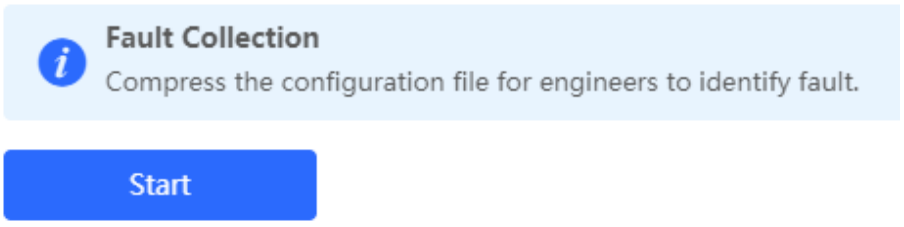
Click **View Unfollowed Alarm** to view the unfollowed alarm. You can follow the alarm again by clicking **Re-follow** in the pop-up window.



5.4 Fault Collection

Choose **WLAN** > **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 the fault.



Note

If the preceding troubleshooting steps fail to resolve the issue, and remote assistance from technical support is needed, you can contact them to assist in enabling the developer mode. The technical support team can then perform diagnostics to identify and address the issue effectively.

6 FAQs

6.1 Fail to Log In to the Web Interface

(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.

6.2 Restore 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 web interface using the default IP address (10.44.77.254).

6.3 Forgot Password

- Forgot the management password of the web interface: You can try to log in with the Wi-Fi password. If the error still persist, restore the device to factory settings.
- Forgot Wi-Fi password: When the AP extends the signal of another router, the Wi-Fi password is often the same as that of the primary router. You can check the configuration of the primary router. If the Wi-Fi password of the primary router is incorrect, you can restore the device to factory settings and reconfigure the password.