Ruijie RG-RAP72-Wall Access Point

Implementation Cookbook

Document Version: V1.0

Date: October 29, 2024

Copyright

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding 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 is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained 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

- Ruijie Networks website: https://www.ruijienetworks.com/
- Online support center: https://ruijienetworks.com/support
- Case portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Email support: service_rj@ruijienetworks.com
- Live chat: https://www.ruijienetworks.com/rita
- Documentation feedback: doc@ruijie.com.cn

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

3. Note

The manual offers configuration information (including model, description, port type, software interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Overview

This cookbook consists of multiple independent volumes, introducing the installation, deployment, and web-based configuration of the RG-RAP72-Wall Access Point, including:

01- Installation Guide

02- OS 2.301 Configuration Guide

Contents

1 Overview

1.1 About the RG-RAP72-Wall

The RG-RAP72-Wall is a Gigabit dual-band wall-plate access point (AP) designed for small- or medium-sized indoor scenarios covering hotels, apartments, villas, residential buildings, and small offices.

Compliant with IEEE 802.11be, IEEE 802.11ax, IEEE 802.11ac Wave 1/Wave 2, IEEE 802.11a/b/g/n protocols, this AP can operate at 2.4 GHz and 5 GHz frequency bands simultaneously. It supports the MU-MIMO dual-stream technology and provides an access rate of 688 Mbps at 2.4 GHz and 2882 Mbps at 5 GHz, achieving a maximum wireless data rate of 3570 Mbps. It also provides four 1 Gigabit Ethernet ports for wired connection, catering to the indoor wired and wireless dual-gigabit deployment requirements.

The RG-RAP72-Wall can be mounted in junction boxes of various standards: Chinese standard (86 mm x 86 mm), European standard (86 mm x 86 mm), South African standard (114 mm x 114 mm), and US standard (108 mm x 59 mm), making it highly versatile for different installation environments.

1.2 Package Contents

Table 1-1 Package Contents

No.	Item	Quantity
1	RG-RAP72-Wall access point (with a decorative cover)	1
2	User Manual	1
3	Warranty Card	1
4	Mounting bracket	1
5	T-key to anti-theft lock	1
6	Phillips pan head screws (M4 x 25 mm)	4

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.

1.3 Product Appearance

1.3.1 Appearance

Figure 1-1 Appearance

1.3.2 Front Panel

Figure 1-2 Front Panel

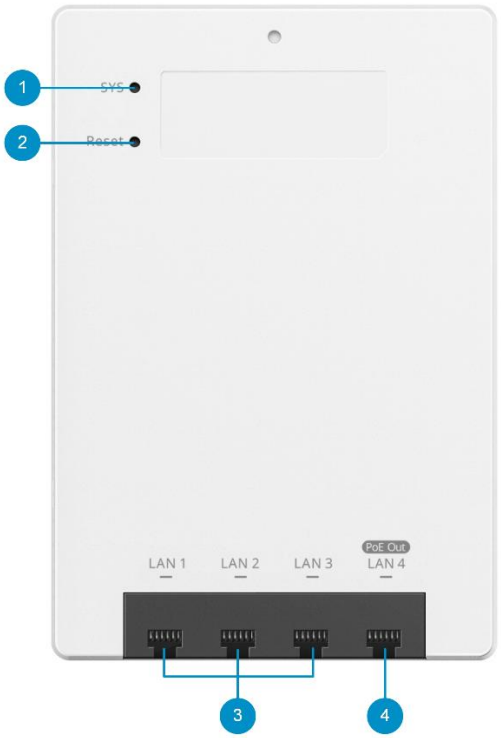


Table 1-2 Components on the Front Panel

No.	Component	Description
2	Reset button	● Press and hold for less than 2 seconds: Restart the access point. ● Press and hold for more than 5 seconds: Restore the access point to factory settings.
3	LAN1 to LAN3 ports	3 x 10/100/1000BASE-T Ethernet ports for connecting wired devices.
4	LAN4 port	10/100/1000BASE-T Ethernet port for connecting to a wired device, supporting PoE output.

Table 1-3 LEDs

No.	Component	Description
1	System LED	Off: ● The AP is not receiving power. ● The LED is manually turned off.
		Solid white: The AP is operating normally without any alarms.
		Fast flashing white: ● The AP is starting up. ● The AP is restarting.
		Slow blinking white: ● The AP is resetting. ● The AP is upgrading. **Caution** Do not power off the AP when the LED is in this state.
		One long blink followed by three slow blinks (white): The AP is recovering.
		One long blink followed by one slow blink (white): The AP has insufficient PoE power.
		Blinking white (on for 1.75s, off for 0.25s): The AP is not connected to the cloud platform.
		Fast blinking white for 3s and then off for 3s: The AP is being located through Ruijie Reyee App.
LED blinking patterns: ● Long blinking: The LED blinks on for 1s and off for 1s. ● Fast blinking: The LED blinks eight times per second. ● Slow blinking: The LED blinks twice per second. ● Blinking white (on for 1.75s, off for 0.25s): The LED blinks on for 1.75s and off for 0.25s.		

1.3.3 Rear Panel

Figure 1-3 Rear Panel

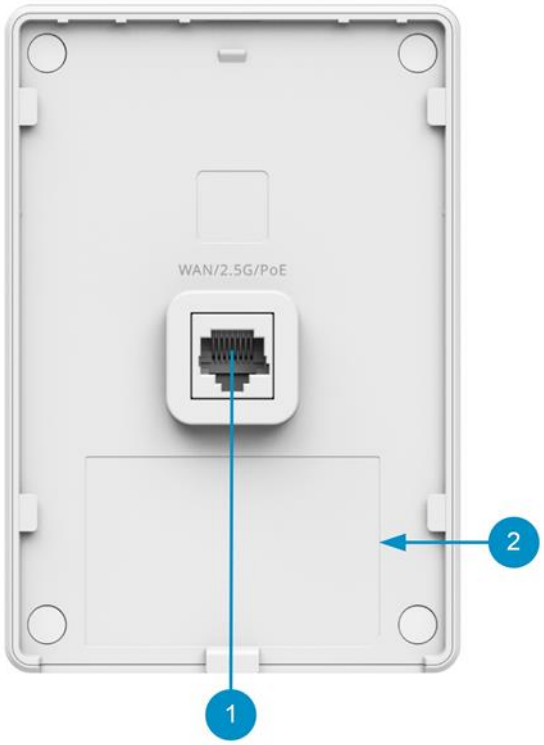


Table 1-4 Components on the Rear Panel

No.	Component	Description
1	WAN/2.5G/PoE port	10/100/1000/2500BASE-T Ethernet port, supporting PoE input and connected to a modem or Ethernet wall outlet.
2	Label	Located on the rear panel of the access point.

1.4 Technical Specifications

Table 1-5 Technical Specifications

Radio Design	Dual-band, dual-stream
Wi-Fi Standards	IEEE 802.11be, IEEE 802.11ax, IEEE 802.11ac Wave 1/Wave 2, and IEEE 802.11a/b/g/n
Operating Frequency Bands	IEEE 802.11b/g/n/ax/be: 2.4 GHz to 2.4835 GHz IEEE 802.11a/n/ac/ax/be: 5.150 GHz to 5.350 GHz, 5.470 GHz to 5.725 GHz, 5.725 GHz to 5.850 GHz
Antenna Type	Built-in omni-directional antennas (2.4 GHz: 2.84 dBi, 5 GHz: 4.56 dBi)

Spatial Streams	2.4 GHz: 2x2 MU-MIMO 5 GHz: 2x2 MU-MIMO
Data Rate	2.4 GHz: 688 Mbps 5 GHz: 2882 Mbps Combined: 3570 Mbps
Modulation	OFDM: BPSK@6/9 Mbps, QPSK@12/18 Mbps, 16QAM@24 Mbps, 64QAM@48/54 Mbps DSSS: DBPSK@1 Mbps, DQPSK@2 Mbps, CCK@5.5/11 Mbps MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM, 4096QAM, OFDMA
Receiver Sensitivity	11b: –91 dBm (1 Mbps), –88 dBm (5.5 Mbps), –85 dBm (11 Mbps) 11a/g: –89 dBm (6 Mbps), –80 dBm (24 Mbps), –76 dBm (36 Mbps), –71 dBm (54 Mbps) 11n: –85 dBm (MCS0), –65 dBm (MCS7), –85 dBm (MCS8), –65 dBm (MCS15) 11ac: 20 MHz: –85 dBm (MCS0), –60 dBm (MCS9) 11ac: 40 MHz: –82 dBm (MCS0), –57 dBm (MCS9) 11ac: 80 MHz: –79 dBm (MCS0), –54 dBm (MCS9) 11ax: 80 MHz: –79 dBm (MCS0), –52 dBm (MCS11) 11ax: 160 MHz: –76 dBm (MCS0), –49 dBm (MCS11) 11be: 80 MHz: –79 dBm (MCS0), –52 dBm (MCS13) 11be: 160 MHz: –76 dBm (MCS0), –49 dBm (MCS13)
Max. Transmit Power	Frequency bands and maximum Effective Isotropic Radiated Power (EIRP): **Note** Country specific restrictions apply. ● European Union & United Kingdom: ○ 2400 MHz to 2483.5 MHz, EIRP ≤ 20 dBm ○ 5150 MHz to 5350 MHz, EIRP ≤ 23 dBm ○ 5470 MHz to 5725 MHz, EIRP ≤ 30 dBm ● United States: ○ 2400 MHz to 2483.5 MHz, max output power ≤ 30 dBm & EIRP ≤ 36 dBm ○ 5150 MHz to 5250 MHz, max output power ≤ 30 dBm & EIRP ≤ 36 dBm ○ 5250 MHz to 5350 MHz, max output power ≤ 24 dBm & EIRP ≤ 30 dBm ○ 5470 MHz to 5725 MHz, max output power ≤ 24 dBm & EIRP ≤ 30 dBm ○ 5725 MHz to 5850 MHz, max output power ≤ 30 dBm & EIRP ≤ 36 dBm

	● Myanmar: ○ 2400 MHz to 2483.5 MHz, EIRP ≤ 23 dBm ○ 5725 MHz to 5825 MHz, EIRP ≤ 30 dBm ● Thailand: ○ 2400 MHz to 2483.5 MHz, EIRP ≤ 20 dBm ○ 5150 MHz to 5350 MHz, EIRP ≤ 23 dBm ○ 5470 MHz to 5725 MHz, EIRP ≤ 30 dBm ○ 5725 MHz to 5825 MHz, EIRP ≤ 30 dBm ● Indonesia: ○ 2400 MHz to 2483.5 MHz, EIRP ≤ 27 dBm ○ 5150 MHz to 5350 MHz, EIRP ≤ 23 dBm ○ 5725 MHz to 5825 MHz, EIRP ≤ 23 dBm ● Egypt: ○ 2400 MHz to 2483.5 MHz, EIRP ≤ 20 dBm ○ 5150 MHz to 5350 MHz, EIRP ≤ 23 dBm
Power Step	1 dBm
Dimensions (W x D x H)	124 mm x 86 mm x 24 mm (4.88 in. x 3.39 in. x 0.94 in.) (The height indicates the distance that the access point protrudes from the wall once installed.)
Net Weight	≤ 0.27 kg (0.60 lbs.)
Service Ports	● 1 x 10/100/1000/2500BASE-T Ethernet uplink port, supporting PoE input. ● 4 x 10/100/1000BASE-T Ethernet downlink ports for connecting wired devices, with LAN4 supporting PoE output.
Management Port	N/A
Status LED	1 x system status LED (white)
Power Supply Options	IEEE 802.3at compliant PoE+ (Under normal operation. The PoE Output function is enabled for LAN4 port and the maximum power output is 10 W.), compatible with IEEE 802.3af compliant PoE (the PoE Out function of LAN4 port is disabled when IEEE 802.3af compliant PoE is used.).
Max. Power Consumption	< 15 W (when the PoE output of LAN 4 port is disabled.)
Environment	Operating temperature: 0°C to 40°C (32°F to 104°F)
	Operating humidity: 5% to 95% (non-condensing)
	Storage temperature: –40°C to +70°C (–40°F to +158°F)
	Storage humidity: 5% to 95% (non-condensing)
Mounting	Junction box-mount
Color	White
Safety Regulations	CE, RoHS, FCC, ISED, and cTUVus

Surge Protection	±2 kV
Mean Time Between Failure (MTBF)	> 400,000 hours

1.5 Technical Specifications of Power Supply

The RG-RAP72-Wall adopts PoE input and supports IEEE 802.3af/802.3at compliant PoE power supply (The PoE Out function of LAN4 port is disabled when IEEE 802.3af compliant PoE power supply is used.)

When PoE is used, ensure that the power sourcing equipment (PSE) is at least IEEE 802.3af capable. For optimal device performance, it is recommended that a PSE that complies with the IEEE 802.3at standard should be used. Alternatively, you are advised to use a PoE adapter certified by Ruijie.

1.6 Cooling

The RG-RAP72-Wall adopts the fanless design. Therefore, when installing the AP, ensure that there is sufficient clearance around the AP for heat dissipation.

2 Preparing for Installation

2.1 Safety Guidelines

Note

- To avoid personal injury and equipment damage, carefully read the safety precautions before you install the access point.
- The following safety precautions may not cover all possible hazardous situations.

2.1.1 General Precautions

- Do not expose the access point to high temperature, dusts, or harmful gases. Do not install the AP in an inflammable or explosive environment. Keep the AP away from EMI sources such as large radar stations, radio stations, and substations. Do not subject the AP to unstable voltage, vibration, and noise.
- Keep the access point at least 500 (0.31 miles) meters away from the ocean and do not face it towards the sea breeze.
- The installation site should be free from water flooding, seepage, dripping, or condensation. The installation site should be selected according to network planning and communications equipment features, and considerations such as climate, hydrology, geology, earthquake, electrical power, and transportation.
- Ensure that the access point and power distribution system are properly grounded.

Caution

Follow the procedures in the user manual to install and remove the access point.

2.1.2 Handling Safety

- Do not move the access point frequently.
- Cut off all the power supplies and unplug all power cords before moving or handling the access point.

2.1.3 Electricity Safety

Warning

- Improper or incorrect electric operations may cause a fire, electric shock, and other accidents, and lead to severe and fatal personal injury and equipment damage.
- Direct or indirect contact with high voltage or mains power supply via wet objects may cause fatal dangers.

- Always observe the local regulations and standards. Only trained and qualified personnel should be allowed to operate the equipment.
- Check whether there are potential risks in the work area. For example, check whether the power supply is grounded, whether the grounding is reliable, and whether the ground is wet.
- Learn about the position of the indoor emergency power switch before installation. Cut off the power switch in case of accidents.

- Check the access point carefully before shutting down the power supply.
- Keep the access point far away from the grounding facility and lightning protection facility of the power equipment.
- Keep the access point far away from radio stations, radar stations, high-frequency high-current devices, and microwave ovens.

2.2 Site Requirements

The access point must be installed and used indoors. For normal operation and prolonged service life of the access point, the installation site must meet the following requirements.

2.2.1 Bearing

Evaluate the weight of the access point and its accessories, and ensure that the installation site (wall) can bear the weight.

2.2.2 Ventilation

The access point adopts natural cooling. Reserve a sufficient clearance around the access point to ensure proper ventilation.

2.2.3 Temperature and Humidity

To ensure the normal operation and prolonged service life of the access point, maintain an appropriate temperature and humidity. Working in an environment with too high or too low temperature and humidity for a long period may damage the access point.

- When exposed to high relative humidity, insulating materials may exhibit poor insulation capabilities, increasing the risk of electrical leakage.
- When exposed to low relative humidity, the insulating strip may dry out and shrink, increasing the risk of static electricity generation.
- In a dry environment, static electricity is prone to occur and damage the internal circuits of the access point.
- High temperature environments can be detrimental to the access point, leading to reduced performance and a shorter service life. Prolonged exposure to elevated temperatures can expedite the access point's aging process.

2.2.4 Cleanliness

Dust poses a major threat to the device. The indoor dust can cause electrostatic adhesion when falling on the device, causing poor contact of the metallic joint. Such electrostatic adhesion occurs more easily when the indoor relative humidity is low, not only affecting the service life of the device, but also causing communication failure easily. The following table lists the requirements on the dust content and diameter in the equipment room.

Table 2-1 Dust and Particles

Particle Size	Unit	Content
≥ 0.5 μm	Particles/m^3	≤ 1.4 x 10^7
≥ 1 μm	Particles/m^3	≤ 7 x 10^5

≥ 3 μm	Particles/m^3	≤ 2.4 x 10^5
≥ 5 μm	Particles/m^3	≤ 1.3 x 10^5

Apart from dust, the salt, acid, and sulfide in the air of the equipment room must meet strict requirement. These harmful substances will accelerate metal corrosion and component aging. The equipment room should be protected from harmful gases (such as sulfur dioxide, hydrogen sulfide, nitrogen dioxide, ammonia, and chlorine). The following table lists the limits of harmful gases in the equipment room.

Table 2-2 Hazardous Gases

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

Note

The average value is measured over one week. The maximum value is the upper limit of the harmful gas measured in one week for up to 30 minutes every day.

2.2.5 Grounding

A proper grounding system is the basis for stable and reliable running and is indispensable for preventing lightning strikes and interference. Carefully check the grounding conditions at the installation site according to the grounding specifications, and complete grounding properly based on the actual situation.

2.2.6 Electromagnetic Interference

- Keep the access point far away from the grounding system or the lightning protection grounding system and f the power facility.
- Keep the access point far away from radio stations, radar stations, high-frequency high-current devices, and microwave ovens.

2.3 Tools

Table 2-3 Tools

Common Tools	Phillips screwdriver, power cords, Ethernet cables, diagonal plier, and binding straps
Special Tools	ESD gloves, wire stripper, crimping plier, RJ45 crimping plier, wire cutter, and waterproof adhesive tape
Meters	Multimeter

Note

This device is delivered without a toolkit. Prepare the preceding tools by yourself.

3 Installing the Access Point

Caution

Before installing the access point, make sure you have carefully read the requirements in Chapter 2.

3.1 Before You Begin

Carefully plan and arrange the installation position, networking mode, power supply, and cabling before installation. Confirm the following requirements before installation:

- The installation site provides sufficient space for proper ventilation.
- The installation site meets the temperature and humidity requirements of the access point.
- The power supply and required current are available in the installation site.
- The selected power supply modules meet the system power requirements.
- The installation site meets the cabling requirements of the access point.
- The installation site meets the site requirements of the access point.
- The customized access point meets the client-specific requirements.

3.2 Precautions

To ensure normal operation and prolonged service life of the access point, observe the following precautions:

- Do not power on the access point during installation.
- Install the access point in a well-ventilated location.
- Do not subject the access point to high temperature.
- Keep the access point away from high voltage cables.
- Do not expose the access point in a thunderstorm or strong electric field.
- Cut off the power switch before cleaning the access point.
- Do not open the enclosure when the access point is working.
- Secure the access point tightly.

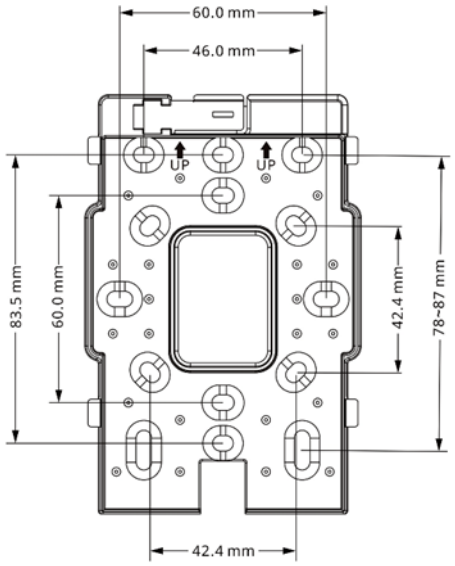
3.3 Installing the Access Point

Caution

The schematic diagram provided is for reference purposes only. The actual product should be installed based on its physical specifications and design.

The following figure shows the mounting bracket dimensions.

Figure 3-1 Dimensions of the Mounting Bracket

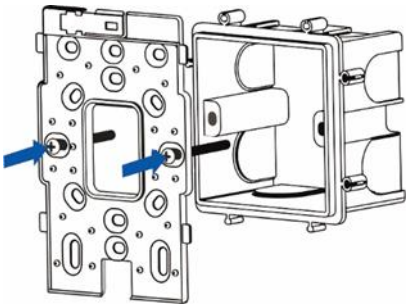


The access point can be installed on various junction boxes, including Chinese-standard and European-standard 86-mm junction boxes, American-standard 118-mm junction box, and South African-standard 120-mm junction box. To mount the access point on a Chinese-standard 86-mm junction box, follow these steps:

(1) Secure the mounting bracket to the junction box using screws.

- Chinese-standard 86 mm x 86 mm Junction Box

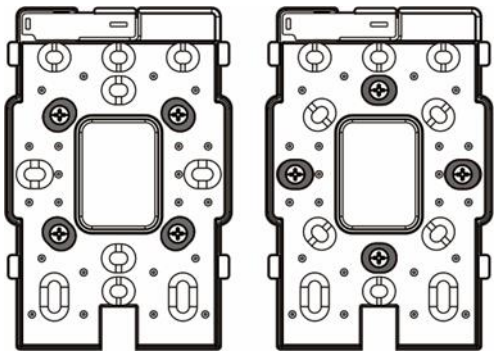
Figure 3-2 Chinese-standard 86 mm x 86 mm Junction Box



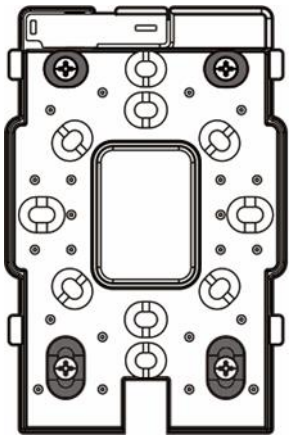
Caution

The following are brackets on European-standard 86 mm x 86 mm junction box, South African-standard 114 mm x 114 mm junction box, and American-standard 108 mm x 59 mm junction box. The access point can be mounted horizontally or vertically on a South African-standard junction box.

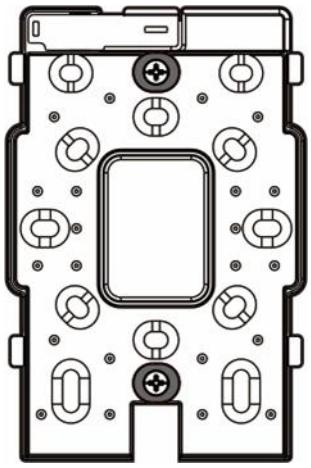
- European-standard 86 mm x 86 mm Junction Box



- American-standard 108 mm x 59 mm Junction Box

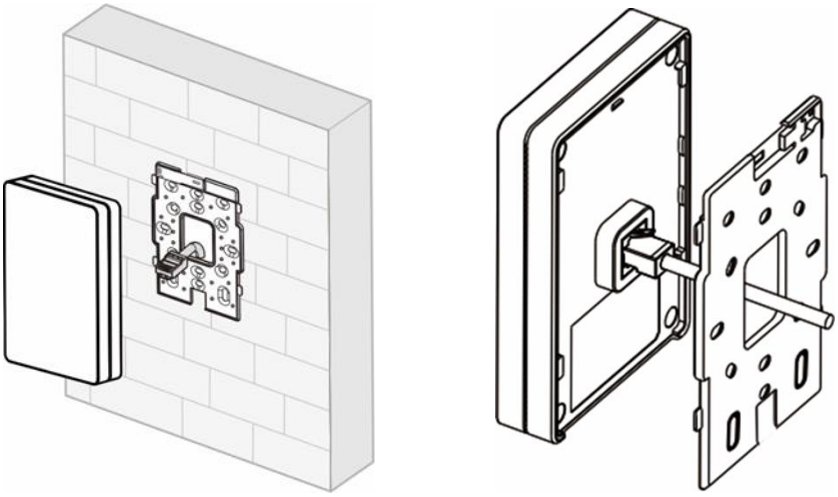


- South African-standard 114 mm x 114 mm Junction Box



(2) Connect cables according to the actual networking. The following describes how to connect cables on the AP side.

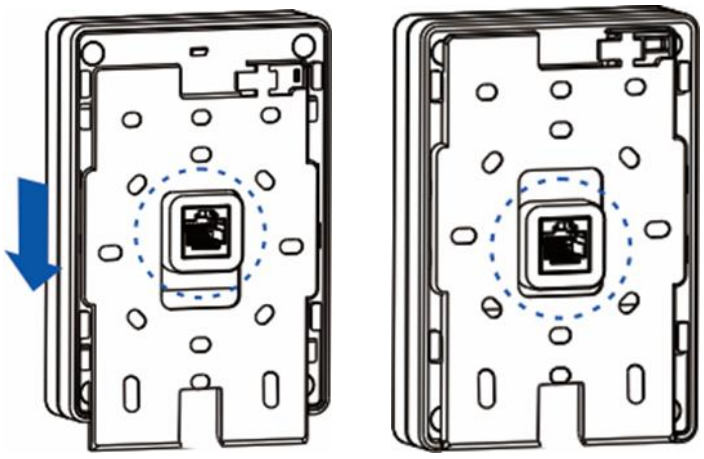
- Ethernet cable: Connect one end of the Ethernet cable to the WAN/2.5G/PoE port on the back of the AP. This port supports PoE input.
- Ethernet cable: Connect one end of the Ethernet cable to one of LAN 1 to LAN 4 ports on the bottom of the AP. LAN 4 port supports PoE output.



Caution

- Make sure that the cables at the connectors have natural bends or bends of large radius instead of small radius.
- When the access point is powered by PoE power supply, make sure that the PSE connected to the WAN/2.5G/PoE port of the access point is 802.3af/802.3at capable. If the 802.3af compliant PoE power supply is adopted, the PoE output function of LAN 4 port is disabled.)

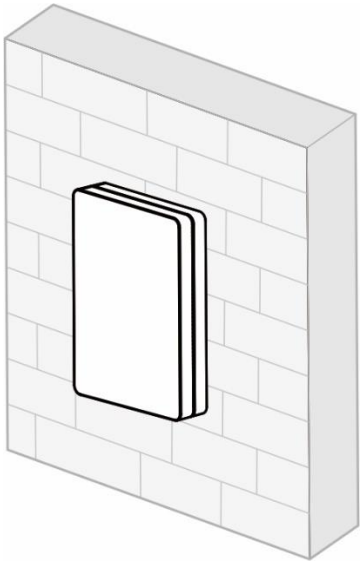
(3) Align the upper edge of the WAN port on the access point with the upper edge of the hole on the mounting bracket. Slide the access point downward to secure it on the mounting bracket.



Caution

Keep the key to the anti-theft lock (T-key) handy after installation. This product is designed with anti-theft function. You need to use the T-key to remove the access point.

(4) The installation is complete.



3.4 Bundling Cables

Note

- The cables should be bound in a visually pleasing way.
- When you bundle twisted pairs, make sure that the cables at the connectors have natural bends or bends of large radius.
- Do not over-tighten cable bundle as it may reduce the cable life and performance.

The steps of cable bundling are as follows:

(1) Bind the drooping part of the cables and place the bundle as near the ports as possible.

(2) Secure the cables in the cable management trough of the mounting bracket.

(3) Route the cables under the AP and run them in straight line.

3.5 Checklist After Installation

(1) Checking the Access Point

- The external power supply matches with the requirement of the access point.
- The access point is securely fastened.

(2) Checking the Cable Connection

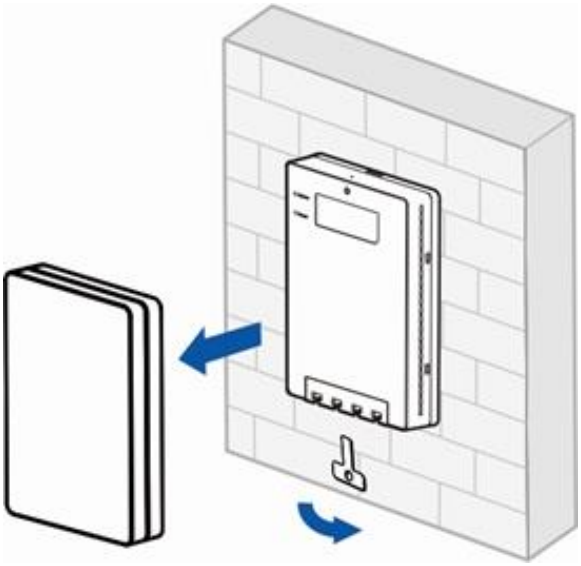
- The cable type matches the port type.
- The cables are properly bundled.

(3) Checking the Power Supply

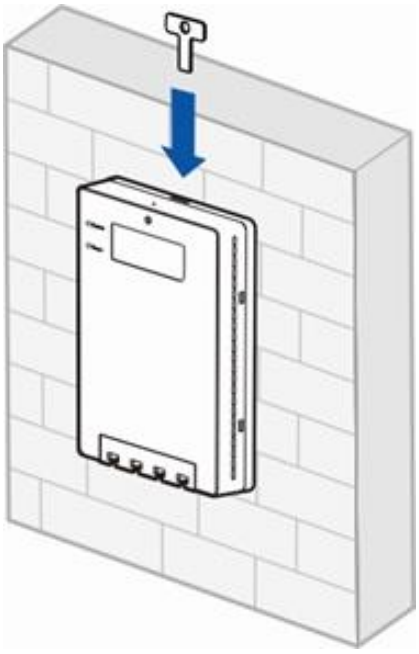
- The power cord is properly connected and meets safety requirements.
- The access point is operational after power-on.

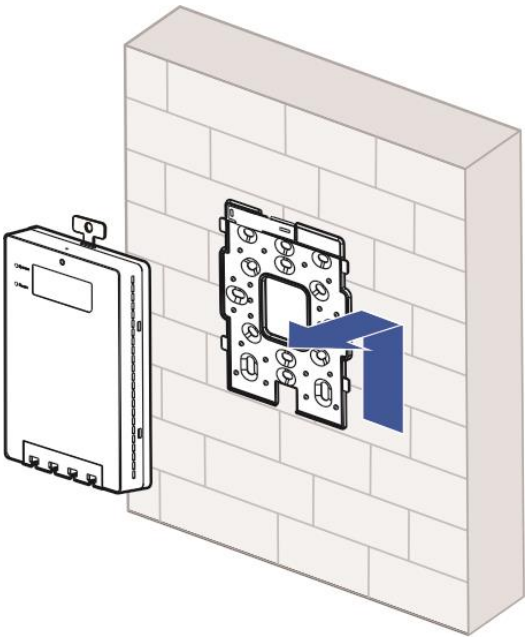
3.6 Removing the Access Point

(1) Insert the T-key into the protruding piece at the bottom of the device, and rotate the key to remove the decorative cover.



(2) Insert the T-key into the slot at the top of the device, and remove the device as indicated by the arrow.





4 Verifying Operating Status

4.1 Setting Up the Configuration Environment

When the AP is powered on through PoE, pay attention to the following points:

- Verify that the power cord is properly connected and compliant with safety requirements.
- Connect the access point with the debugging device through an Ethernet cable.

4.2 Powering on the Access Point

4.2.1 Checklist Before Power-On

- Verify that the power cord is properly connected.
- Check if the power source device connected to the WAN/2.5G/PoE port supports IEEE 802.3af or IEEE 802.3at standards. Note that if IEEE 802.3af power is used, the POE Out function on the LAN4 port will be disabled.

4.2.2 Checklist After Power-on

- Verify the LED status.
- After the AP is powered on, check whether the SSID (@Ruijie-mXXXX for multiple devices and @Ruijie-sXXXX for a single device) can be detected by a mobile phone or other wireless devices.

5 Monitoring and Maintenance

5.1 Monitoring

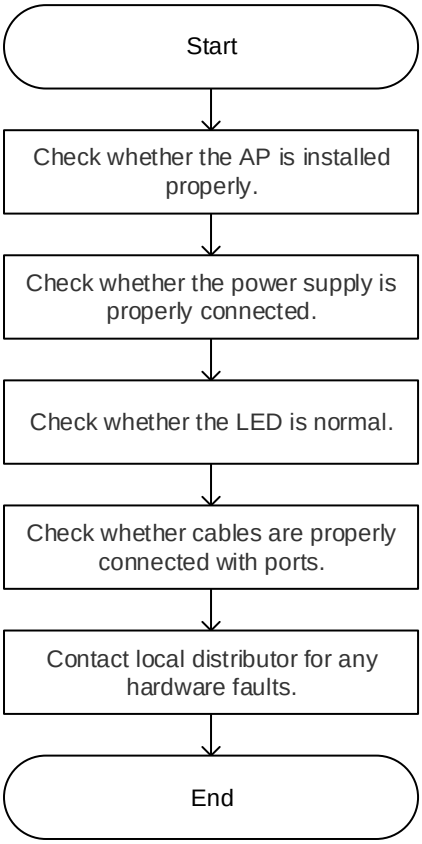
You can observe the LED color to monitor the access point status.

5.2 Maintenance

If the hardware is faulty, please contact local distributor.

6 Common Troubleshooting

6.1 General Troubleshooting Flowchart



6.2 Common Faults

- Why the LED off is after the access point is powered on?

  Verify that the PSE connected to the WAN/2.5G/PoE port of the access point is 802.3af/802.3at compliant. Check whether the Ethernet cable is connected properly and works normally.

- Why does Ethernet port not work after the Ethernet cable is plugged in?

  Check whether the peer device is working properly. Then verify that the Ethernet cable is capable of providing the required data rate and is properly connected.

- Why can’t clients discover the access point?
  - Verify that the access point is properly powered.
  - Verify that the Ethernet port is correctly connected.
  - Verify that the access point is correctly configured.
  - Move the client endpoint to adjust the distance between the client and the access point.

- Why can’t clients discover the 5 GHz SSID?
  - Verify that the PSE supplying power to the access point is 802.3at compliant.
  - Verify that the access point is configured with the 5 GHz SSID.
  - Log in to the web interface and choose **One-Device** > **Config** > **Advanced** > **PoE Settings** to verify that the **Power Mode** is set to **IEEE 802.3at**.

7 Appendix

7.1 Ports, Connectors, and Media

7.1.1 2500BASE-T/1000BASE-T/100BASE-TX/10BASE-T Ports

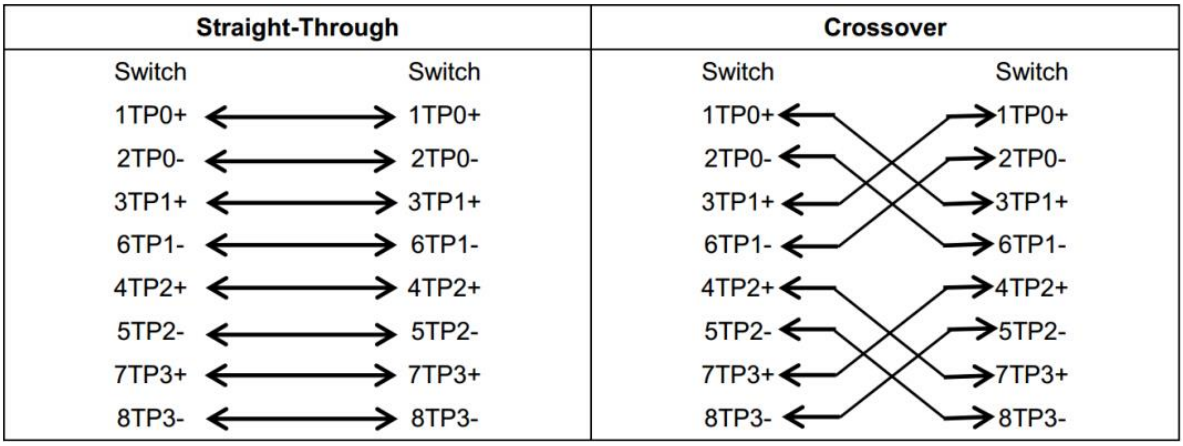
2500BASE-T/1000BASE-T/100BASE-TX/10BASE-T ports are Ethernet ports with auto-negotiation of four data rates: 10 Mbps, 100 Mbps, 1000 Mbps, and 2500 Mbps. They supports auto MDI/MDIX Crossover, and use RJ 45 connectors.

Compliant with the IEEE 802.3bz standard, a 2500BASE-T port requires 100-ohm Category 6 or 5e unshielded twisted pair (UTP), or shielded twisted pair (STP) (recommended) cables, and supports a maximum distance of 100 meters (328 feet). When PoE power supply is used, Category 6 STP cables are recommended, and both the port and the cable should be properly shielded.

Compliant with the IEEE 802.3ab standard, a 1000BASE-T port requires 100-ohm Category 6 or 5e unshielded twisted pair (UTP) or shielded twisted pair (STP) (recommended) cables, and supports a maximum distance of 100 meters (328 feet). When PoE power supply is used, Category 6 STP cables are recommended, and both the port and the cable should be properly shielded.

The 2500BASE-T/1000BASE-T port all four pairs of wires to be connected for data transmission.Figure 7-1 shows the connection of four pairs of wires for the 2500BASE-T/1000BASE-T port.

Figure 7-1 2500BASE-T/1000 BASE-T Twisted Pair Connections



A 100BASE-TX/10BASE-T port can also be connected using 100-ohm Category 5 cables, and supports a maximum distance of 100 meters (328 feet).

Table 7-1 shows 100BASE-TX/10BASE-T pin assignments.

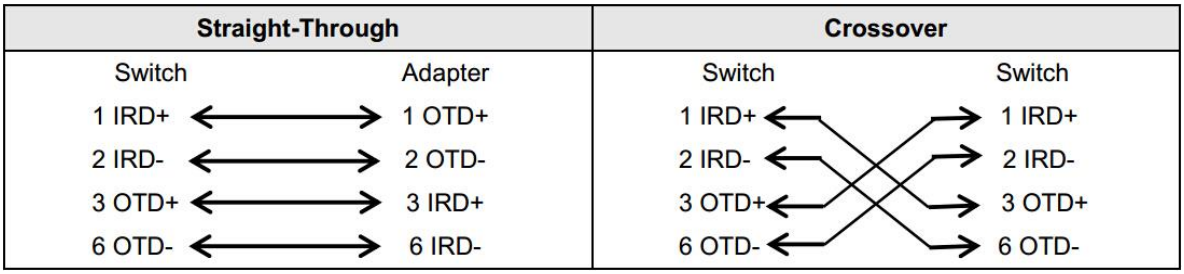
Table 7-1 100BASE-TX/10BASE-T Pin Assignments

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-
4, 5, 7, 8	Not Used	Not Used

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

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



7.2 Recommended Cabling

When installing the RG-RAP72-Wall, route the cables through the cable management brackets. Top cabling or bottom cabling is adopted according to the actual situation in the equipment room. All conversion connectors should be placed at the bottom of the rack instead of outside the rack that is easily accessible. Power cords are routed beside the cabinet, and top cabling or bottom cabling is adopted according to the actual situation in the equipment room, such as the locations of the DC power distribution box, AC power socket, or surge protection box.

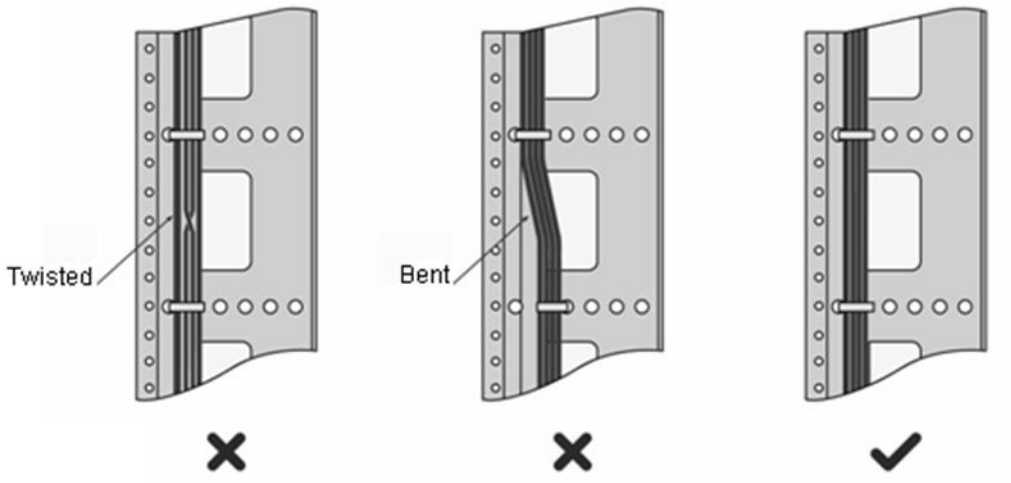
Requirements for the Minimum Bend Radius of an Ethernet Cable

- The bend radius of a fixed power cord, Ethernet cable, or flat cable should be over five times greater than their respective external diameter. The bend radius of these cables that are often bent or plugged should be over seven times greater than their respective external diameter.
- The bend radius of a fixed common coaxial cable should be over seven times greater than its external diameter. The bend radius of the common coaxial cable that is often bent or plugged should be over 10 times greater than its external diameter.
- The bend radius of a fixed high-speed cable (such as SFP+ cable) should be over five times greater than its external diameter. The bend radius of the fixed high-speed cable that is often bent or plugged should be over 10 times greater than its external diameter.

Precautions for Bundling Cables

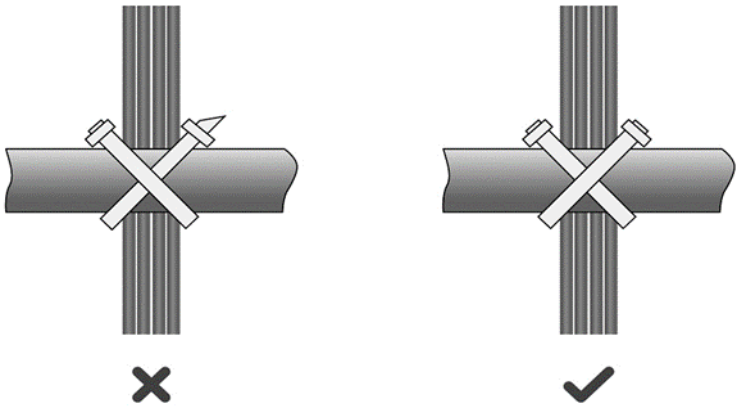
- Before cables are bundled, mark labels and stick the labels to cables wherever appropriate.
- Cables should be neatly and properly bundled in the rack without twisting or bending, as shown in Figure 7-3.

Figure 7-3 Bundling Cables (1)



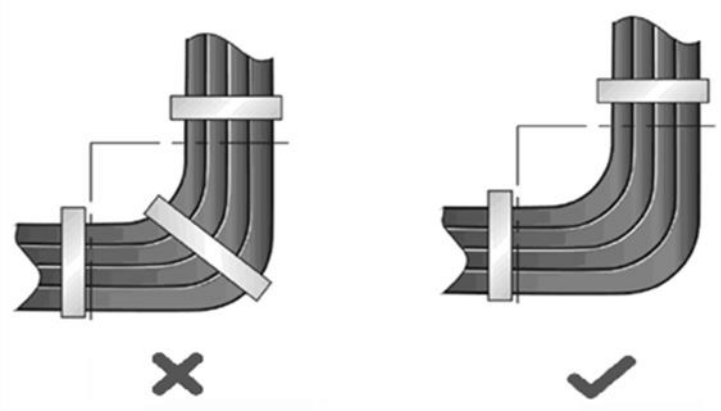
- Cables of different types (such as power cords, signal cables, and ground cables) should be separated in cabling and bundling. Mixed bundling is prohibited. When they are close to each other, you are advised to adopt crossover cabling. In the case of parallel cabling, maintain a minimum distance of 30 mm (1.18 in.) between power cords and signal cables.
- The cable management brackets and cabling troughs inside and outside the rack should be smooth without sharp corners.
- The metal hole traversed by cables should have a smooth and fully rounding surface or an insulated lining.
- Use cable ties to bundle up cables properly. Please do not connect two or more cable ties to bundle up cables.
- After bundling up cables with cable ties, cut off the remaining part. The cut should be smooth and trim, without sharp corners, as shown inFigure 7-4.

Figure 7-4 Bundling Cables (2)



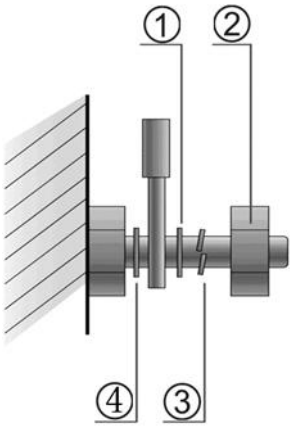
- When cables need to be bent, bundle them up but do not tie them where the cables will be bent, as shown inFigure 7-5.

Figure 7-5 Bundling Cables (3)



- Cables not to be assembled or remaining parts of cables should be folded and placed in a proper position of the rack or cable trough. The proper position refers to a position that does not affect device running or damage the device or cable.
- Do not bind 220V or 48V power cords to the guide rails of moving parts.
- The power cords connecting moving parts such as door grounding cables should be reserved with a margin after being assembled to avoid suffering tension or stress. When the moving part is installed, the remaining cable part should not touch heat sources, sharp corners, or sharp edges. If heat sources cannot be avoided, high-temperature cables should be used.
- When screw threads are used to fasten cable terminals, the anchor or screw must be tightly fastened, as shown inFigure 7-6.

Figure 7-6 Cable Fastening



① Flat washer	③ Spring washer
② Screw nut	④ Flat washer

- Hard power cords should be fastened in the terminal connection area to prevent stress on terminal connection and cable.

- Do not use self-tapping screws to fasten terminals.
- Power cords of the same type and in the same cabling direction should be bundled up into cable bunches, with cables in cable bunches clean and straight.
- Bundle up cables by using cable ties.

Cable Bunch Diameter	Distance Between Every Binding Point
10 mm (0.39 in.)	80 mm to 150 mm (3.15 in. to 5.91 in.)
10 mm to 30 mm (0.39 in. to 1.18 in.)	150 mm to 200 mm (5.91 in. to 7.87 in.)
30 mm (1.18 in.)	200 mm to 300 mm (7.87 in. to 11.81 in.)

- Do not tie cables or bundles in a knot.
- For wiring terminal sockets (such as circuit breakers) with cord end terminals, the metal part of the cord end terminal should not be exposed outside the terminal socket when assembled.

Contents

1 Fast Internet Access

1.1 Configuration Environment Requirements

1.1.1 PC

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

1.2 Default Configuration

Table 1-1 Default Web Configuration

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

1.3 Login to Web Interface

1.3.1 Connecting to the Access Point

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

- Wired Connection

Connect a local area network (LAN) port of the access point to the network port of the PC, and set the IP address of the PC. See 1.3.2 Configuring the IP Address of the Management Client.

- Wireless Connection

On a mobile phone or laptop, search for wireless network **@Ruijie-S***XXXX* (XXXX is the last four digits of the MAC address of each device). In this mode, you do not need to set the IP address of the management Client, and you can skip the operation in 1.3.2 Configuring the IP Address of the Management Client.

1.3.2 Configuring the IP Address of the Management Client

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

Caution

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

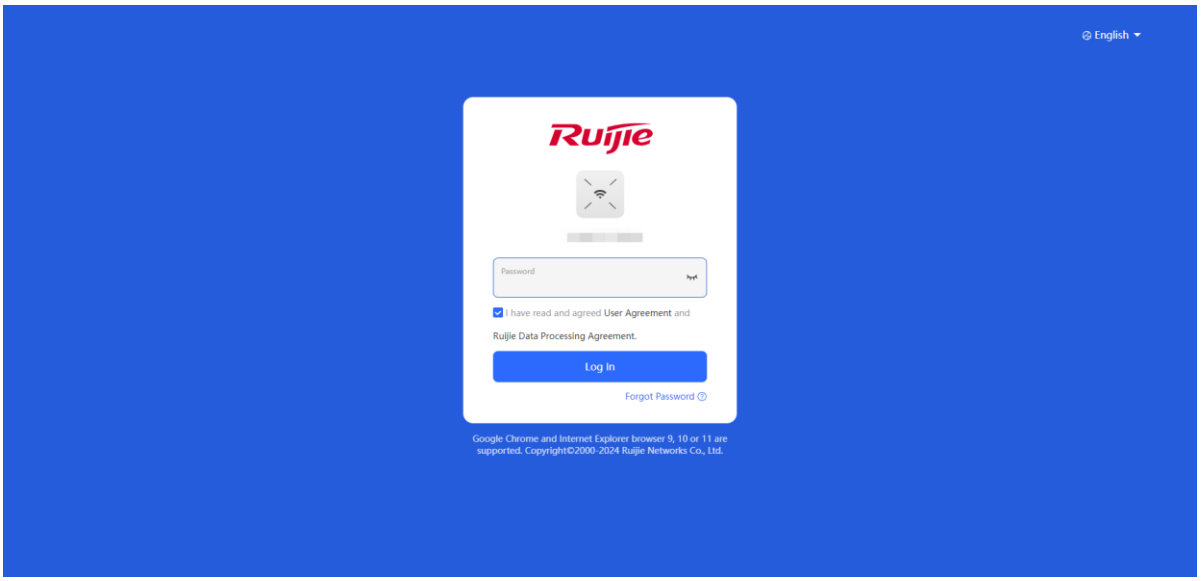
1.3.3 Logging in to the Web Page

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

Note

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

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



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

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

Caution

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

1.4 Work Mode

The device can work in the router mode, AP mode or wireless repeater mode. The displayed system menu page and function ranges vary with the work mode. The RAP works in the AP mode by default.

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

Self-organizing network mode: After the self-organizing network discovery function is enabled, the new device and other unconnected devices can be discovered. Devices connect with each other to form a network based on their status and synchronize their configurations globally. You can log in to the web interface of the device to view management information of all devices on the network. After the self-organizing network discovery function is enabled, you can efficiently maintain and manage the network. You are advised to keep this function enabled.

When the device connect with each other to form a network, two configuration modes are displayed: network-wide mode and local device mode. See1.8 Introduction to the Web Interface.

Local device mode: After the self-organizing network discovery function is disabled, the device will not be discovered. After logging in to the web interface, you can configure and manage only the new 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.

To switch the work mode, see 4.1 Switching Work Mode.

1.4.1 AP Mode

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

1.4.2 Router Mode

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

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

Caution

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

1.4.3 Wireless Repeater Mode

The device does not support the routing and DHCP server functions in the wireless repeater mode. IP addresses of the clients are assigned and managed by the primary router. On an available network, the device can be connected to the primary router through wireless connection to expand the Wi-Fi coverage and increase the number of LAN ports and wireless access devices.

1.5 Configuration Wizard (Router Mode)

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

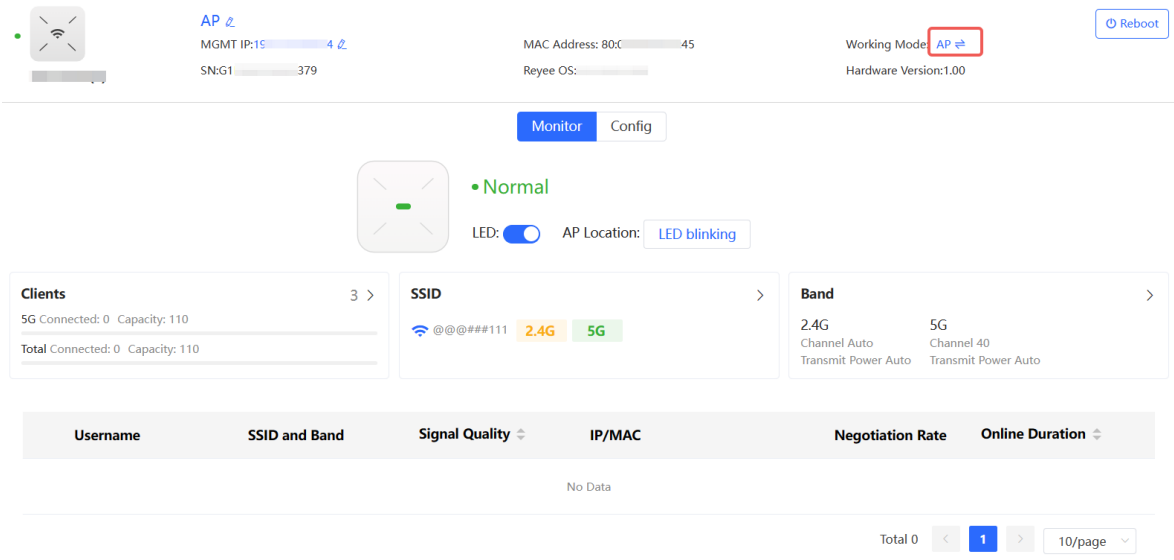
1.5.1 Getting Started

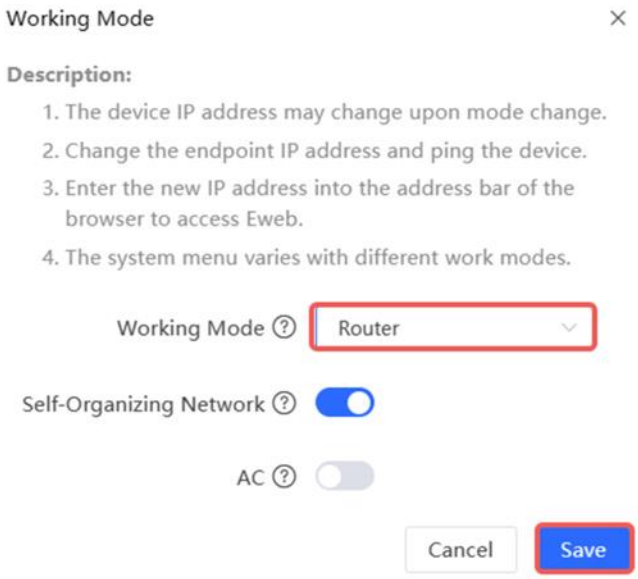
(1) Connect the device to a power supply and connect the port of the device to an upstream device with an Ethernet cable. Or you can connect an Ethernet cable to the device.

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

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

(3) The device works in the AP mode by default. If you want to switch the work mode to the router mode, perform the configuration on the work mode setting page. See 4.1 Switching Work Mode for more details.





1.5.2 Configuration Steps

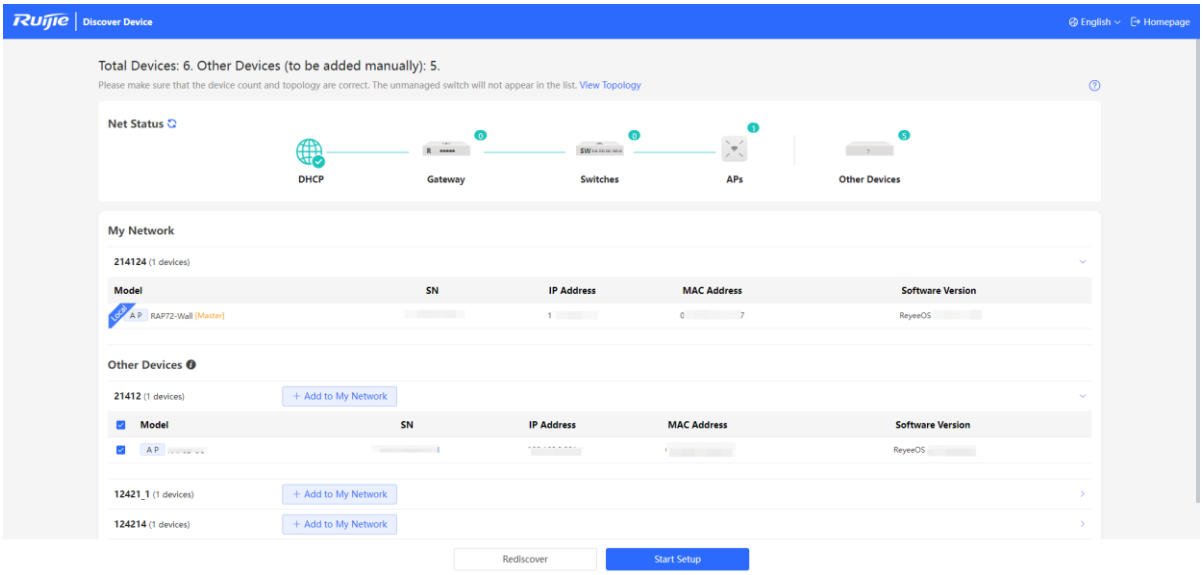
1. Add a Device to Network

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

Note

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

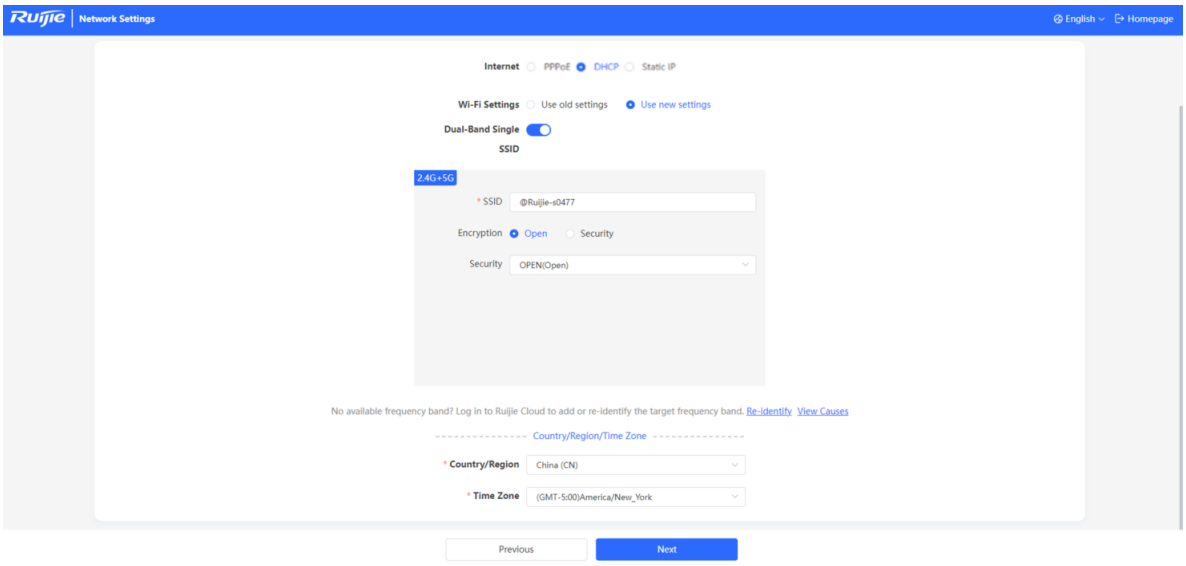
If a new device is detected not in the network, click **Add to My Network** and enter its management password to add the device manually.



2. Creating a Network Project

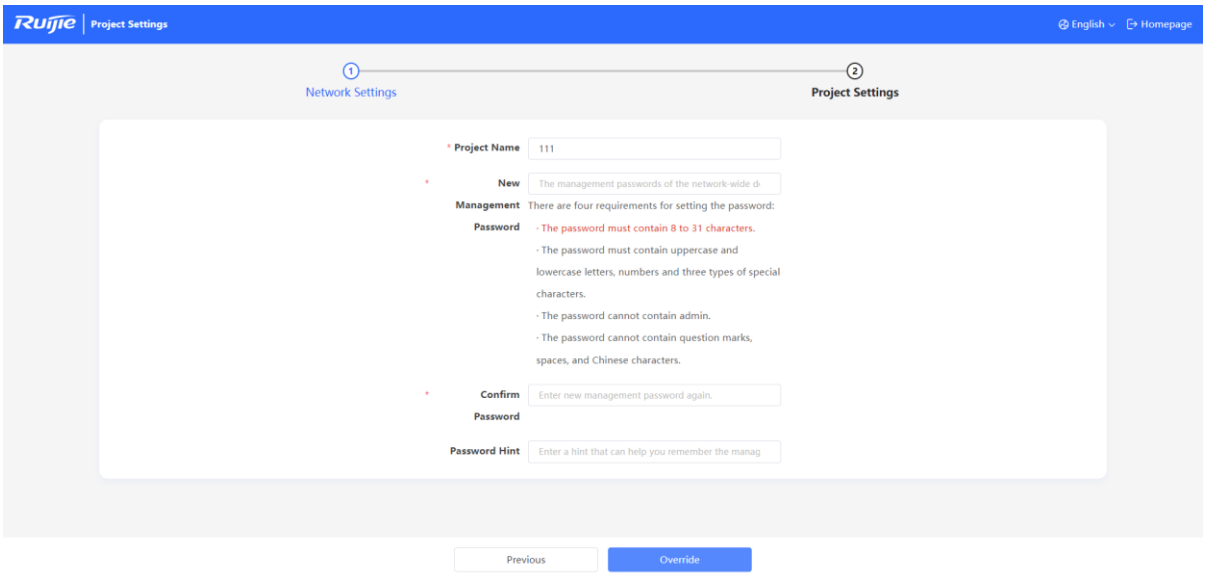
(1) Click **Start Setup** to configure the Internet connection type and Wi-Fi network.

- **Internet**: Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).
  - DHCP: The access point detects whether it can obtain an IP address via DHCP by default. If the access point connects to the Internet successfully, you can click Next without entering an account.
  - PPPoE: Click PPPoE, and enter the username, password, and service name. Click Next.
  - Static IP: Enter the IP address, subnet mask, gateway, and DNS server, and click Next.
- **Wi-Fi Settings**: Select the Wi-Fi configuration mode. This configuration option is unavailable for a new project.
  - Use Old Settings: Use the Wi-Fi settings of an existing project.
  - Use New Settings: Configure the Wi-Fi network using new settings.
- **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.
- **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.
- **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.

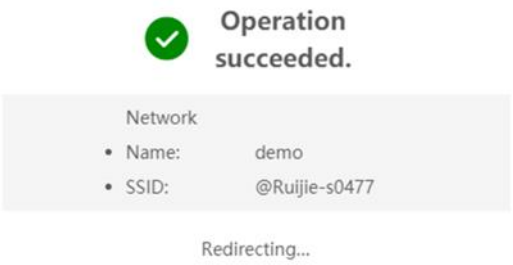


(2) Click **Next**. On the page that is displayed, set the project name and management password.

- **Project Name**: Identify the network project where the device is located.
- **Management Password**: The password is used for logging in to the management page.



Click **Finish**. The device will deliver the initialization and check the network connectivity.



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

Note

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

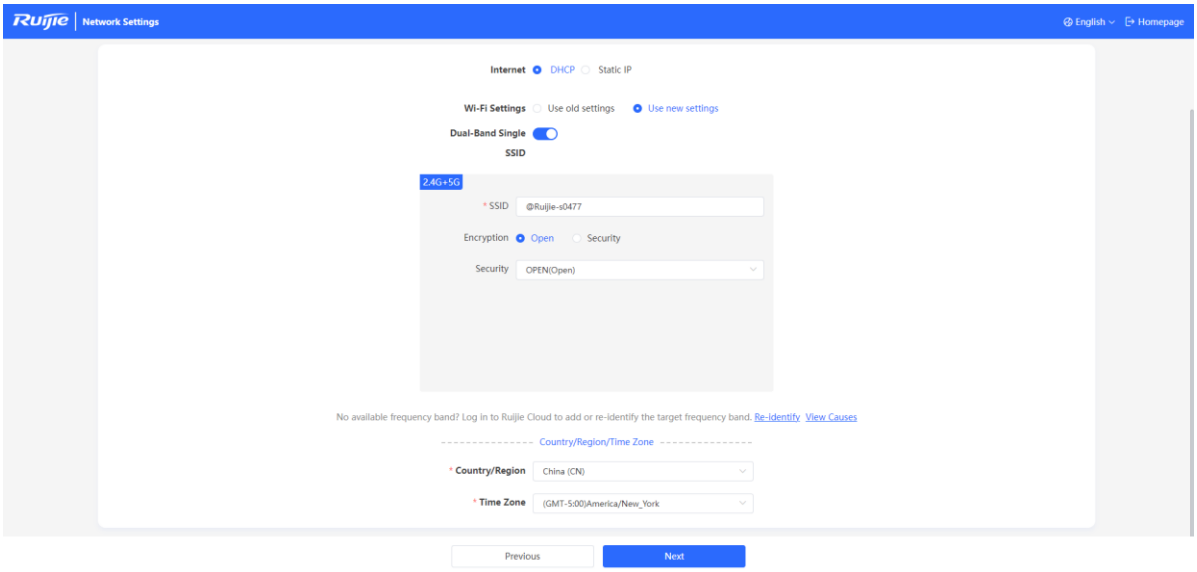
1.6 Configuration Wizard (AP Mode)

1.6.1 Getting Started

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

1.6.2 Configuration Steps

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



1.7 Configuration Wizard (Wireless Repeater Mode)

1.7.1 Getting Started

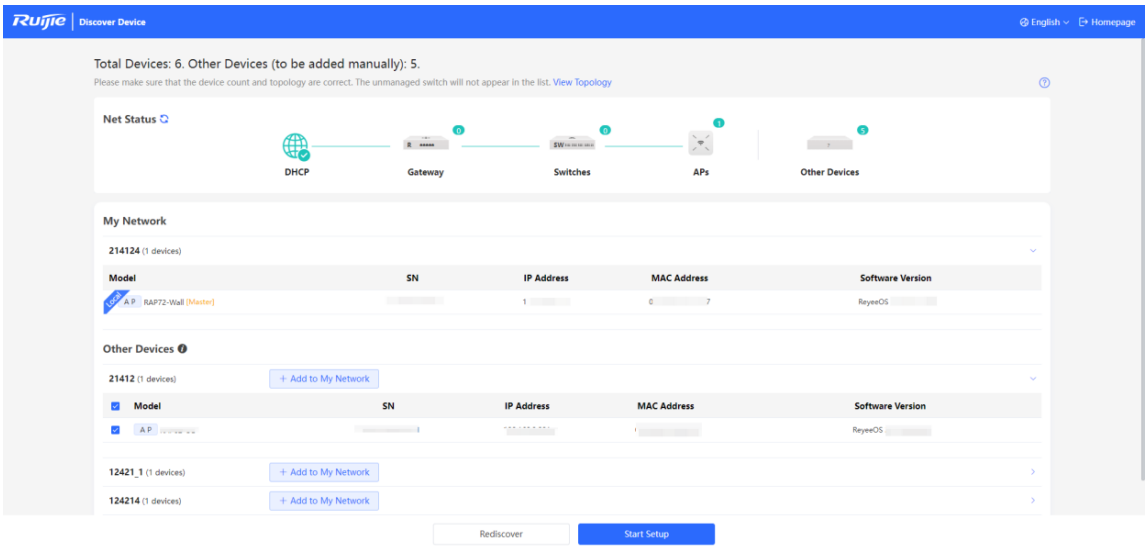
- Before configuring the wireless repeater mode, configure the primary router and test that the primary router can access the Internet.
- Place the device where it can discover at least two-bar Wi-Fi signal of the primary router.

Caution

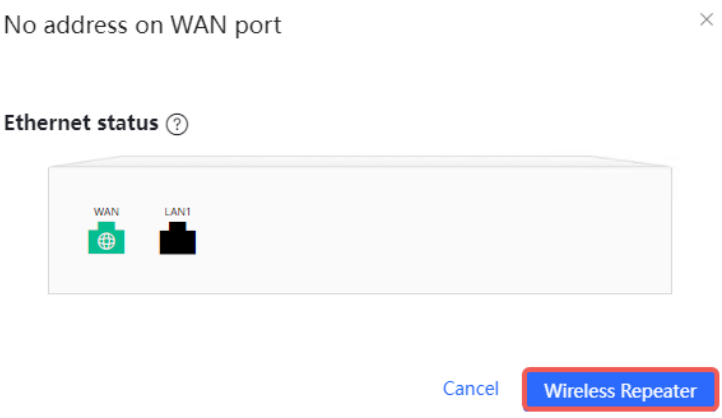
No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

1.7.2 Configuration Steps

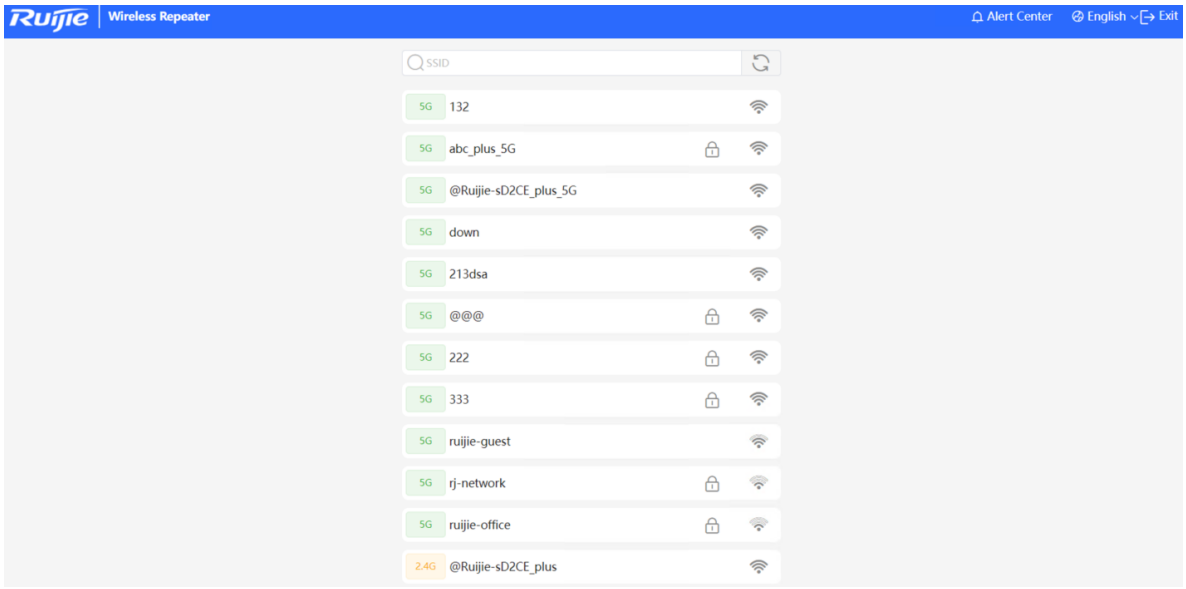
(1) Connect the device to a power supply without connecting an Ethernet cable to the uplink port, and click **Start Setup**.

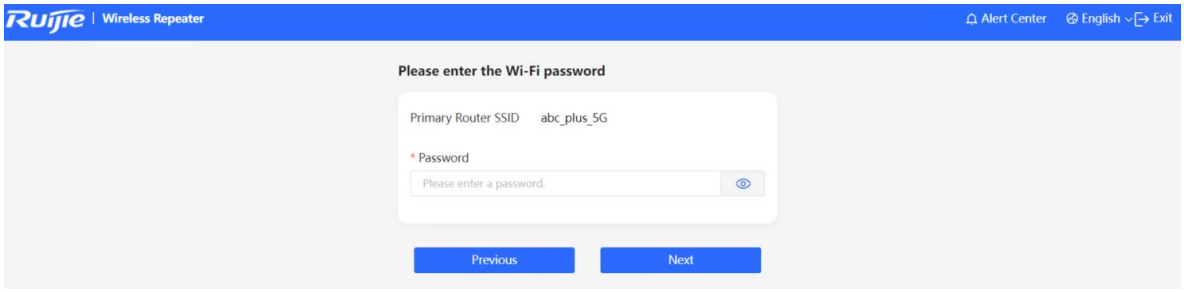


(2) If you see a dialogue box indicating that the Ethernet cable is not connected to the WAN port, click **Wireless Repeater**.

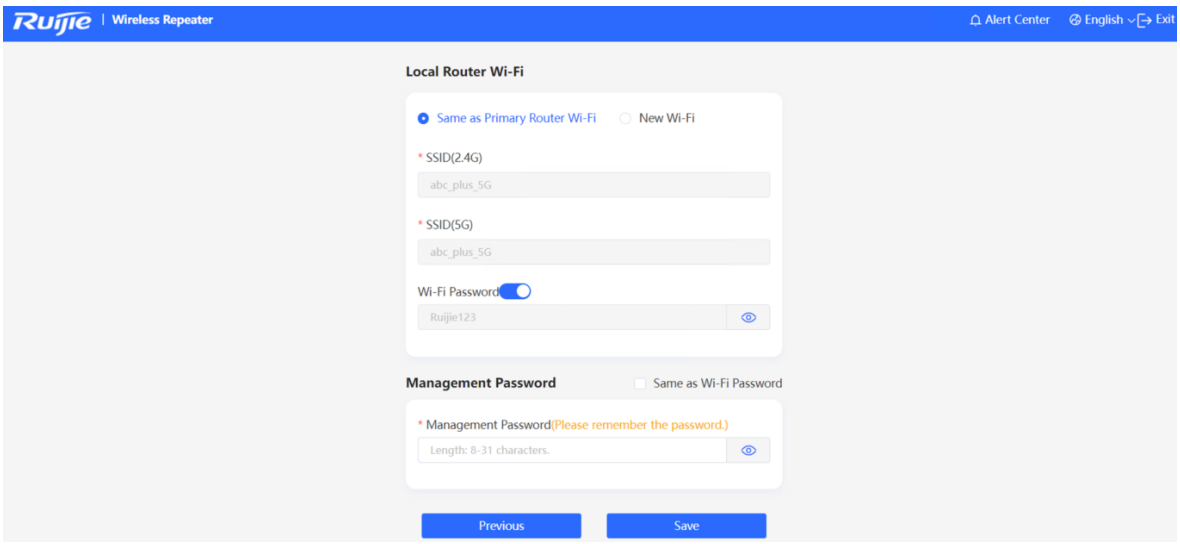


(3) Select the primary router SSID that requires expanding the Wi-Fi coverage, enter the Wi-Fi password of the primary router, and click **Next**.

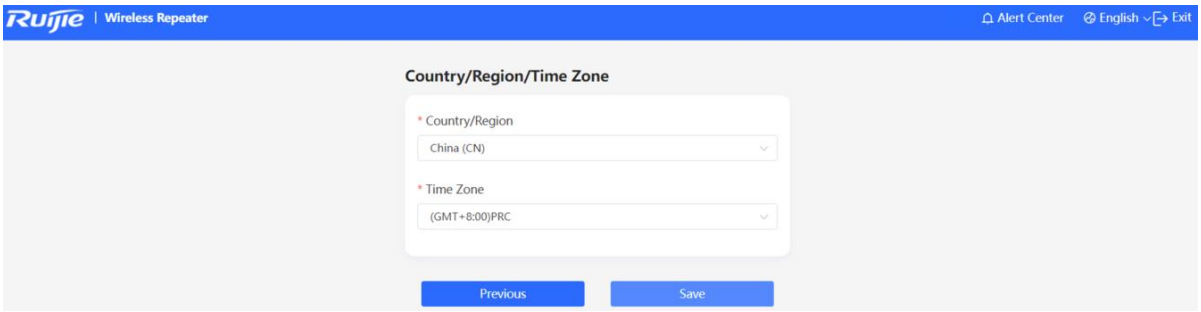




(4) Set the SSID and password and click **Save**. Then, the Wi-Fi network will be restarted.



(5) Set the country/region code and time zone, and click **Save**.



1.8 Introduction to the Web Interface

To facilitate flexible device management, the Web page displays different system configuration menus in different work modes. For details about the work mode, see 4.1 Switching Work Mode.

As to the RG-RAP72-Wall model, please refer to 1.8.1 Management Page for Wi-Fi 7 Products.

The self-organizing network discovery function is enabled by default, but can be disabled manually. After this function is disabled, the web interface displays the local device mode.

When the self-organizing network discovery function is enabled, you can switch between the network-wide mode and the local device mode. The displayed function menus vary with the mode.

Note

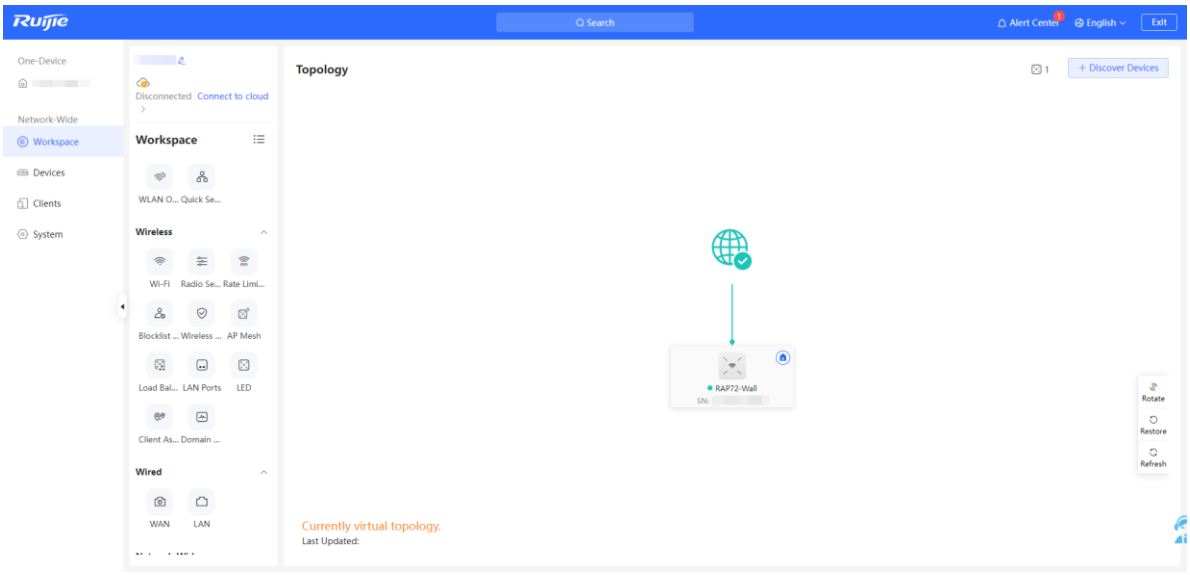
After the self-organizing network discovery function is enabled, the system configuration menus on the web interface depends on the master device on the network. If the master device supports Wi-Fi 6 or later, the web interface of the other devices on the network is the same as that of the master device.

1.8.1 Management Page for Wi-Fi 7 Products

1. Enabling Self-Organizing Network Discovery

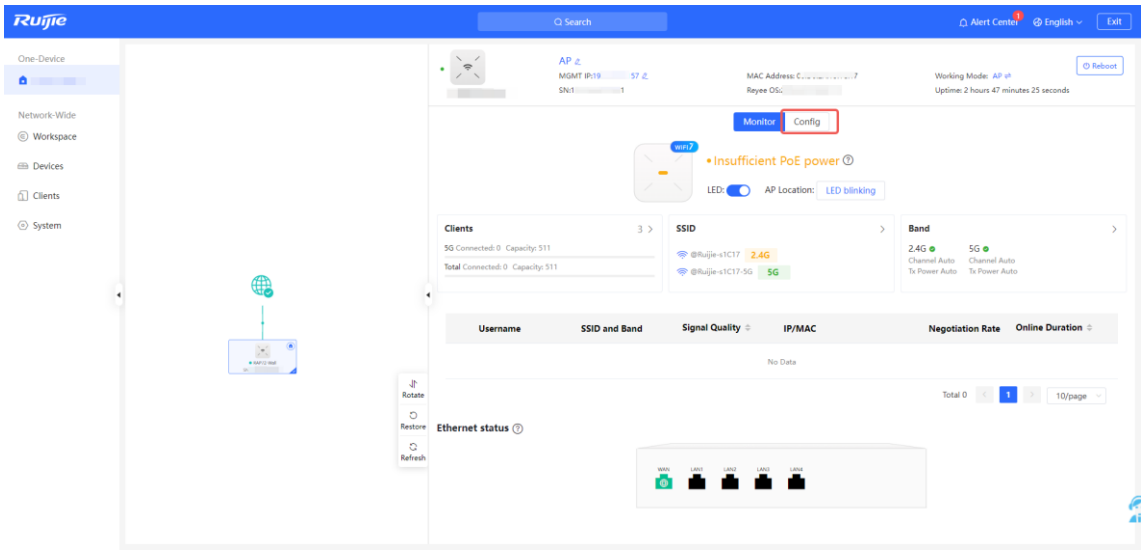
- Network-Wide Mode: Displays the management information of all devices on the network. You can configure all devices on the network from a network-wide perspective.
- Local Device Mode: You can only configure the current logged in device.

Network–Wide Mode

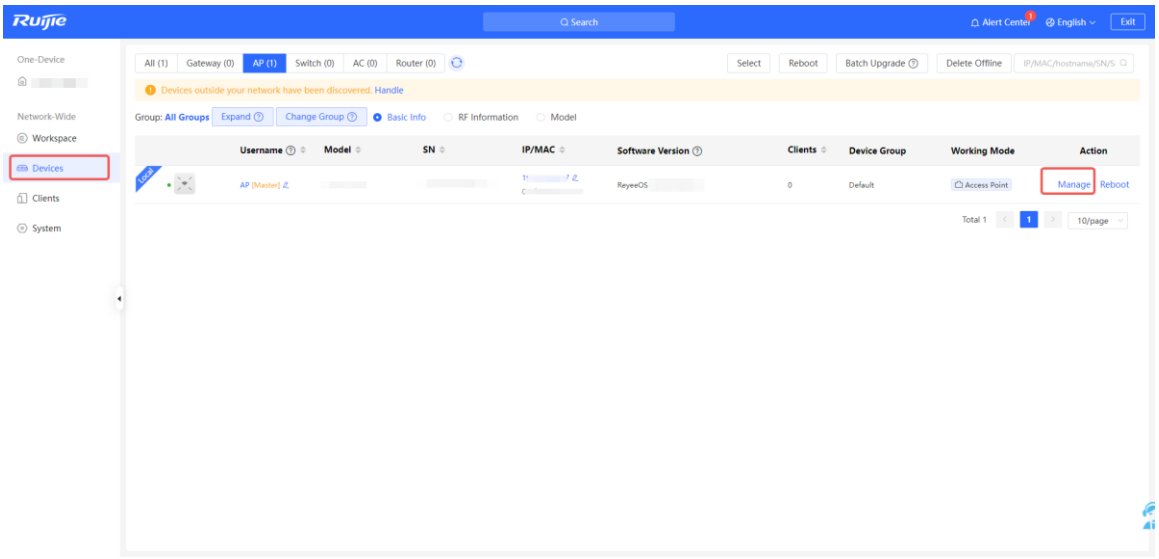


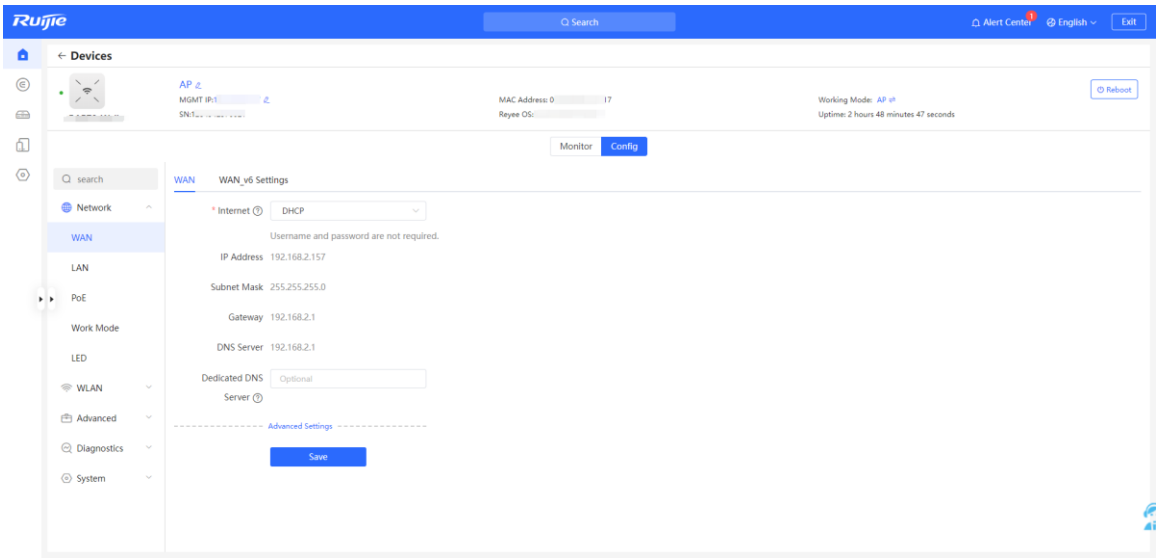
Local Device Mode

- To access the local device mode for the configuration and management of a single device, perform the following steps:
  - Method 1: Click the device name in the One Device menu and then click Config.



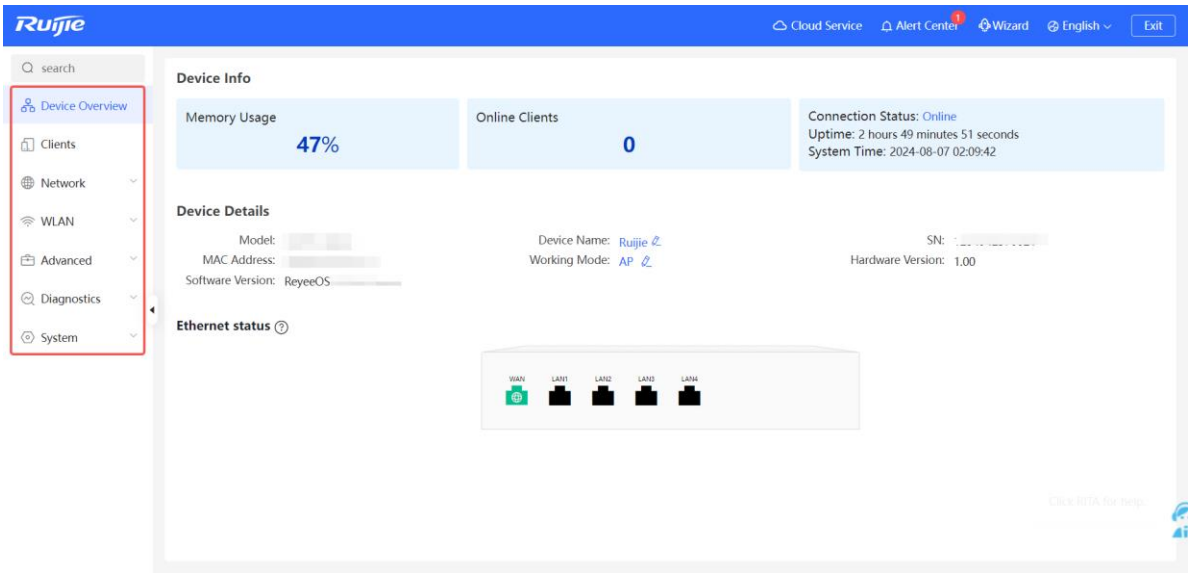
  - Method 2: Choose Network-Wide > Devices and click Manage next to a device in the AP list.





2. Disabling Self-Organizing Network Discovery

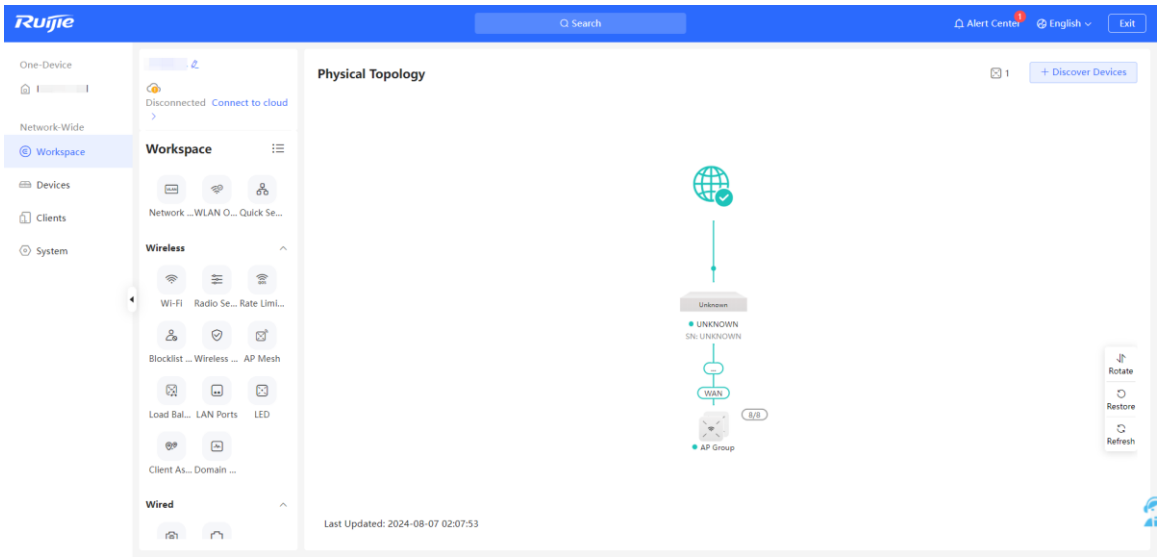
If a device is in standalone mode, you can configure and manage only the currently logged in device. The web interface displays the configuration menu of a single device on the left side.


Ruijie
Cloud Service
Alert Center
Wizard
English
Exit
search
Device Overview
Clients
Network
WLAN
Advanced
Diagnostics
System
Device Info
Memory Usage
47%
Online Clients
0
Connection Status: Online
Uptime: 2 hours 49 minutes 51 seconds
System Time: 2024-08-07 02:09:42
Device Details
Model:
MAC Address:
Software Version: ReyeeOS
Device Name: Ruijie
Working Mode: AP
SN:
Hardware Version: 1.00
Ethernet status
WAN
LAN1
LAN2
LAN3
LAN4

2 Network Monitoring

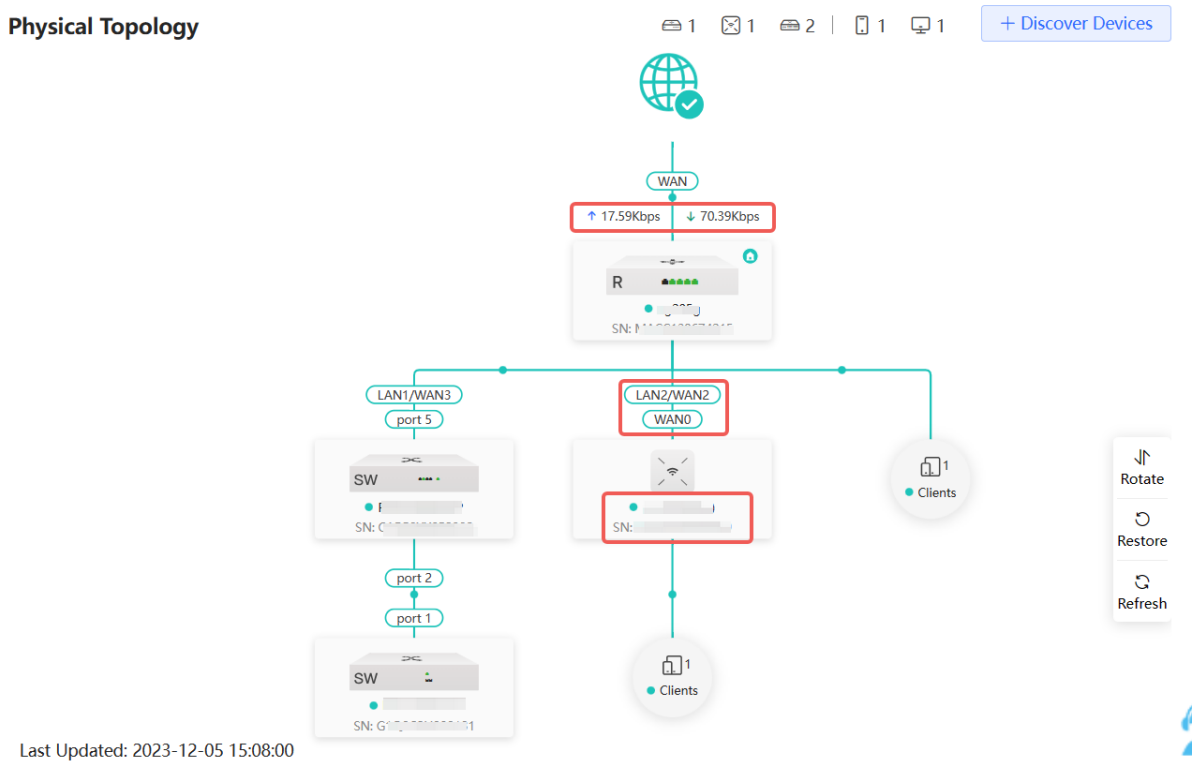
Choose **Network-Wide > Workspace** > **Topology**.

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

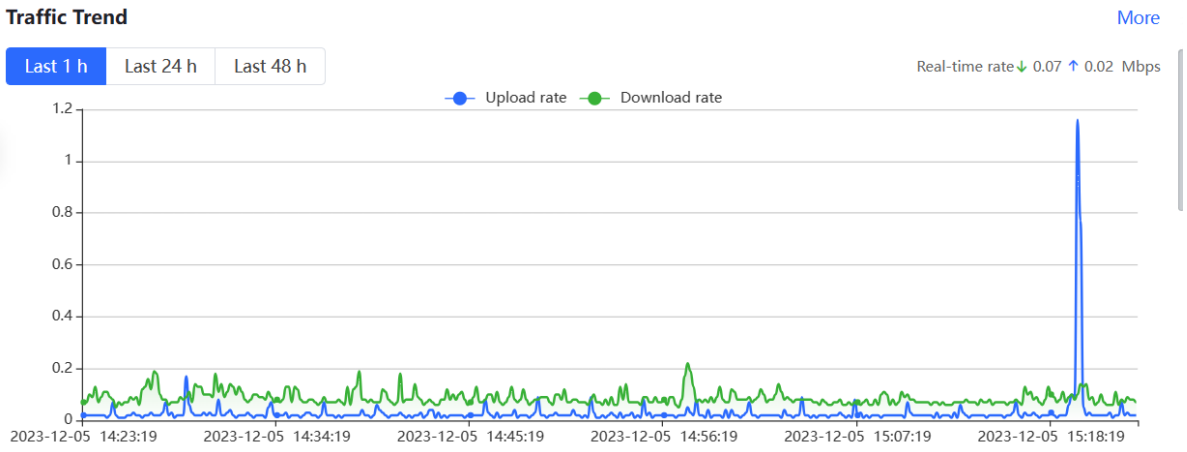


2.1 Viewing the Network Information

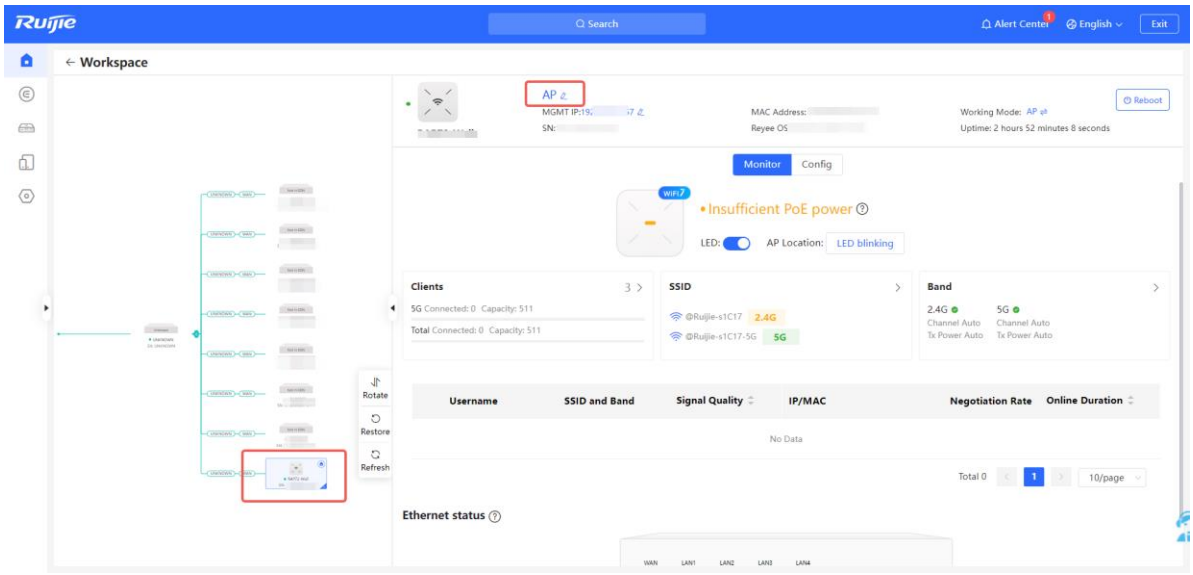
You can view the online device, port ID, device SN as well as the real-time uplink and downlink flow in the network topology.



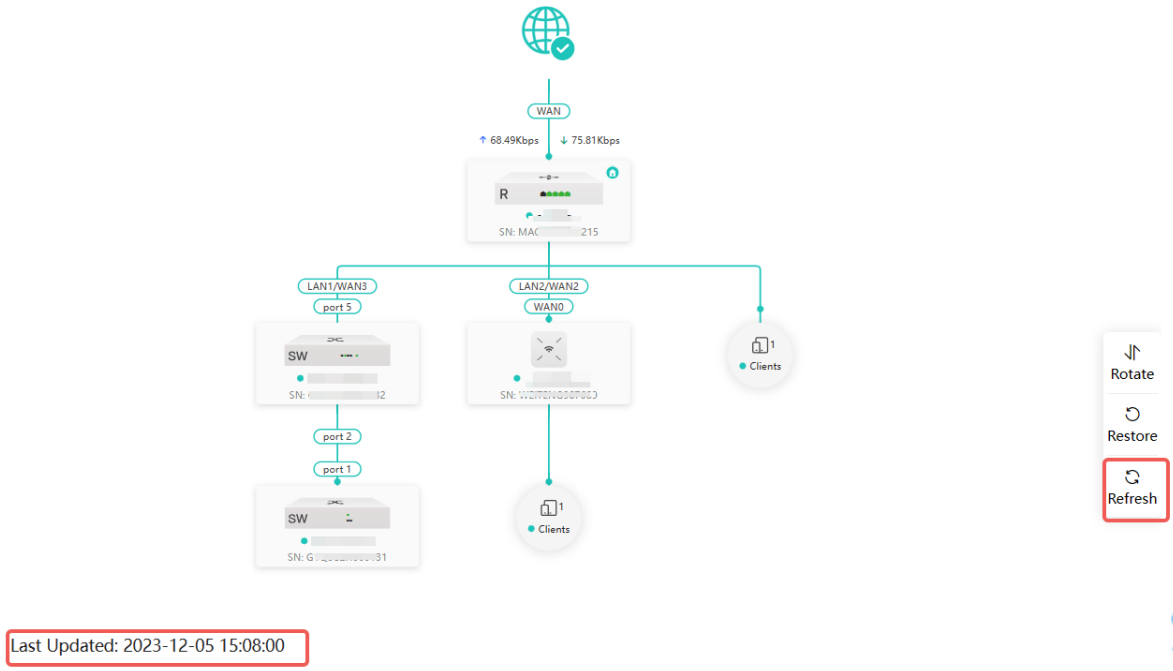
- Click the egress gateway to view real-time traffic information of the device.



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



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

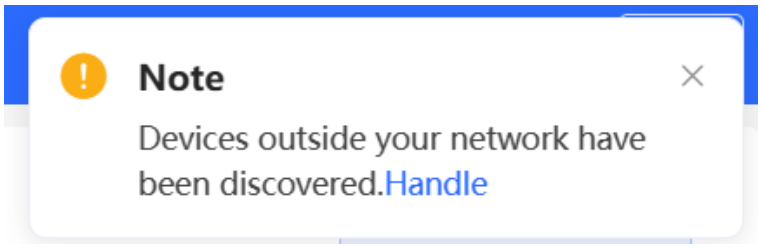


2.2 Adding Network Devices

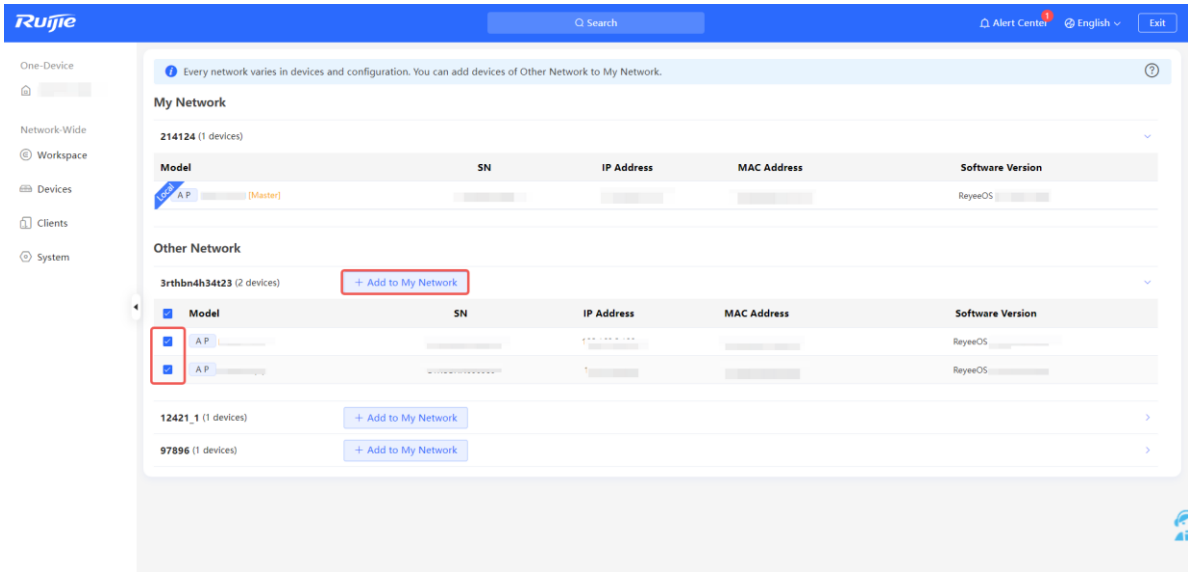
2.2.1 Wired Connection

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

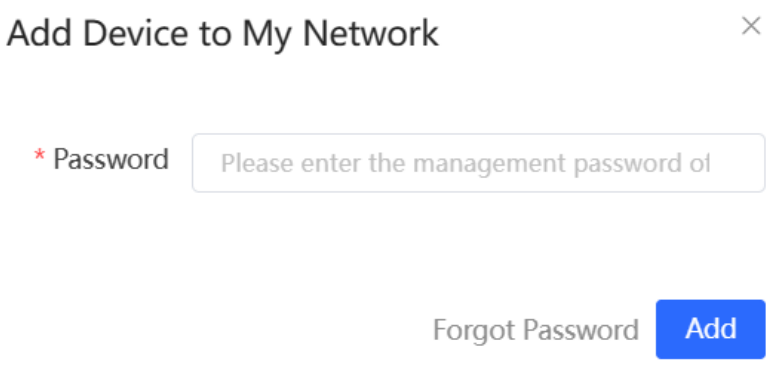
of devices that are not in SON is displayed under the **Devices** at the top left corner of the page. Click **Handle** to add the device to the current network.



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



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



2.2.2 AP Mesh

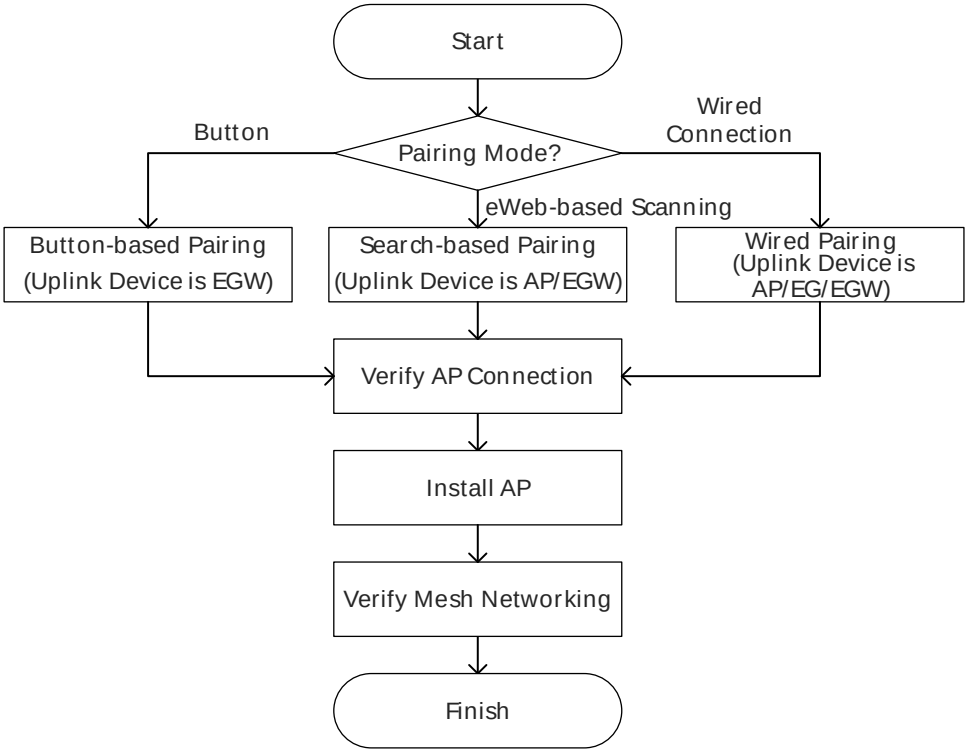
1. Overview

After being powered on and enabled with Mesh (see 3.21 Enabling AP Mesh for details), a Mesh-capable new AP can be paired with other Mesh-capable wireless devices on the target network through multiple ways. Then the AP will be synchronized its Wi-Fi configuration with other devices automatically. Mesh networking addresses pain points such as complex wireless networking and cabling. A new AP can be connected to any uplink wireless device among AP, EG router, and EGW router in the following ways:

- Button-based pairing: Short press the Mesh button on the EGW router on the target network to implement fast pairing of the AP with the EGW router.
- Search-based pairing: Log in to the web interface of a device on the target network. Search and add APs to be paired.
- Wired pairing: Connect the new AP to a wireless device on the target network using an Ethernet cable. The new AP will go online on the target network.

After pairing finishes, the new AP obtains the wireless backhaul information from network-wide neighboring APs. Install the new AP as planned, and it will connect to the optimal neighboring AP.

2. Configuration Steps



3. Configuration Steps for Button-based Pairing

Caution

- The uplink device is an EGW router.
- Only EG105GW-X and EG105GW(T) support button-based pairing, and each router can be paired with up to 15 new APs.

- The master device must be properly configured. Otherwise, AP mesh failure may occur due to constant channel scanning.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.21 Enabling AP Mesh for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

(1) Power on the new AP and place it near the EGW router on the target network.

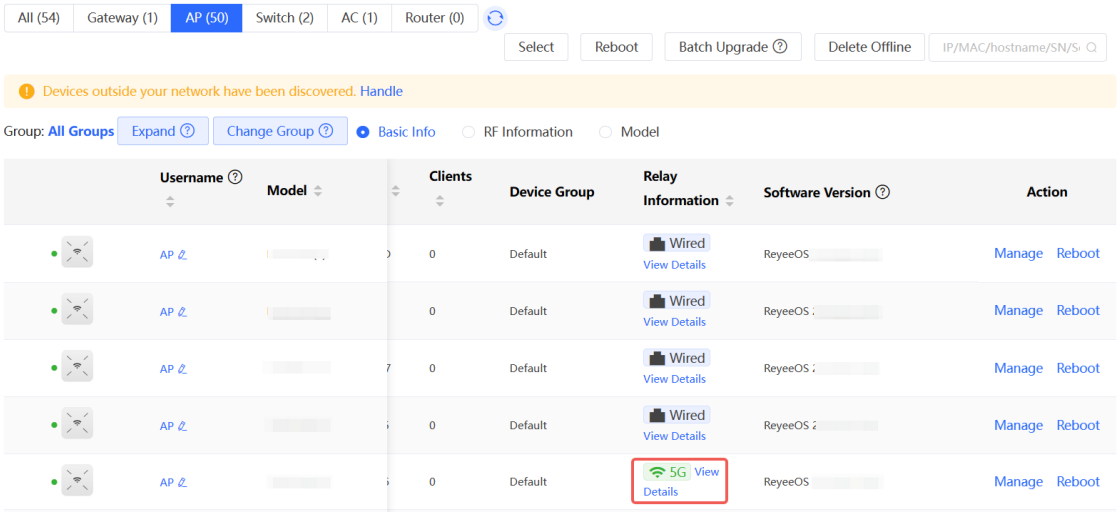
(2) Press and hold the Mesh button  on the EGW router for no more than two seconds to start pairing. The pairing process takes about one minute.

(3) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.

(4) Power off the new AP and install it as planned.

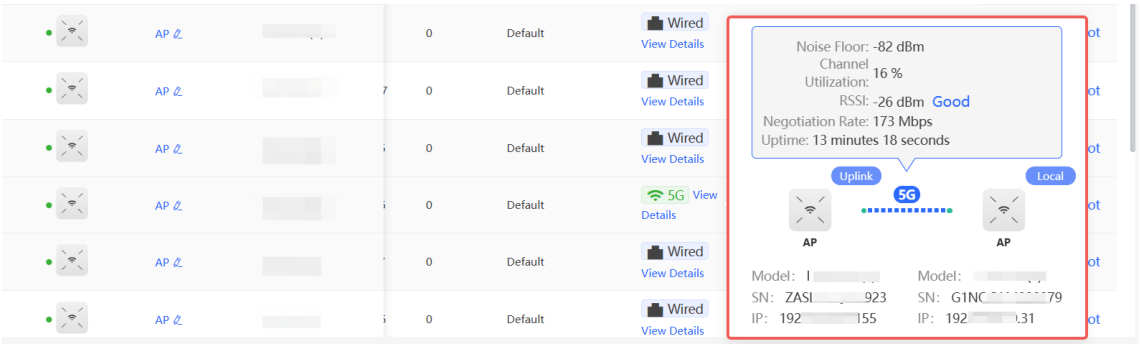
(5) Log in to the web interface of a device on the target network. In **Network-Wide** mode, choose **Devices** > **AP**. Make sure that the new AP is online and the corresponding entry contains icon 

in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



(6) Click **View Details** following the 

icon to obtain information about the uplink device and RSSI.



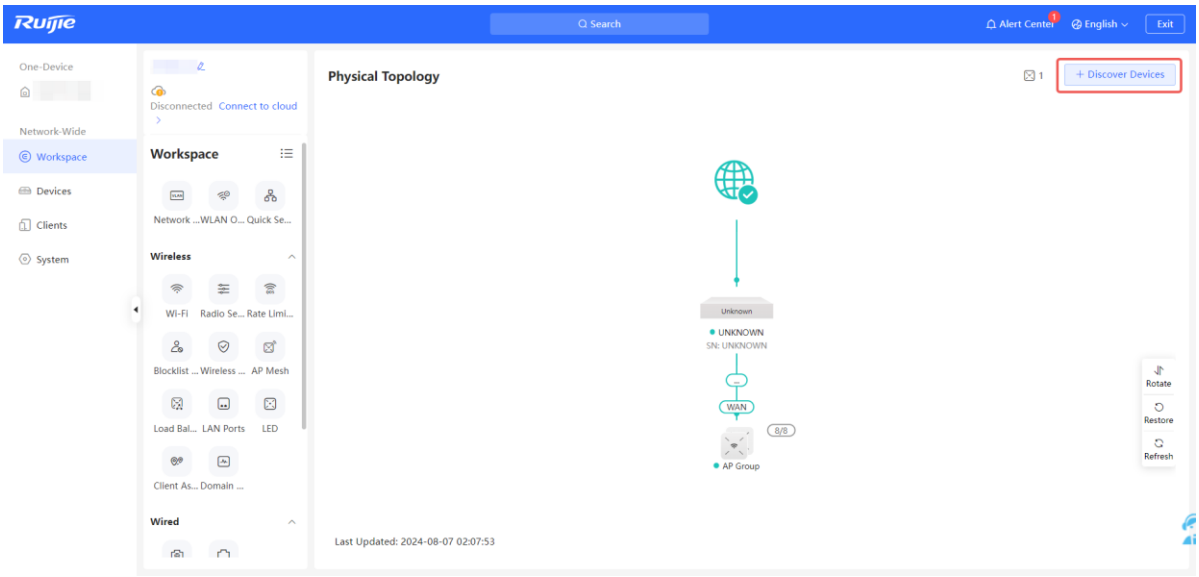
4. Configuration Steps for Search-based Pairing

Caution

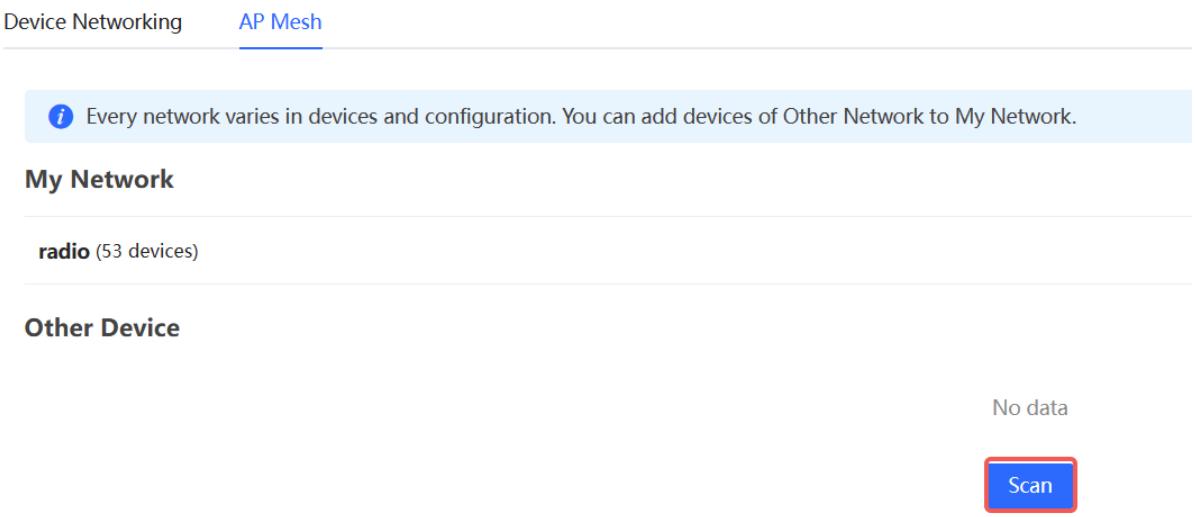
- Uplink device is an AP or EGW router.
- The master device must be properly configured. Otherwise, AP mesh failure may occur due to constant channel scanning.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.21 Enabling AP Mesh for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.
- You can scan to discover new APs on the AP Mesh page only when there are APs supporting the AP Mesh function on the network.

(1) Power on the new AP and place it near the AP or EGW router on the target network.

(2) Log in to the web interface of a device on the target network. In **Network-Wide** mode, click **+Discover Devices** in the upper right corner of the **Physical Topology** page to scan the APs in other networks not plugged in with Ethernet cables.



(3) On the **AP Mesh** page, click **Scan** to scan devices that are not connected to the network via an Ethernet cable.



(4) Select the APs to be added and click **Add to My Network**. No more than eight APs are allowed at a time. Wait until network merging finishes.

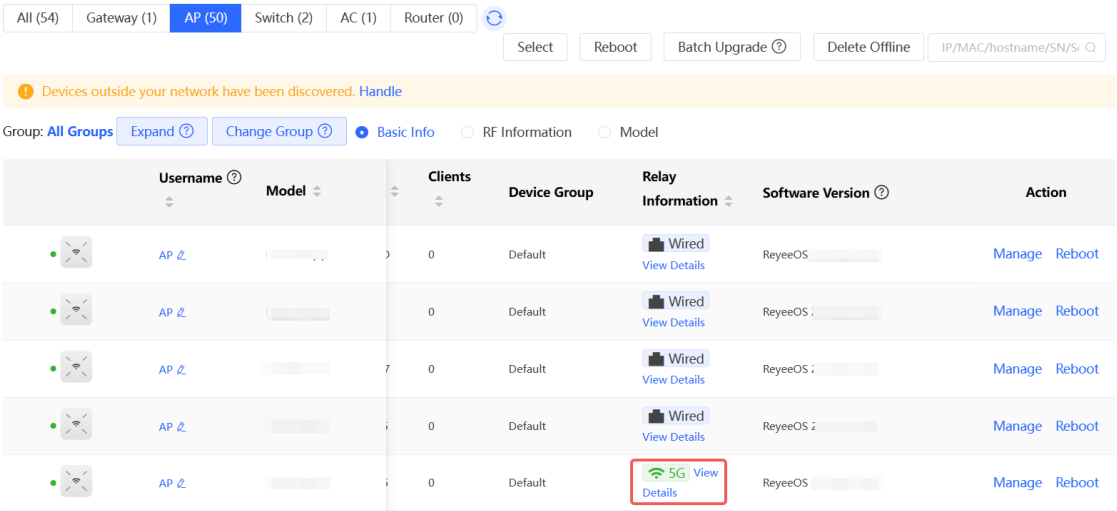
(5) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.

(6) Power off the new AP and install it as planned.

(7) Log in to the web interface of a device on the target network. In **Network-Wide** mode, choose **Devices** > **AP**.

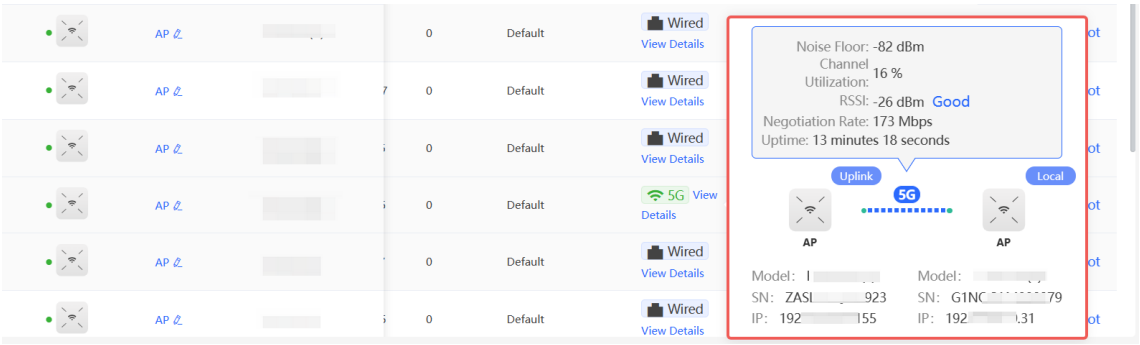
Make sure that the new AP is online and the corresponding entry contains icon 

in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



(8) Click **View Details** following the 

icon to obtain information about the uplink device and RSSI.



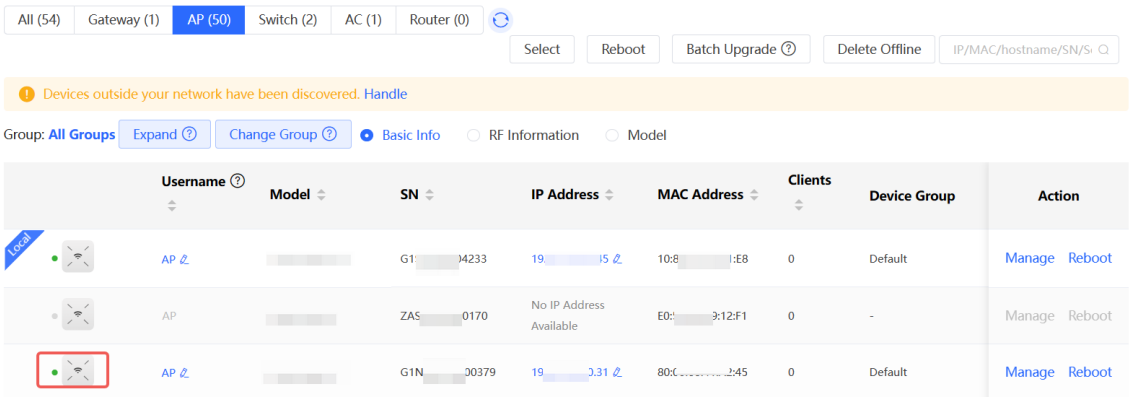
5. Configuration Steps for Wired Pairing

Caution

- Uplink device is an AP, EG router, or EGW router.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.21 Enabling AP Mesh for details).

(1) Plug one end of the Ethernet cable to the uplink port of the new AP, and the other end to the downlink port of an AP, EG router, or EGW router on the target network. Mesh networking takes one to three minutes. When the system status LED is steady on, it indicates that Mesh networking finishes.

(2) Log in to the web interface of a device on the target network. In **Network-Wide** mode, choose **Devices** and make sure that the new AP is online.



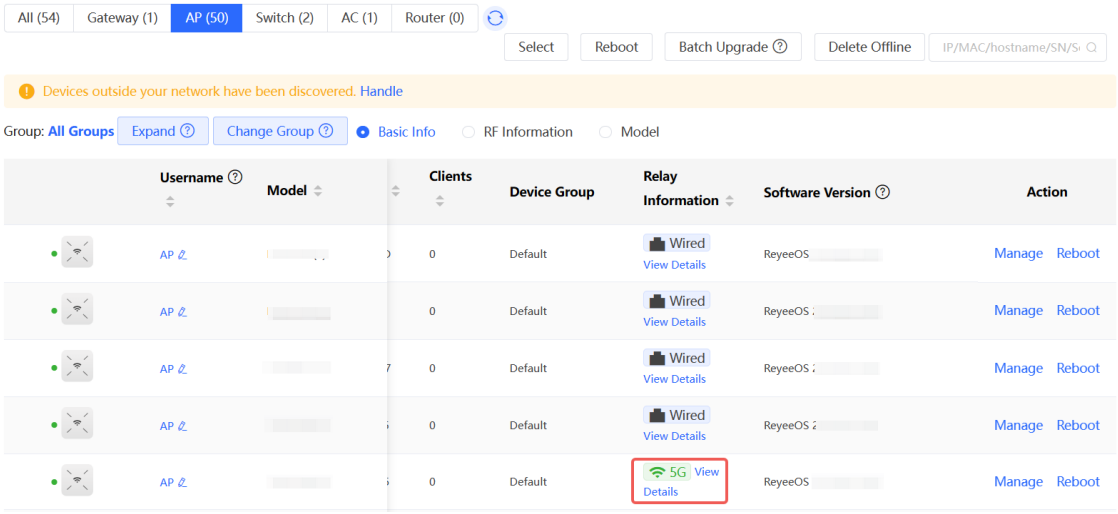
(3) **Self-Healing Mesh** is disabled by default. You need to enable it first (for details, see4.12 Configuring Self-Healing Mesh) to complete the wired-to-wireless handoff process.

(4) Unplug the Ethernet cable, power off the new AP, and install it as planned.

(5) Log in to the web interface of a device on the target network. In **Network-Wide** mode, choose **Devices** > **AP**.

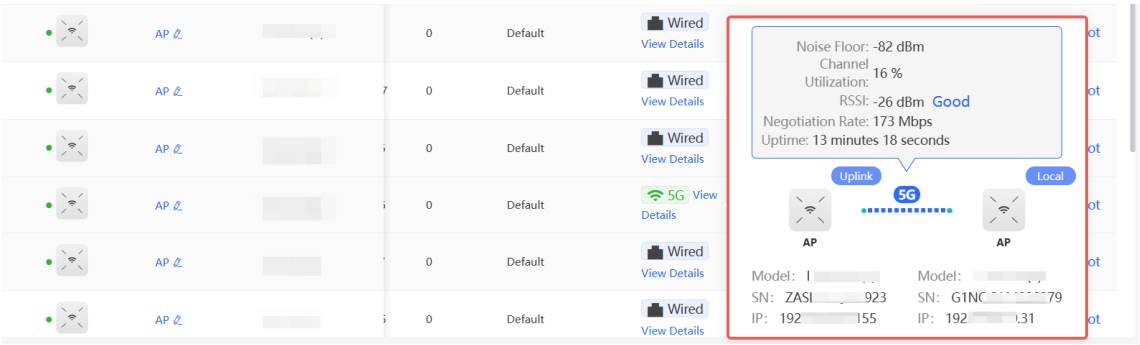
Make sure that the new AP is online and the corresponding entry contains icon 

in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



(6) Click **View Details** following the 

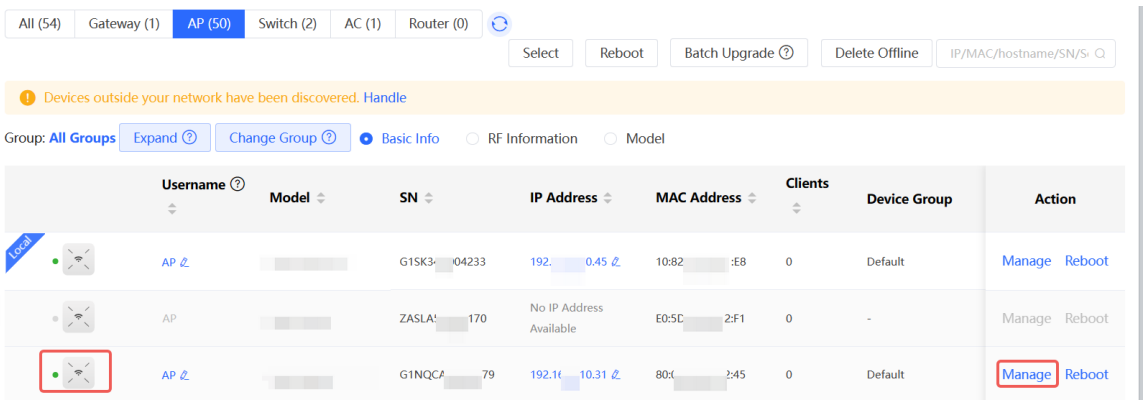
icon to obtain information about the uplink device and RSSI.



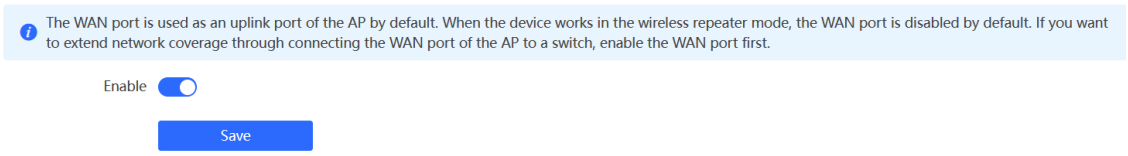
6. Enabling WAN Port

The WAN port works as the wired uplink port of the AP by default. For the AP added to the target network through Mesh pairing, the WAN port is disabled by default. If you want to connect the Mesh AP to other downlink device in wired mode to expand the network, enable this port.

(1) Log in to the web interface of the network project. Choose **Network-Wide** > **Devices** > **AP**, and click **Manage** next to a device in the AP list.



(2) Choose **Config** > **Advanced** > **Enable WAN**, toggle on **Enable**, and click **Save**.



7. Querying Mesh APs and Mesh Details

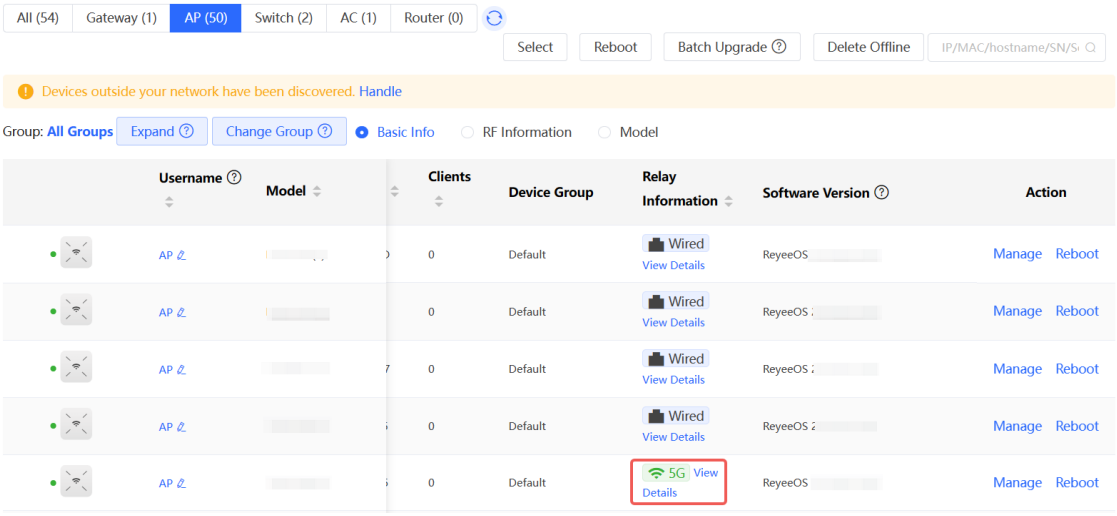
(1) Log in to the web interface of a device on the target network.

(2) Query Mesh APs.

- Method 1: In **Network-Wide** mode, check the topology on the **Physical Topology** page. The AP that connects to the uplink device in wireless mode is a Mesh AP.

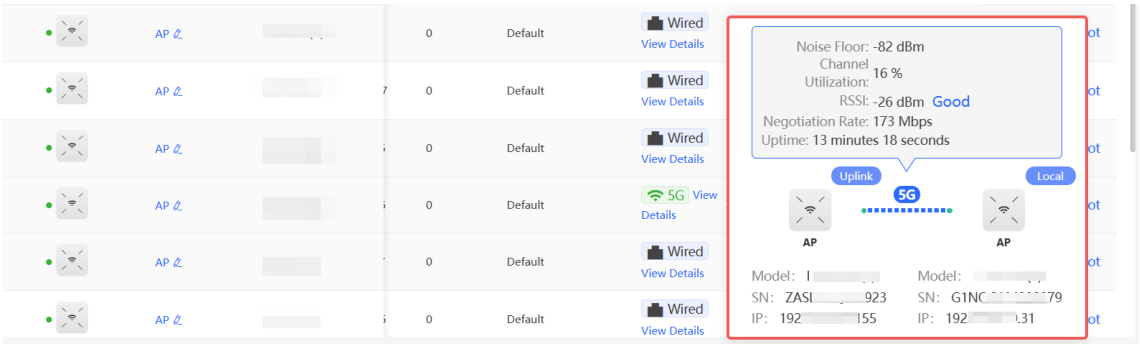
- Method 2: In **Network-Wide** mode, choose **Devices** > **AP**. If an entry contains icon 

in the **Relay Information** column, the corresponding AP is a Mesh AP.



(3) Query Mesh networking details.

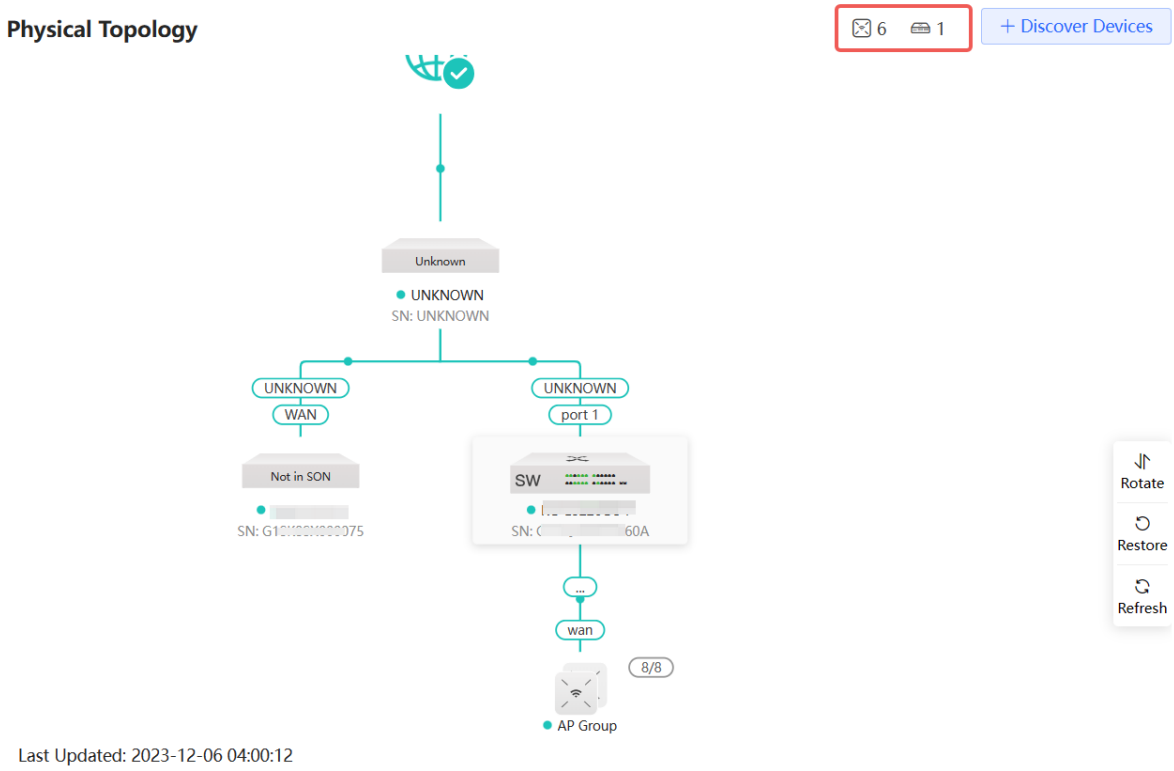
In **Network-Wide** mode, choose **Devices** > **AP**. Select the target AP, and click **View Details** in the **Relay Information** column to obtain the Mesh networking details.



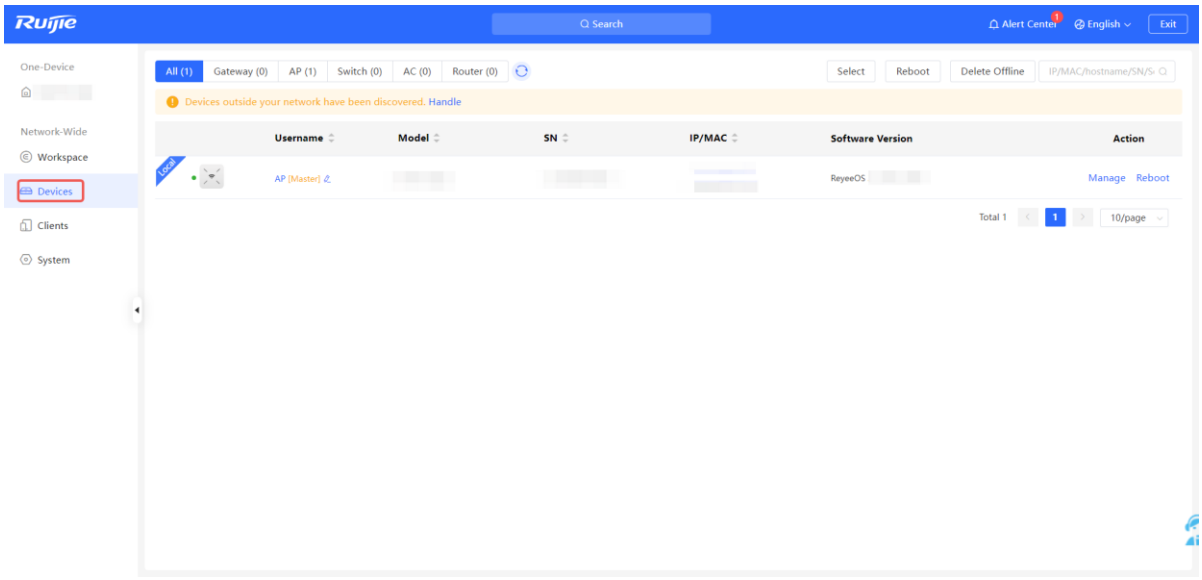
2.3 Managing Network Devices

You can view information of all devices on the network. You can configure and manage all devices on the network by simply logging in to only one device on the network. Follow the following steps to access the device's management page:

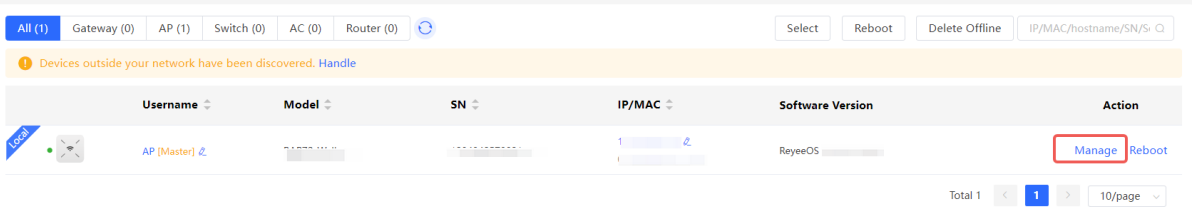
- Method 1: Click the device icon in the upper right corner of the topology to switch to the device list view.



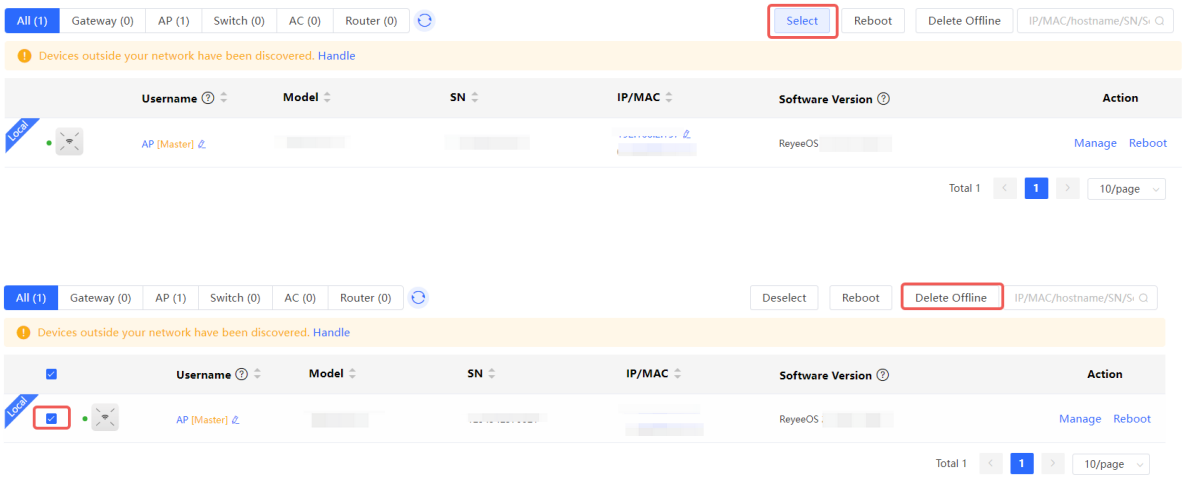
- Method 2: Choose **Network-Wide** > **Devices**.



- Click **Manage** to configure the selected device.

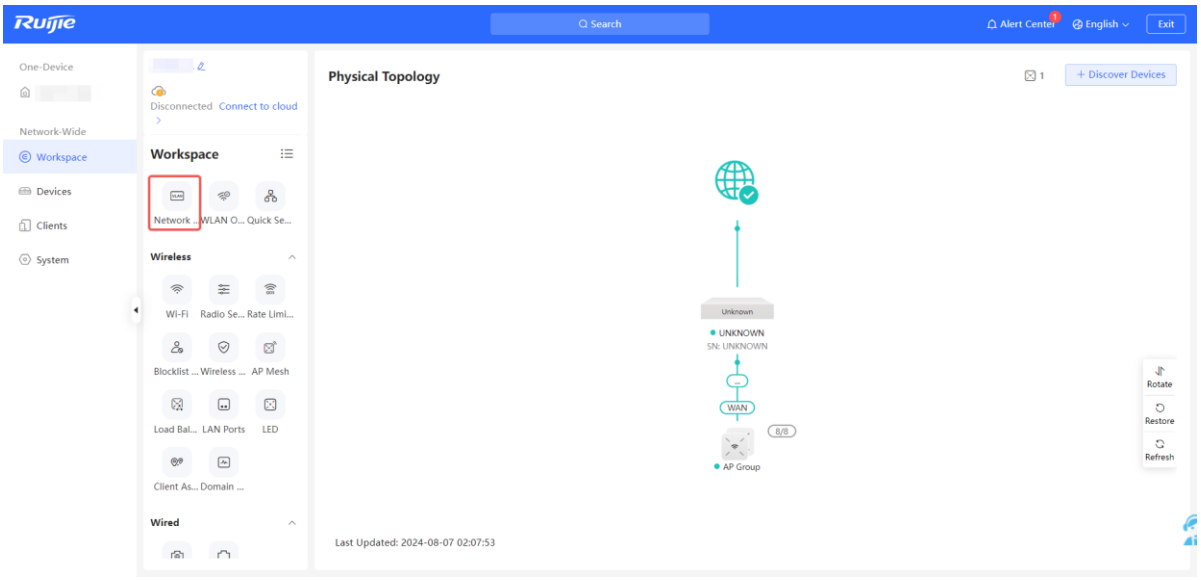


- Click **Select** to select an offline device, and click **Delete Offline** to remove the selected device from the list and the topology.

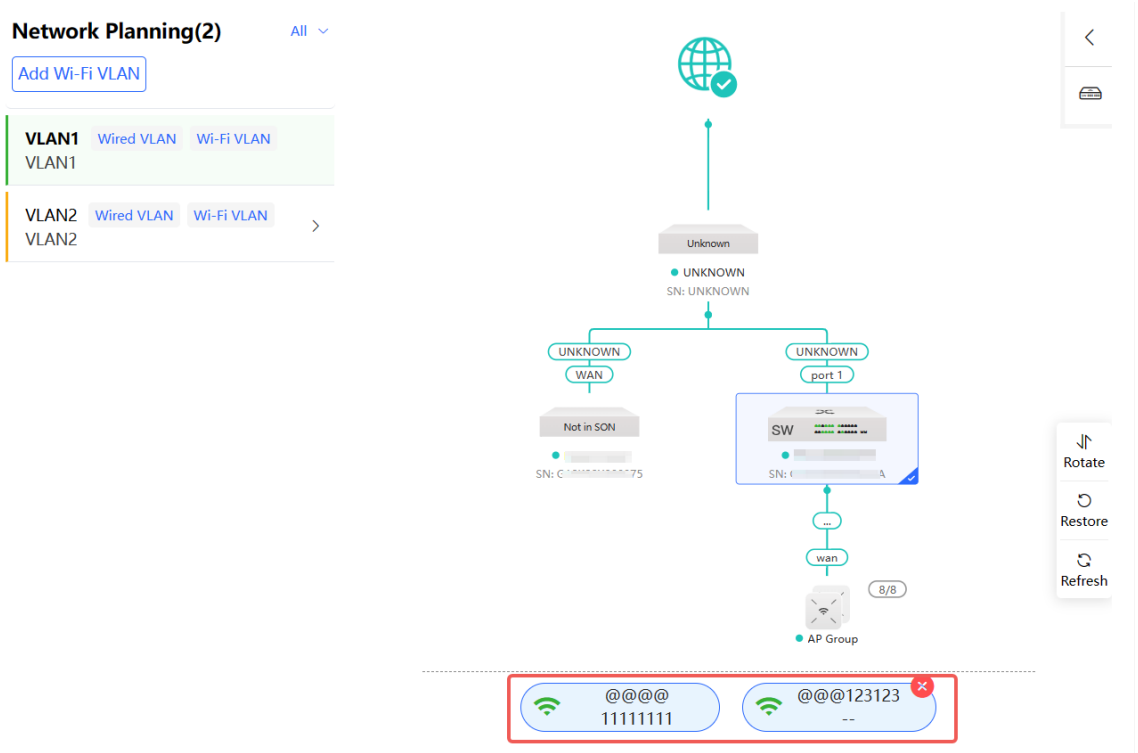


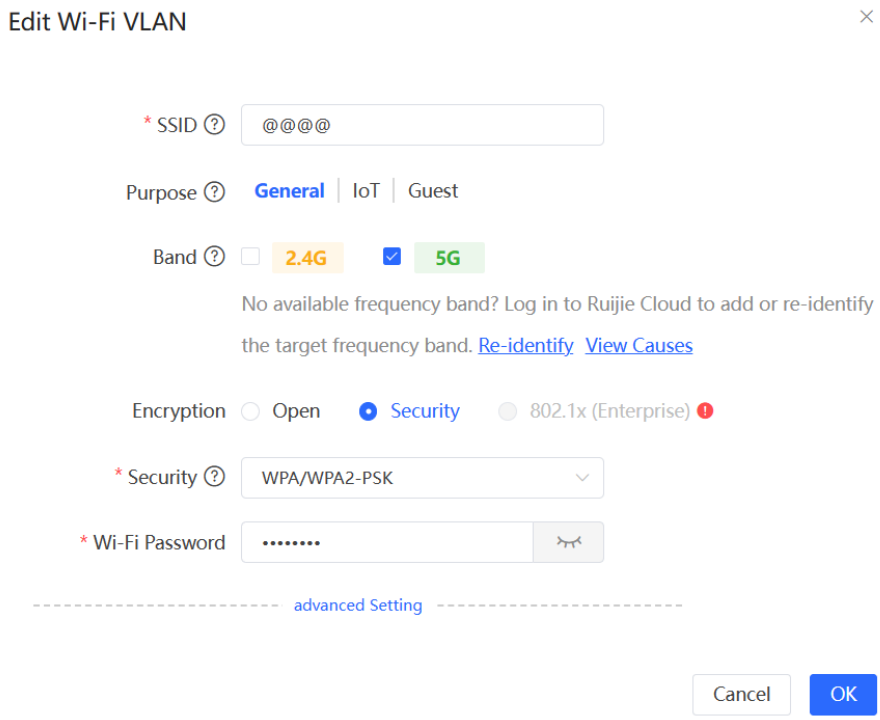
2.4 Configuring Network Planning

Choose **Network-Wide** > **Workspace** > **Network Planning**.



Click the SSID to edit the Wi-Fi configuration. For details, see Chapter 3 [Wi-Fi Network Settings.]

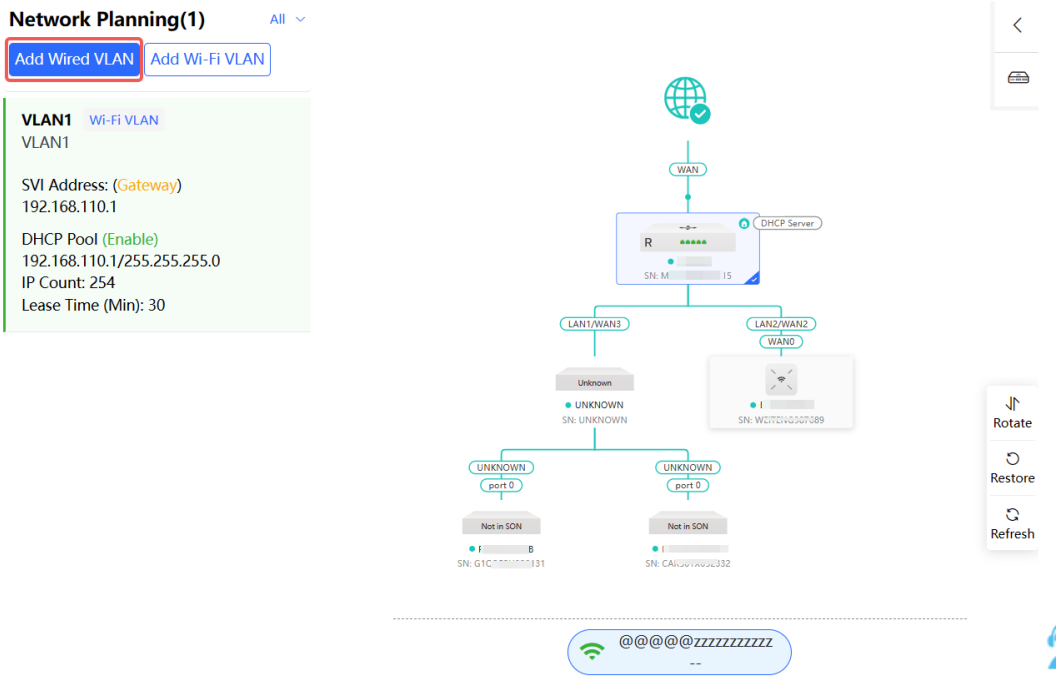




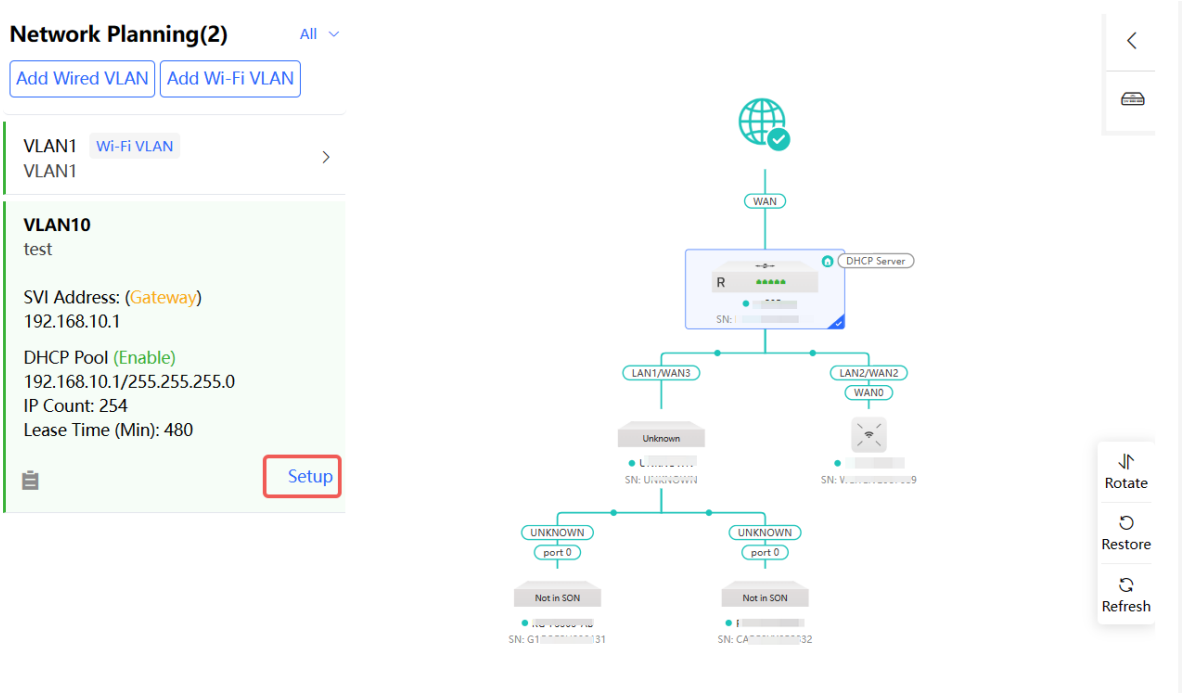
2.4.1 Configuring Wired VLAN

Choose **Network-Wide** > **Workspace** > **Network Planning**.

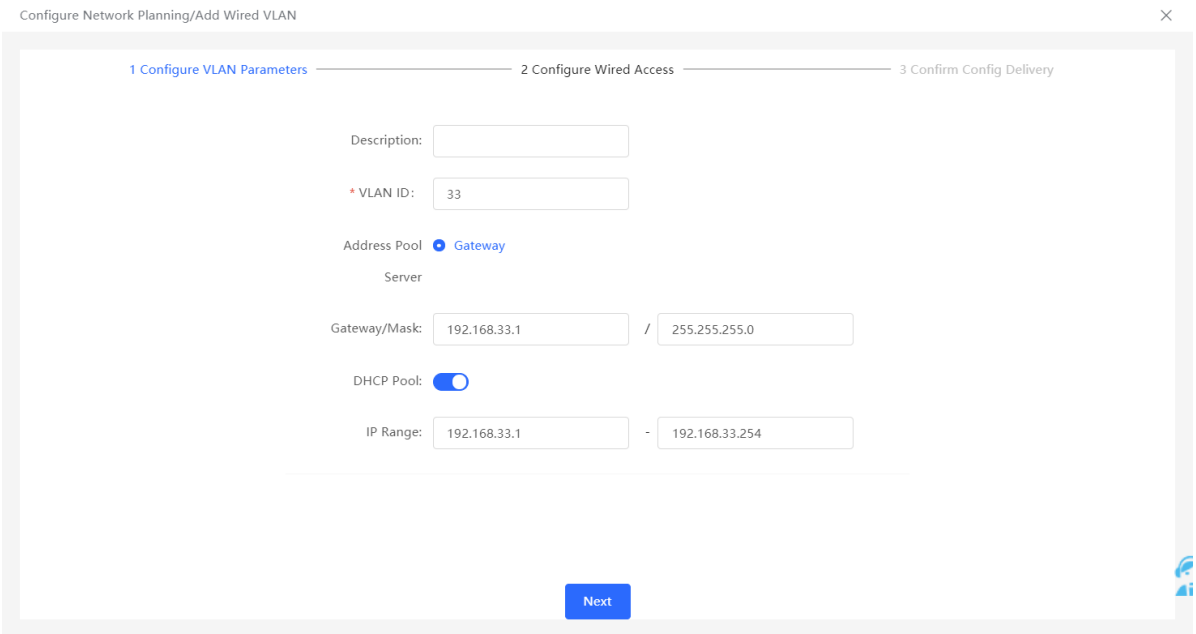
On the **Network Planning** page, click **Add Wired VLAN**.



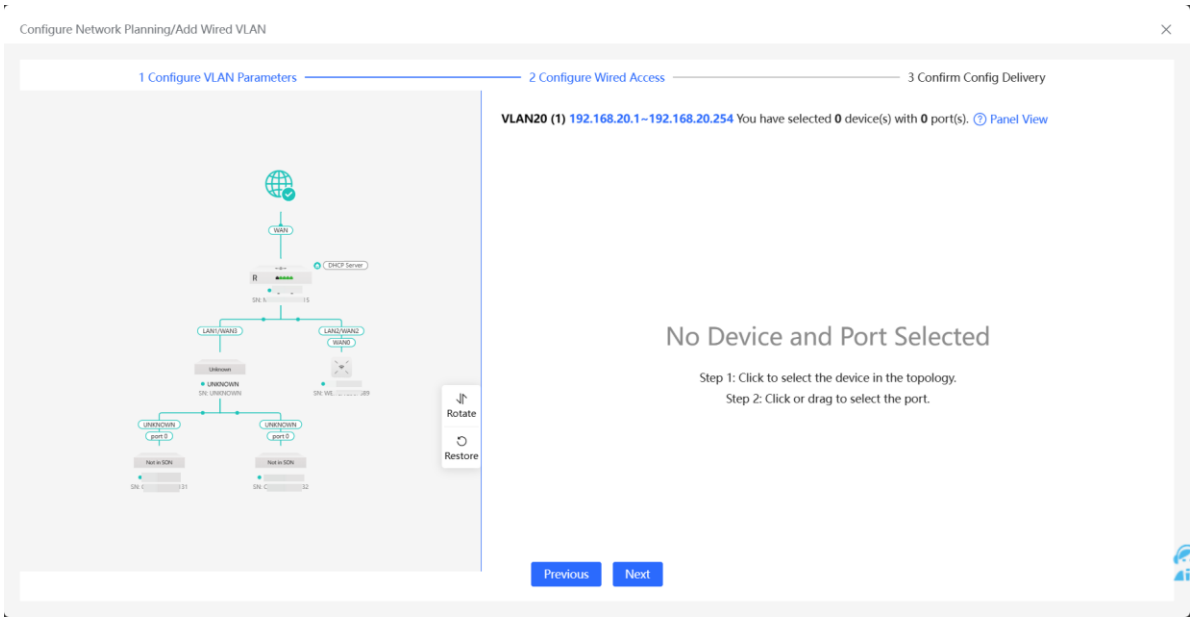
Alternatively, you can select an existing wired VLAN and click **Setup** to edit the VLAN.



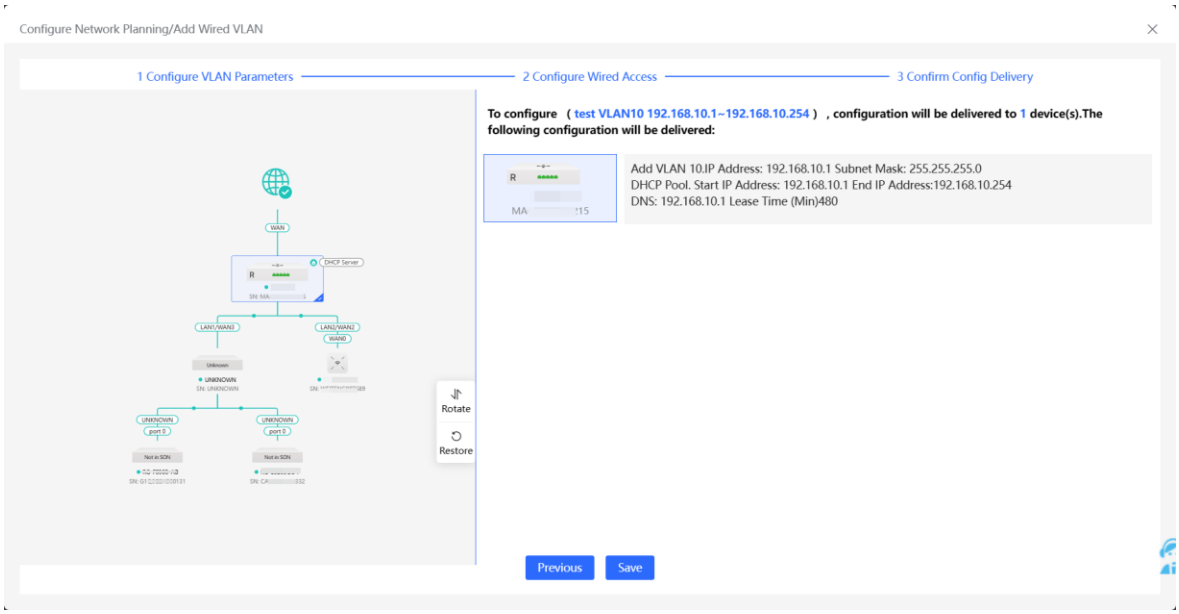
(1) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters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



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



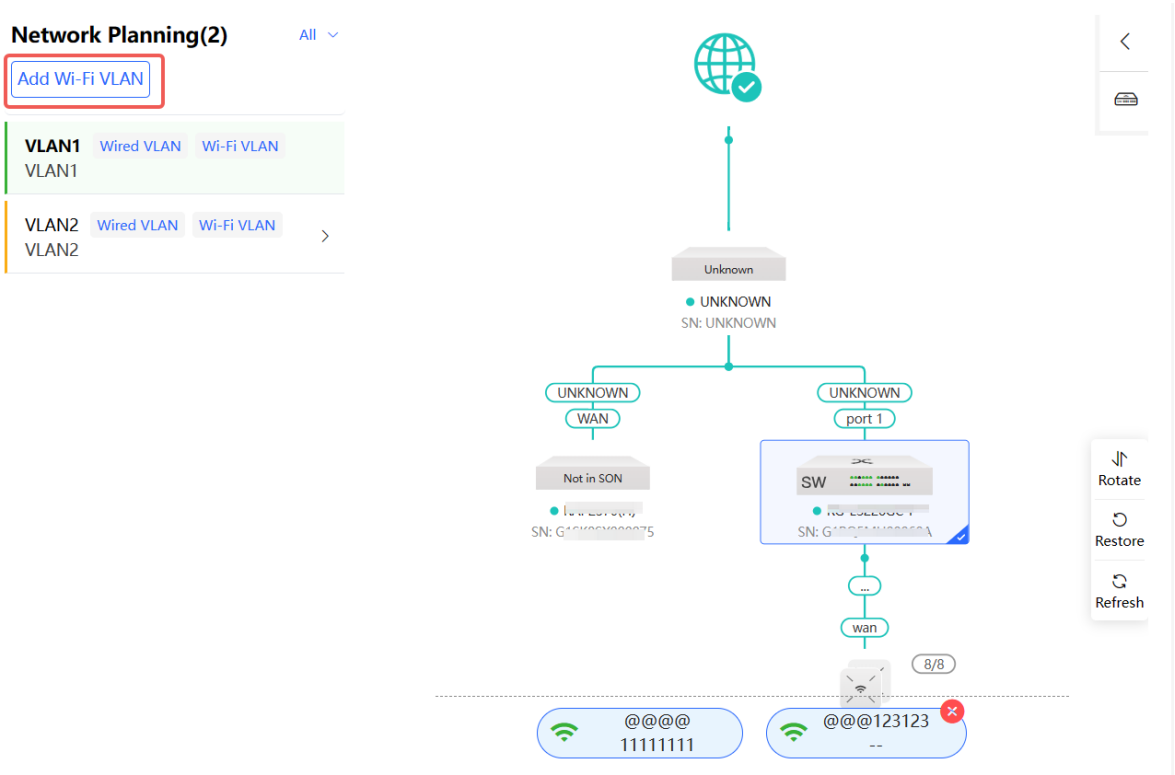
(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



2.4.2 Configuring Wi-Fi VLAN

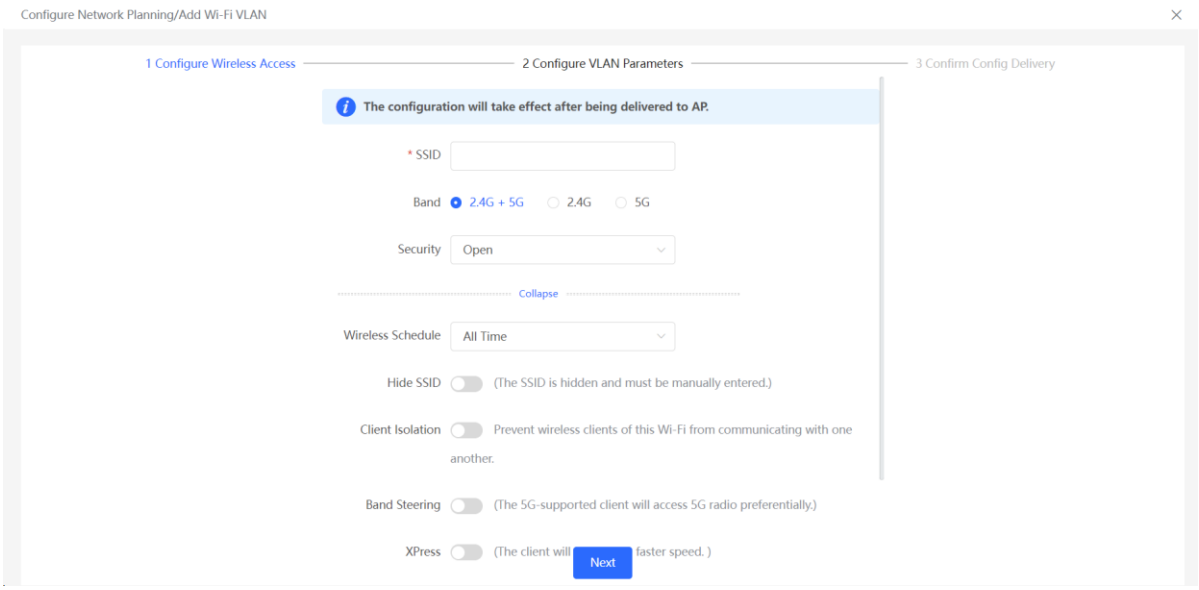
Choose **Network-Wide** > **Workspace** > **Network Planning**.

On the **Network Planning** page, click **Add Wi-Fi LAN**.

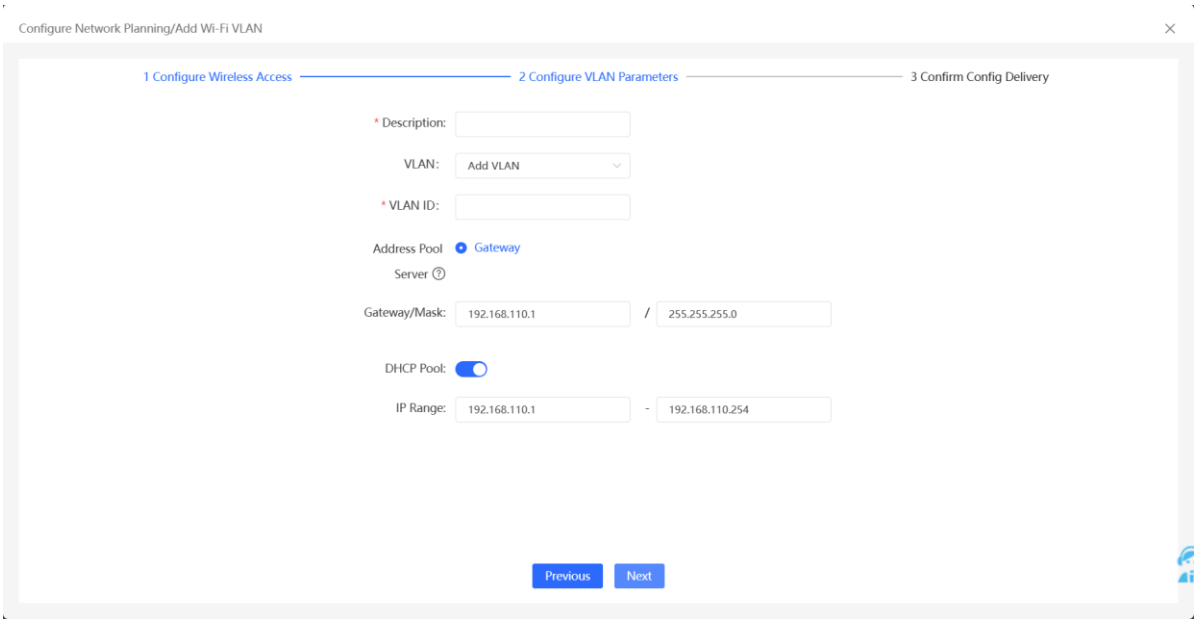


Alternatively, you can select an existing wireless VLAN and click **Setup** to edit the VLAN.

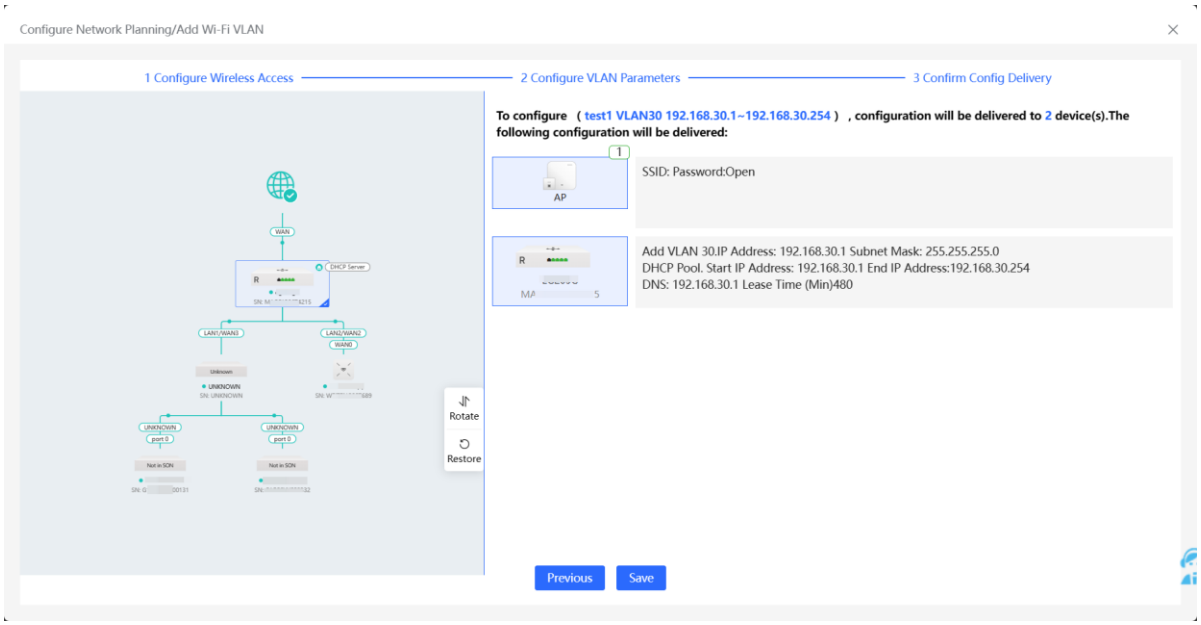
(1) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.



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



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



3 Wi-Fi Network Settings

Note

Wi-Fi network settings covers the Wi-Fi settings of the currently logged in devices and the management of all wireless devices in the network. In **Network** mode, the Wi-Fi network settings are synchronized to all wireless devices in the network. You can configure device groups to limit the synchronization range. For details, see 3.1 Configuring AP Groups.

3.1 Configuring AP Groups

3.1.1 Overview

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

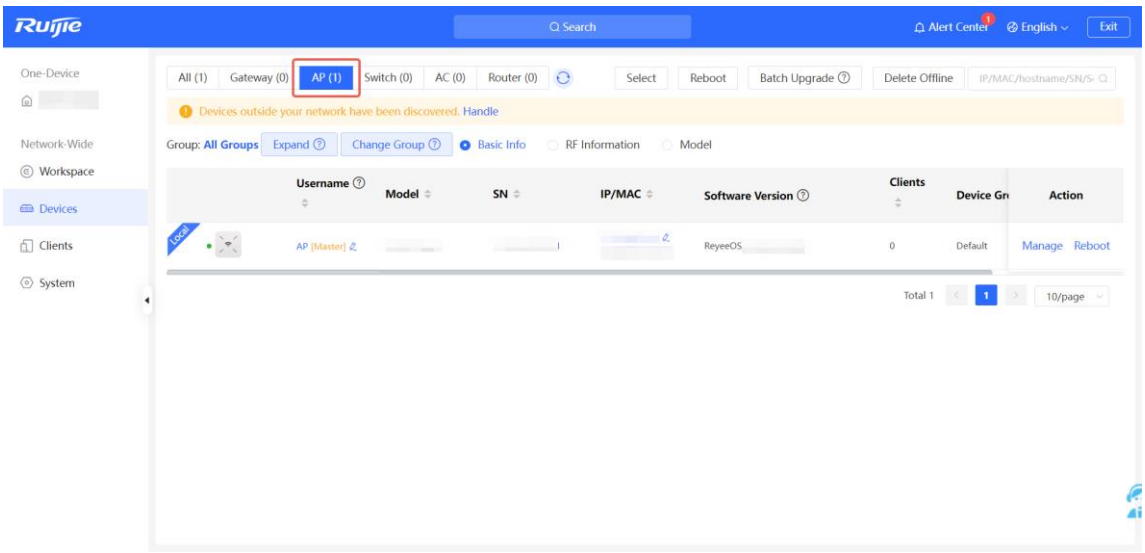
Note

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

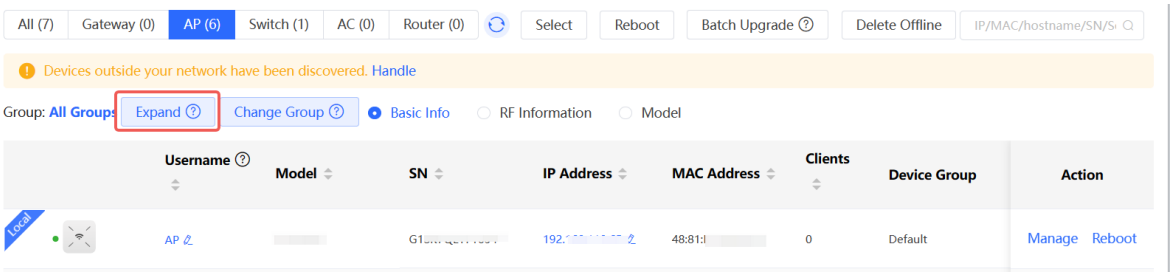
3.1.2 Configuration Steps

Choose **Network-Wide** > **Devices** > **AP**.

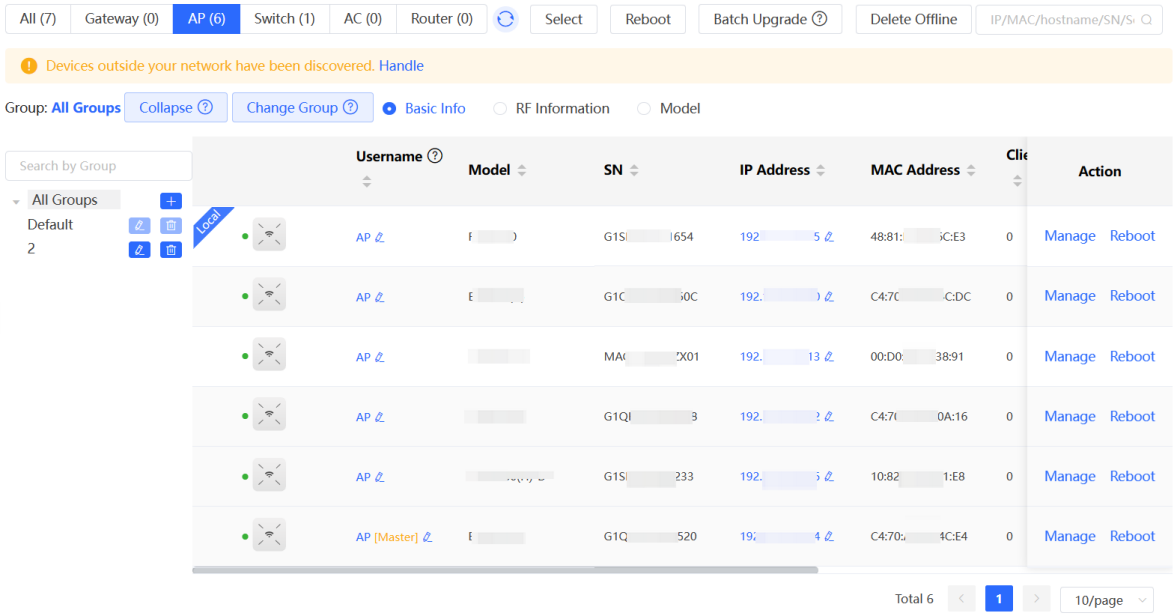
(1) The **AP** page displays all APs on the network. Click **Manage** to configure the selected device.



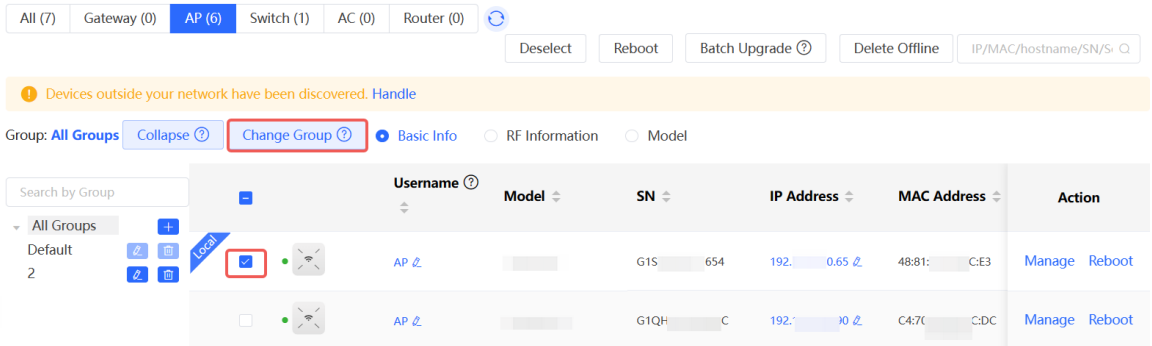
(2) Click **Expand** to view all device groups on the left section of the **Devices** page.

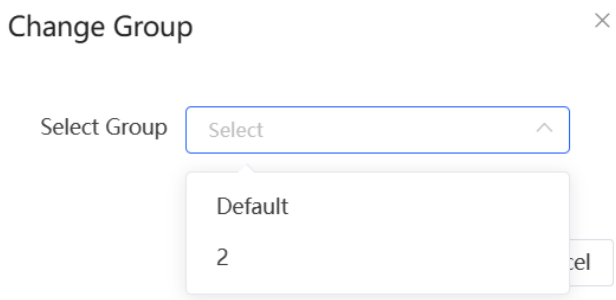


(3) Click  to create a new group. Up to 8 groups can be added. You can click  to edit the group name and click  to delete the group. The default group cannot be deleted and its name cannot be edited.



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



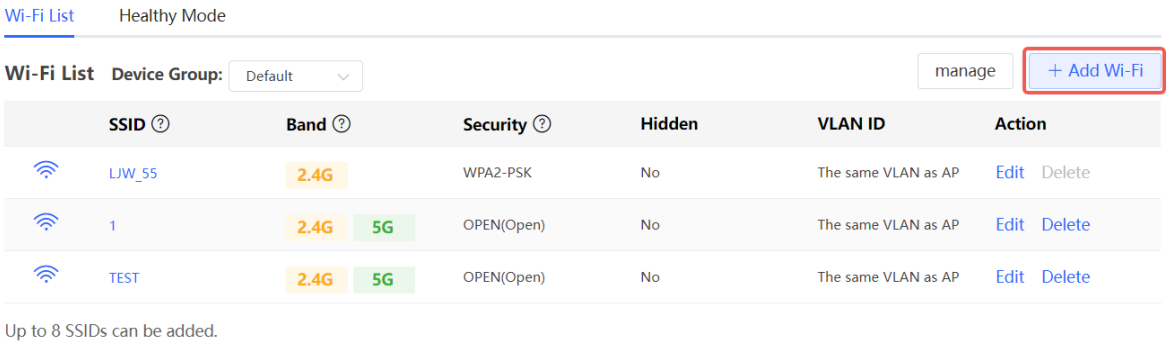


3.2 Adding a Wi-Fi Network

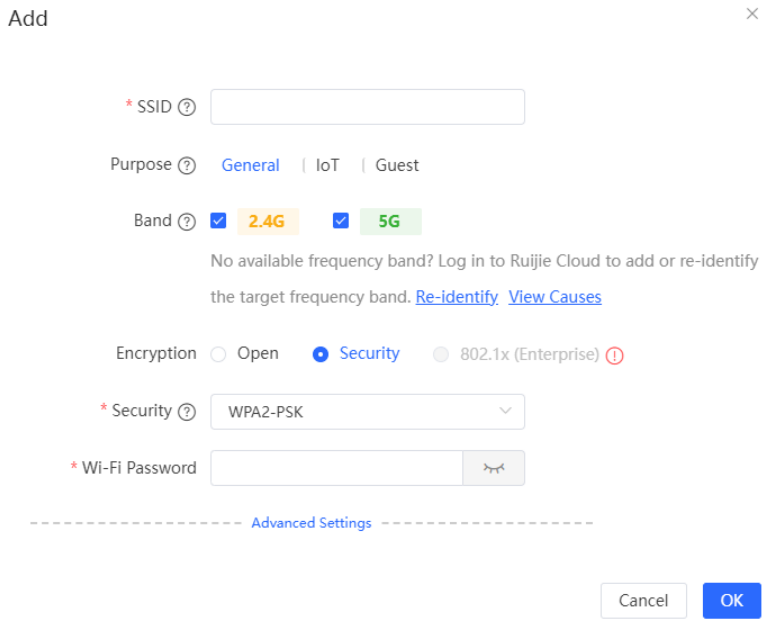
(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide > Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**.

(2) Click **Add Wi-Fi**.



(3) Configure the SSID, password, and other information.



(4) Click **advanced Settings** to configure more Wi-Fi parameters. After configuration, click **OK**. After the Wi-Fi is added, a client can detect the SSID, and the Wi-Fi information is displayed in the Wi-Fi list.

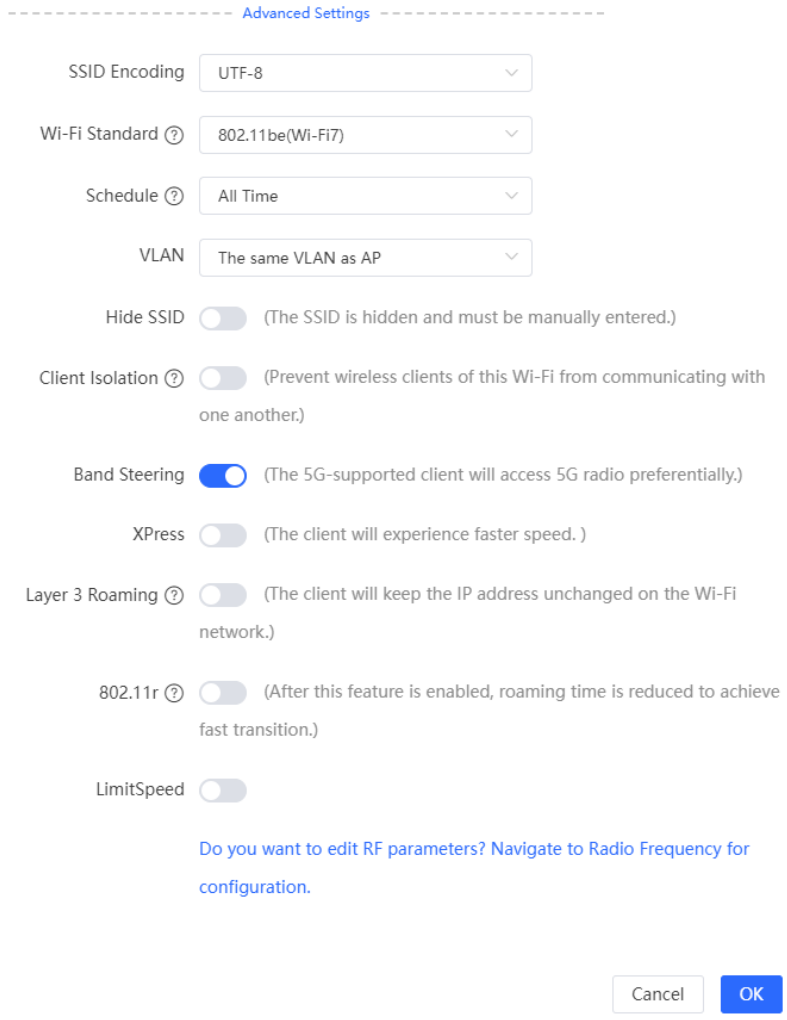


Table 3-1 Wi-Fi Configuration Parameters

Parameter	Description
SSID	Enter 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 "GB2312" as the SSID encoding standard.
Purpose	Set the Wi-Fi usage scenario. The options include **General**, **IoT**, and **Guest**. The system will recommend different Wi-Fi parameter combinations based on the selected purpose.

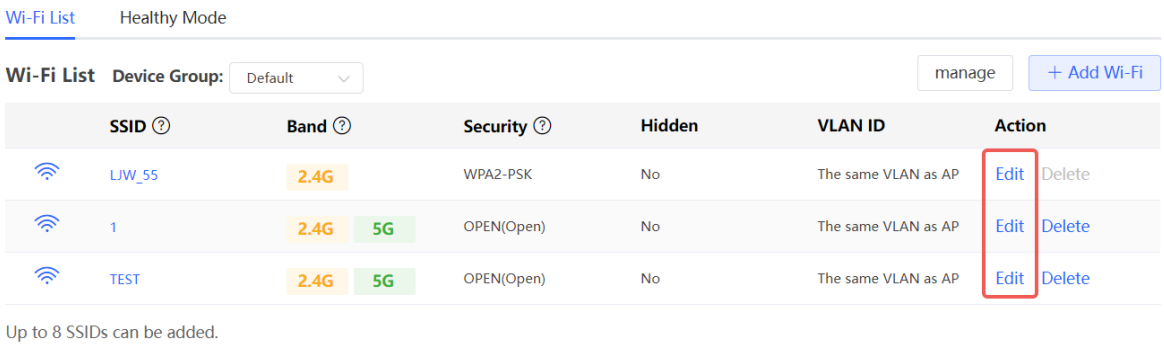
Parameter	Description
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is **2.4G + 5G**, indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.
Encryption	The encryption options for a Wi-Fi network include **Open**, **Security**, and **802.1x (Enterprise)**.
Wi-Fi Password	When the **Security** is set to WEP, you need to set the password for connecting to the wireless network. The password is a string of 8 to 63 characters.
Select server group	When the **Encryption** is set to **802. 1x (Enterprise)**, you need to configure a remote server set for authentication and authorization.
Wi-Fi Standard	The Wi-Fi standards include **802.11be (Wi-Fi 7)**, **802.11ax (Wi-Fi 6)**, or **Compatibility Mode**. The final effective Wi-Fi standard depends on the support of Wi-Fi standards on each device. The latest standard is recommended. If there is a compatibility issue, try use an older standard. However, an old standard setting will affect the bandwidth.
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 choose from the available VLANs or click **Add New VLAN**, and go to the **LAN Settings** page to add a VLAN.
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 SSID after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current SSID before you enable this function.
Client Isolation	After you enable this parameter, 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, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when **Band** is set to **2.4G + 5G**.

Parameter	Description
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.
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.
802.11r	Enabling the 802. 11r function can shorten the roaming handover time. The 802. 11r function is supported only when **Encryption** is set to **Security** or **802. 1x (Enterprise)**. Once 802. 11r is enabled, the encryption type can only be WPA2-PSK or WPA2-802.1X.
LimitSpeed	After enabling Wi-Fi rate limiting, you can set the uplink and downlink rate limits for users. ● Rate Limit Per User: The rate limit applies to all clients connected to the SSID. ● Rate Limit All Users: All clients connected to the SSID share the configured rate limit equally. The rate limit of each client changes dynamically with the number of clients connected to the SSID.

3.3 Configuring SSID and Wi-Fi Password

(1) Go to the page for configuration.

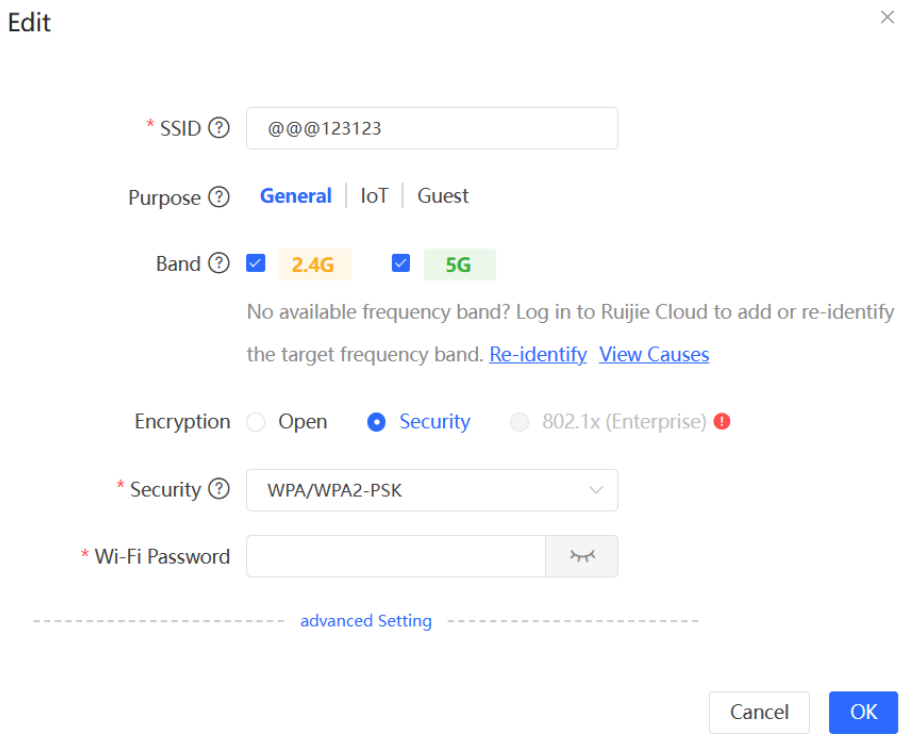
- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.



(2) Click the target Wi-Fi network, change the SSID and Wi-Fi password of the Wi-Fi network, and click **OK**.

Caution

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

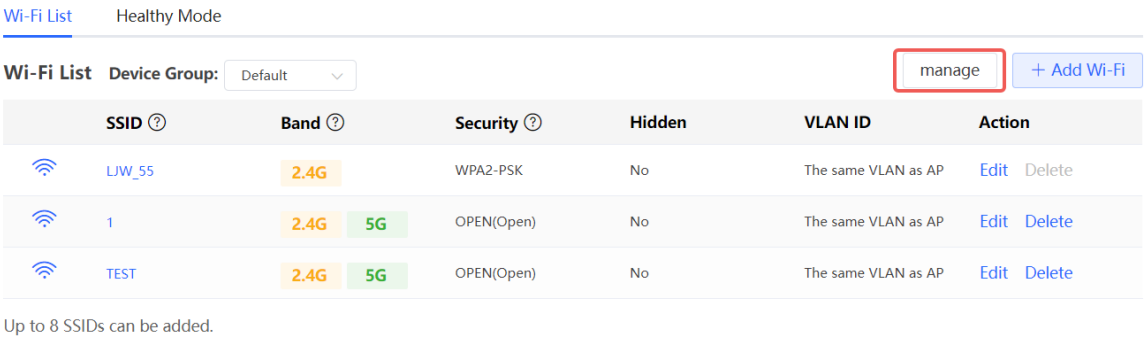


3.4 Managing Wi-Fi Networks

(1) Go to the configuration page.

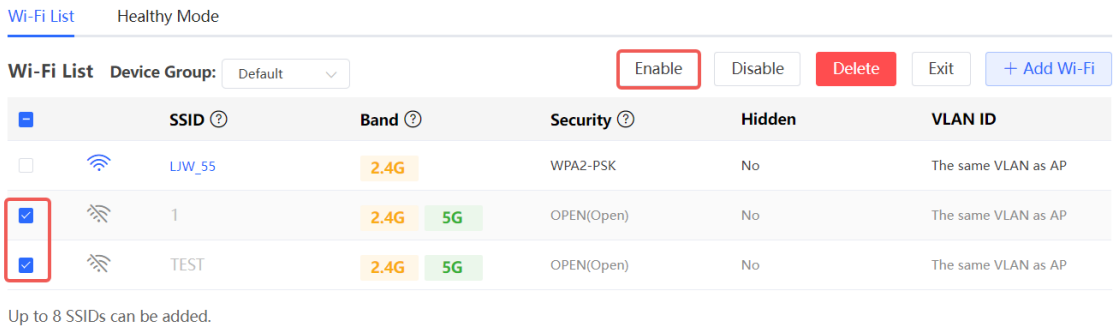
- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**.

(2) Click **manage** to batch manage Wi-Fi networks.

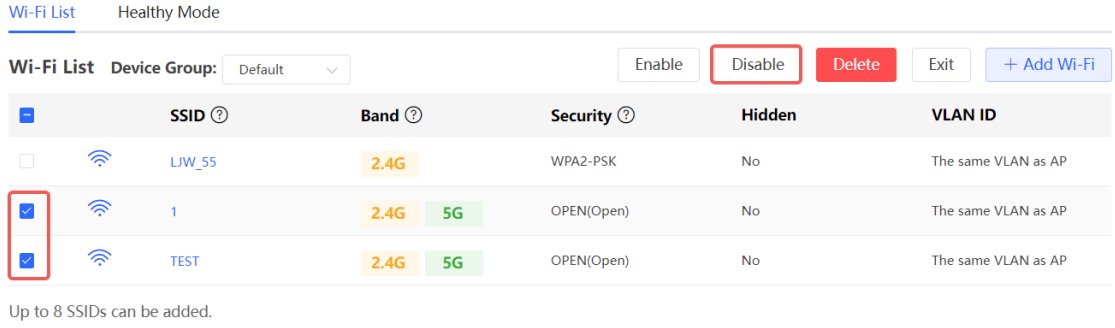


(3) Batch manage Wi-Fi networks.

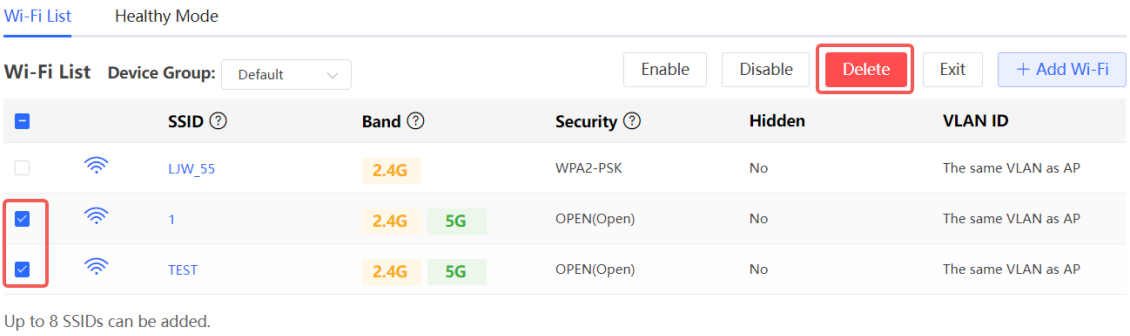
- Batch enable Wi-Fi networks: Select the desired Wi-Fi networks, and click **Enable**.



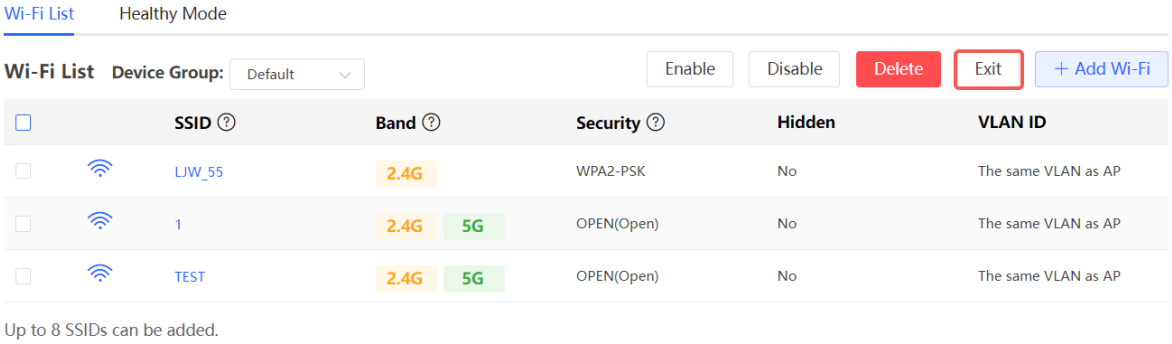
- Batch disable Wi-Fi networks: Select the desired Wi-Fi networks, and click **Disable**.



- Batch delete Wi-Fi networks: Select the desired Wi-Fi networks, and click **Delete**.



(4) Click **Exit** to exit Wi-Fi network batch management.



3.5 Hiding the SSID

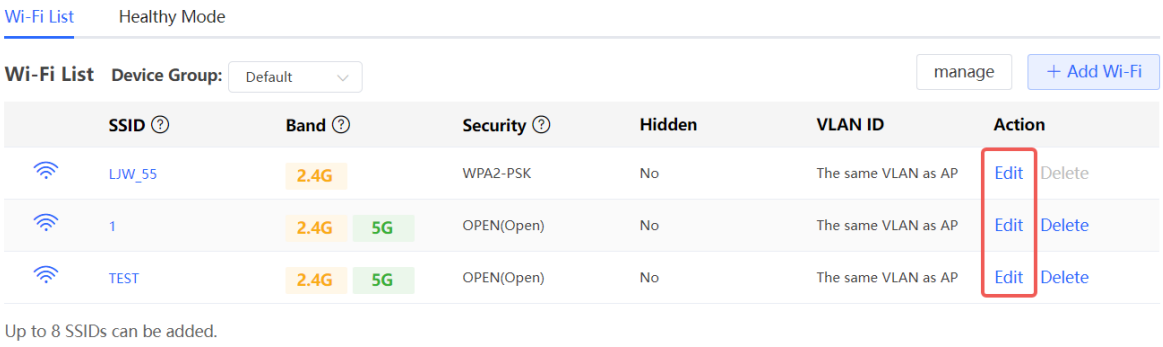
3.5.1 Overview

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

3.5.2 Configuration Steps

(1) Go to the page for configuration.

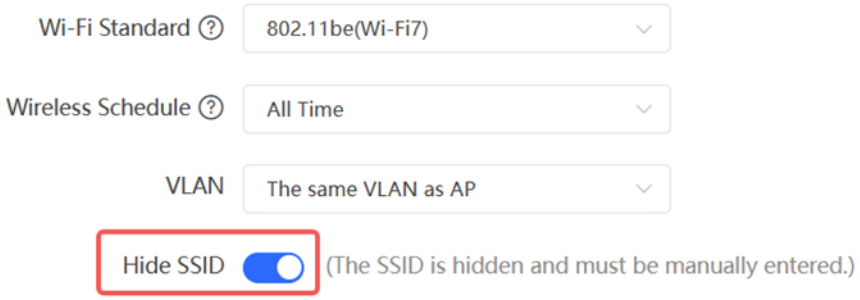
- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.



(2) Click to expand advanced settings, turn on **Hide SSID** in the expanded settings and click **OK**.

Caution

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

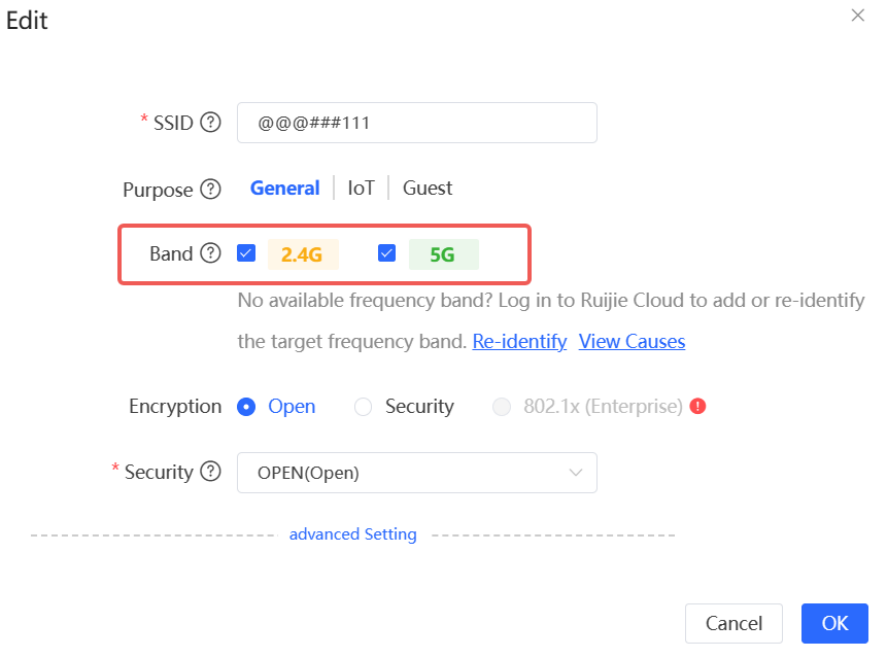


3.6 Configuring Wi-Fi Band

(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

(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.



3.7 Configuring Band Steering

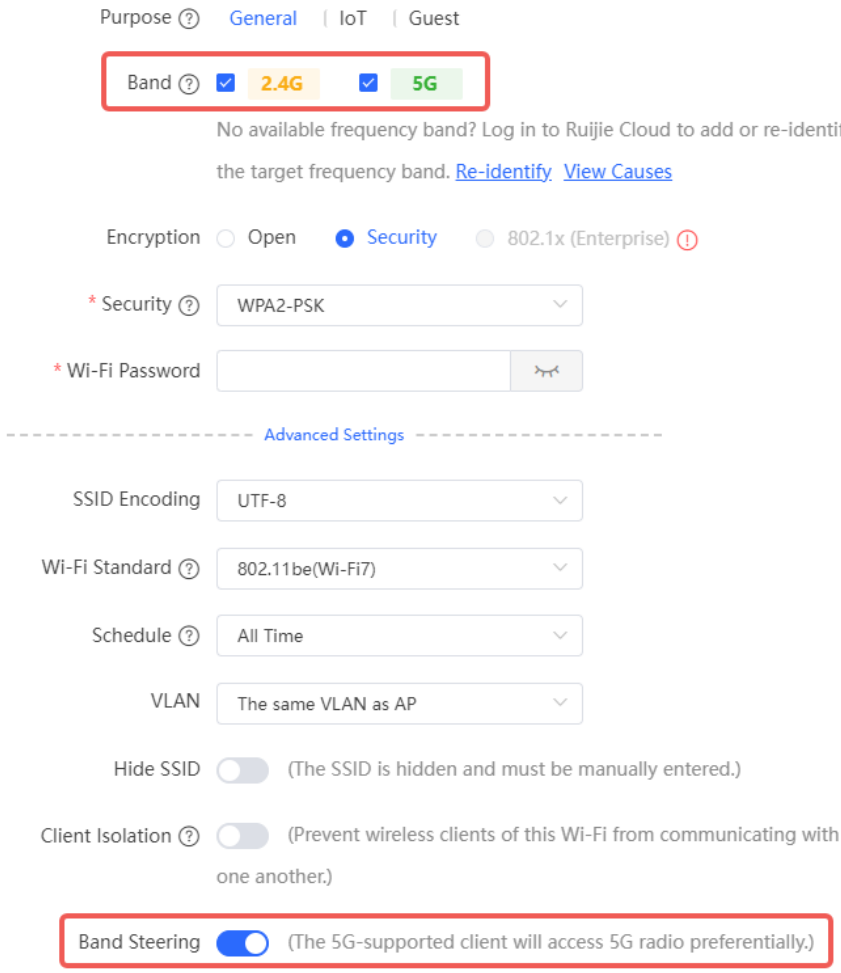
Caution

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 page for configuration.

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

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



3.8 Configuring Wi-Fi 6

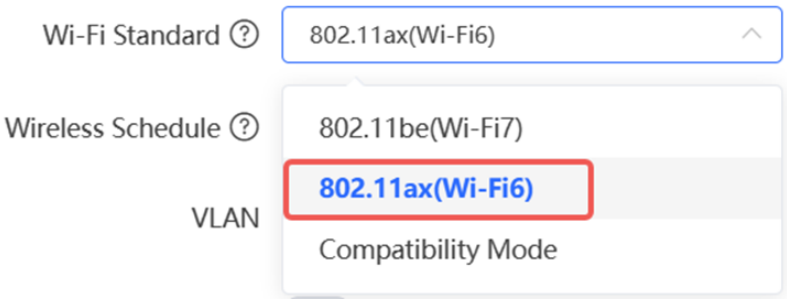
Caution

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 page for configuration.

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

(2) Click **advanced Settings** to set the **Wi-Fi Standard** to **802.11ax(Wi-Fi6)**. Click **OK**. After this function is enabled, wireless clients can have faster network speed and optimized network experience.



3.9 Configuring Wi-Fi 7

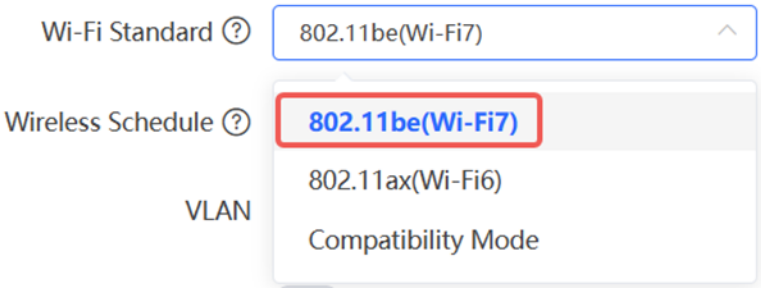
Caution

This configuration takes effect only on APs that support the IEEE 802.11be protocol. Clients also need to support the IEEE 802.11be protocol in order to experience high-speed Internet access brought by Wi-Fi 7. Disable this feature if the client does not support Wi-Fi 7.

(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

(2) Click **advanced Settings** to set the **Wi-Fi Standard** to **802.11be(Wi-Fi7)**. Click **OK**. After this function is enabled, wireless clients can have faster network speed and optimized network experience.

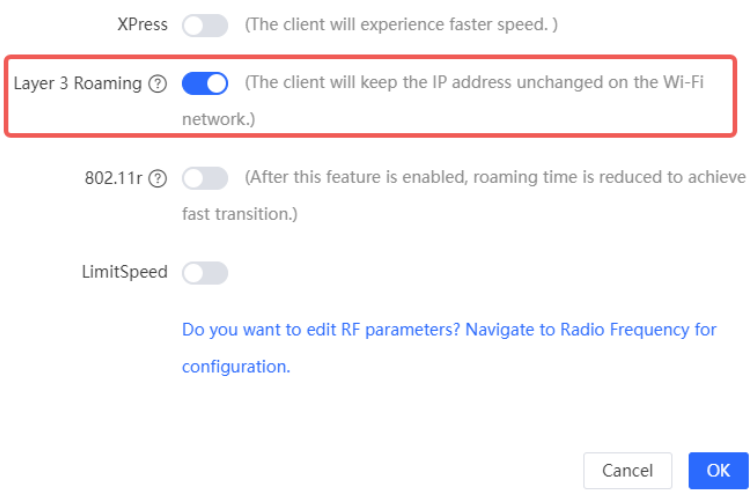


3.10 Configuring Layer-3 Roaming

(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

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

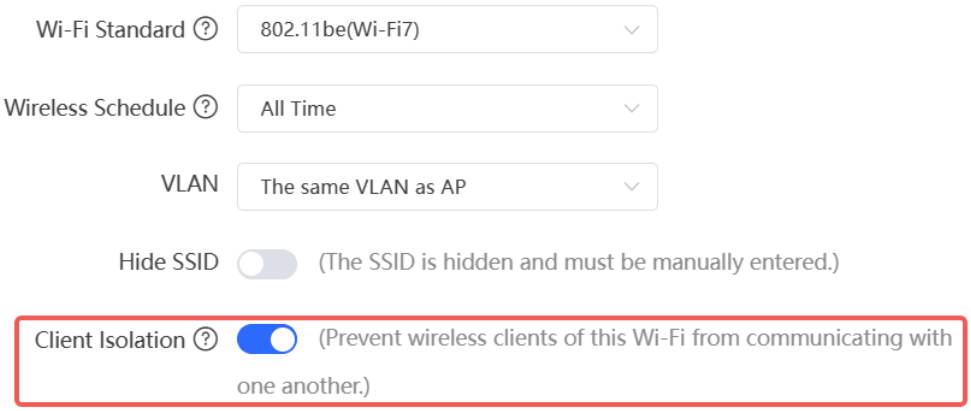


3.11 Configuring Client Isolation

(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

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



3.12 Configuring 802.11r

The **802.11r** function is available only when the Encryption is set to **Security** or **802.1x(Enterprise)**. Once **802.11r** is enabled, **Security** can only be set to WPA2-PSK or WPA2-802.1X.

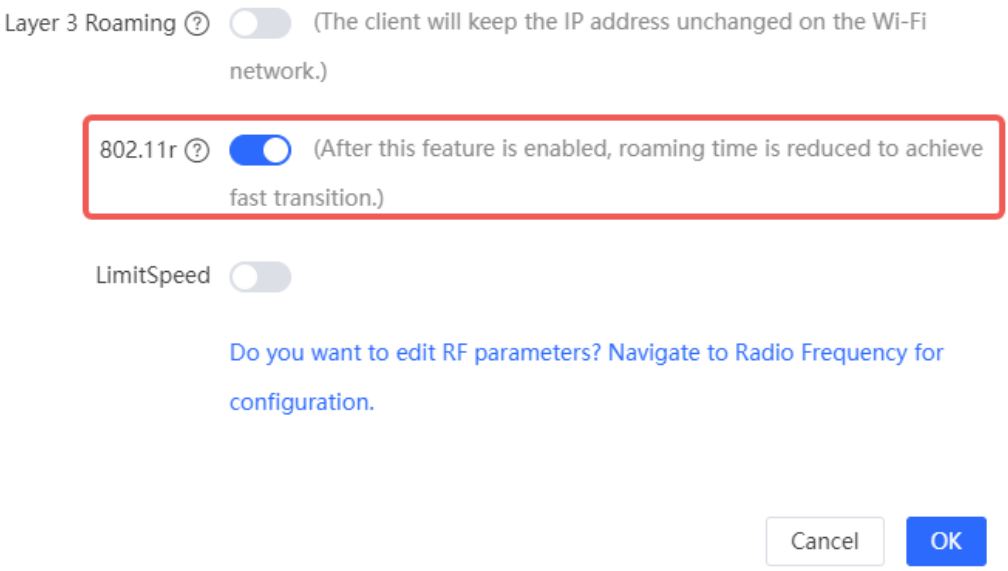
(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network,

and click **Edit**.

- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

(2) Click **advanced Settings**. Enable **802.11r**, and click OK.



3.13 Configuring a Guest Wi-Fi

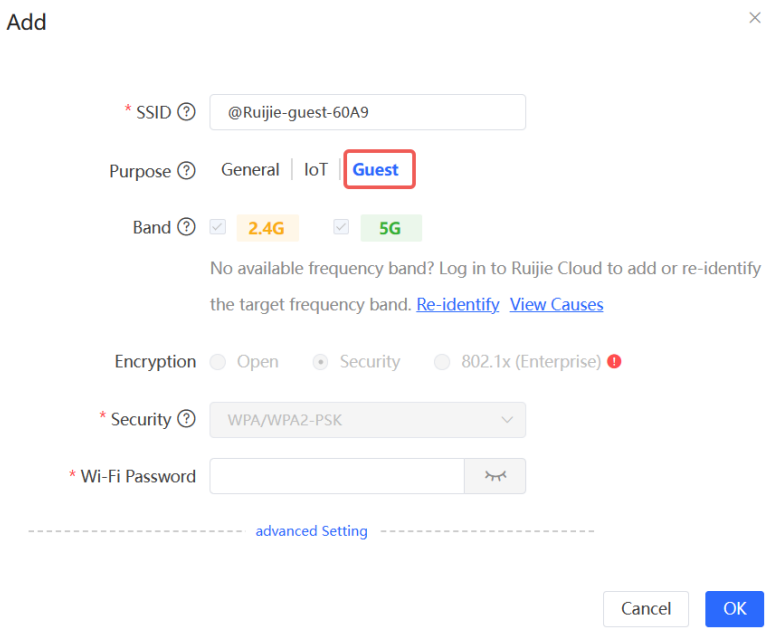
3.13.1 Overview

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

3.13.2 Configuration Steps

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**.

Click **Add Wi-Fi**. Set the purpose to **Guest** and configure the SSID and password. Click **advanced Settings** to configure the effective time of the guest Wi-Fi and other Wi-Fi parameters. After the settings are saved, guests can connect to the Internet through the set SSID and password.



3.14 Configuring Wireless Rate Limiting

3.14.1 Overview

The device supports four rate limiting modes: client-based rate limiting, SSID-based rate limiting, AP-based rate limiting, and packet-based rate limiting. For the same client, if multiple rate limiting modes are configured, the priority order is as follows: client-based rate limiting > SSID-based rate limiting > AP-based rate limiting > packet-based rate limiting.

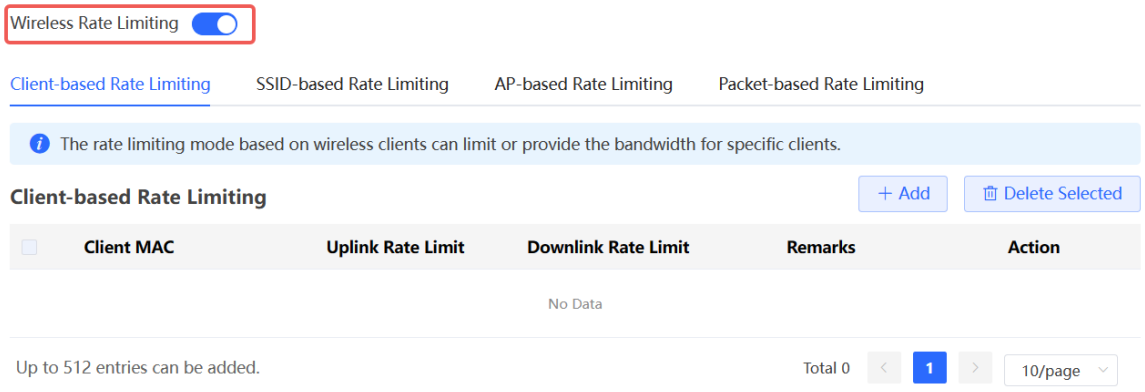
- Client-based rate limiting: This function allows you to limit the rate based on the MAC address of the client, so as to limit or guarantee the bandwidth required by specific clients.
- SSID-based rate limiting: This function provides two rate limiting modes for a specified SSID: **Rate Limit Per User** and **Rate Limit All Users**. **Rate Limit Per User** means that all clients connected to the SSID use the same rate limit. **Rate Limit All Users** means that the configured rate limit value is evenly allocated to all clients connected to the SSID. The rate limit value of each client dynamically changes with the number of clients connected to the SSID.
- AP-based rate limiting: This function limits the client rates based on the whole network. All clients connected to the network will work according to the configured rate limit value.
- Packet-based rate limiting: This function limits the client rates based on the downlink broadcast and multicast packets. The device supports rate limiting for specific broadcast packets (such as ARP and DHCP), multicast packets (such as MDNS and SSDP), or all types of broadcast and multicast packets. If network stalling remains during network access and there is no client with large traffic, you are advised to adjust the rate between 1 kbps and 512 kbps.

3.14.2 Configuration Steps

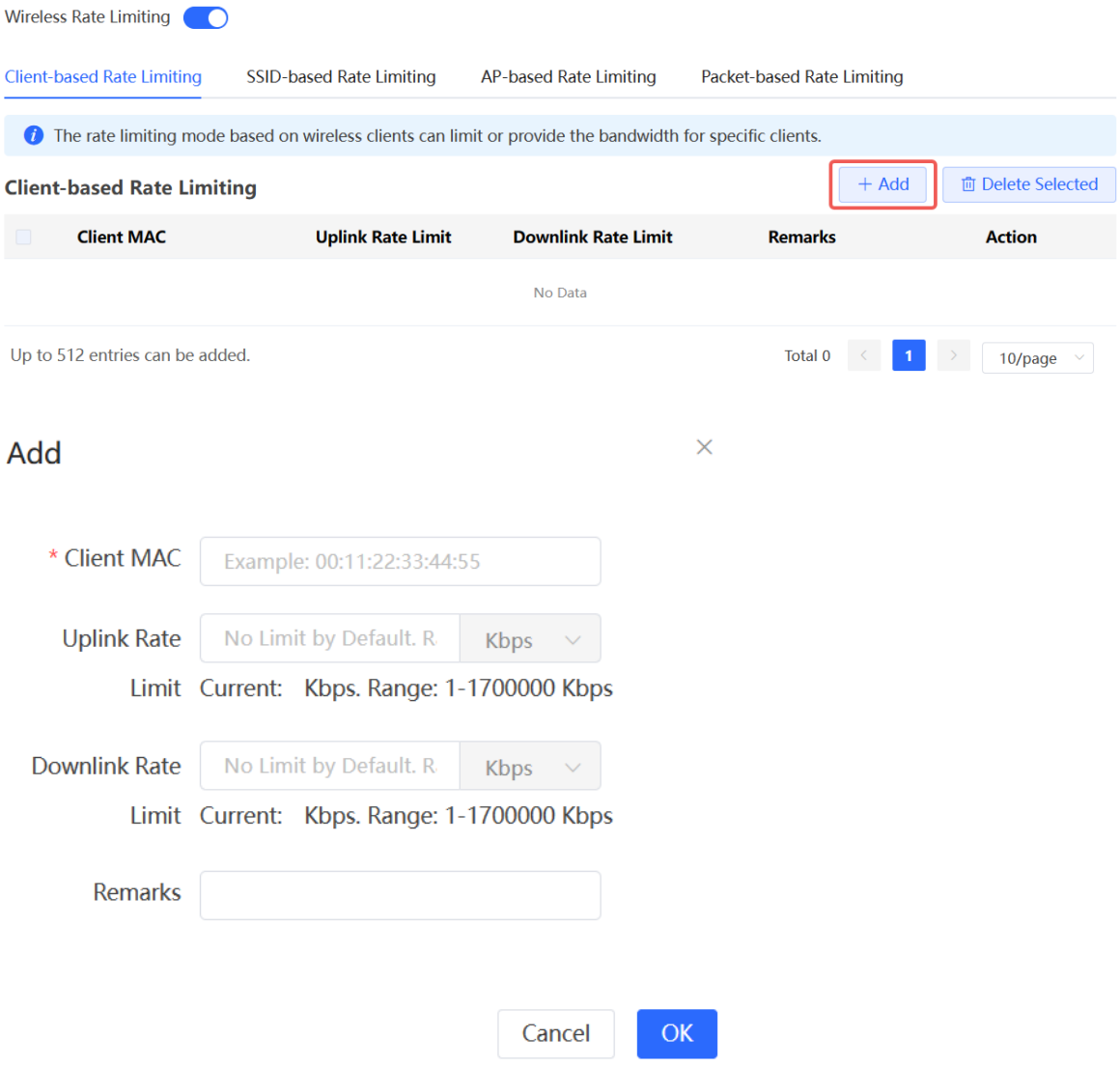
1. **Configuring Client-based Rate Limiting**

Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **Client-based Rate Limiting**.

(1) Enable **Wireless Rate Limiting**.



(2) Click **Add**. In the dialog box that appears, set the MAC address and uplink and downlink rate limit values of the client, and click **OK**.

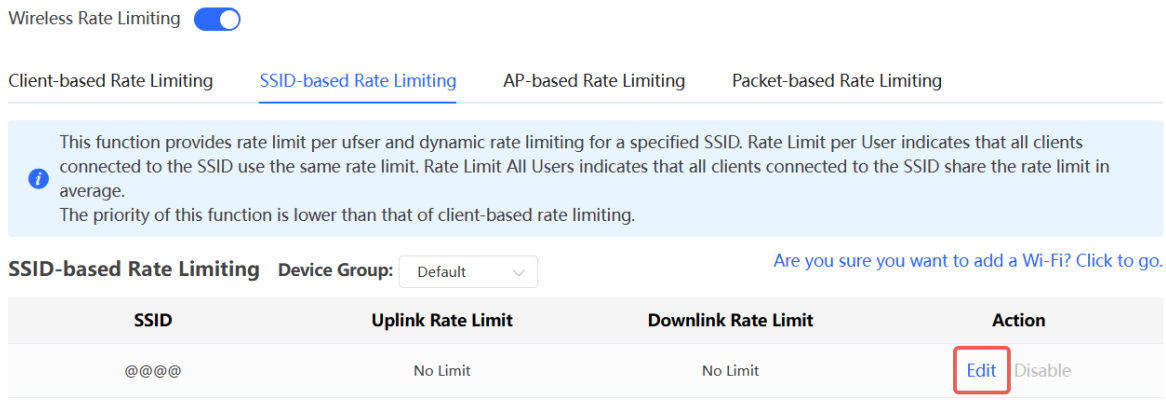


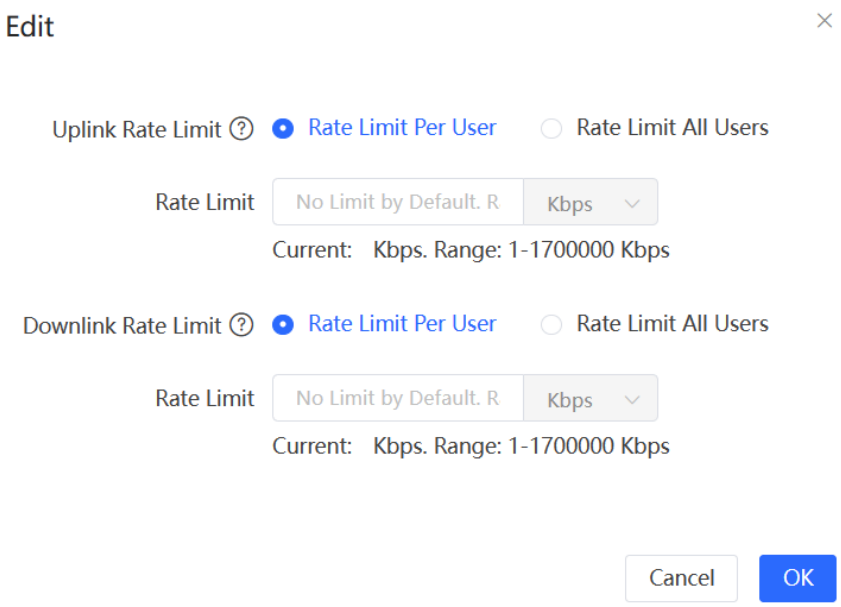
2. Configuring SSID-based Rate Limiting

Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **SSID-based Rate Limiting**.

(1) Enable **Wireless Rate Limiting**.

(2) Click **Edit** in the **Action** column of the target SSID. In the dialog box that appears, set the uplink and downlink rate limit modes and values, and click **OK**.



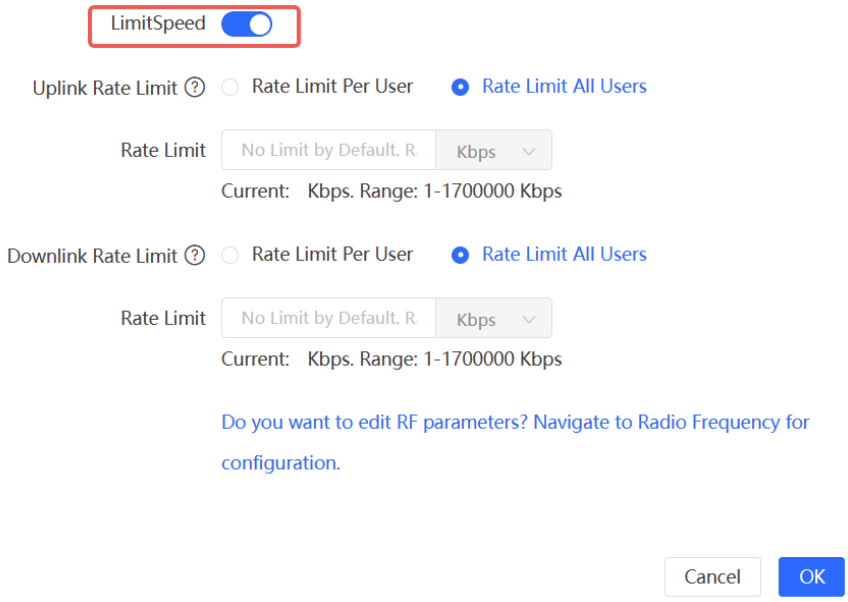


Method 2:

(1) Go to the configuration page:

- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

(2) Click to expand advanced settings. Enable **LimitSpeed**, set the uplink and downlink rate limit modes and rate limits, and click **OK**.

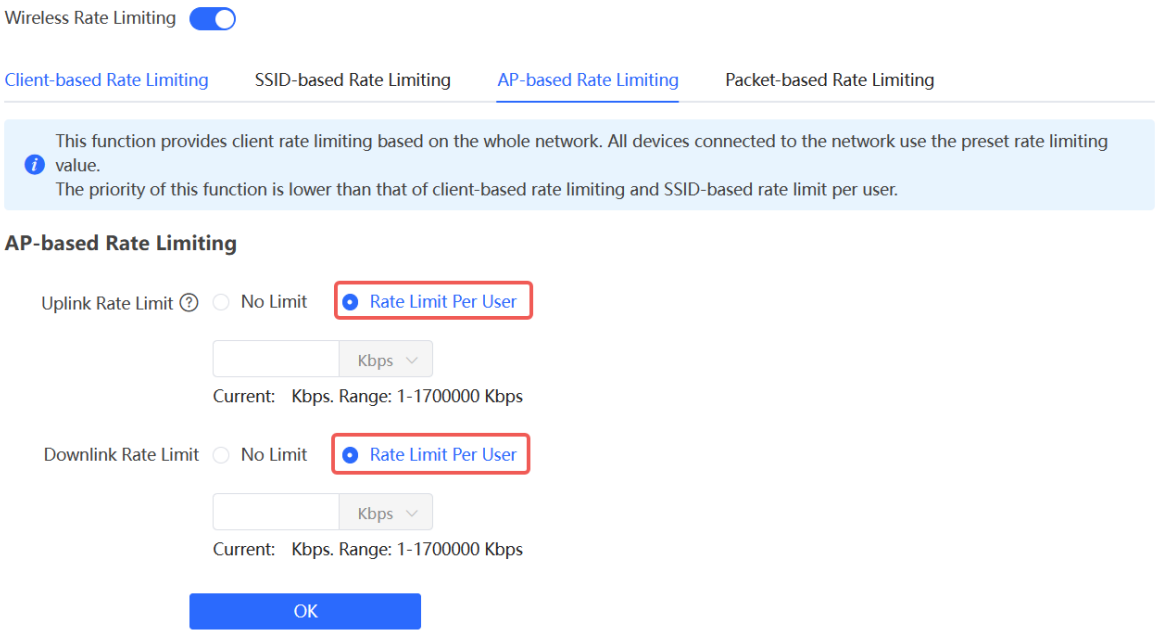


3. Configuring AP-based Rate Limiting

Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **AP-based Rate Limiting**.

(1) Enable **Wireless Rate Limiting**.

(2) Set the uplink and downlink rate limit modes to **Rate Limit Per User**, configure the rate limit values, and click **OK**.

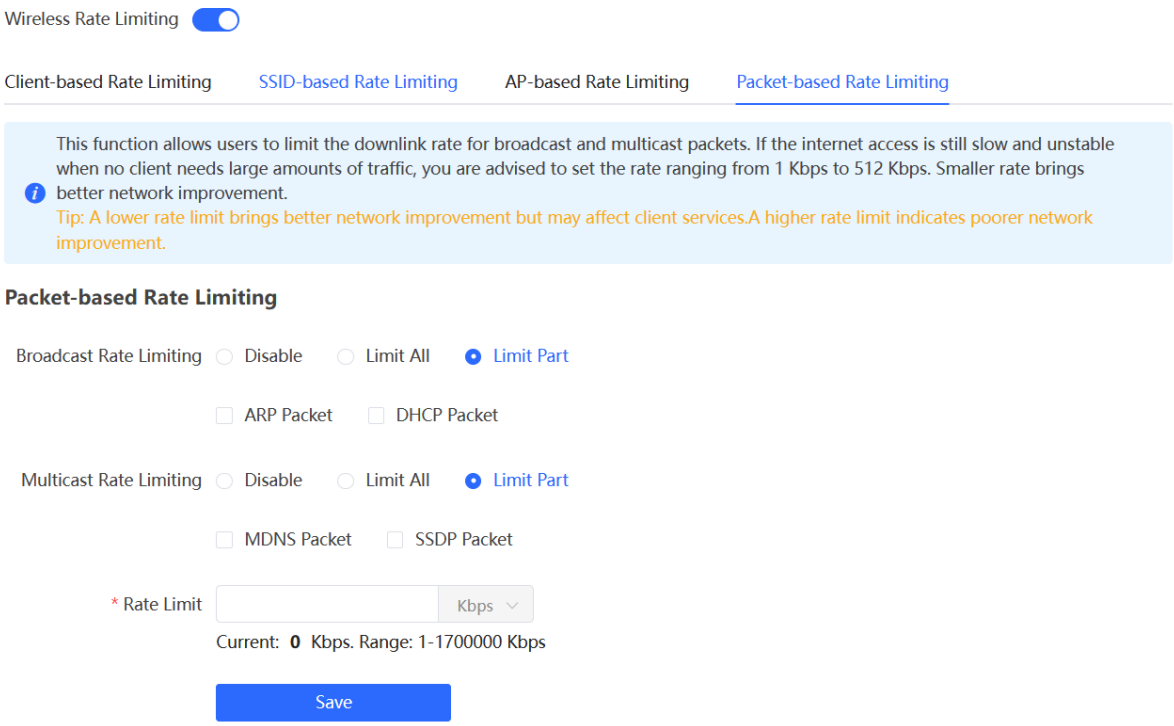


4. Configuring Packet-based Rate Limiting

Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **Packet-based Rate Limiting**.

(1) Enable **Wireless Rate Limiting**.

(2) Select the specific type of packets for rate limiting, configure the rate limit value, and click **Save**.



3.15 Configuring Wi-Fi Blocklist or Allowlist

3.15.1 Overview

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

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

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

Caution

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

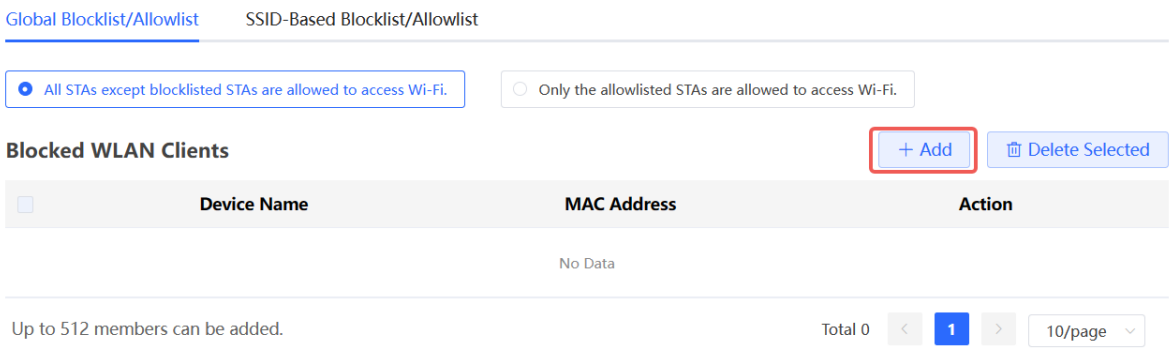
3.15.2 Configuration Steps

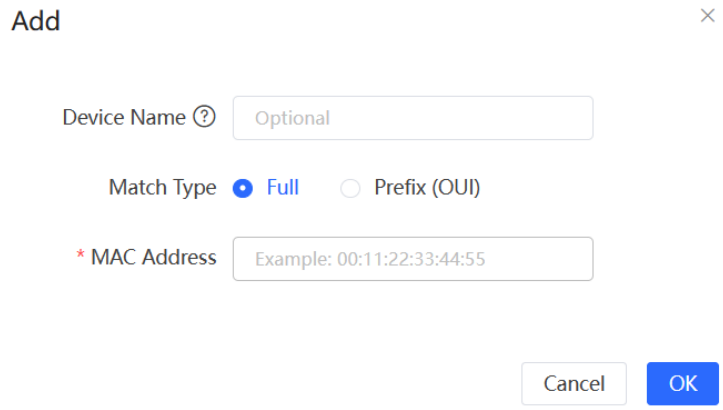
1. Configuring a Global Blocklist/Allowlist

Choose **Network-Wide > Workspace > Wireless > Blocklist and Allowlist** > **Global Blocklist/Allowlist**.

Select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. Enter the device name, match type, and MAC address of the client to be added to the blacklist or whitelist in the displayed dialog box, and click **OK**. If a client is already associated with the access point, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blocklist will be forced offline

and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the access point.

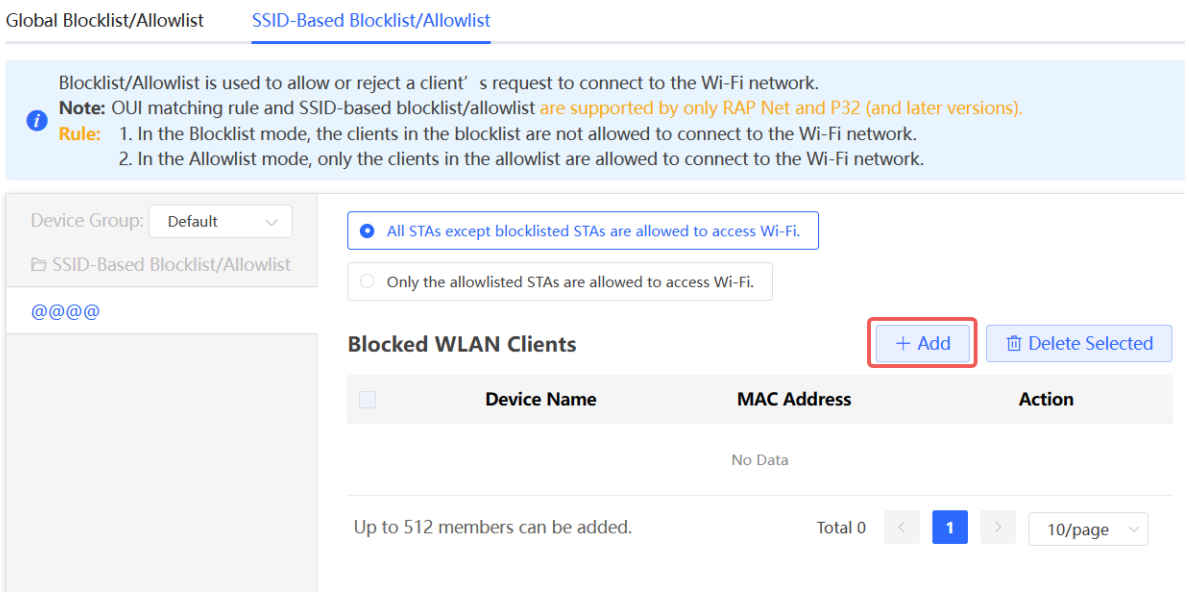




2. Configuring an SSID-based Blocklist/Allowlist

Choose **Network-Wide > Workspace > Wireless > Blocklist and Allowlist** > **SSID-Based Blocklist/Allowlist**.

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



3.16 Optimizing Wi-Fi Network

3.16.1 Overview

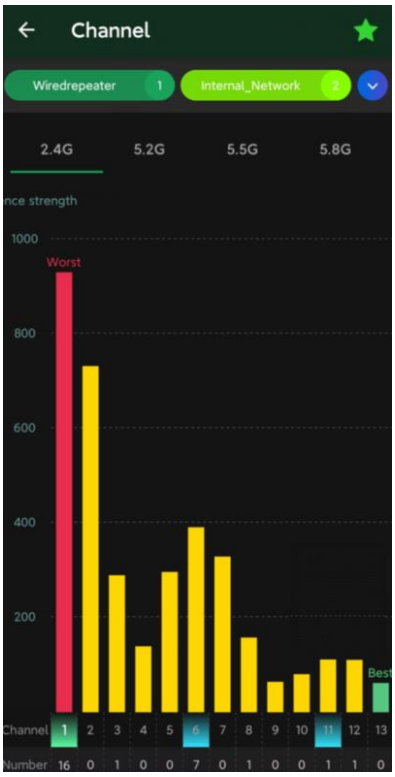
The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point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

Caution

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

3.16.2 Getting Started

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



3.16.3 Configuring Global Radio Settings

1. Optimizing the Channel Width

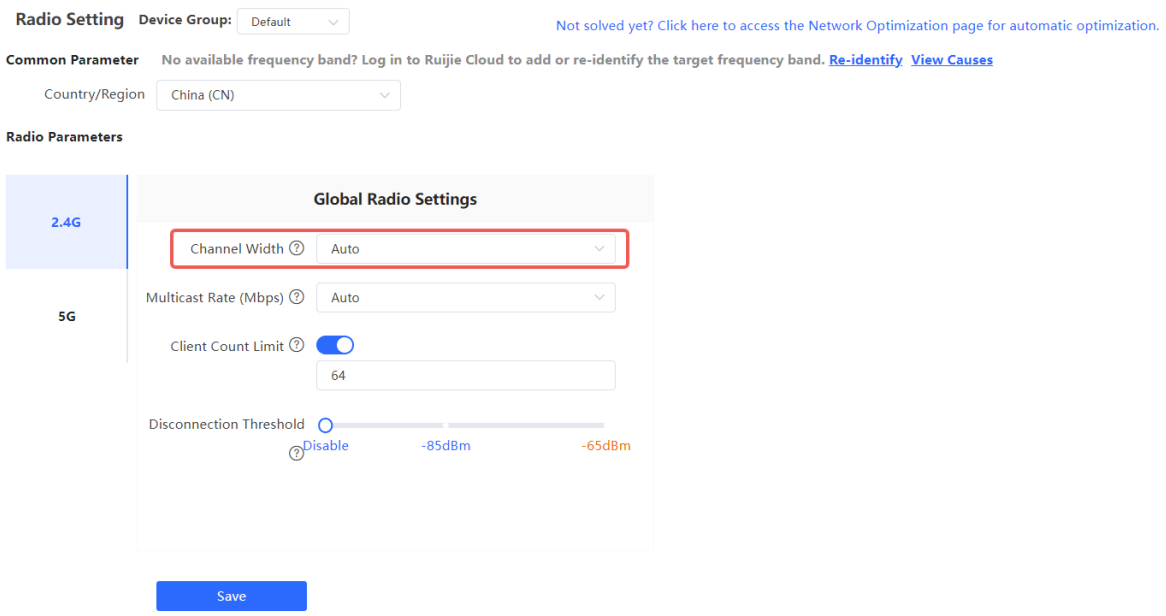
Choose **Network-Wide** > **Workspace > Wireless > Radio Setting**.

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

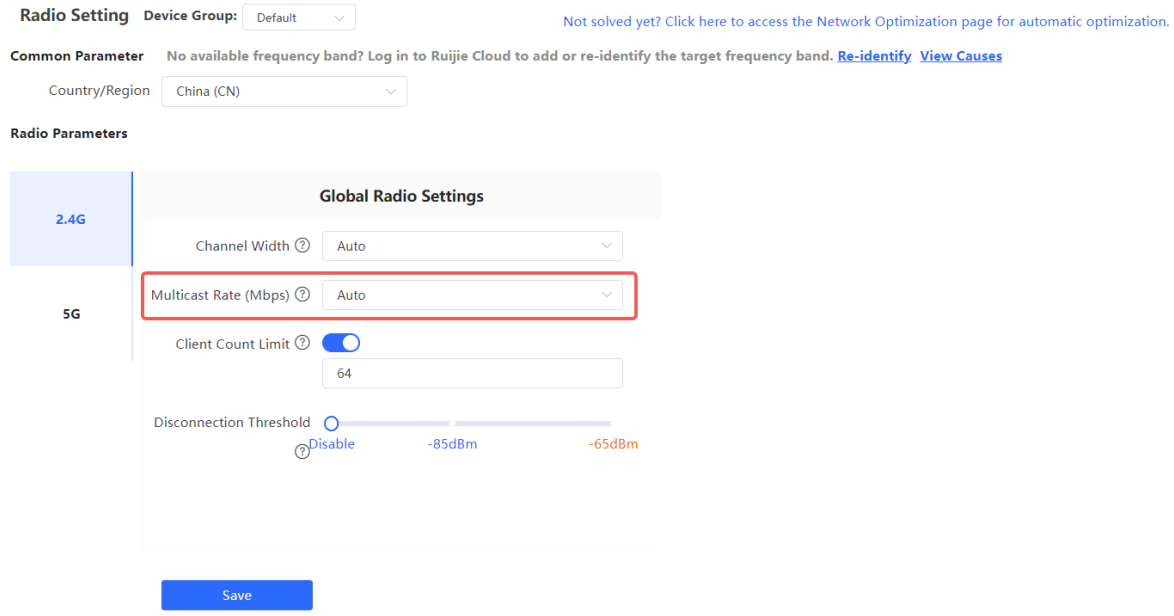
In the self-organizing network mode, the channel width settings will be synchronized to all devices in the network.



2. Configuring the Multicast Rate

Choose **Network-Wide** > **Workspace** > **Wireless** > **Radio Setting**.

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

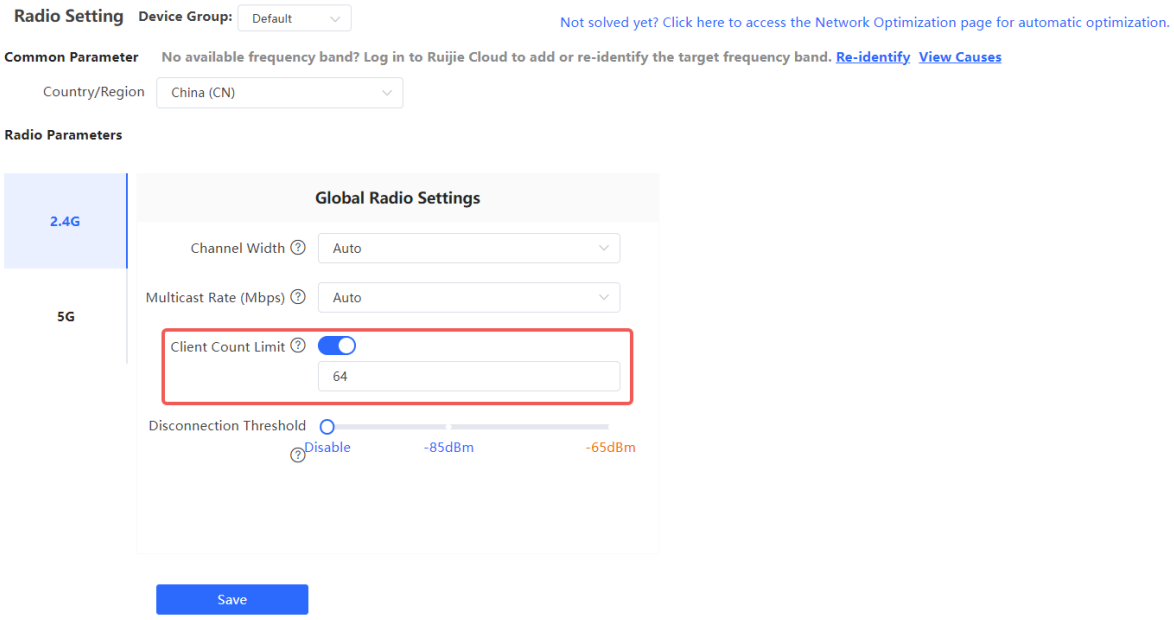


3. Configuring the Client Limit

Choose **Network-Wide** > **Workspace** > **Wireless** > **Radio Setting**.

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. The **Client Count Limit** toggle switch is disabled by default. If there is no need to set a client limit, please keep the default setting.

You can toggle on the **Client Count Limit** toggle switch to set a client limit, and then click **Save**.



Note

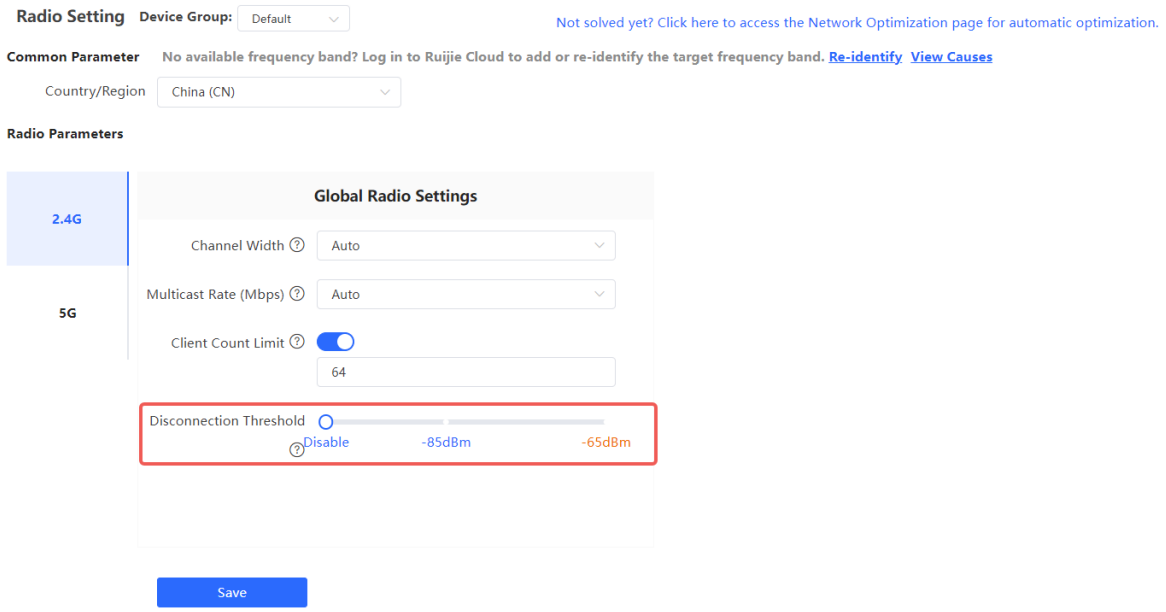
The **Client Count Limit** refers to the maximum number of clients that can be connected to a single access point.

4. Configuring the Kick-off Threshold

Choose **Network-Wide** > **Workspace** > **Wireless** > **Radio Setting**.

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

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



Caution

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

3.16.4 Configuring Standalone Radio Settings

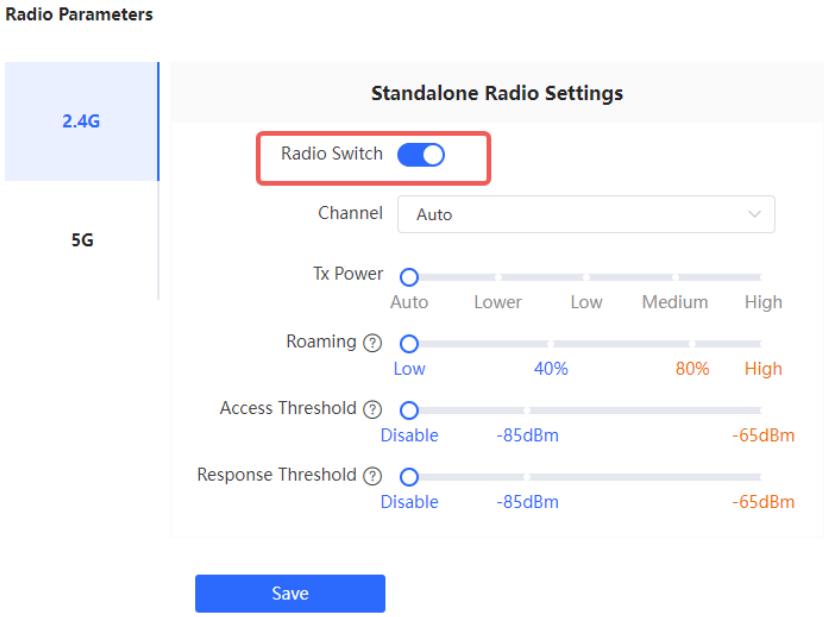
Go to the configuration page.

- Method 1: Choose **One-Device** > **Config** > **WLAN** > **Radio Setting**.
- Method 2: Choose **Network-Wide** > **Devices**> **Manage** > **Config** > **WLAN** > **Radio Setting**.

In high-density client environments, you can fine-tune radio settings to alleviate radio frequency interference resulting from too many access points in close proximity. This include disabling the radio of neighboring APs that are causing significant interference, aiming to minimize signal conflicts and enhance the overall quality and stability of wireless communication.

In environments like conference rooms, offices, and smart homes, disabling the 2.4GHz radio of specific APs can enhance the performance of wireless devices such as mice, keyboards, Bluetooth and Zigbee devices when they experience signal interference or operational lag.

The **Radio Switch** is enabled by default, and can be disabled as required.



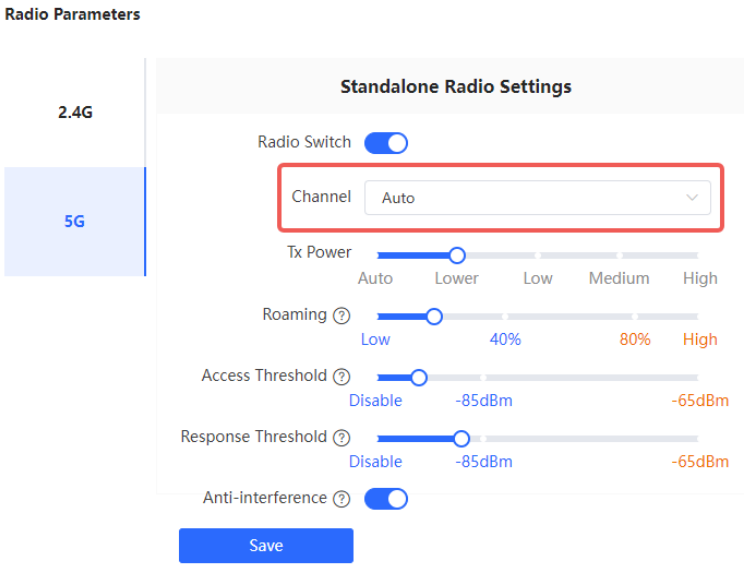
1. Optimizing the Radio Channel

- Method 1: Choose **One-Device** > **Config** > **WLAN** > **Radio Setting**.
- Method 2: Choose **Network-Wide** > **Devices** > **Manage** > **Config** > **WLAN** > **Radio Setting**.

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

Note

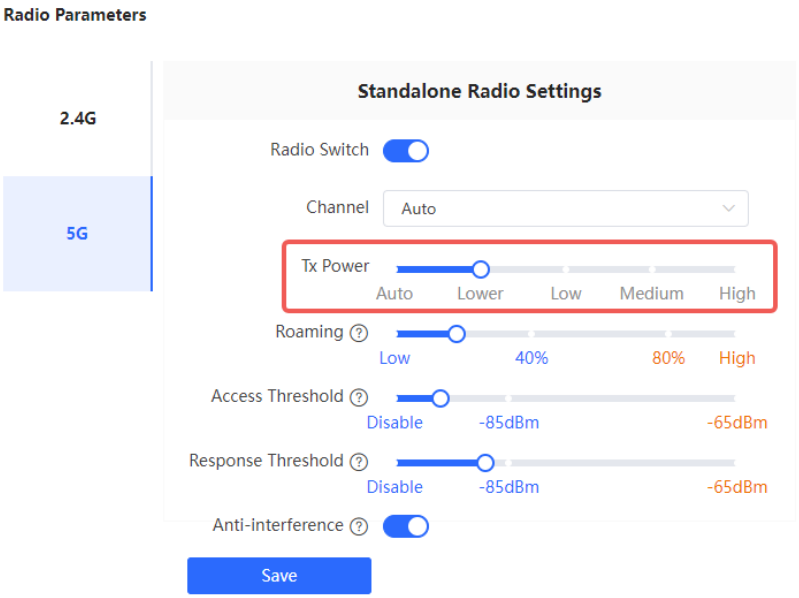
The available channels are subject to the country/region code. Please configure the correct country/region code in the **Global Radio Settings** configuration pane.



2. Optimizing the Transmit Power

- Method 1: Choose **One-Device** > **Config** > **WLAN** > **Radio Setting**.
- Method 2: Choose **Network-Wide** > **Devices** > **Manage** > **Config** > **WLAN** > **Radio Setting**.

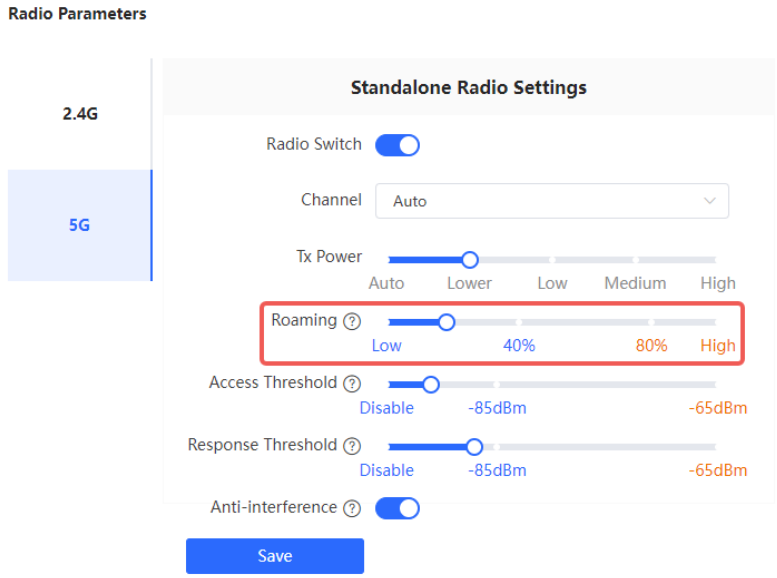
A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. In a high-density scenario, you are advised to set the transmit power to a small value. The **Auto** mode is recommended, indicating automatic adjustment of the transmit power. After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



3. Configuring the Roaming Sensitivity

- Method 1: Choose **One-Device** > **Config** > **WLAN** > **Radio Setting**.
- Method 2: Choose **Network-Wide** > **Devices** > **Manage** > **Config** > **WLAN** > **Radio Setting**.

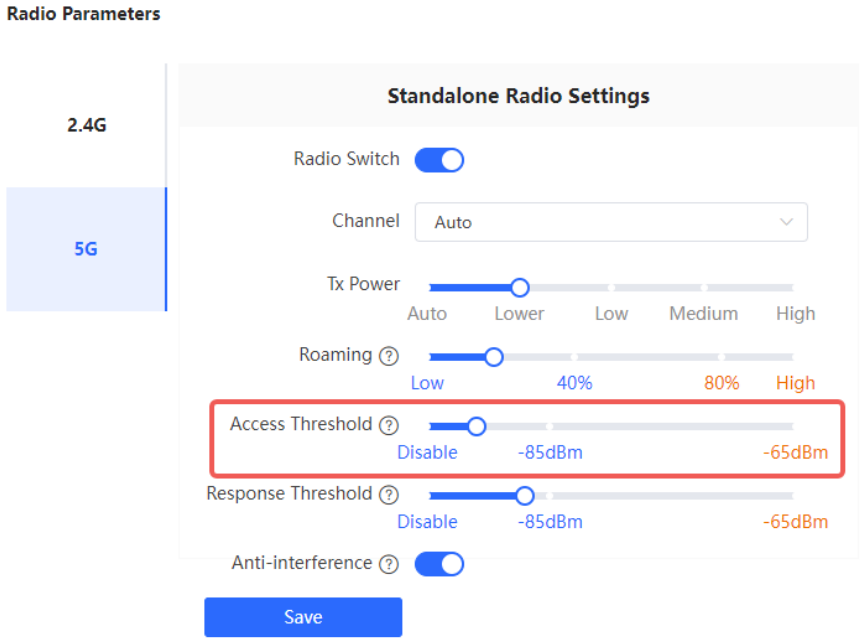
The roaming sensitivity enables the device to actively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving the sensitivity of wireless roaming. Higher the roaming sensitivity level, smaller the wireless signal coverage.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



4. Configuring Access Threshold

- Method 1: Choose **One-Device** > **Config** > **WLAN** > **Radio Setting**.
- Method 2: Choose **Network-Wide** > **Devices** > **Manage** > **Config** > **WLAN** > **Radio Setting**.

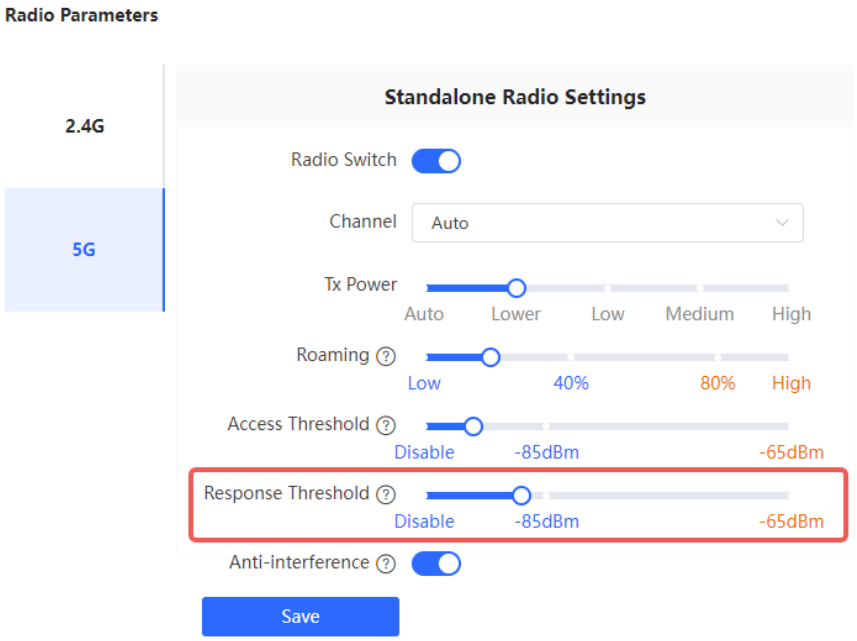
When the wireless signal of the end user is lower than the access threshold set on the device, the client cannot detect the wireless signal of the device. After adjusting the configuration, click **Save**.



5. Configuring Response RSSI Threshold

- Method 1: Choose **One-Device** > **Config** > **WLAN** > **Radio Setting**.
- Method 2: Choose **Network-Wide** > **Devices** > **Manage** > **Config** > **WLAN** > **Radio Setting**.

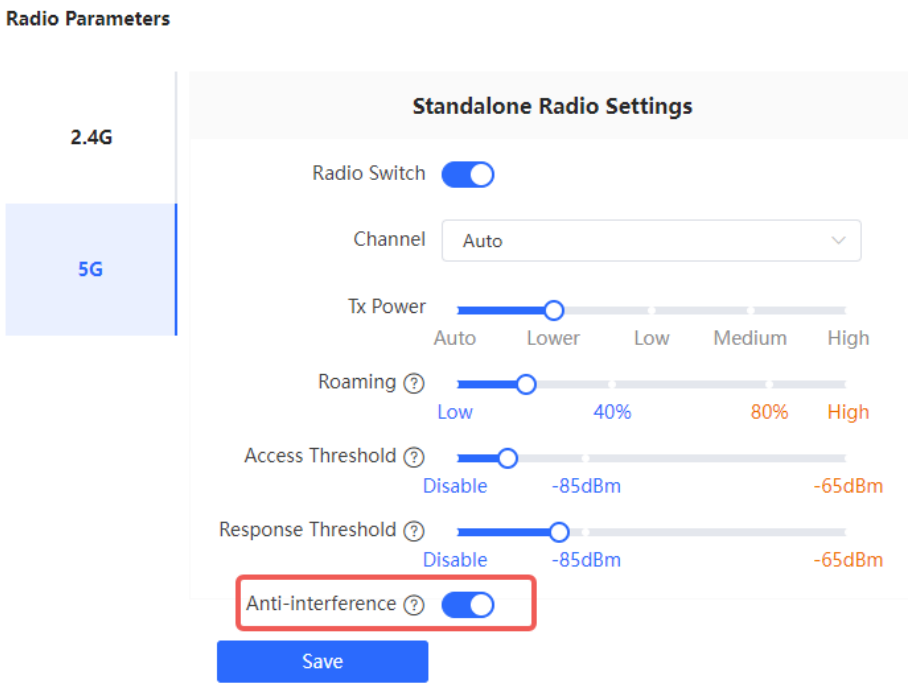
When the wireless signal of the end user is lower than the response RSSI threshold configured on the device, the client cannot detect the wireless signal of the device. The smaller the response RSSI threshold is configured, the less the environmental factors interfere with the AP. However, the connection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



6. Configuring WLAN Anti-interference

- Method 1: Choose **One-Device** > **Config** > **WLAN** > **Radio Setting**.
- Method 2: Choose **Network-Wide** > **Devices** > **Manage** > **Config** > **WLAN** > **Radio Setting**.

Preamble Puncturing is a wireless communication technique designed to enhance performance and speed in environments with significant interference. By intelligently selecting and bundling channels, this technology effectively mitigates the impact of interference. In the 5G Radio Setting interface, toggle on Anti-interference. This allows devices to bypass severely interfered channels and choose optimal channels for bundling and data transmission, thus enhancing the overall wireless speed.



3.16.5 Configuring WIO

Choose **Network-Wide** > **Workspace** > **WLAN Optimization**.

Select the optimization mode. Then, click **OK** to optimize the wireless network.

Caution

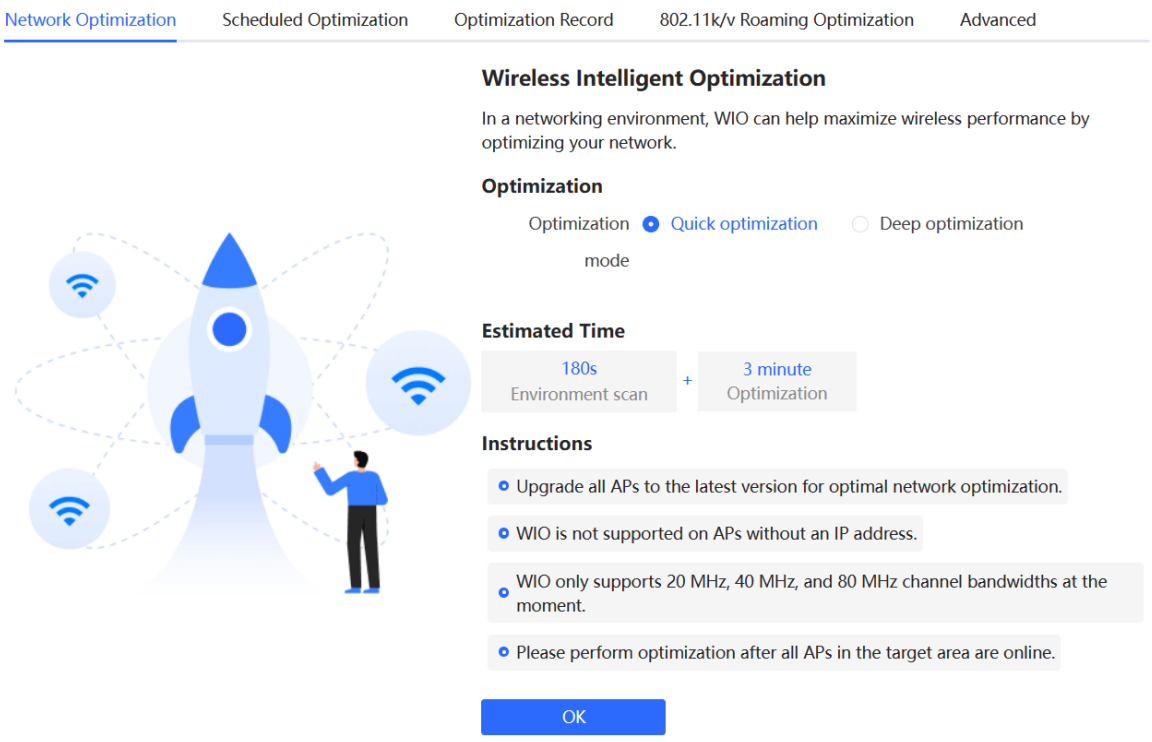
- WIO is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.

Table 3-2 Tuning Mode Configuration Parameters

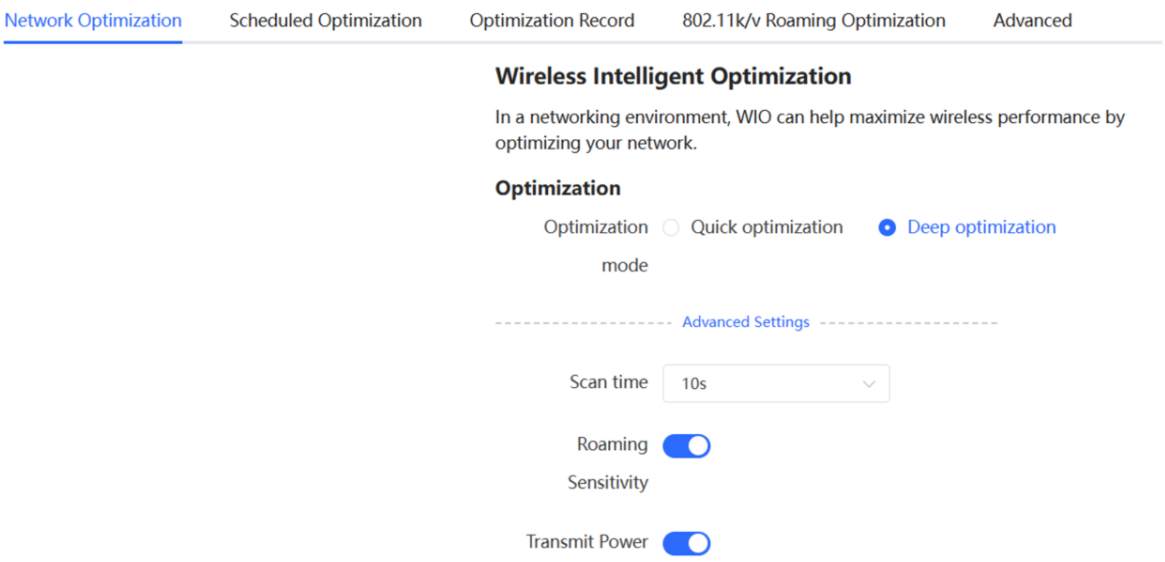
Parameter	Description
Quick tuning	In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power.

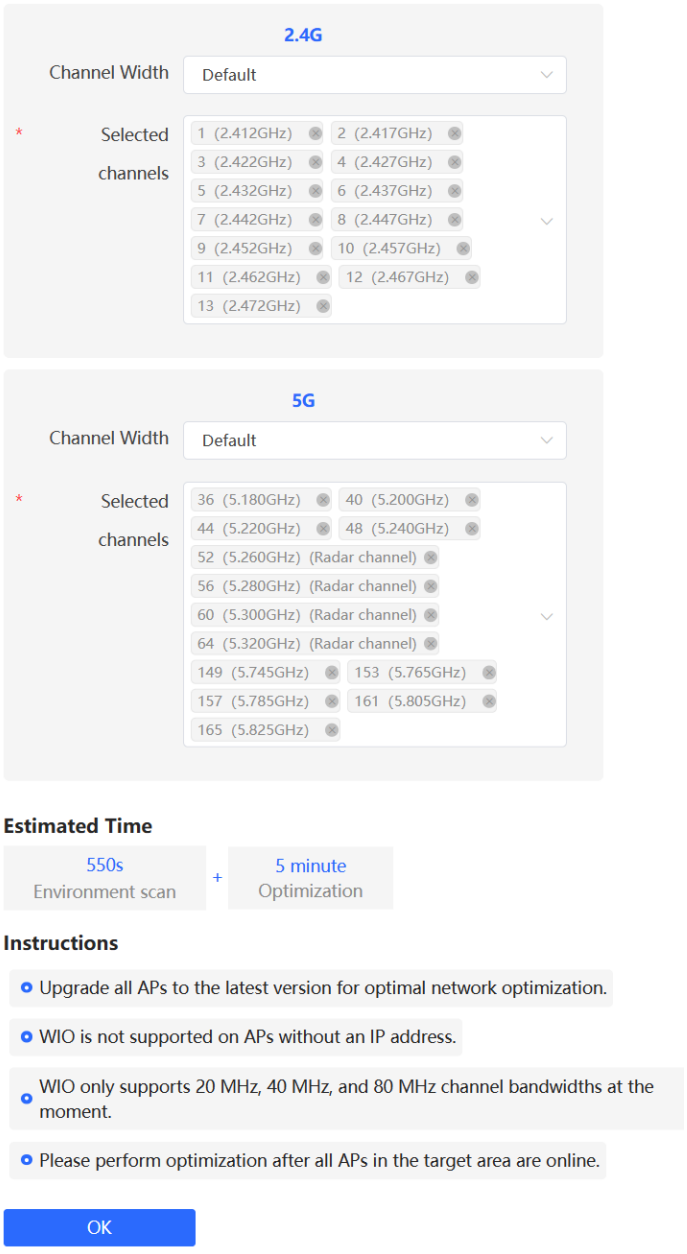
Parameter	Description
Deep tuning	In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand **Advanced Settings** to configure the scanning time, channel bandwidth and channels. ● Scanning time: Indicates the time for scanning channels during the optimization. ● Roaming Sensitivity: The roam sensitivity can be optimized based on the actual environment to ensure fast roaming of wireless devices. ● Transmit power: Increasing the transmit power enhances both the strength and coverage of the wireless signal, but it may also introduce interference to surrounding wireless networks. With this feature enabled, the AP will automatically adjust the transmit power based on the environment. ● 2.4G o Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. o Selected channels: Indicates the channels to be optimized. ● 5G o Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. o Selected channels: Indicates the channels to be optimized.

- Choose **Quick optimization**, and click **OK**.

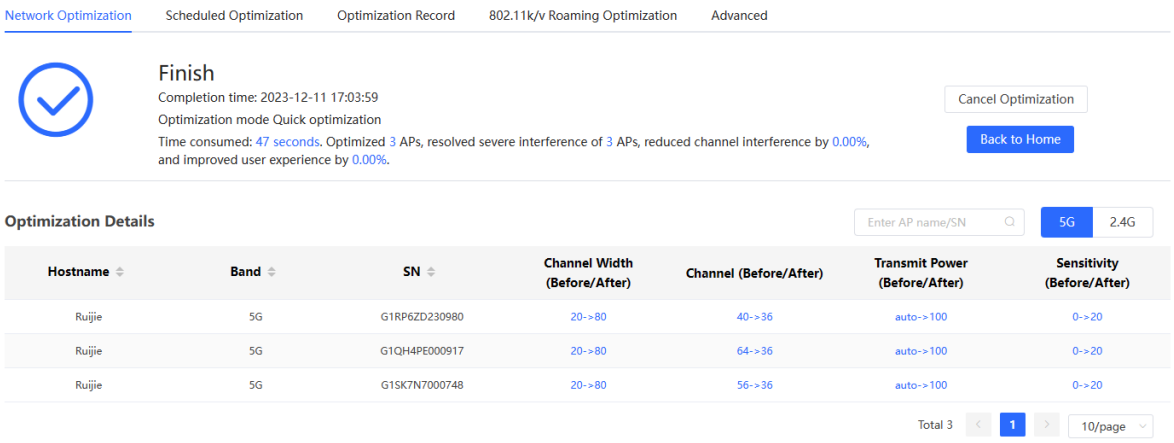


- Choose **Deep optimization**. Click to expand **Advanced Settings** to set the scanning time, channel bandwidth and selected channels. Then, click **OK**.

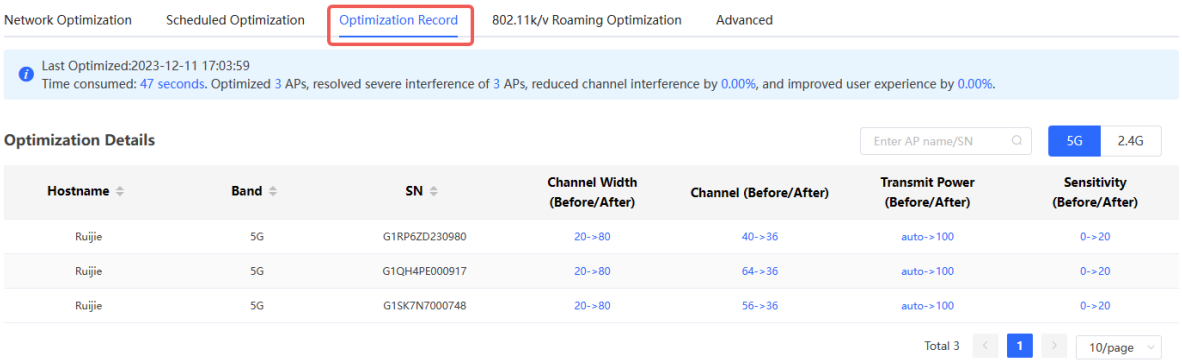

Network Optimization
Scheduled Optimization
Optimization Record
802.11k/v Roaming Optimization
Advanced
Wireless Intelligent Optimization
In a networking environment, WIO can help maximize wireless performance by optimizing your network.
Optimization
Optimization mode
Quick optimization
Deep optimization
Advanced Settings
Scan time
10s
Roaming Sensitivity
Transmit Power



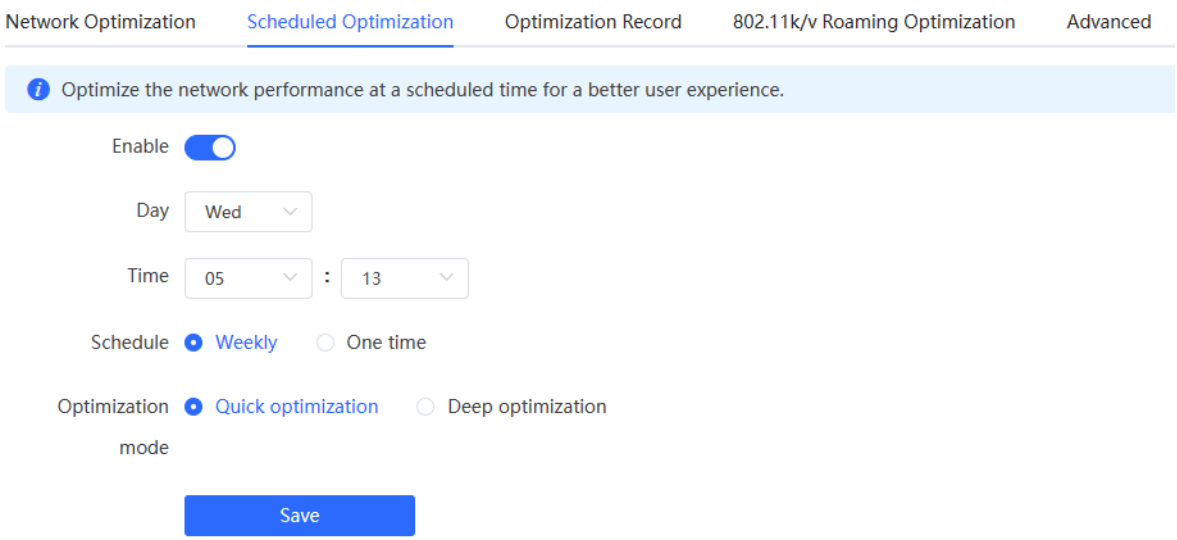
After the optimization starts, please be patient and wait for the optimization to complete. After optimization is completed, you can click **Cancel Optimization** to restore the optimized RF parameters to their default values. Click **Back to Home** to perform wireless optimization again.



Click **Optimization Record** to view the details of the latest optimization.



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.



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

Choose **Network-Wide** > **Workspace** > **WLAN Optimization** > **802.11k/v Roaming Optimization**.

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

Caution

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

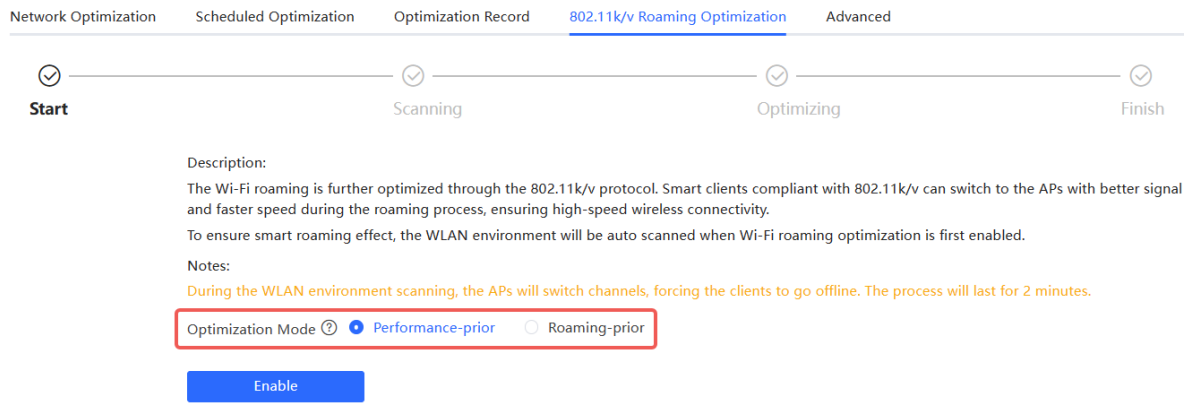
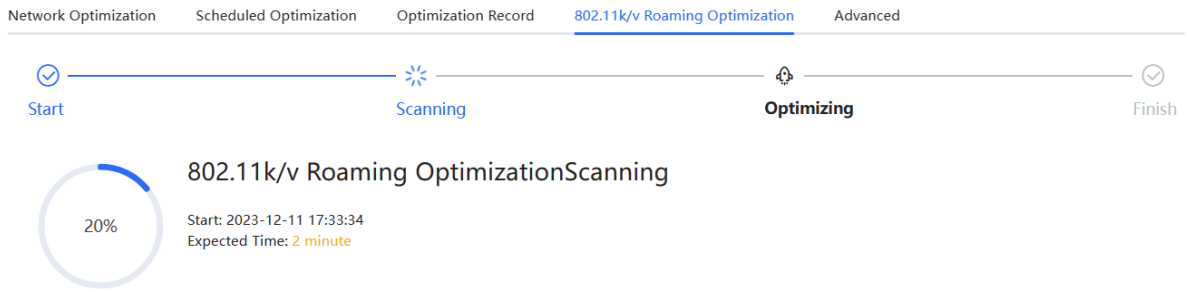
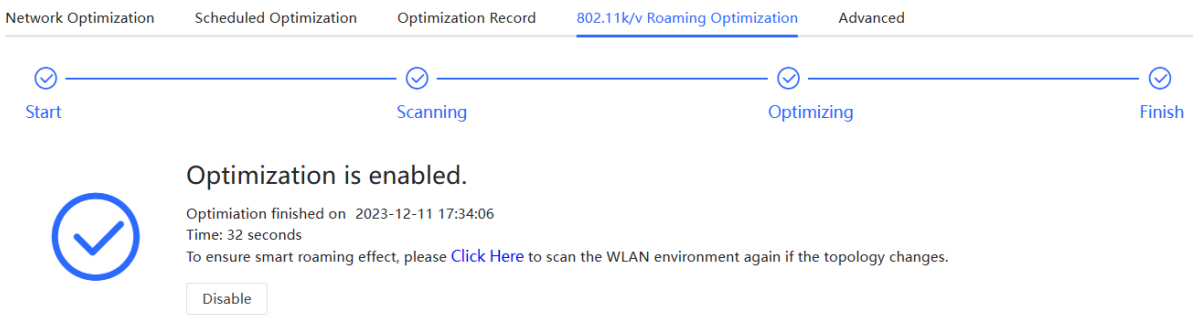


Table 3-3 Optimization Mode

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





3.17 Configuring IGMP Snooping

3.17.1 Overview

1. IGMP Snooping

IGMP snooping allows switches to listen for and analyze IGMP (Internet Group Management Protocol) messages in order to determine which switch ports are connected to hosts that are interested in specific multicast groups. By forwarding multicast traffic only to these ports, IGMP snooping helps to prevent unnecessary flooding of multicast traffic to all ports on the network, thereby improving network efficiency and security.

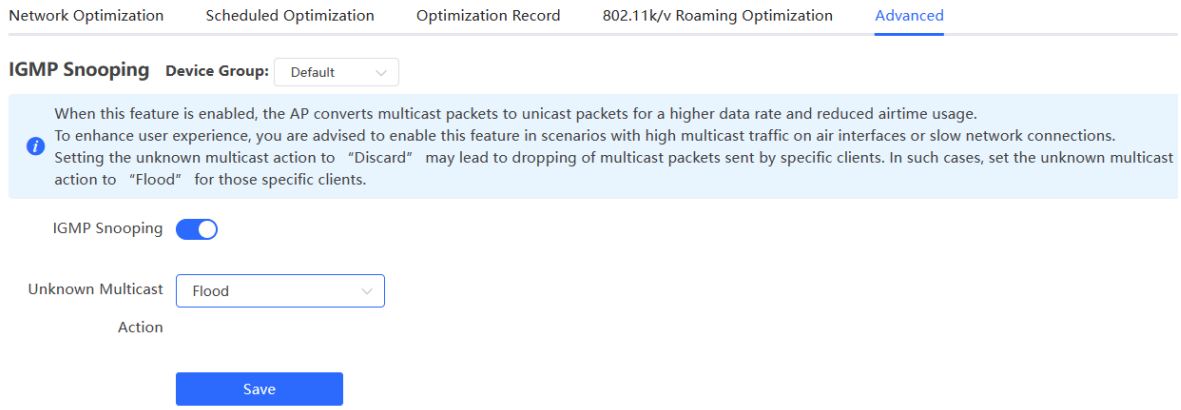
2. Unknown Multicast Packet

Unknown multicast packets are multicast packets transmitted on a network, whose destination addresses are multicast group addresses that are not learned or identified by the switch.

3.17.2 Configuration Steps

Choose **Network-Wide** > **Workspace** > **WLAN Optimization** > **Advanced Settings**.

Enable **IGMP Snooping**, select the action for unknown multicast packets, and click **Save**.



Caution

- You are advised to enable this function when a large number of multicast packets are transmitted and the network is congested to improve the user experience.
- If you set the action for unknown multicast packets to **Discard**, multicast packets sent by certain clients may be discarded. Therefore, exercise caution when performing this configuration.

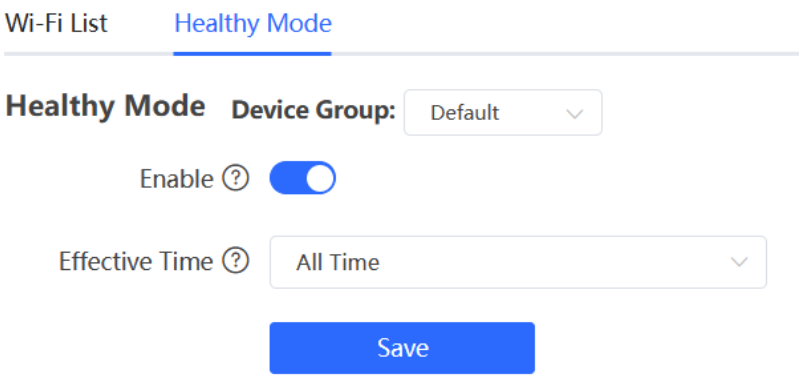
3.18 Configuring Healthy Mode

Go to the configuration page:

- Method 1: **Choose Network-Wide > Workspace > Wireless > Wi-Fi** > **Healthy Mode**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Healthy Mode**.

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

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

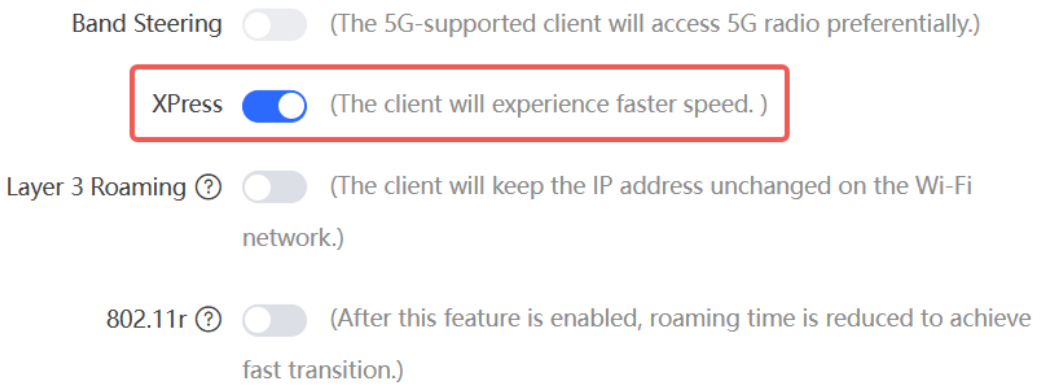


3.19 Configuring XPress

(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide > Workspace > Wireless > Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

(1) Click to expand advanced settings, turn on **XPress** in the expanded settings and click **OK**. After XPress is enabled, the gaming traffic will be prioritized, ensuring a more stable gaming experience.

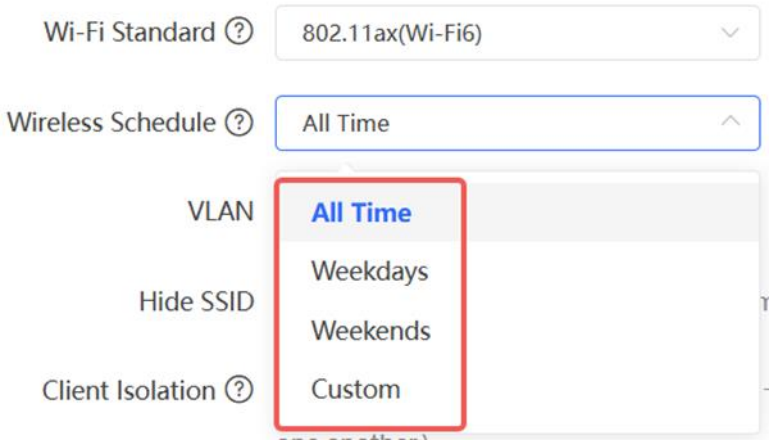


3.20 Configuring Wireless Schedule

(1) Go to the page for configuration.

- Method 1: Choose **Network-Wide > Workspace > Wireless > Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Wi-Fi** > **Wi-Fi List**. Select the Wi-Fi network, and click **Edit**.

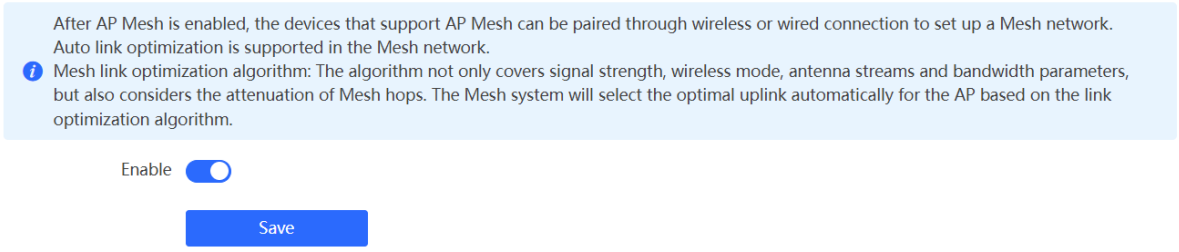
(2) Click to expand advanced settings, select a scheduled time span to turn on Wi-Fi and click **OK**. Clients will be allowed to access the Internet only in the specified time span.



3.21 Enabling AP Mesh

Choose **Network-Wide** > **Workspace** > **Wireless > AP Mesh**.

After AP Mesh is enabled, you can set up a Mesh network through Mesh pairing between the devices that support AP Mesh. You can press the **Mesh** button on the device to automatically discover a new device for Mesh pairing or log in to the management page to select a new device for Mesh pairing. AP Mesh is enabled on the device by default.



3.22 Domain Proxy

Go to the configuration page:

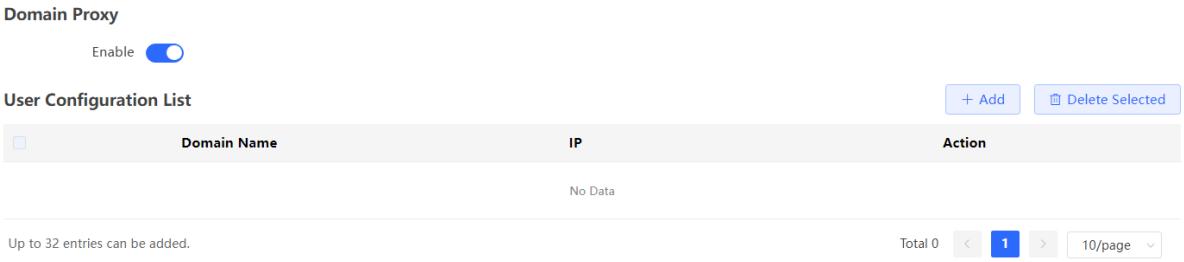
- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **Domain Proxy**.
- Method 2: Choose **One-Device** > **Config** > **WLAN** > **Domain Proxy**.

Note

The method 2 is supported only when the AP is the master device.

When a client accesses a Wi-Fi network, the message "No Internet connection" or "The Wi-Fi is not connected to the Internet" may be displayed. The possible cause is that the client's operating system introduces an Internet detection mechanism. Generally, the detection mechanism sends a probe packet to a specified domain name and evaluates whether the wireless network can access the Internet based on the detection result. If the DNS server takes a long time to parse a domain name or returns a probe node with a long delay, the probe may be deemed unreachable, causing a false network unavailability.

After the **Domain Proxy** function is enabled, the device returns the preset domain name node to the client, reducing the misjudgment of network unavailability of the client.



Click **+Add**, enter the preset domain name and IP address, and click **OK**.

3.23 Client Association

3.23.1 Configuring Intelligent Association

Go to the configuration page by choosing **Network-Wide > Workspace** > **Wireless** > **Client Association** > **Intelligent Association**.

After certain smart home devices are associated with a remote AP, they are unable to re-associate with a nearby AP, resulting in poor user experience and significant delays.

With the Intelligent Association feature enabled, clients can dynamically select the access point for association, eliminating issues related to poor user experience caused by remote associations.

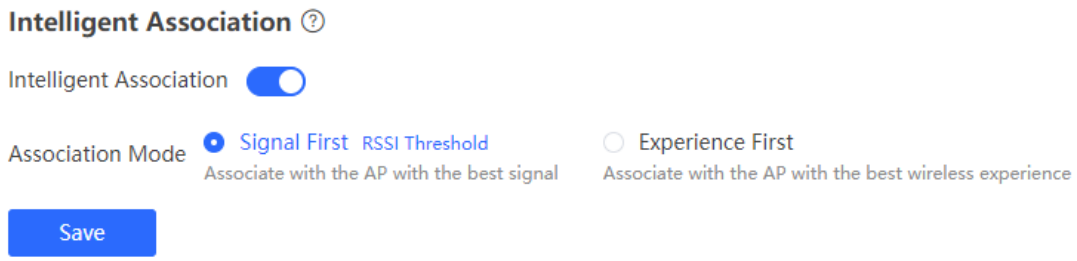
Toggle on the **Intelligent Association** switch, select the association mode, and click **Save**.

- Signal First

  Associate with the AP with the best signal.

- Experience First

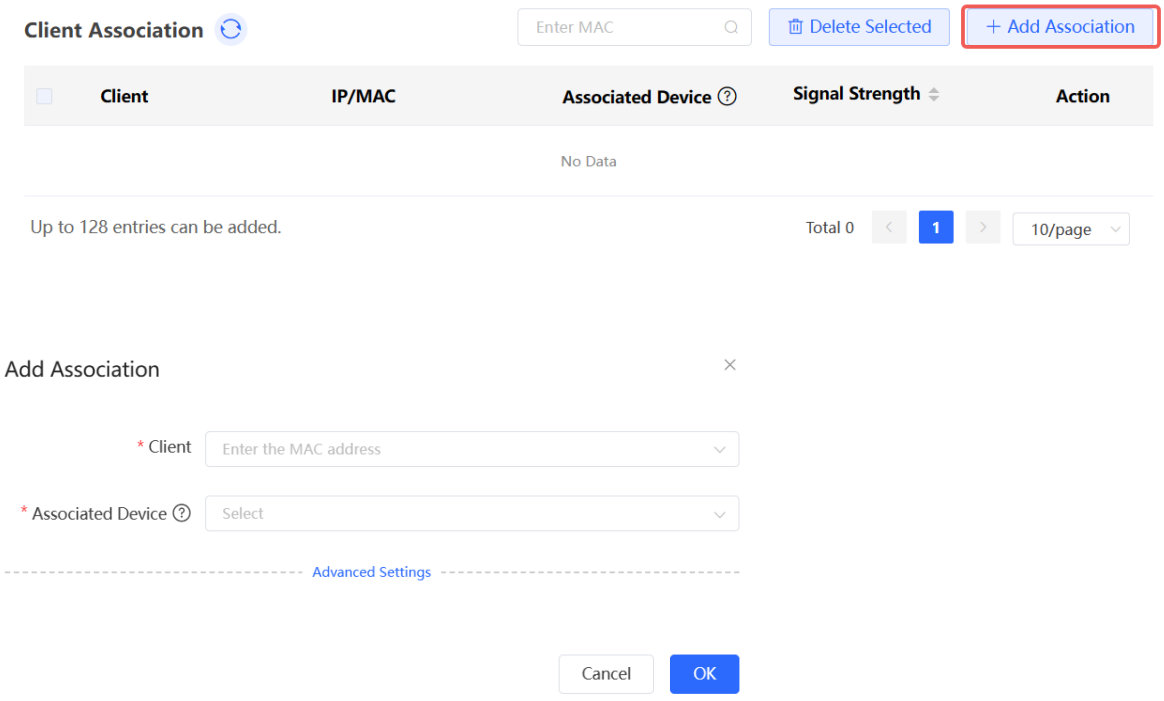
  Associate with the AP with the best wireless experience.



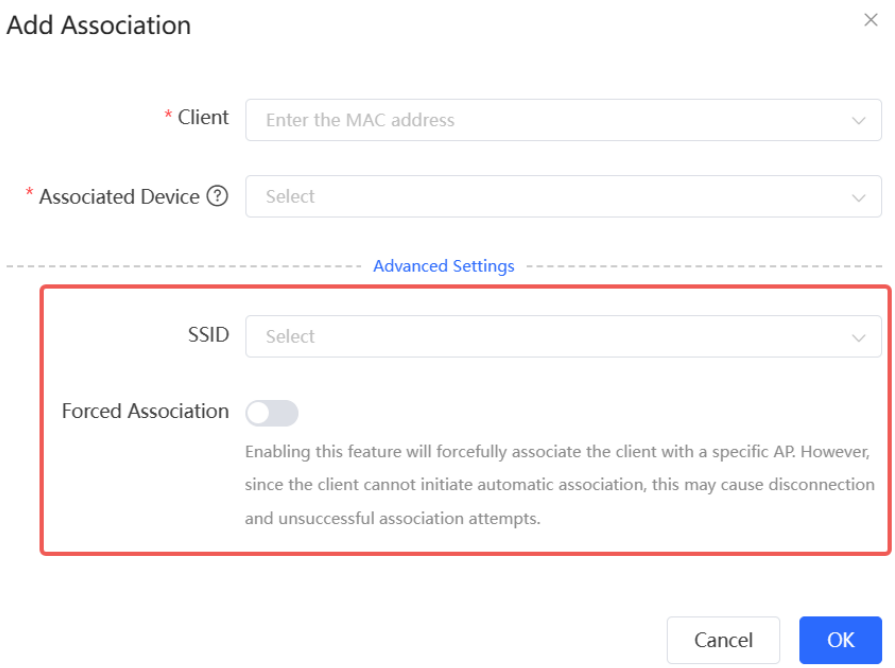
3.23.2 Configuring Client Association

Choose **Network-Wide** > **Workspace** > **Wireless** > **Client Association** > **Client Association**.

Click **Add Association**. Select the client and the associated device. You can associate the client with a specified AP on the network to reduce remote association and improve the wireless experience.



Click **Advanced Settings** to configure the SSID for client association and to enable **Forced Association**.



Caution

The **Forced Association** feature may cause the client to go offline or fail to associate with the AP. Therefore, exercise caution when performing this configuration.

3.24 Configuring AP Load Balancing

3.24.1 Overview

The AP load balancing function is used to balance the load of APs in the wireless network. When APs are added to a load balancing group, clients will automatically associate with the APs with light load when the APs in the group are not load balanced. AP load balancing supports two modes:

- Client Load Balancing: The load is balanced according to the number of associated clients. When a large number of clients have been associated with an AP and the count difference to the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.
- Traffic Load Balancing: The load is balanced according to the traffic on the APs. When the traffic on an AP is large and the traffic difference to the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.

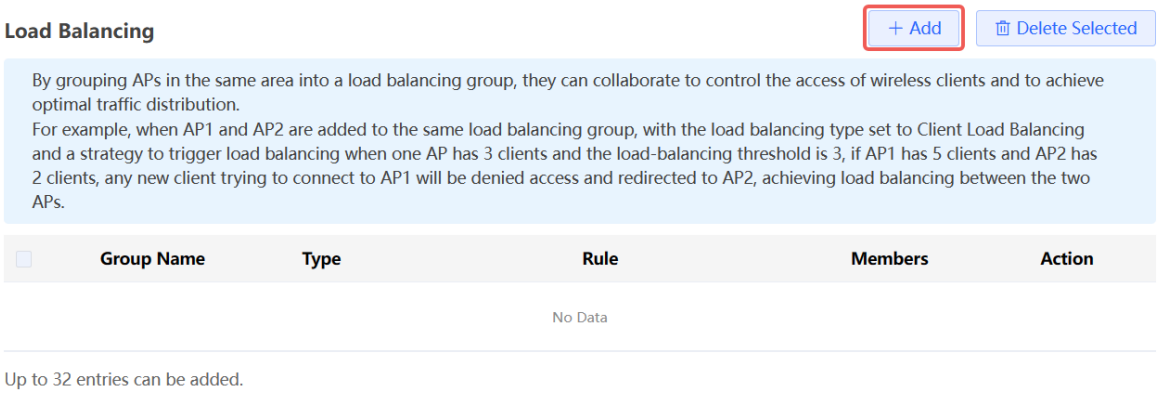
Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only with AP2.

After a client request is denied by an AP and it fails to associate with another AP in the group, the client will keep trying to associate with this AP. If the client attempts reach the specified value, the AP will permit connection of this client, ensuring that the user can normally access the Internet.

3.24.2 Configuring Client Load Balancing

Choose **Network-Wide** > **Workspace** > **Wireless** > **Load Balancing**.

Click **Add**. In the dialog box that appears, set **Type** to **Client Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.



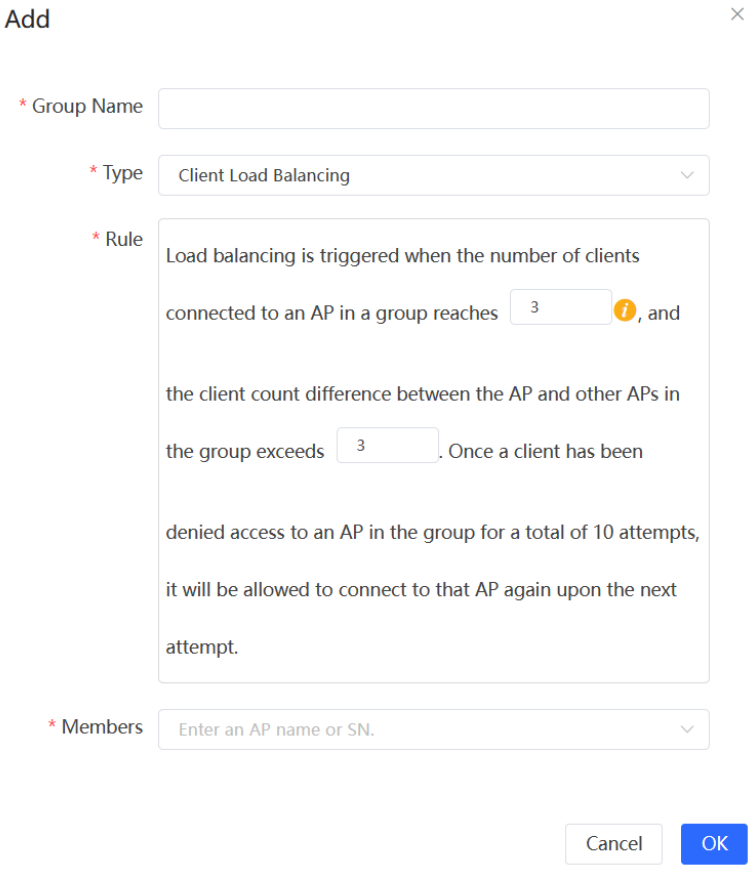


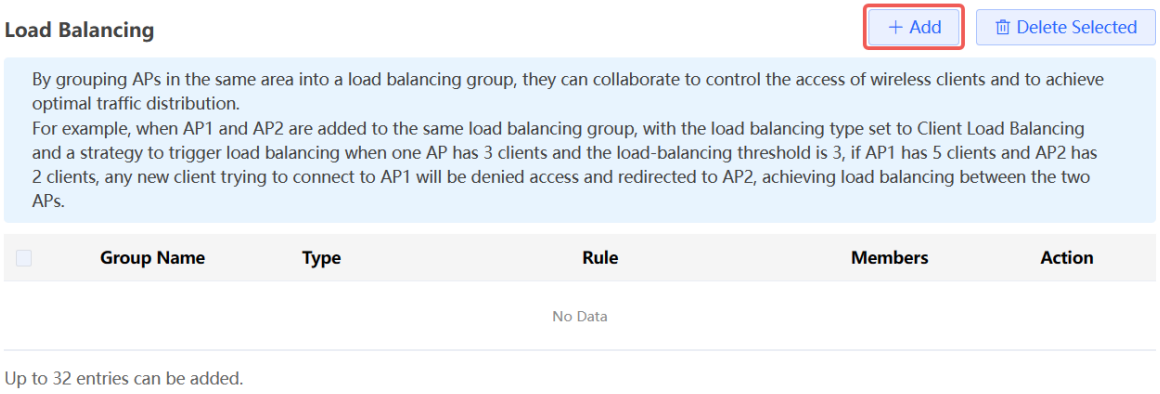
Table 3-4 Client Load Balancing Configuration Parameters

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select **Client Load Balancing**.
Rule	Configure a detailed load balancing rule, including the maximum number of clients allowed to associate with an AP, the difference between the currently associated client count and client count on the AP with the lightest load, and the number of attempts to the AP with full load. By default, when an AP is associated with 3 clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches 3, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.
Members	Specify the APs to be added to the AP load balancing group.

3.24.3 Configuring Traffic Load Balancing

Choose **Network-Wide** > **Workspace** > **Wireless** > **Load Balancing**.

Click **Add**. In the dialog box that appears, set **Type** to **Traffic Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.



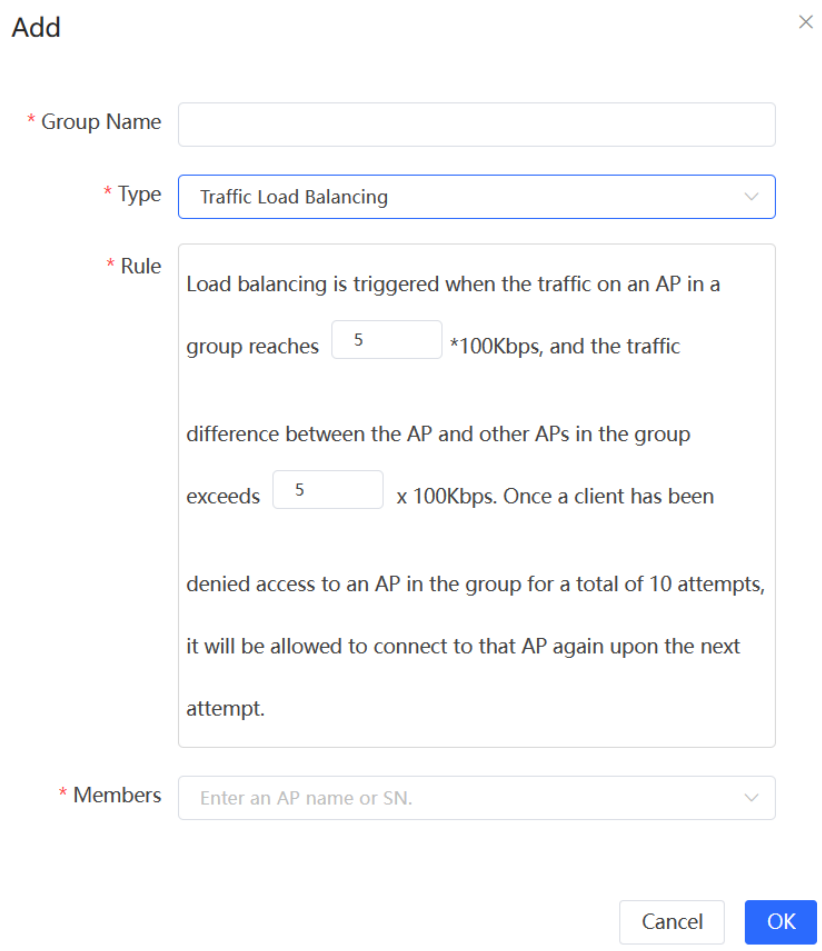


Table 3-5 Traffic Load Balancing Configuration Parameters

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select **Traffic Load Balancing**.
Rule	Configure a detailed load balancing rule, including the maximum traffic allowed on an AP, the difference between the current traffic and the traffic on the AP with the lightest load, and the number of attempts to the AP with full load. By default, when the traffic load on an AP reaches 500 Kbit/s and the difference between the current traffic and the traffic on the AP with the lightest load reaches 500 Kbit/s, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.
Members	Specify the APs to be added to the AP load balancing group.

3.25 Wireless Authentication

3.25.1 Overview

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

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

The following four authentication modes are supported:

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

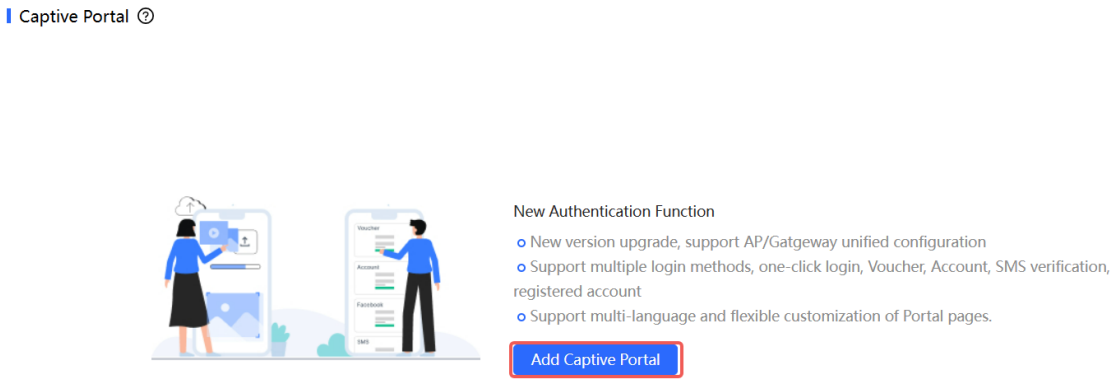
Two or more authentication modes can be configured in a portal template. When multiple authentication modes are configured, users can select an authentication mode on the portal page.

3.25.2 Configuring One-click Login on Ruijie Cloud

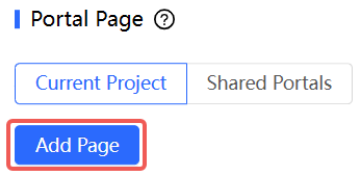
1. Configuring a Portal Template with the Authentication Mode Set to One-click Login

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

(2) Click **Add Captive Portal** to open the portal template configuration page.



(3) Click **Add Page** to customize a portal page.



(4) Configure basic information of the portal template.

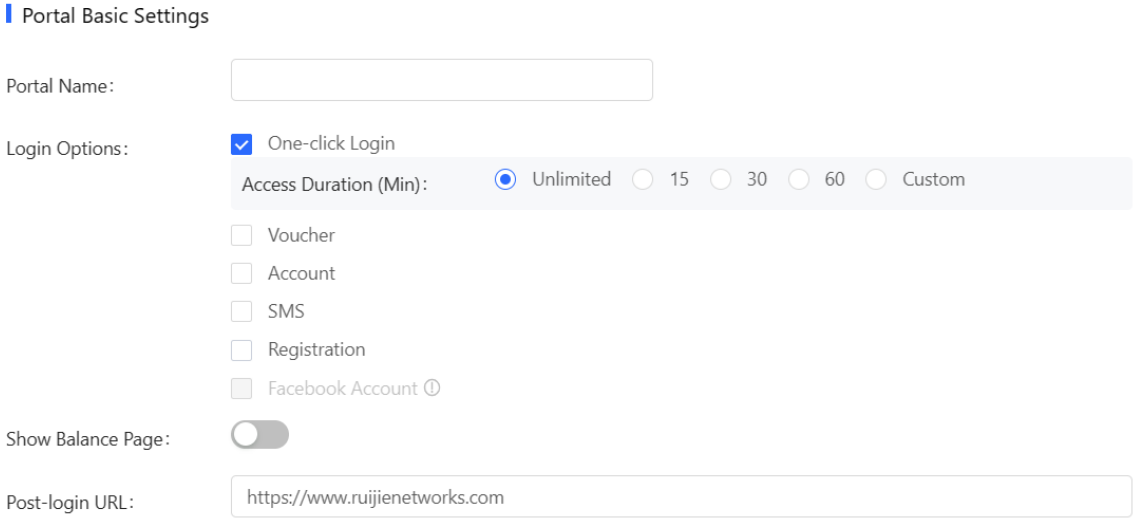
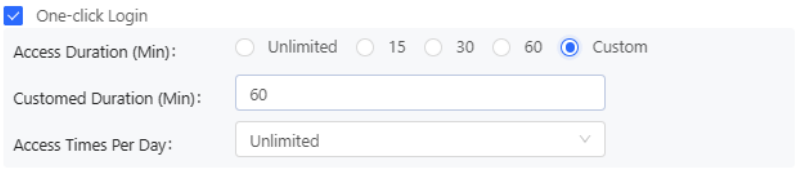


Table 3-6 Portal Template Configuration Parameters

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

(5) Configure visual settings of the portal template.

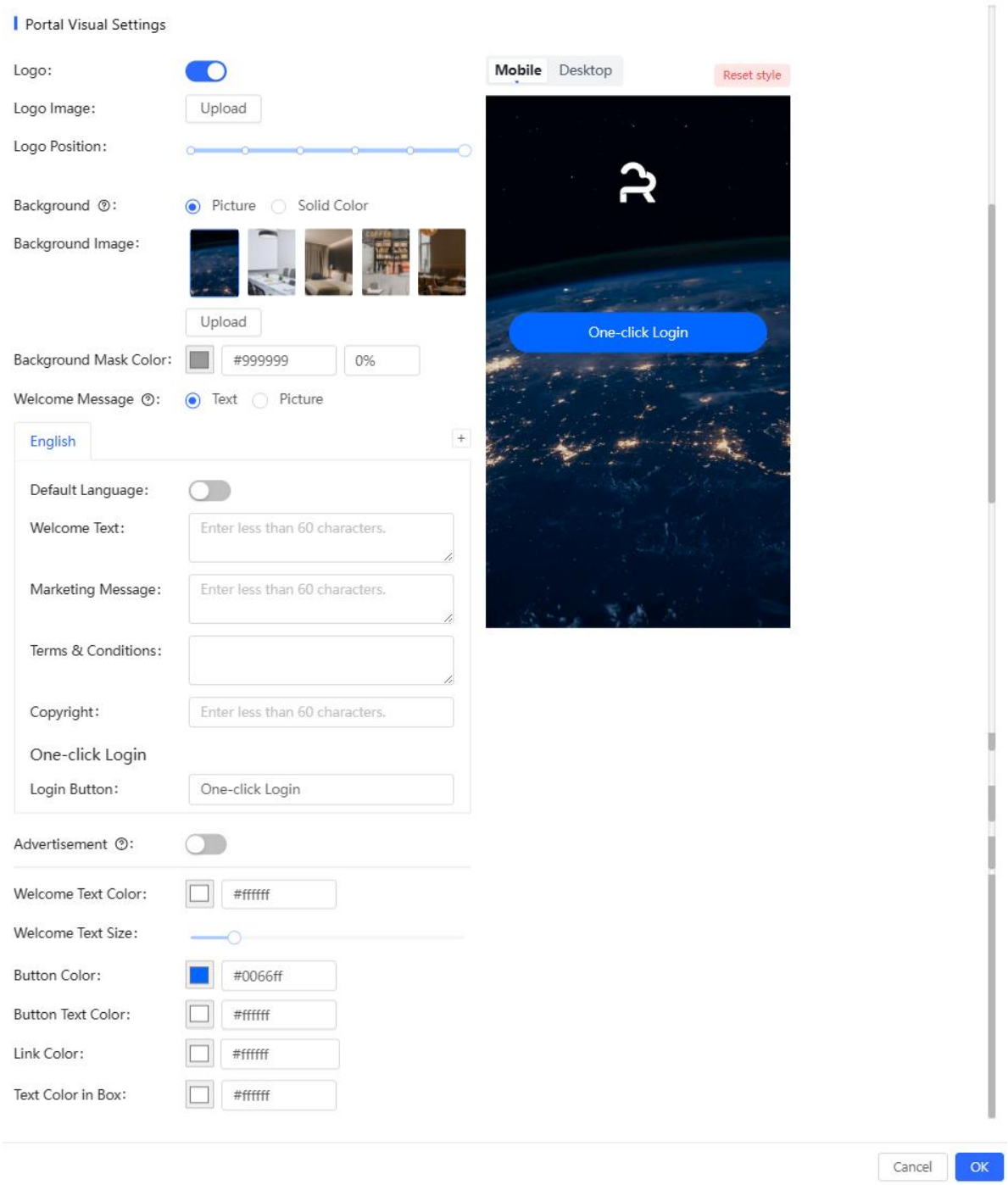
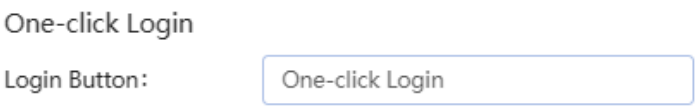


Table 3-7 Portal Page Configuration Parameters

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

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

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

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

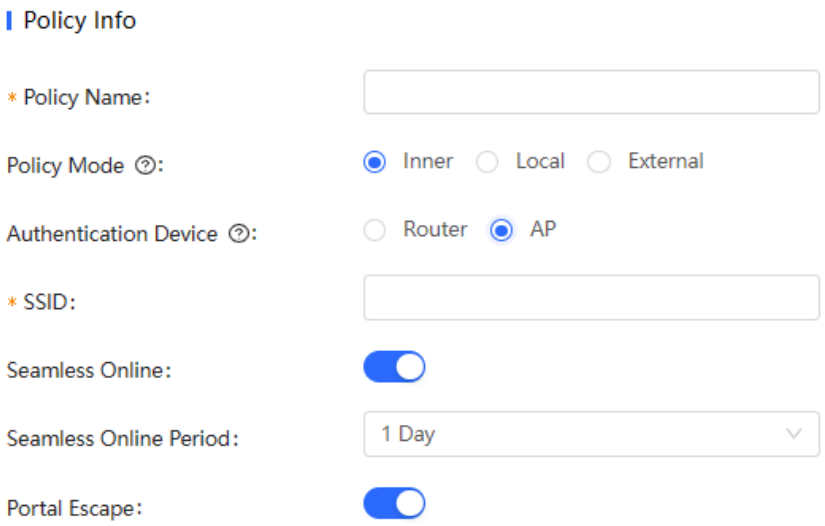


Table 3-8 Captive Portal Configuration Parameters

Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the N/AS. Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit. AP Authentication: RAP, ReyeeOS 1.219 or later version. This parameter is not required if the policy mode is Local.

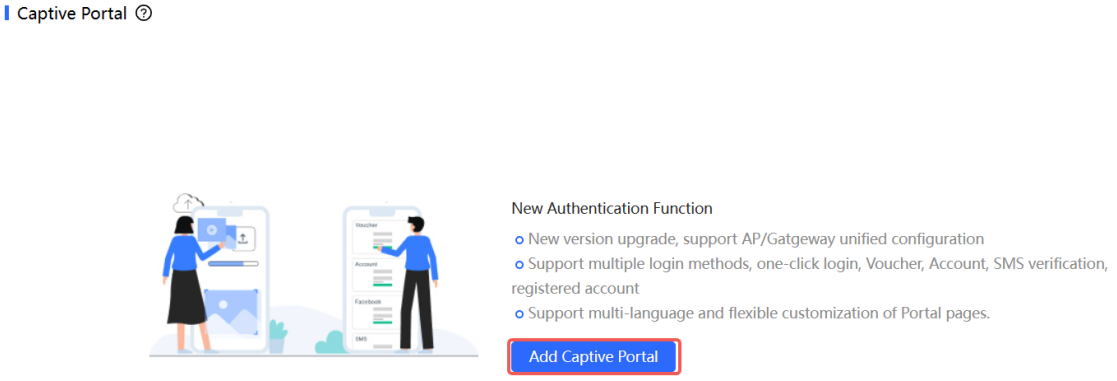
Parameter	Description
Network	Indicates the wired network that requires authentication. Enter the network segment in this field. Users connecting to the wired network corresponding to this network segment must be authenticated. This parameter is required if the Authentication Device is Router.
SSID	Indicates the network name of the Wi-Fi network that requires authentication. Users connecting to this wireless network must be authenticated. This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
Portal Page	Indicates the portal page that is displayed after portal authentication. Click Current Project to select the portal page for an existing project. Click Shared Portals to select an existing portal page. Click Add Page to customize a portal page.

3.25.3 Configuring Voucher Authentication on Ruijie Cloud

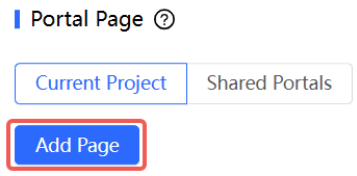
1. Configuring a Portal Template with the Authentication Mode Set to Voucher

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

(2) Click **Add Captive Portal** to open the portal template configuration page.



(3) Click **Add Page** to customize a portal page.



(4) Configure basic information of the portal template.

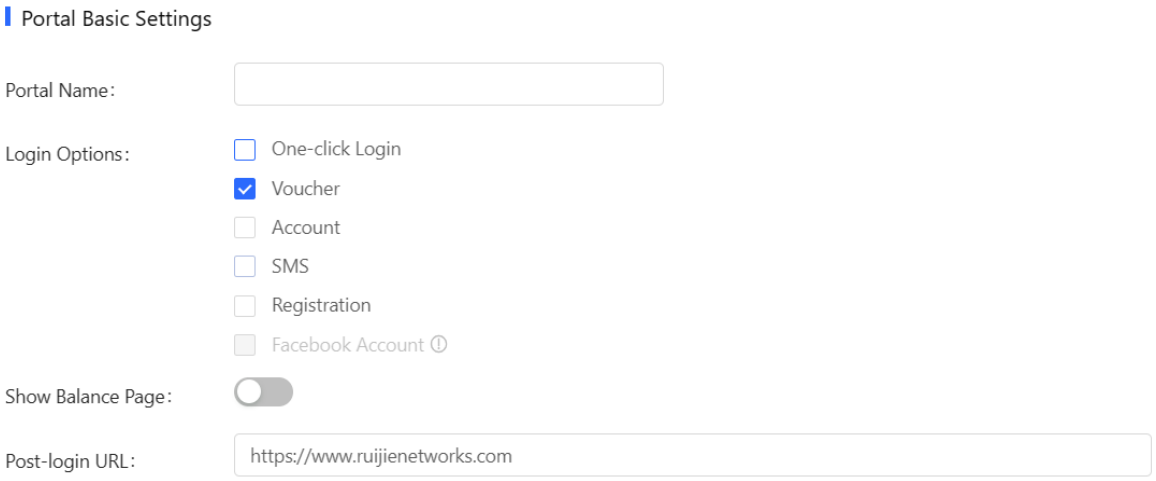


Table 3-9 Portal Template Configuration Parameters

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

(5) Configure visual settings of the portal template.

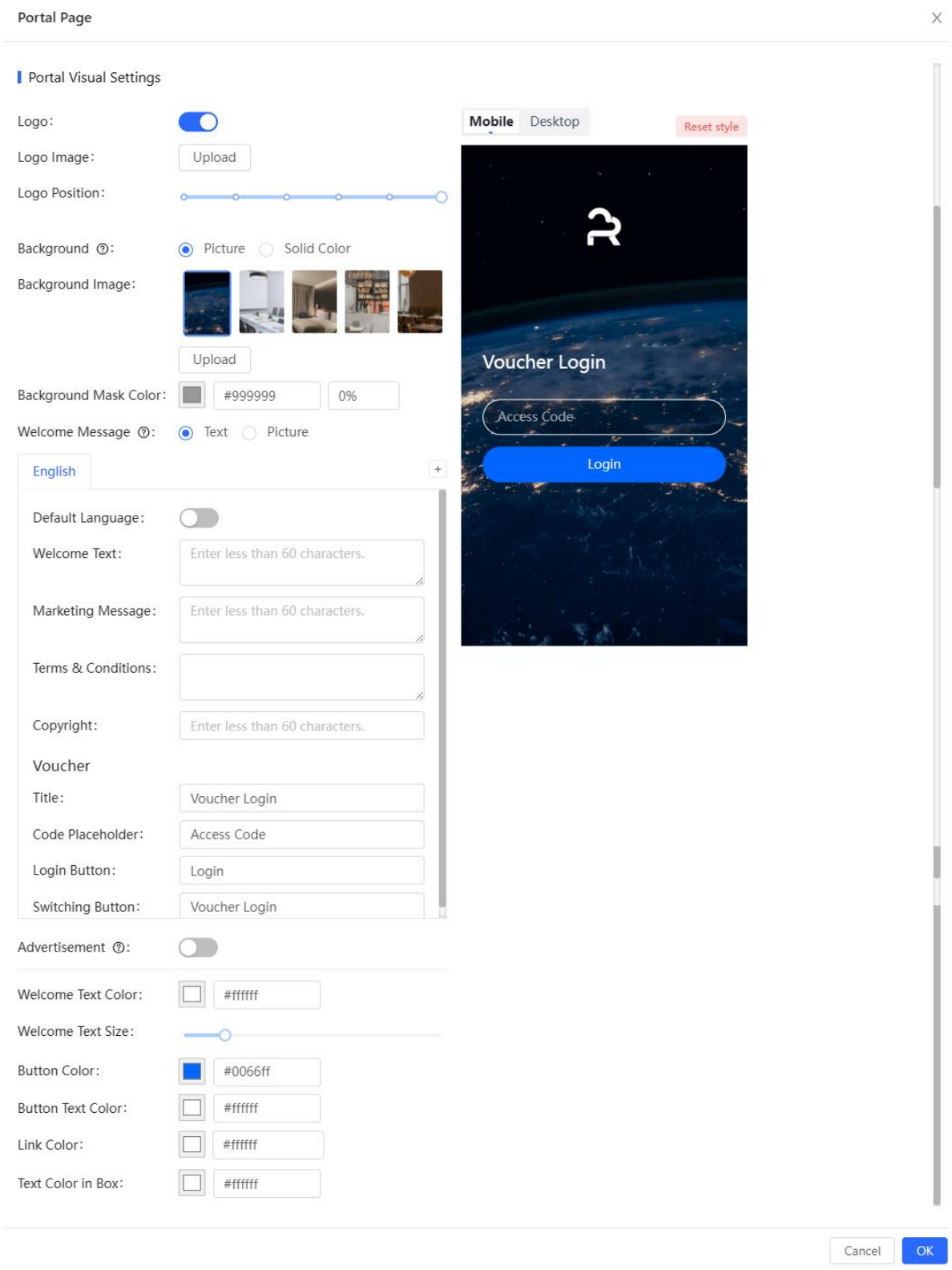
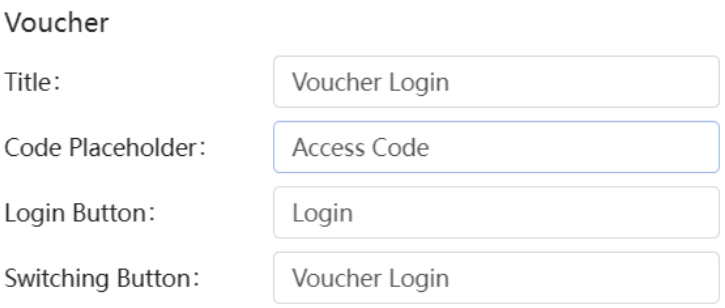


Table 3-10 Portal Page Configuration Parameters

Parameter	Description
Logo	Select whether to display the logo image.

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

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

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

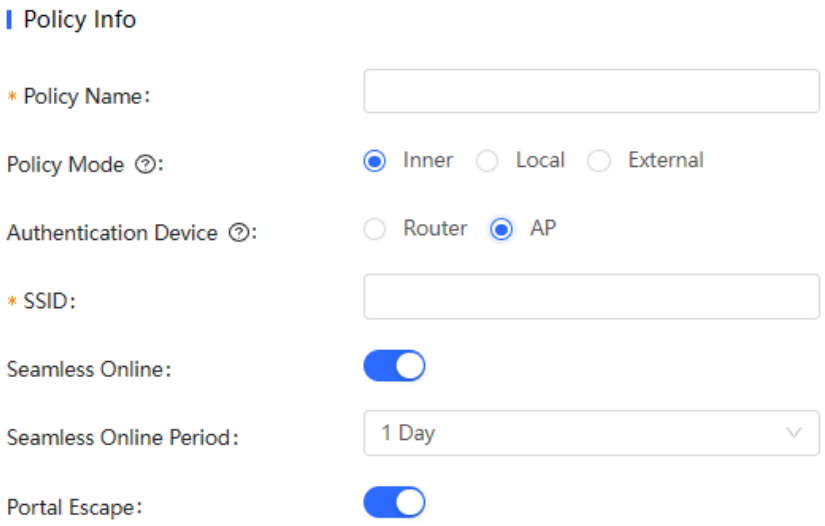


Table 3-11 Captive Portal Configuration Parameters

Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.

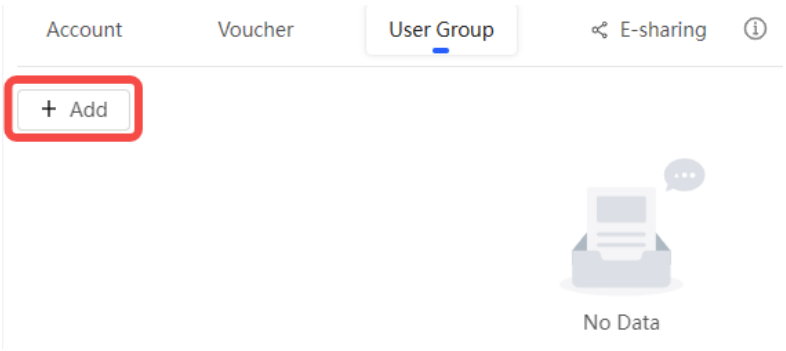
Parameter	Description
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the N/AS. Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit. AP Authentication: RAP, ReyeeOS 1.219 or later version. This parameter is not required if the policy mode is Local.
Network	Indicates the wired network that requires authentication. Enter the network segment in this field. Users connecting to the wired network corresponding to this network segment must be authenticated. This parameter is required if the Authentication Device is Router.
SSID	Indicates the network name of the Wi-Fi network that requires authentication. Users connecting to this wireless network must be authenticated. This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
Portal Page	Indicates the portal page that is displayed after portal authentication. Click Current Project to select the portal page for an existing project. Click Shared Portals to select an existing portal page. Click Add Page to customize a portal page.

3. Adding a Voucher

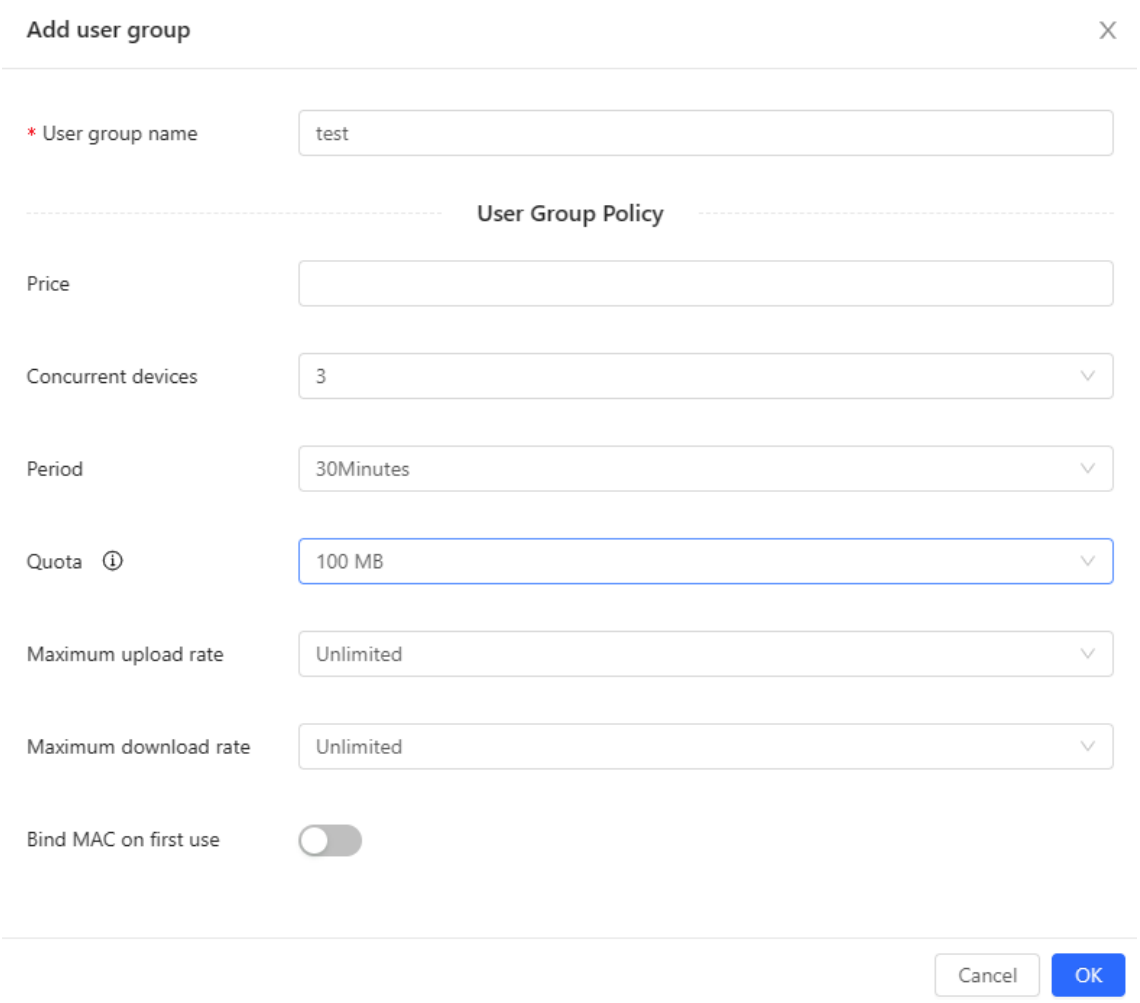
(1) Log in to Ruijie Cloud, choose **Project** > **Auth & Accounts** > **Accounts** > **User Management**, **and** select a network in this account**.**

(2) Configure a user group.

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



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



User Group Name: indicates the user group name.

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

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

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

Quota: indicates the maximum amount of data transfer.

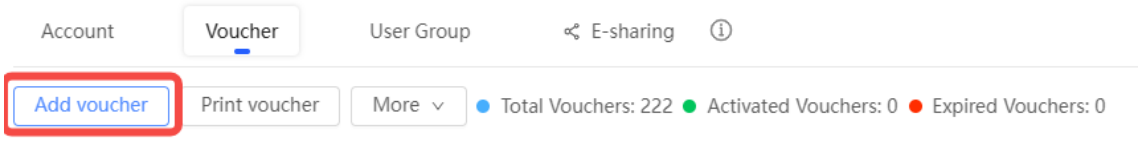
Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

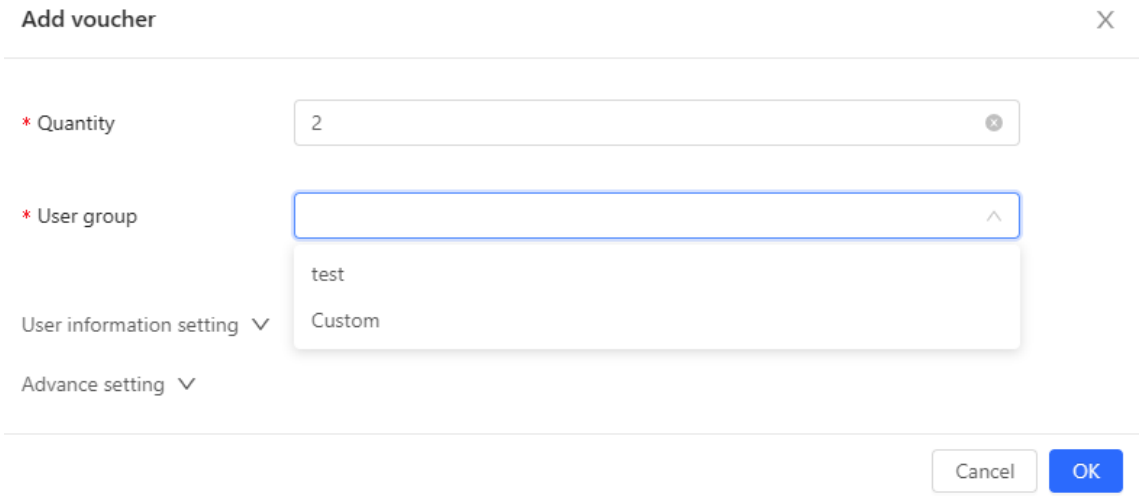
Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) Configure a voucher.

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



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



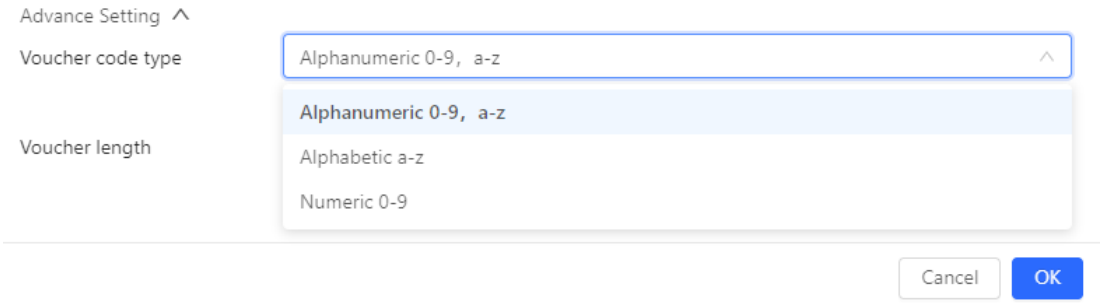
Quantity: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the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

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

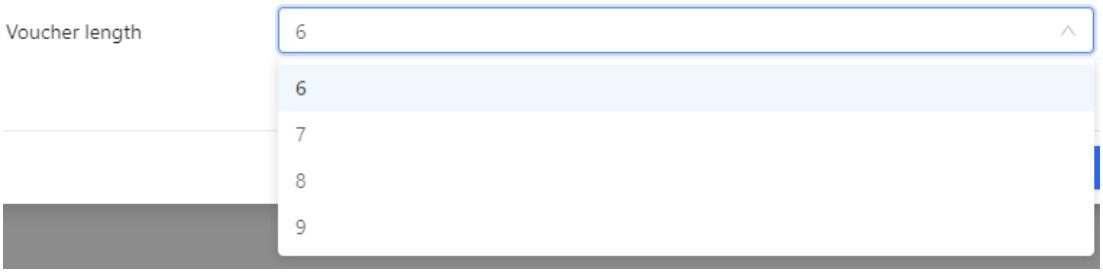
User information setting: Configure user information, which is optional.

Advance setting:

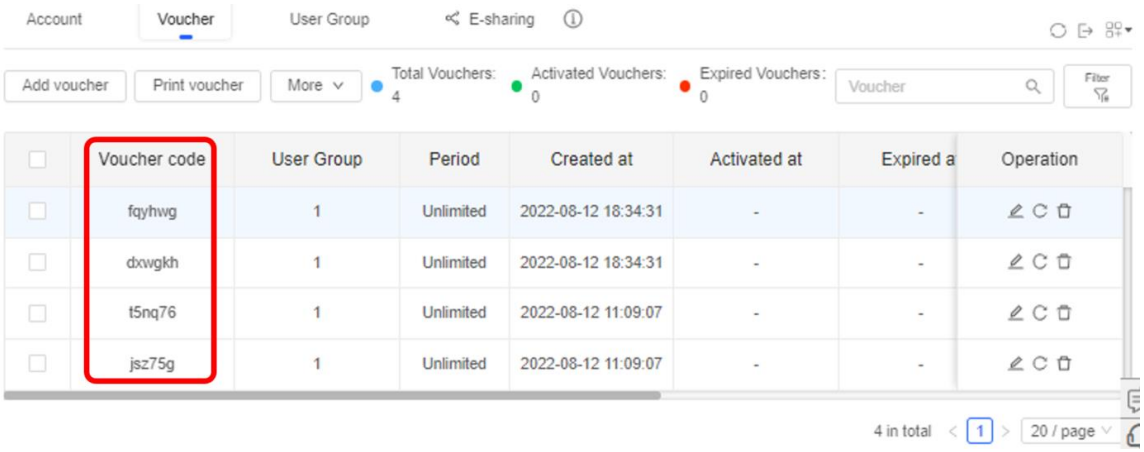
- Voucher code type: Set the value to Alphanumeric 0-9, a-z, Alphabetic a-z, or Numeric 0-9.



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



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

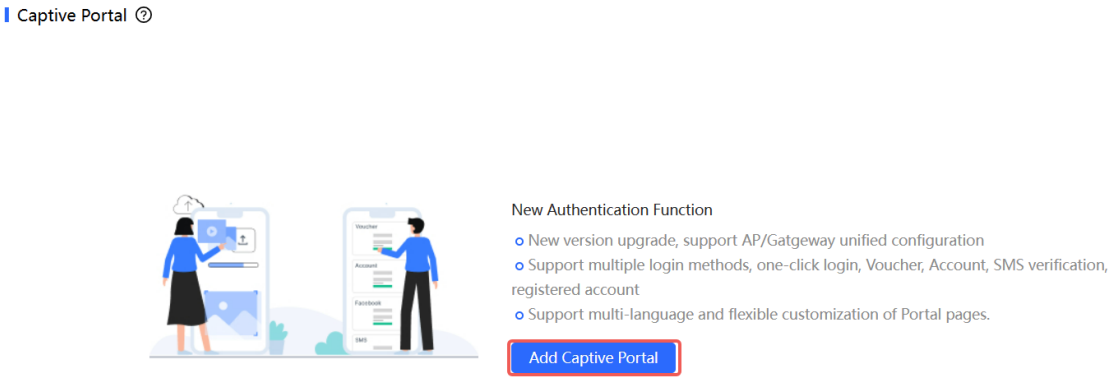


3.25.4 Configuring Account Authentication on Ruijie Cloud

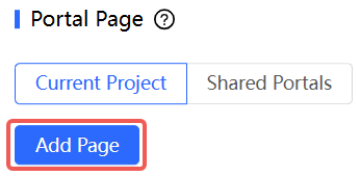
1. Configuring a Portal Template with the Authentication Mode Set to Account

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

(2) Click **Add Captive Portal** to open the portal template configuration page.



(3) Click **Add Page** to customize a portal page.



(4) Configure basic information of the portal template.

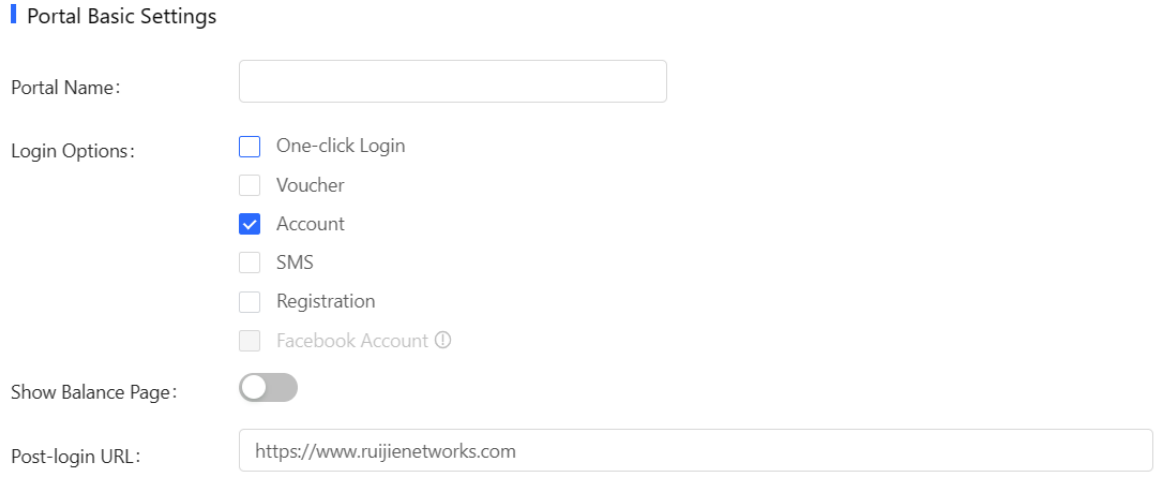


Table 3-12 Portal Template Configuration Parameters

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

(5) Configure visual settings of the portal template.

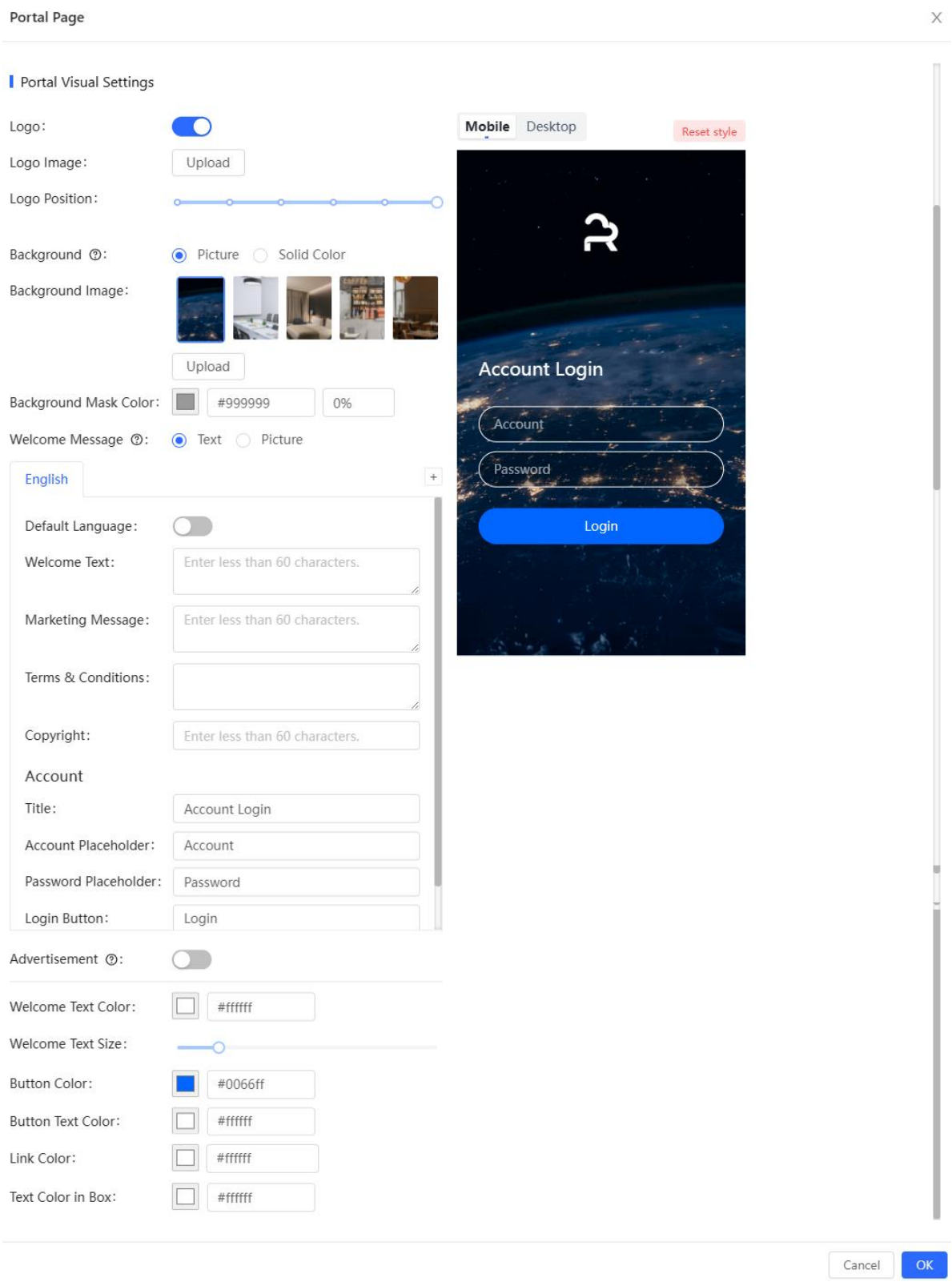
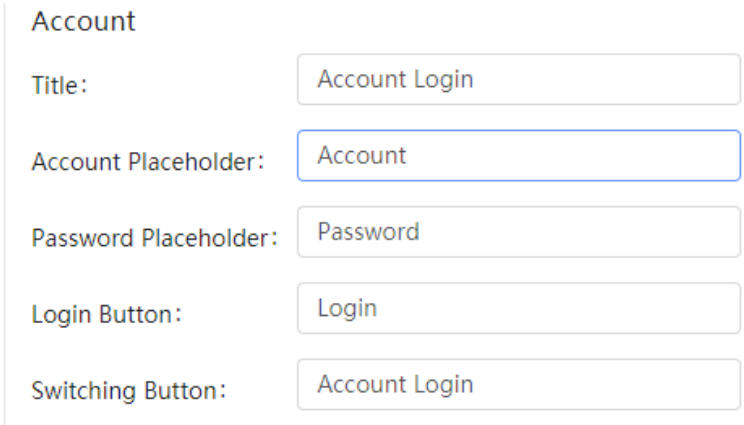


Table 3-13 Portal Page Configuration Parameters

Parameter	Description
Logo	Select whether to display the logo image.

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

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

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

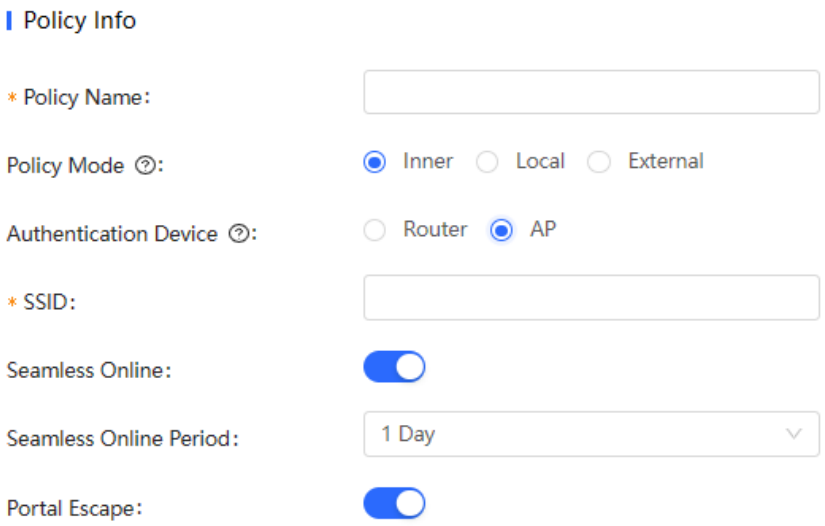


Table 3-14 Captive Portal Configuration Parameters

Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.

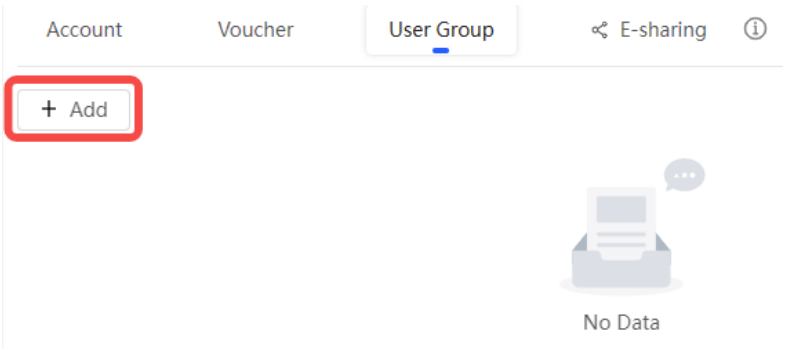
Parameter	Description
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the N/AS. Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit. AP Authentication: RAP, ReyeeOS 1.219 or later version. This parameter is not required if the policy mode is Local.
Network	Indicates the wired network that requires authentication. Enter the network segment in this field. Users connecting to the wired network corresponding to this network segment must be authenticated. This parameter is required if the Authentication Device is Router.
SSID	Indicates the network name of the Wi-Fi network that requires authentication. Users connecting to this wireless network must be authenticated. This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
Portal Page	Indicates the portal page that is displayed after portal authentication. Click Current Project to select the portal page for an existing project. Click Shared Portals to select an existing portal page. Click Add Page to customize a portal page.

3. Adding an Account

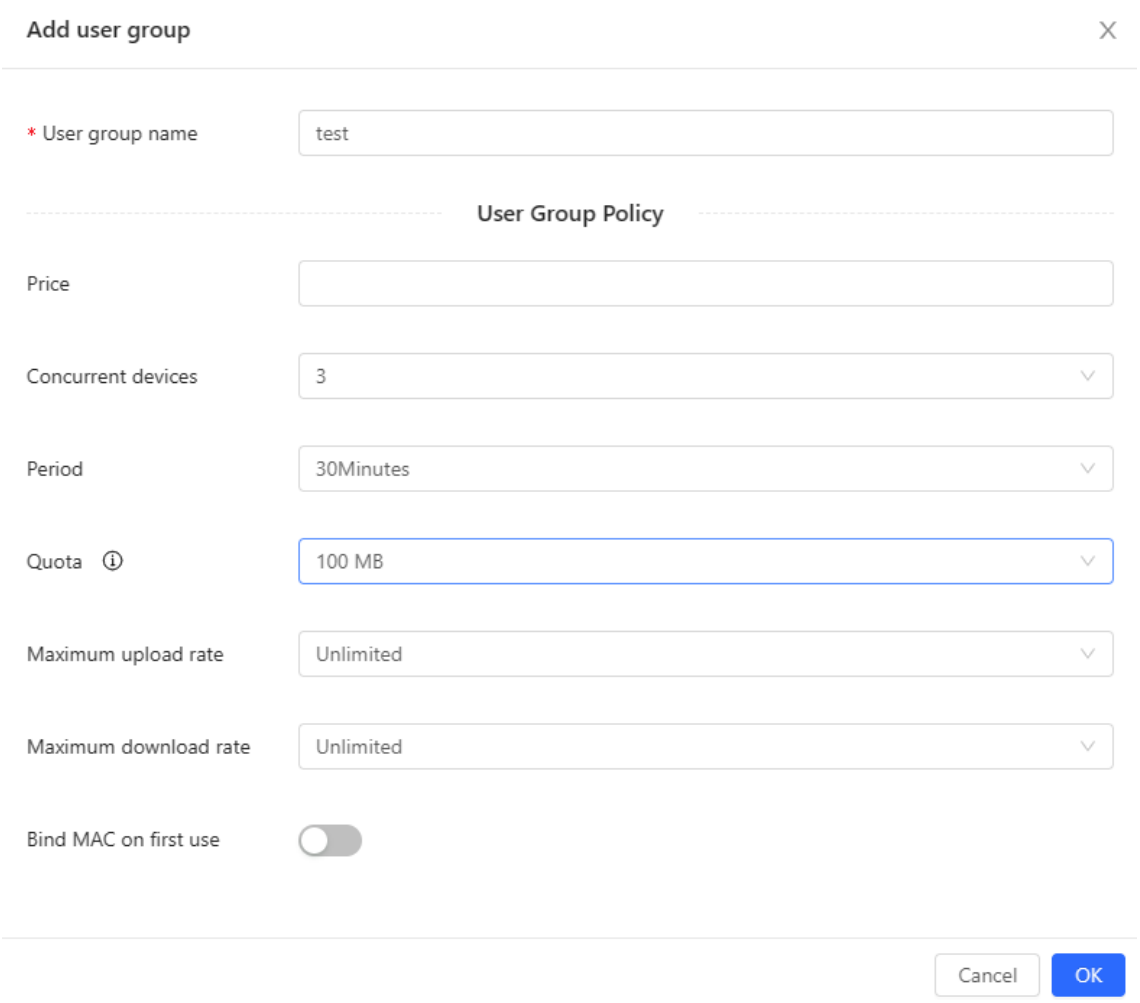
(1) Log in to Ruijie Cloud, choose **Project** > **Auth & Accounts** > **Accounts** > **User Management**, and select a network in this account**.**

(2) Configure a user group.

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



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



User Group Name: indicates the user group name.

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

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

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

Quota: indicates the maximum amount of data transfer.

Maximum upload rate: indicates the maximum upload rate.

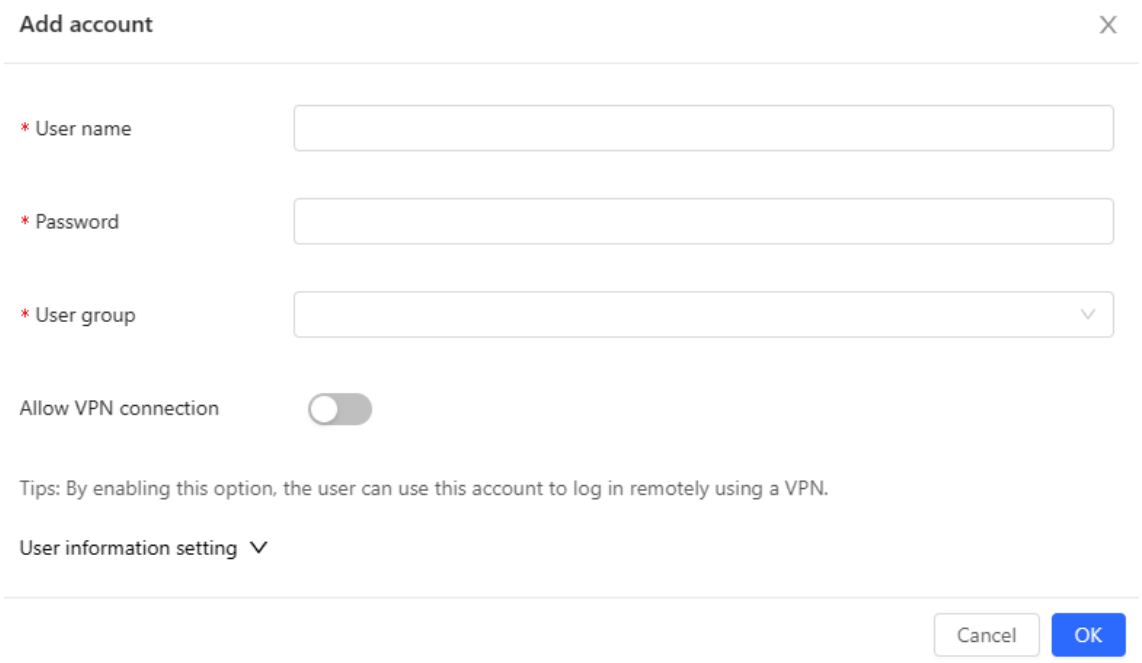
Maximum download rate: indicates the maximum download rate.

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

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

- Adding an account manually

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



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

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

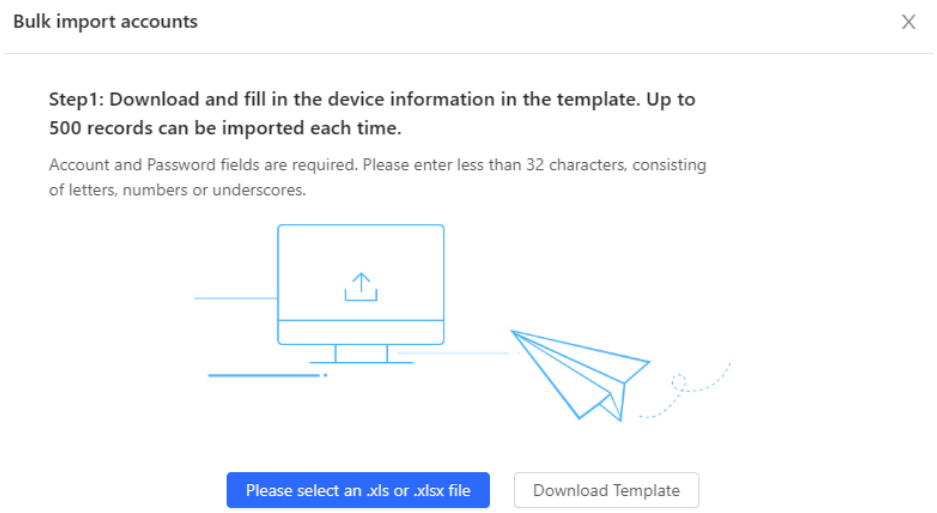
User group: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click **Custom** to create a user group.

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

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

- Adding accounts through batch import

  a Click **Bulk import**.



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

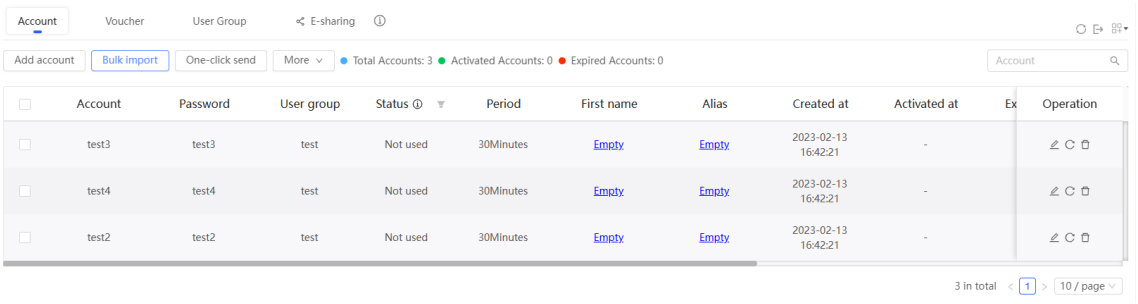
c Edit the template and save it.

Caution

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

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

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



3.25.5 Configuring SMS Authentication on Ruijie Cloud

1. Adding a Twilio Account

Prerequisites

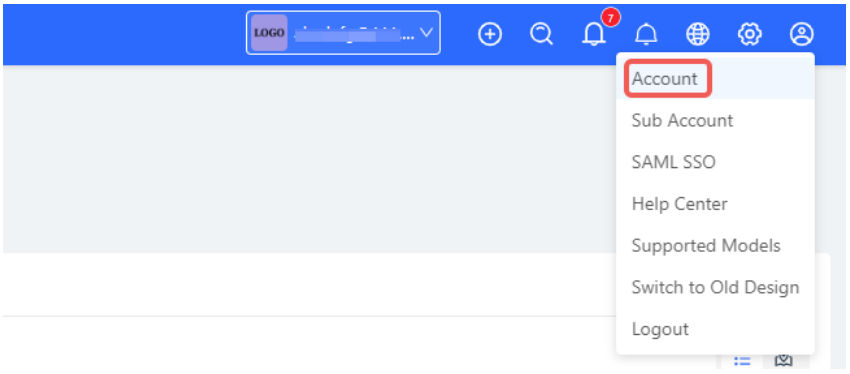
A Twilio account has been applied for from the Twilio official website (https://www.twilio.com/login).

Note

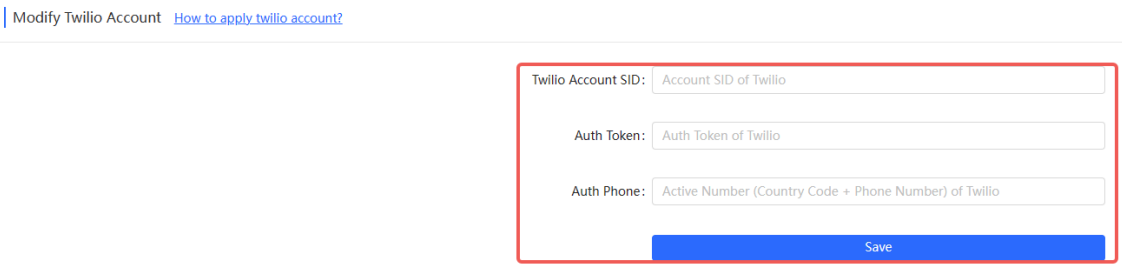
A Twilio account is used to send the SMS verification code.

Configuration Steps

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



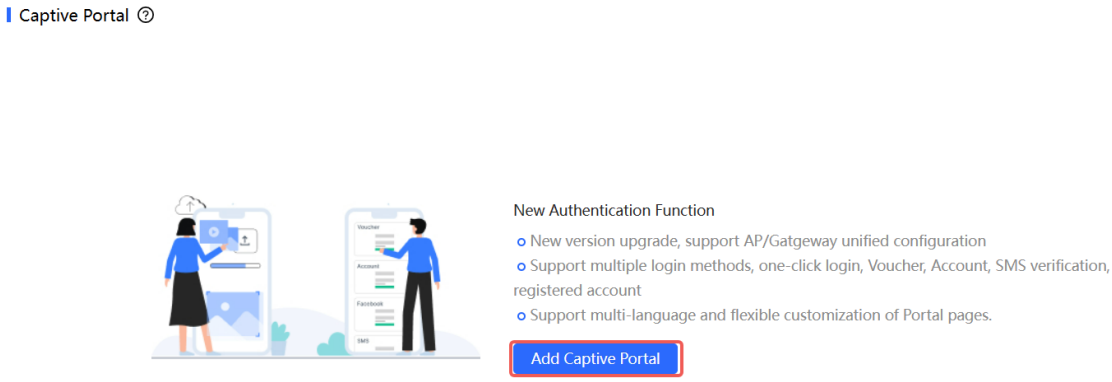
(2) Add Twilio account information and click **Save**.



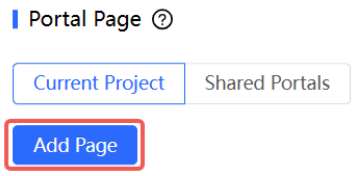
2. Configuring a Portal Template with the Authentication Mode Set to SMS

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

(2) Click **Add Captive Portal** to open the portal template configuration page.



(3) Click **Add Page** to customize a portal page.



(4) Configure basic information of the portal template.

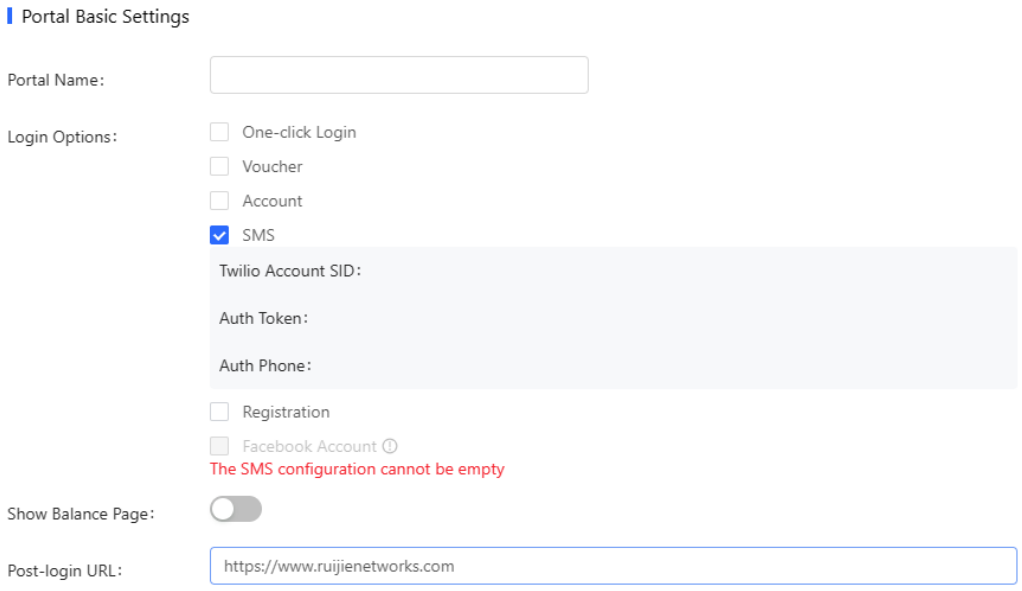


Table 3-15 Portal Template Configuration Parameters

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

(5) Configure visual settings of the portal template.

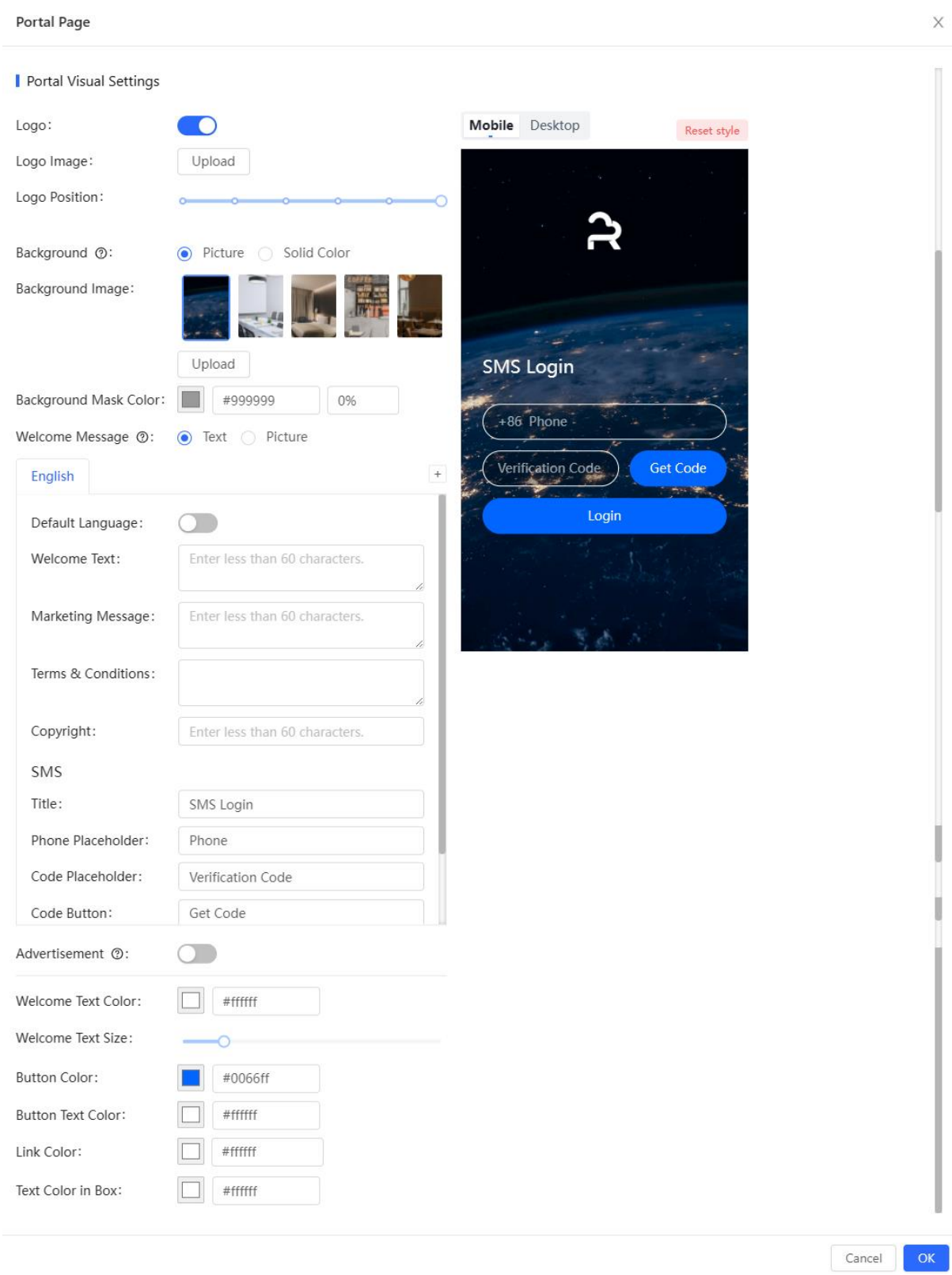
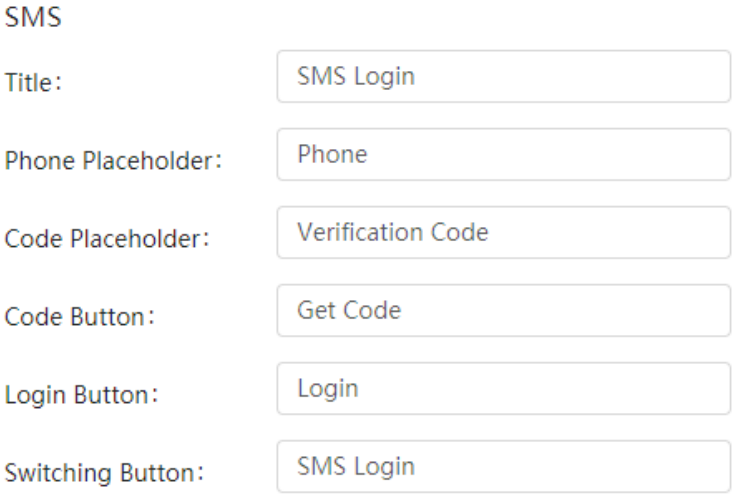

Portal Page
Portal Visual Settings
Logo:
Logo Image:
Upload
Logo Position:
Background:
Picture
Solid Color
Background Image:
Upload
Background Mask Color:
#999999
0%
Welcome Message:
Text
Picture
English
Default Language:
Welcome Text:
Enter less than 60 characters.
Marketing Message:
Enter less than 60 characters.
Terms & Conditions:
Copyright:
Enter less than 60 characters.
SMS
Title:
SMS Login
Phone Placeholder:
Phone
Code Placeholder:
Verification Code
Code Button:
Get Code
Advertisement:
Welcome Text Color:
#ffffff
Welcome Text Size:
Button Color:
#0066ff
Button Text Color:
#ffffff
Link Color:
#ffffff
Text Color in Box:
#ffffff
Mobile
Desktop
Reset style
SMS Login
+86 Phone
Verification Code
Get Code
Login
Cancel
OK

Table 3-16 Portal Page Configuration Parameters

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

Parameter	Description
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

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

3. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, **Go to the "Captive Portal" page** is available and you can select whether to perform wireless authentication.

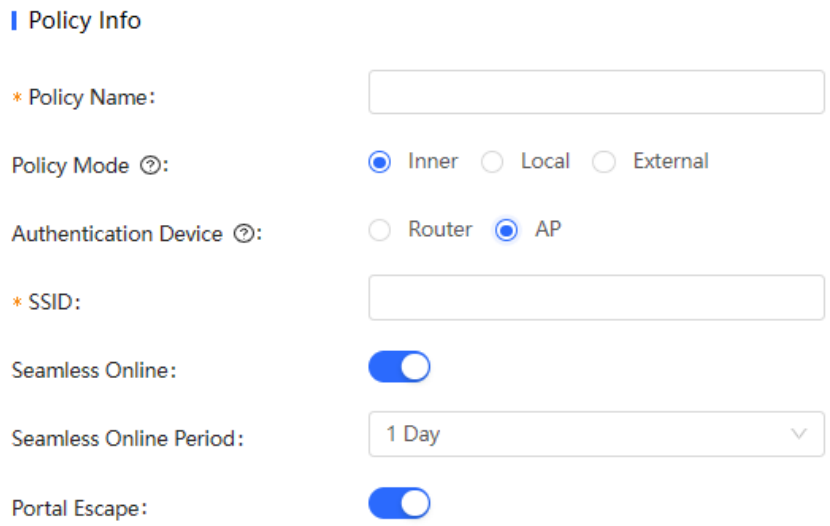


Table 3-17 Captive Portal Configuration Parameters

Parameter	Description
Policy Name	Indicates the name of a captive portal template.

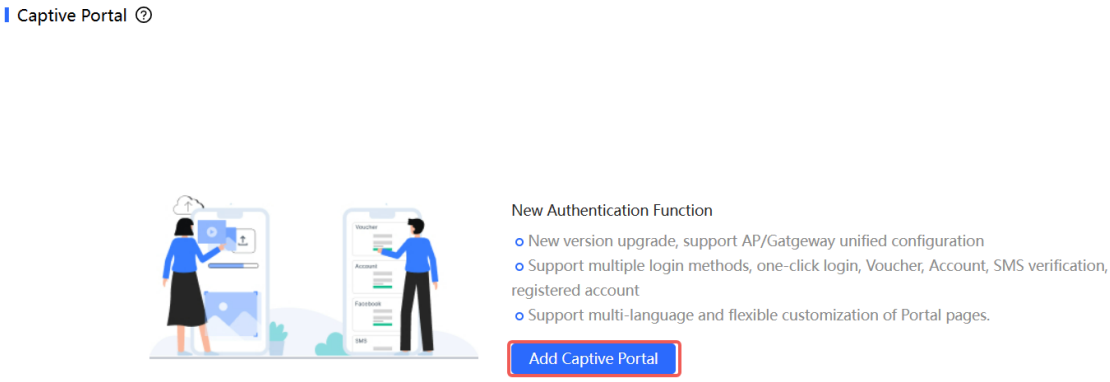
Parameter	Description
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the N/AS. Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit. AP Authentication: RAP, ReyeeOS 1.219 or later version. This parameter is not required if the policy mode is Local.
Network	Indicates the wired network that requires authentication. Enter the network segment in this field. Users connecting to the wired network corresponding to this network segment must be authenticated. This parameter is required if the Authentication Device is Router.
SSID	Indicates the network name of the Wi-Fi network that requires authentication. Users connecting to this wireless network must be authenticated. This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
Portal Page	Indicates the portal page that is displayed after portal authentication. Click Current Project to select the portal page for an existing project. Click Shared Portals to select an existing portal page. Click Add Page to customize a portal page.

3.25.6 Configuring Registration on Ruijie Cloud

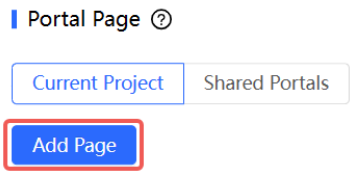
1. Configuring a Portal Template with the Authentication Mode Set to One-click Login

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

(2) Click **Add Captive Portal** to open the portal template configuration page.



(3) Click **Add Page** to customize a portal page.



(4) Configure basic information of the portal template.

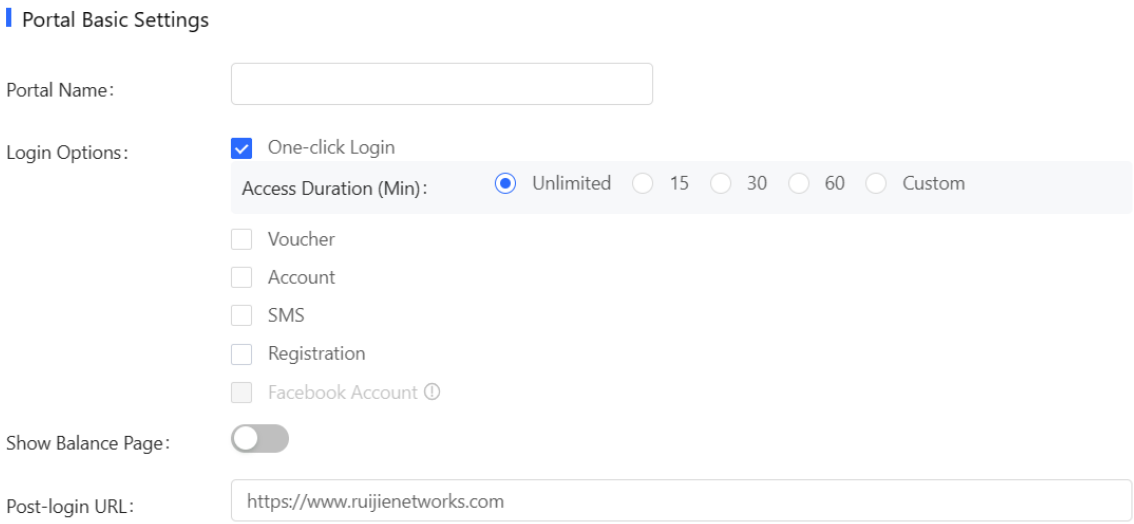
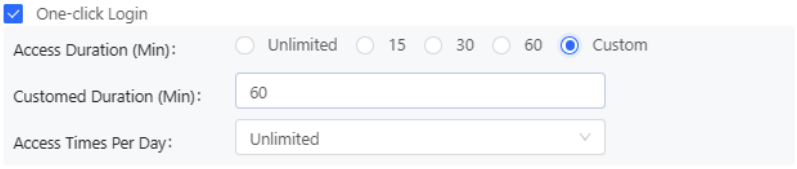


Table 3-18 Portal Template Configuration Parameters

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

(5) Configure visual settings of the portal template.

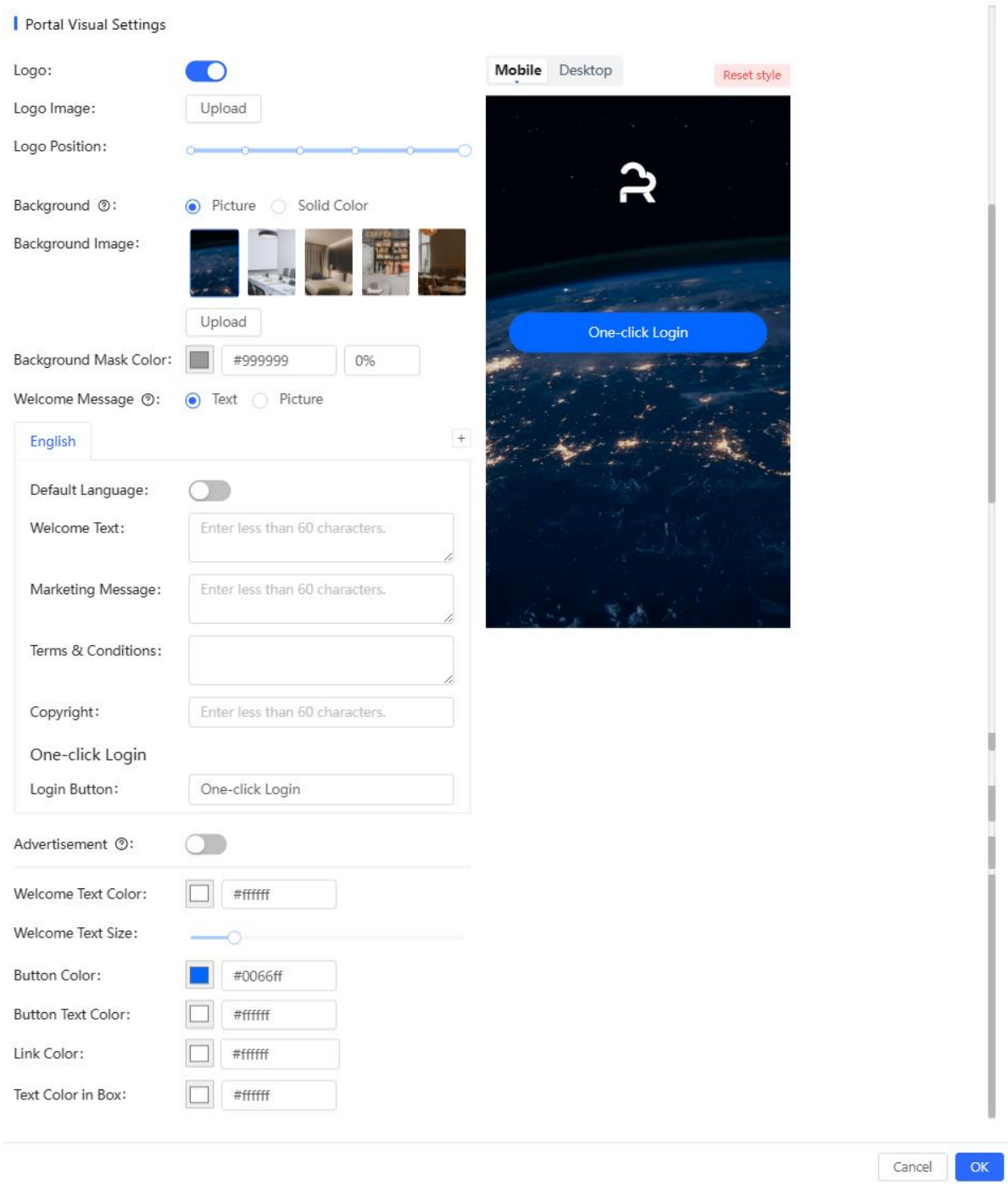
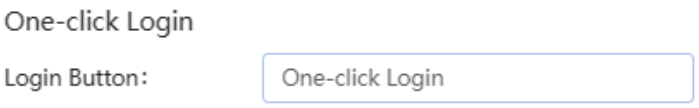


Table 3-19 Portal Page Configuration Parameters

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

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

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

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

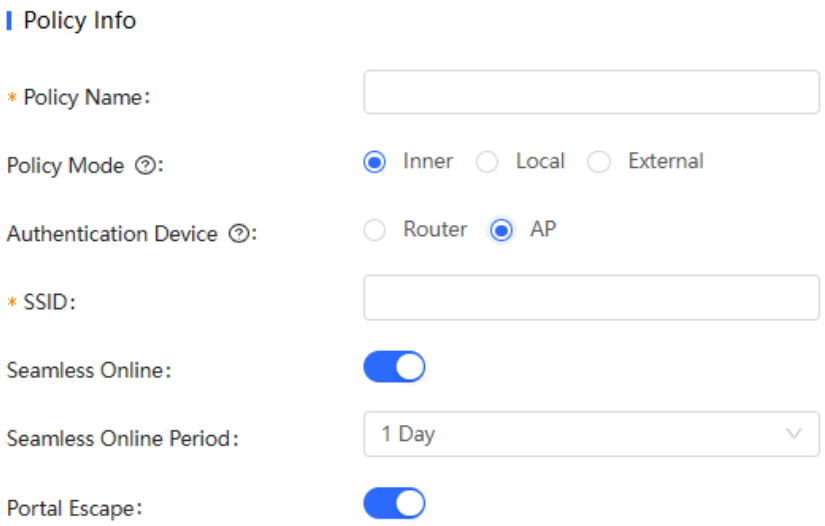


Table 3-20 Captive Portal Configuration Parameters

Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the N/AS. Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit. AP Authentication: RAP, ReyeeOS 1.219 or later version. This parameter is not required if the policy mode is Local.

Parameter	Description
Network	Indicates the wired network that requires authentication. Enter the network segment in this field. Users connecting to the wired network corresponding to this network segment must be authenticated. This parameter is required if the Authentication Device is Router.
SSID	Indicates the network name of the Wi-Fi network that requires authentication. Users connecting to this wireless network must be authenticated. This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
Portal Page	Indicates the portal page that is displayed after portal authentication. Click Current Project to select the portal page for an existing project. Click Shared Portals to select an existing portal page. Click Add Page to customize a portal page.

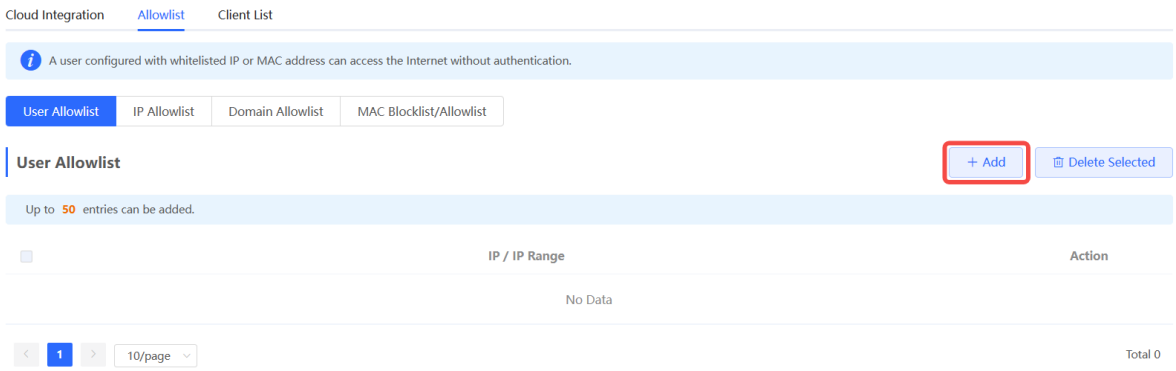
3.25.7 Configuring an Authentication-Free User List on Web Interface

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

1. Configuring an Authentication-Free User

(1) Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Allowlist > User Allowlist.**

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



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

2. Configuring an Authentication-Free Public IP Address

(1) Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Allowlist > IP Allowlist.**

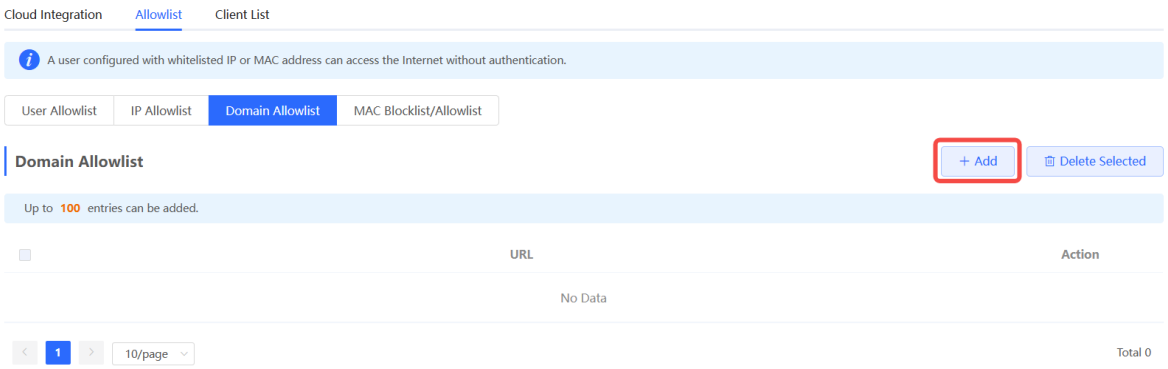
(2) Click **Add** to open the configuration page.

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

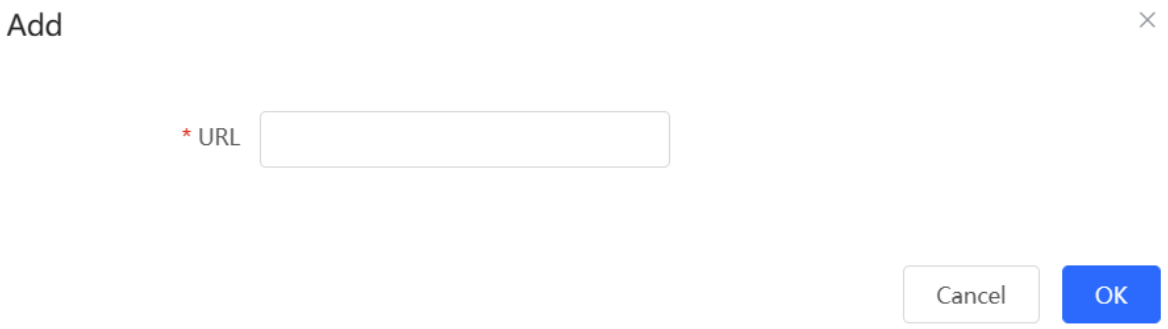
3. Configuring a Domain Name Allowlist

(1) Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Allowlist > Domain Allowlist.**

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



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

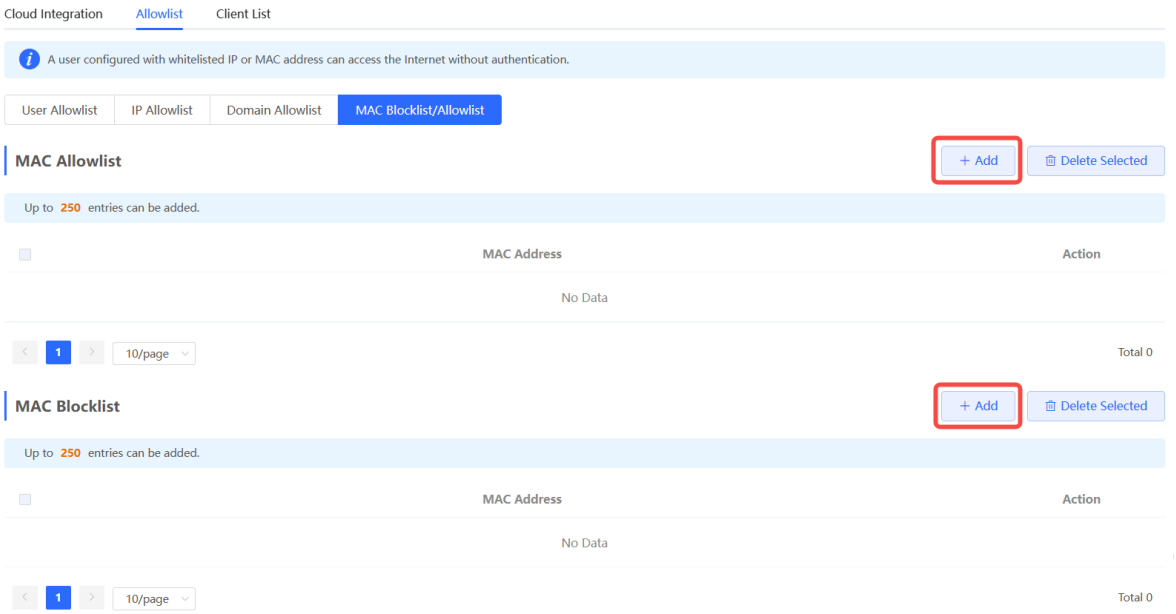


4. Configuring a MAC Address Allowlist and Blocklist

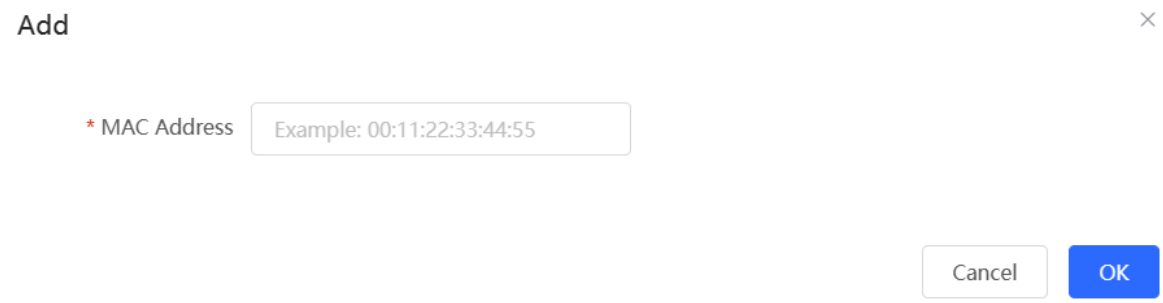
STAs whose MAC addresses are added to the MAC address allowlist can access the network without authentication, and STAs whose MAC addresses are added to the MAC address blocklist are forbidden to access the network.

(1) Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Allowlist > MAC Blocklist/Allowlist.**

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



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

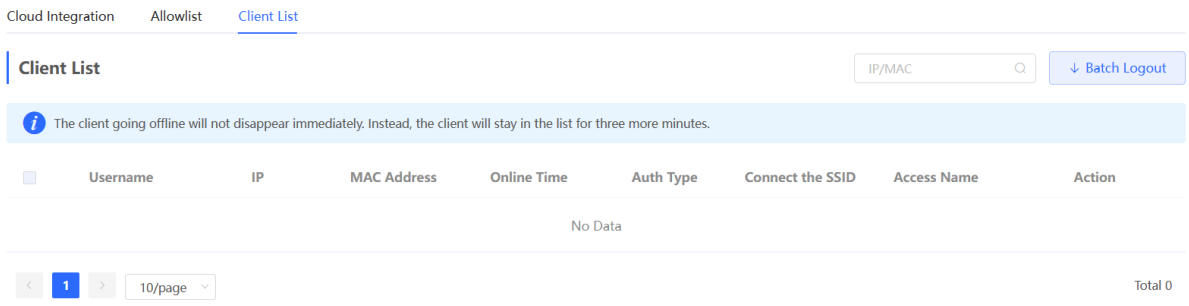


3.25.8 Displaying Authenticated Users on web interface

Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Client List** to display authenticated users.

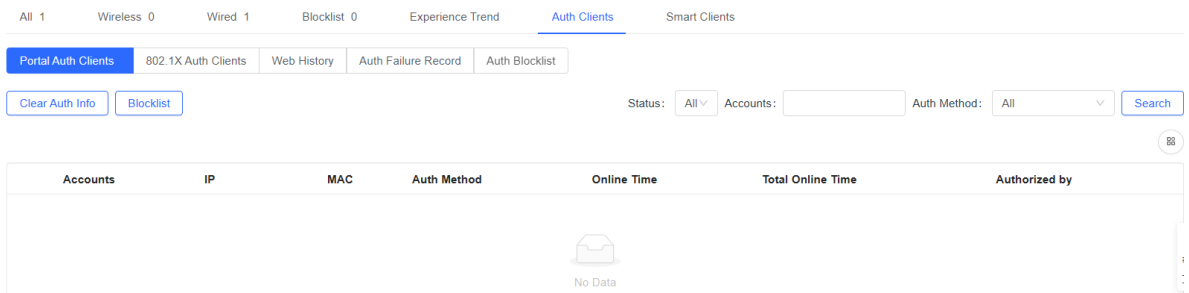
Note

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



3.25.9 Displaying Authenticated Users on Ruijie Cloud

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



3.26 Configuring 802.1X Authentication

3.26.1 Overview

IEEE 802.1X is a port-based network access control standard that provides secure access services for LANs.

On an IEEE 802 LAN, a user can directly access network resources without authentication and authorization as long as it can connect to a network device. This uncontrolled behavior can bring security risks to the network. The IEEE 802.1X protocol was proposed to address the security issues on an IEEE 802 LAN.

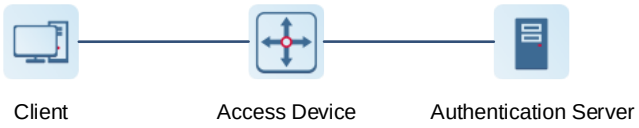
The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

- Authentication: Determines whether a user can obtain access, and restricts unauthorized users.
- Authorization: Authorizes services available for authorized users, and controls the permissions of unauthorized users.
- Accounting: Records the usage of network resources by users, and provides a basis for traffic billing.

The 802.1X feature can be deployed on networks to control user authentication, authorization, and more.

An 802.1X network uses a typical client/server architecture, consisting of three entities: client, access device, and authentication server. A typical architecture is shown here.

Figure 3-1 Typical Architecture of 802.1X Network



- The client is usually an endpoint device which can initiate 802.1X authentication through the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL) on the local area network.
- The access device is usually a network device (AP or switching device) that supports the IEEE 802.1X protocol. It provides an interface for clients to access the local area network, which can be a physical or a logical interface.
- The authentication server can realize user authentication, authorization, and accounting. Usually a RADIUS server is used as the authentication server.

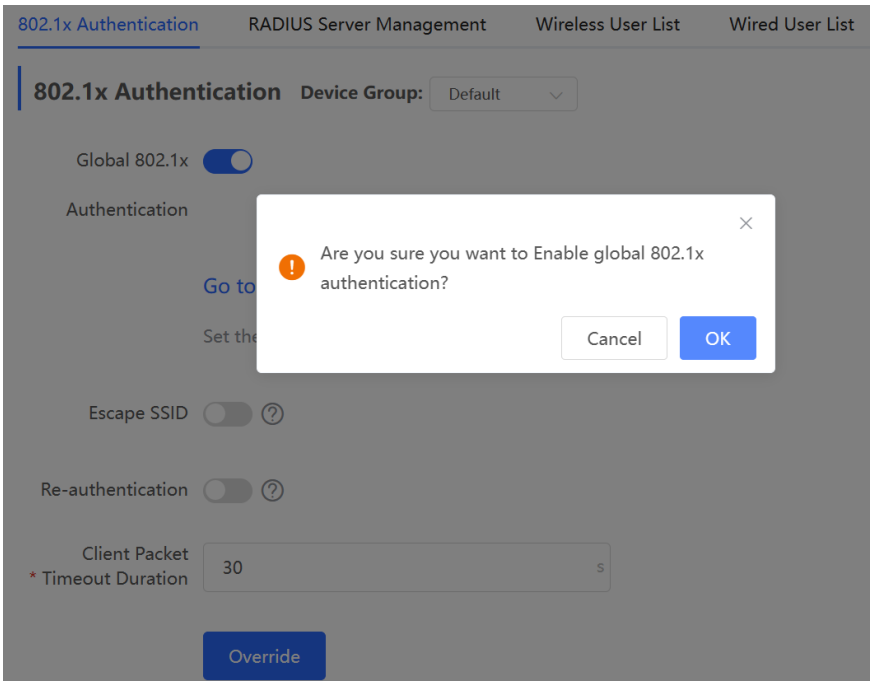
Note

The RG-RAP APs only support the authentication.

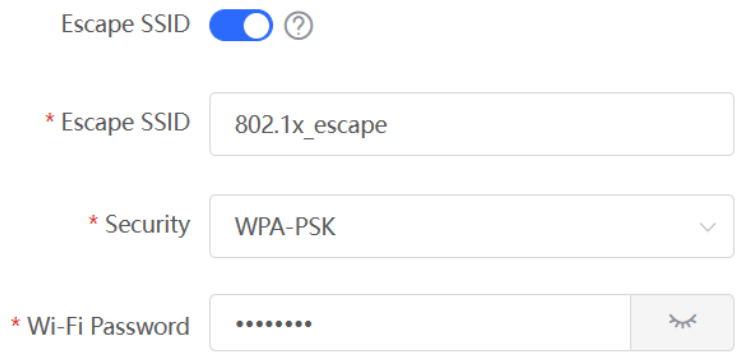
3.26.2 Configuring 802.1X Authentication

(1) Choose **Network-Wide** > **Workspace** > **Wireless** > **802.1x Authentication**.

(2) Click **Global 802.1x.** A pop-up window is displayed. Click **OK**.



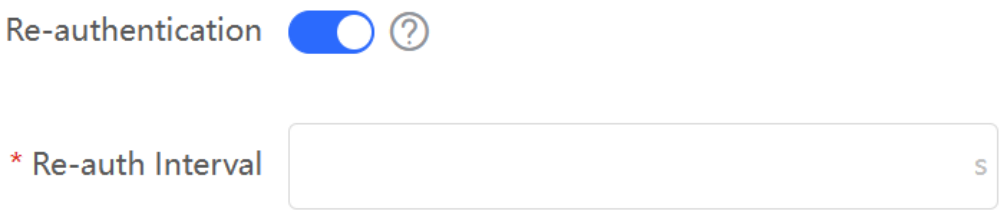
Enable the **Escape SSID** and configure parameters such as Escape SSID. Users can temporarily connect to the Escape SSID without a password when the authentication server is unavailable.



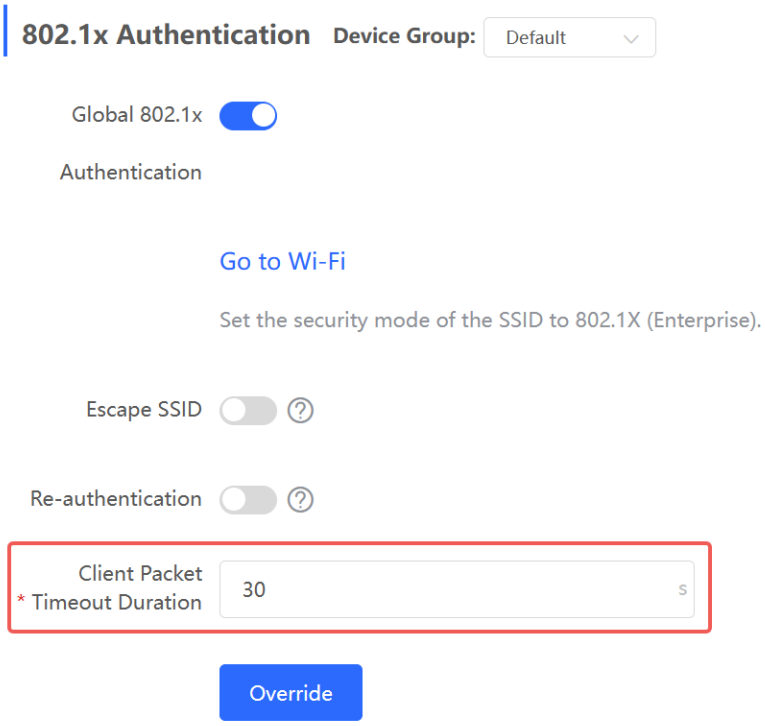
Toggle on **Re-authentication** and set the re-authentication interval. The re-authentication function performs periodic user authentication, and users who do not pass the periodic authentication will be disconnected.

Caution

The re-authentication interval must be set to 10800 seconds or above.



Client Packet Timeout Duration: The time limit for a client to wait for a response from the server. An authentication failure occurs after this time limit expires. The value range is 1 to 65535 seconds.



(3) Add a server.

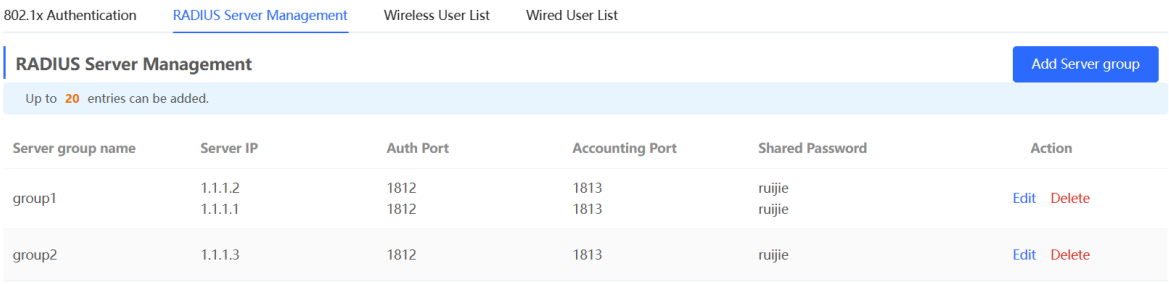
Before proceeding, make sure that the following conditions are met:

- The RADIUS server is ready and the following configurations have been completed.
  - A username and a password have been added for client login.
  - The firewall has been disabled. Otherwise, authentication messages may be blocked, leading to authentication failure.
  - The IP address of the device to be authenticated has been added as a trusted IP address on the RADIUS server.
- The network between the device and the RADIUS server is reachable.
- The IP addresses of the RADIUS server and the device to be authenticated have been obtained.

Click **Add Server group** to configure server group parameters. You can click **Edit** to edit the server group, and click **Delete** to delete the server group.

Note

- You need to add at least one server for each server group, and a maximum of five servers can be added.
- Up to 20 server groups can be added under **RADIUS Server Management**.



You can click ⊕ Add Server to add multiple servers to a server group, and click 🗑 Server to delete a selected server.

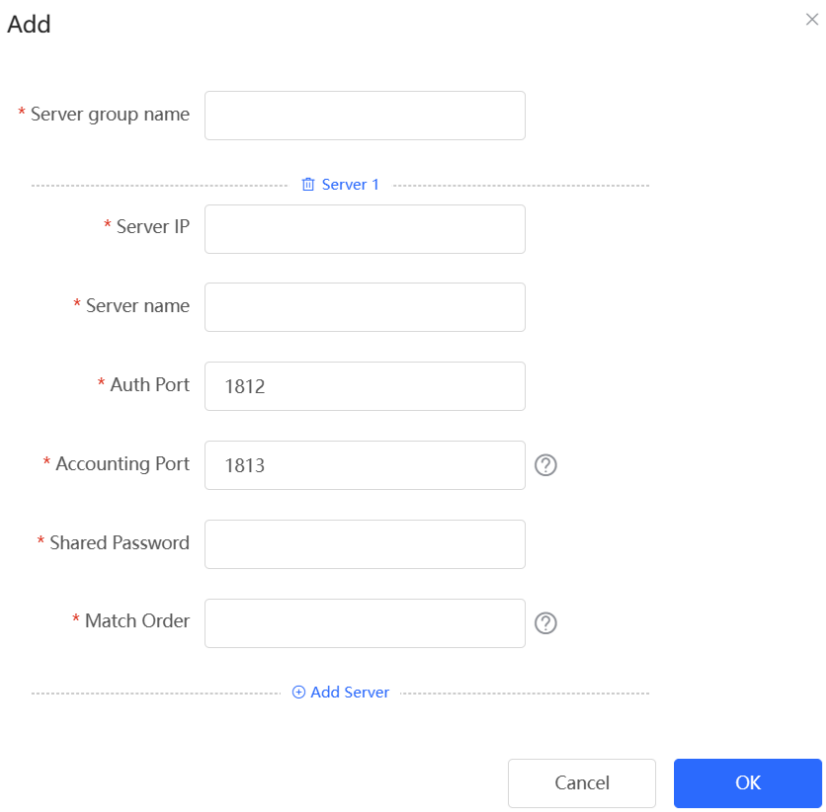


Table 3-21 Server Group Configuration Parameters

Parameter	Description
Server group name	Name of RADIUS server group
Server IP	IP address of the RADIUS server.
Server name	Name of RADIUS server
Auth Port	The port number for the RADIUS server to perform user authentication.
Accounting Port	The port number for the RADIUS server to perform user accounting.

Parameter	Description
Shared Password	Shared key of the RADIUS server.
Match Order	The system supports up to five RADIUS servers. A larger value indicates a higher priority.

(4) Configure the server and click **Save**.

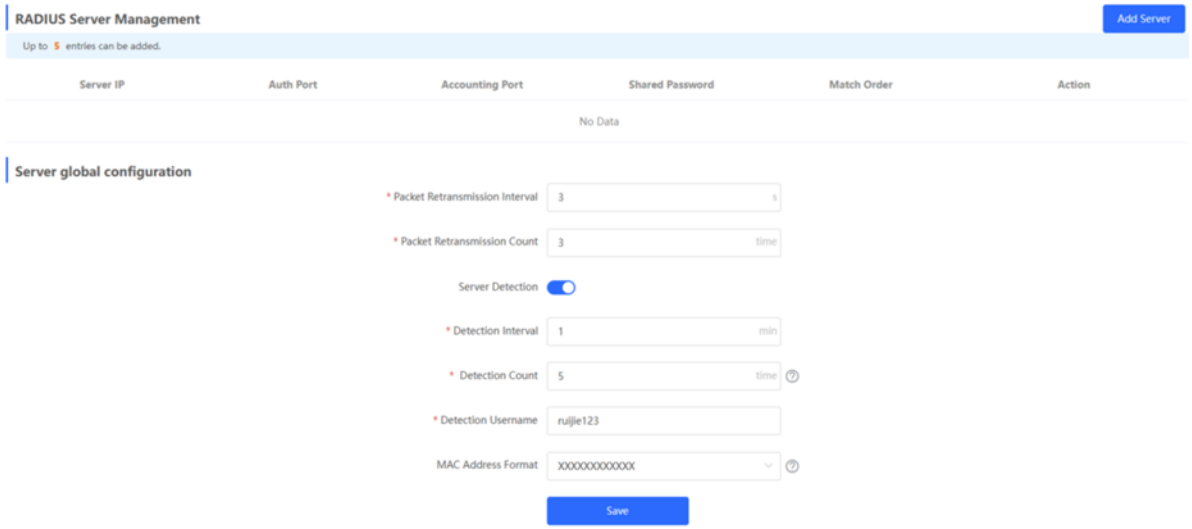


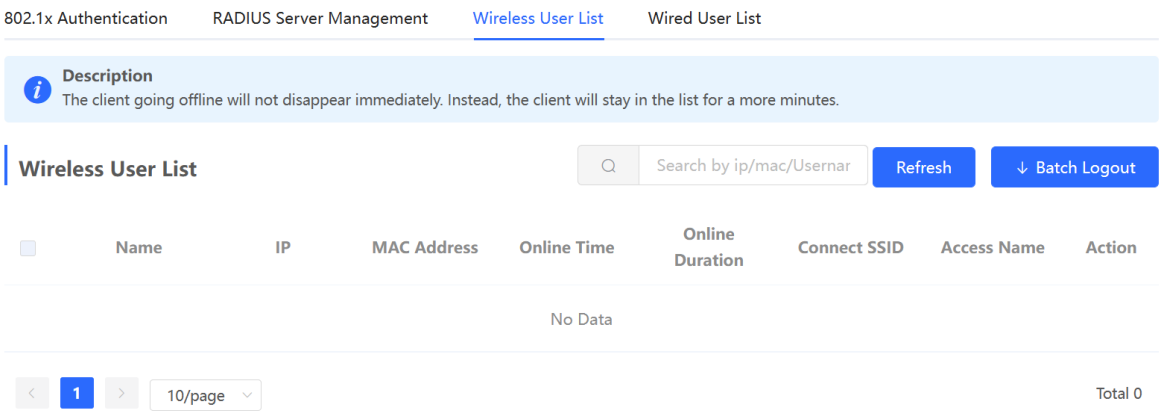
Table 3-22 Server Global Configuration Parameters

Parameter	Description
Packet Retransmission Interval	Configure the interval during which the device sends a request to a RADIUS server before confirming that the RADIUS server is unreachable.
Packet Retransmission Count	Configure the number of times that the device sends requests to a RADIUS server before confirming that the RADIUS server is unreachable.
Server Detection	If this function is enabled, it is necessary to set the server detection cycle, server detection times, and server detection username. Determines the server status and whether to enable functions such as the escape function.
MAC Address Format	Configure the format of the MAC address used in attribute 31 (**Calling-Station-ID**) of a RADIUS message. The following formats are supported: ● Dotted hexadecimal format. For example, 00d0.f8aa.bbcc. ● IETF format. For example: 00-D0-F8-AA-BB-CC. ● Unformatted (default). For example: 00d0f8aabbcc

3.26.3 Viewing Wireless User List

When the 802.1X feature is configured globally, and a client is authenticated and connected to the network in a wireless manner, you can view the client in the **Wireless User List**.

Choose **Network-Wide** > **Workspace** > **Wireless** > **802.1x Authentication** > **Wireless User List**.



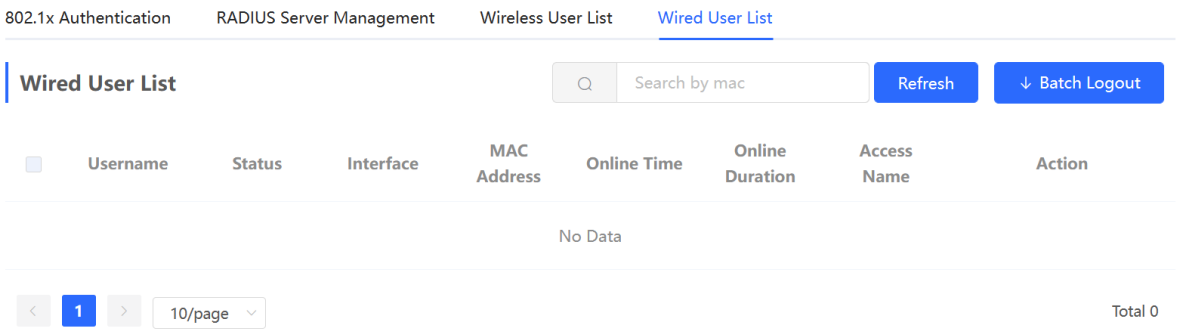
Click **Refresh** to view the latest user list.

If you want to disconnect a user from the network, select the user and click **Logout** under the **Action** column. You can also select multiple users and click **Batch Logout** to disconnect selected users.

3.26.4 Viewing Wired User List

When the 802.1X feature is configured globally, and a client is authenticated and connected to the network in a wired manner, you can view the client in the **Wired User List**.

Choose **Network-Wide** > **Workspace** > **Wireless** > **802.1x Authentication** > **Wired User List.**



Click **Refresh** to view the latest user list.

If you want to disconnect a user from the network, select the user and click **Logout** under the **Action** column. You can also select multiple users and click **Batch Logout** to disconnect selected users.

4 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: For RG-RAP72-Wall, Click 2.3 Managing Network Devices.

4.1 Switching Work Mode

4.1.1 Work Mode

See 1.4 Work Mode for details.

4.1.2 Self-Organizing Network Discovery

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

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

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

4.1.3 Configuration Steps

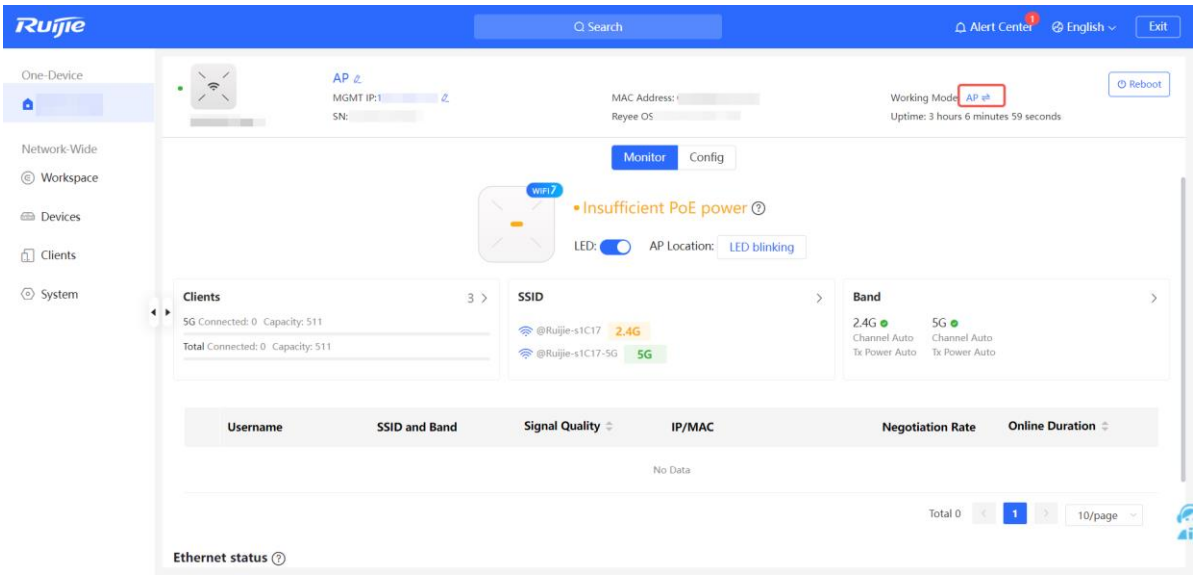
Note

If you need to switch the work mode to wireless bridging mode, please see 4.5.2 Wireless Repeater for details.

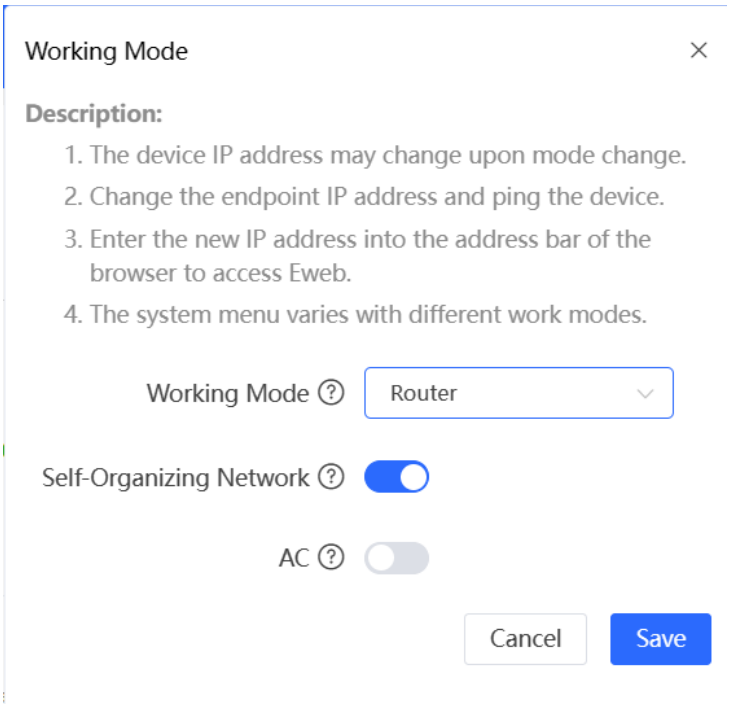
Go to the configuration page:

- Method 1: Choose **One-Device**. Click the device model.
- Method 2: Choose **Network-Wide** > **Devices** > **AP**. Select the target device in the list and click **Manage**.

Click the current work mode to change the work mode.



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



Caution

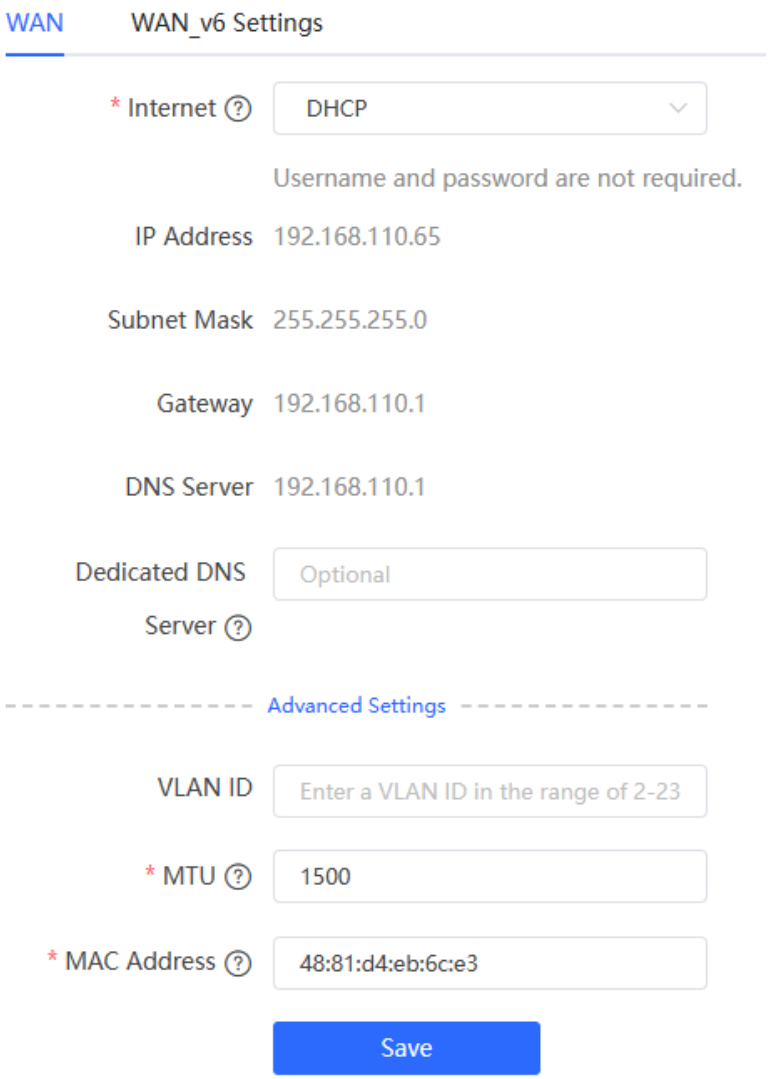
After the self-organizing network discovery is enabled, you can check the role of the device in self-organizing network mode.

4.2 Configuring Internet Connection Type (IPv4)

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network** > **WLAN** > **WAN.**
- Method 2: Choose **Network-Wide** > **Workspace** > **Wired** > **WAN** > **WAN**.

Select the Internet connection type after confirming with the ISP. For detailed configuration, see 1.5 Configuration Wizard (Router Mode). After completing the configuration, click **Save**.



The device supports the following Internet connection types:

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

4.3 Configuring Internet Connection Type (IPv6)

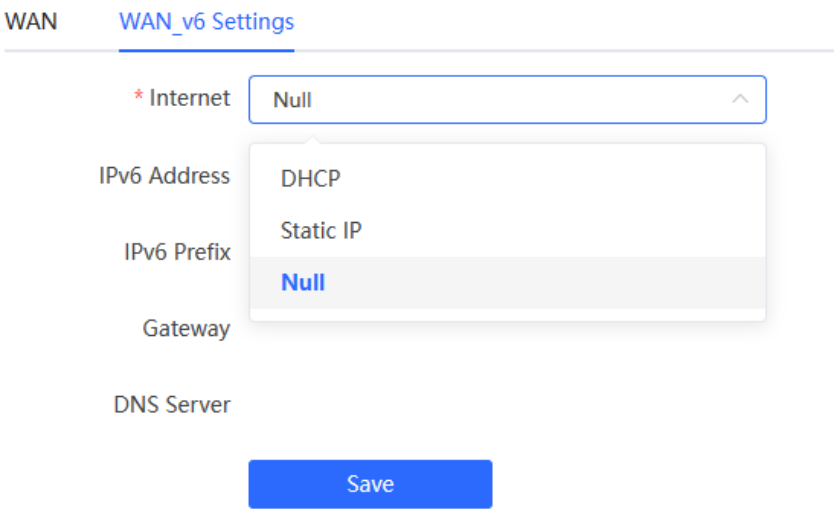
Caution

This function is supported when the device works in AP mode.

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network** > **WLAN** > **WAN_V6 Settings.**
- Method 2: Choose **Network-Wide** > **Workspace** > **Wired** > **WAN** > **WAN_V6 Settings**.

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

4.4 Configuring LAN Port

Caution

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

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network** > **LAN** > **LAN Settings.**
- Method 2: Choose **Network-Wide** > **Workspace** > **Wired** > **LAN** > **LAN Settings**.

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

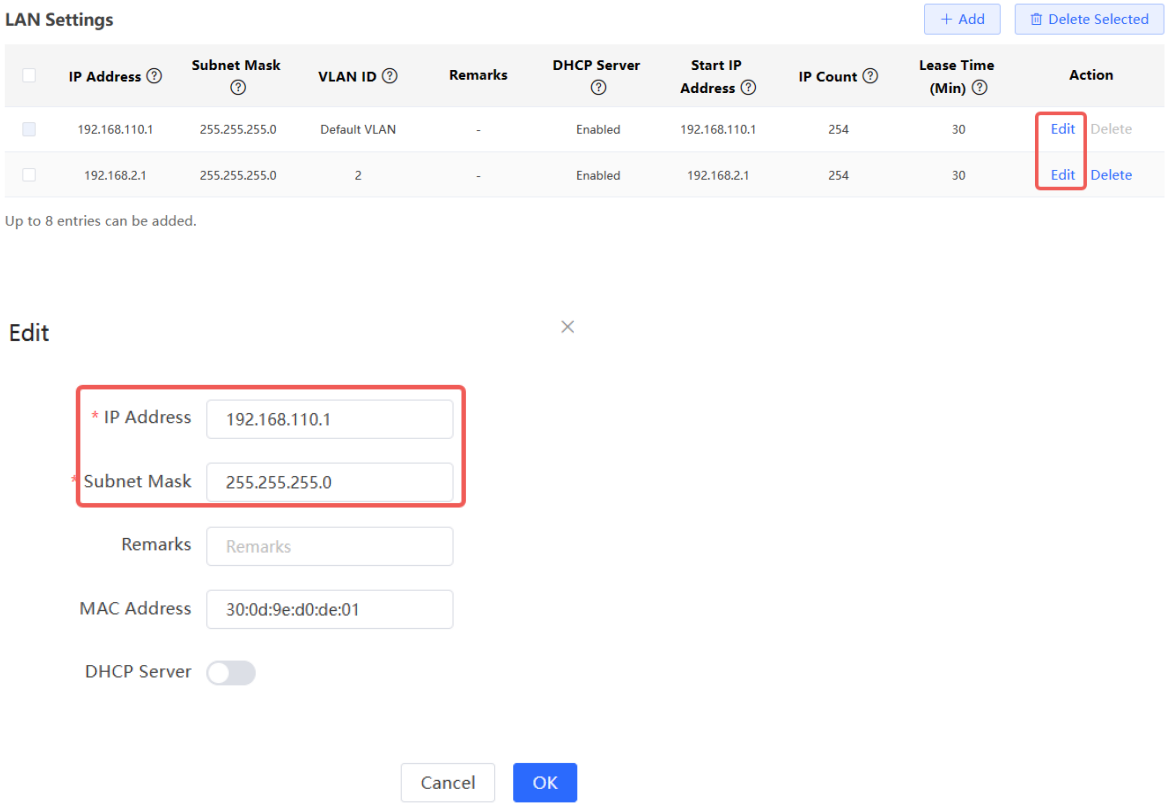


Table 4-1 LAN Settings

Parameter	Description
IP Address	Default gateway for devices connected to the Internet through this LAN.
Subnet Mask	Subnet mask of devices on the LAN.
VLAN ID	VLAN ID.
Remarks	VLAN description.
DHCP Server	After this function is enabled, devices on the LAN can automatically obtain the IP address. You need to configure the start IP address, IP count and lease time, as well as DHCP server options. For details, see4.10 Configuring DHCP Server
Start IP Address	Start IP address that a DHCP server automatically assigns to clients. The start IP address must be within the network segment calculated based on the IP address and subnet mask.
IP Count	The number of assignable IP addresses depends on the LAN segment and the start IP address.

Parameter	Description
Lease Time (Min)	Lease time of the automatically assigned IP addresses. When the lease time expires, devices on the LAN will obtain IP addresses again.

4.5 Configuring Repeater Mode

4.5.1 Wired Repeater

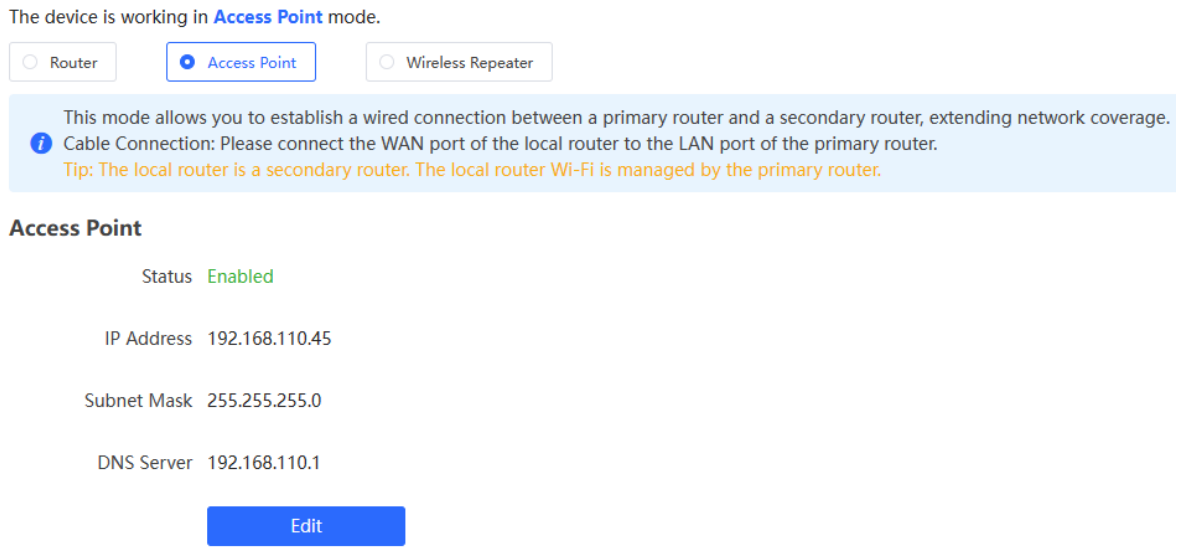
Choose **One-Device**. Click the device mode, and then choose **Config** > **Network** > **Work Mode**.

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

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

Caution

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



4.5.2 Wireless Repeater

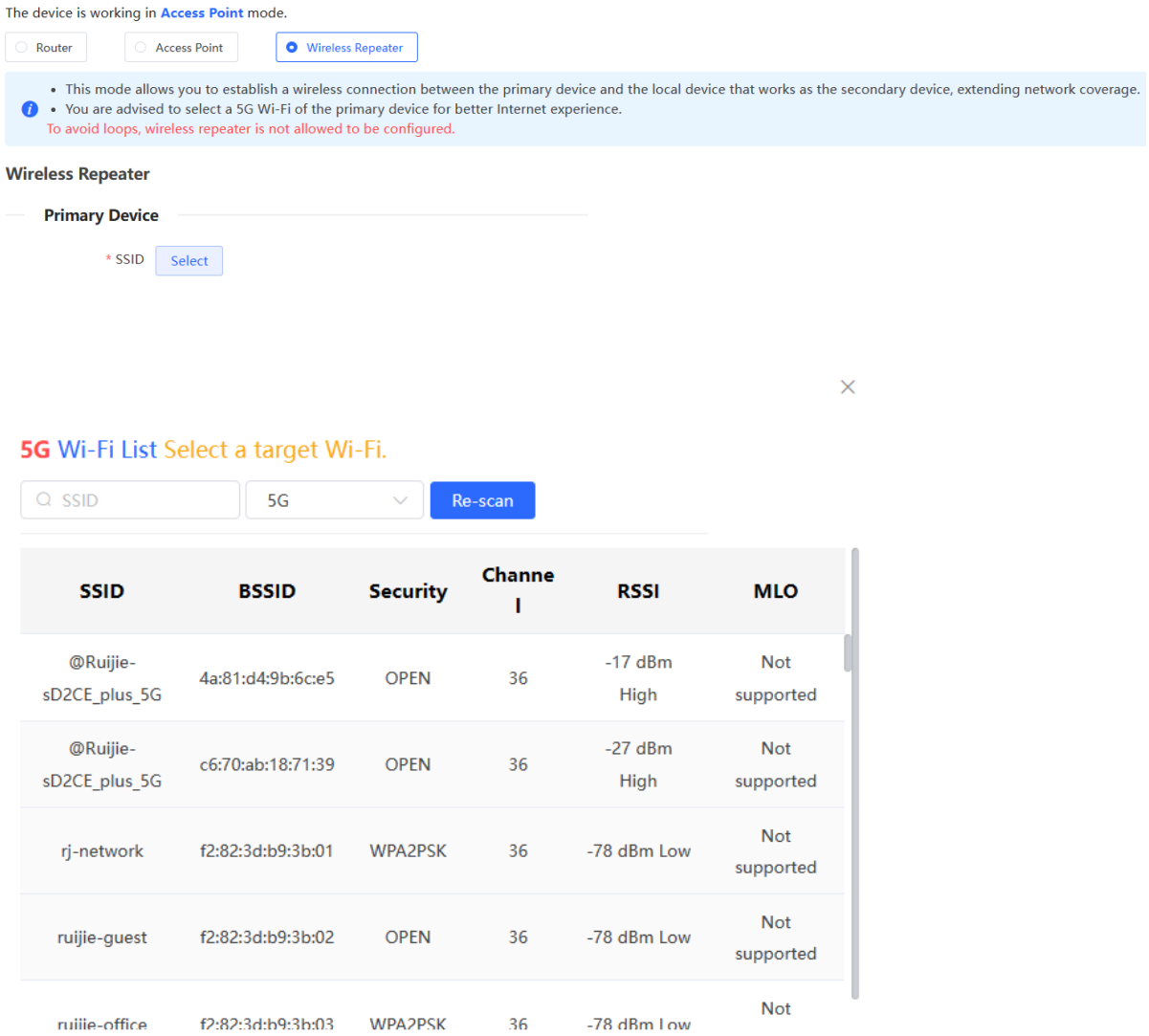
The wireless repeater mode extends the Wi-Fi coverage range of the primary device. The device supports the dual-link wireless repeater mode and can extend both 2.4 GHz and 5 GHz signals of the primary device.

Note

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

Choose One-Device. Click the device mode, and then choose **Config** > **Network** > **Work Mode**.

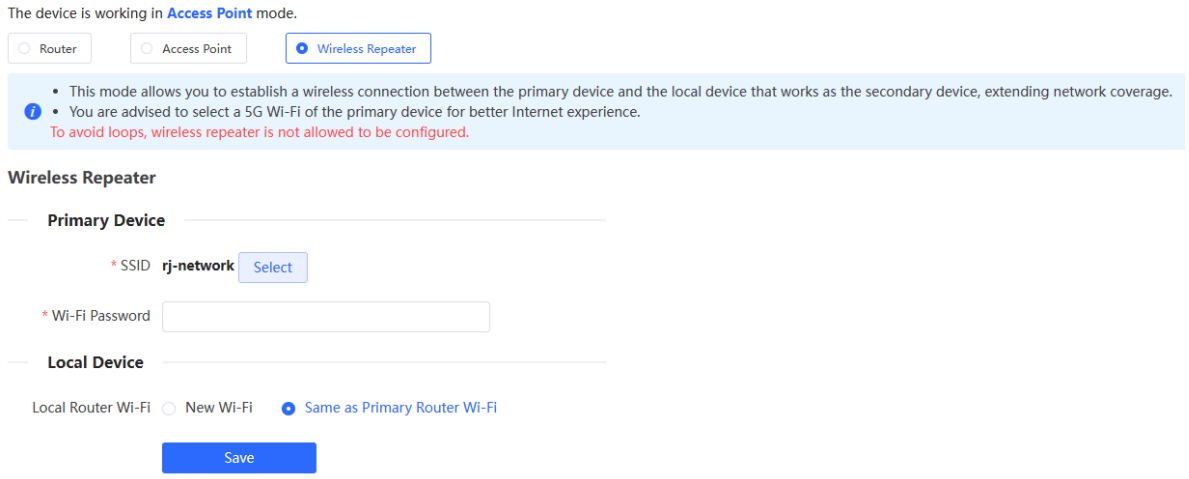
Click **Wireless Repeater** and then click **Select**. A list of surrounding Wi-Fi signals pops up. A list of nearby 5 GHz Wi-Fi networks is displayed by default. You can switch from 5 GHz to 2.4 GHz band by selecting **2.4G** from the drop-down list box. You are advised to select a strong 5 GHz Wi-Fi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



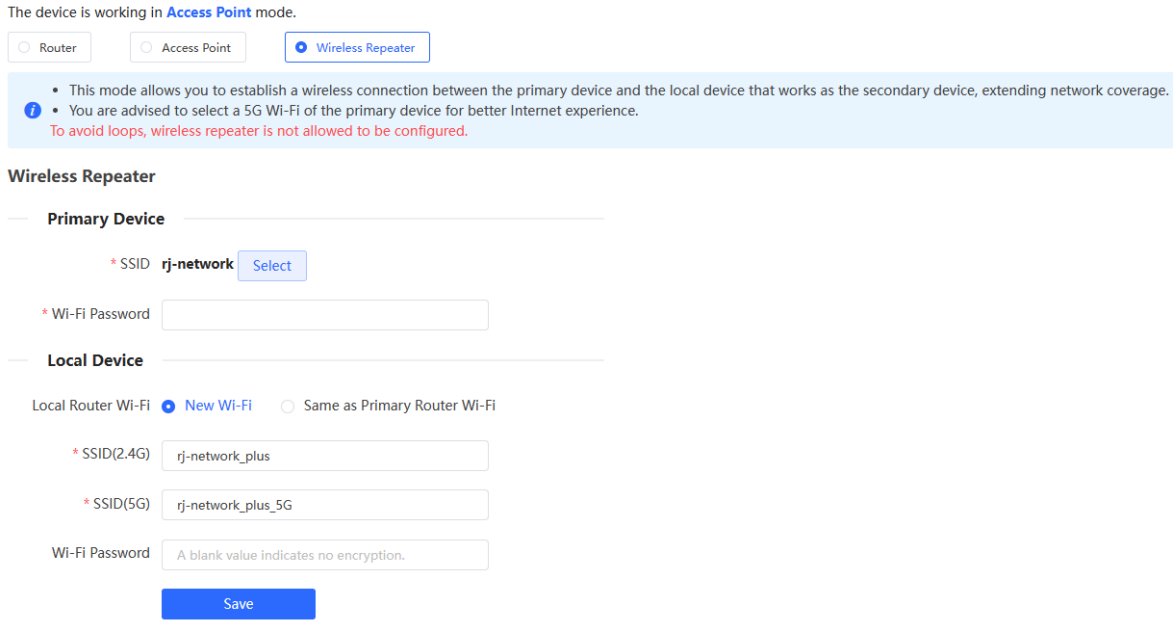
(1) Select the Wi-Fi signal of the upper-layer device that you want to extend. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.

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

- If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the router are automatically synchronized with those on the primary router. Generally, clients merge Wi-Fi signals with the same name into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.



- If **New Wi-Fi** is selected, you can set a local Wi-Fi name and password. Clients will search out different Wi-Fi signals.



Caution

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

4.6 Creating a VLAN

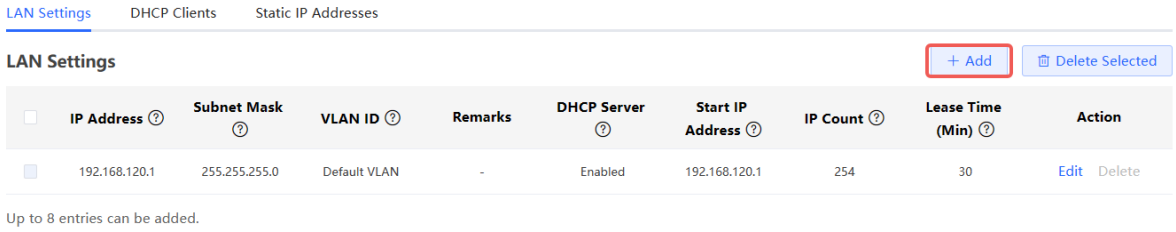
Caution

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

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network > LAN > LAN Settings**.
- Method 2: Choose **Network-Wide > Workspace > Wired > LAN > LAN Settings**.

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



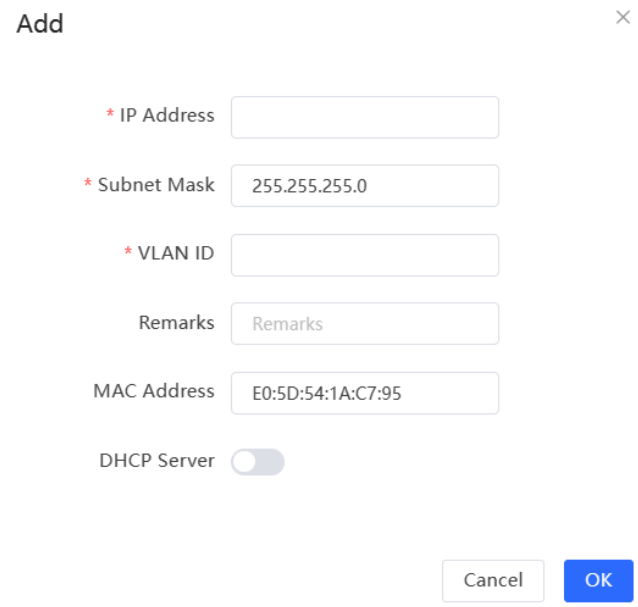


Table 4-2 VLAN Configuration Parameters

Parameter	Description
IP Address	IP address of the VLAN interface. The default gateway of devices that access the Internet through the current LAN should be set to this IP address.
Subnet Mask	Subnet mask of the IP address of the VLAN interface.
VLAN ID	VLAN ID.
Remark	VLAN description.
MAC	MAC address of the VLAN interface.

Parameter	Description
DHCP Server	Enable the DHCP server function. After it is enabled, devices on the LAN can automatically obtain IP addresses. After the DHCP service is enabled, you need to configure the start IP address to be assigned, number of IP addresses to be assigned, and address lease term for the DHCP server, and other DHCP server options. For details, see 4.10 Configuring DHCP Server.

Caution

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

4.7 Configuring Port VLAN

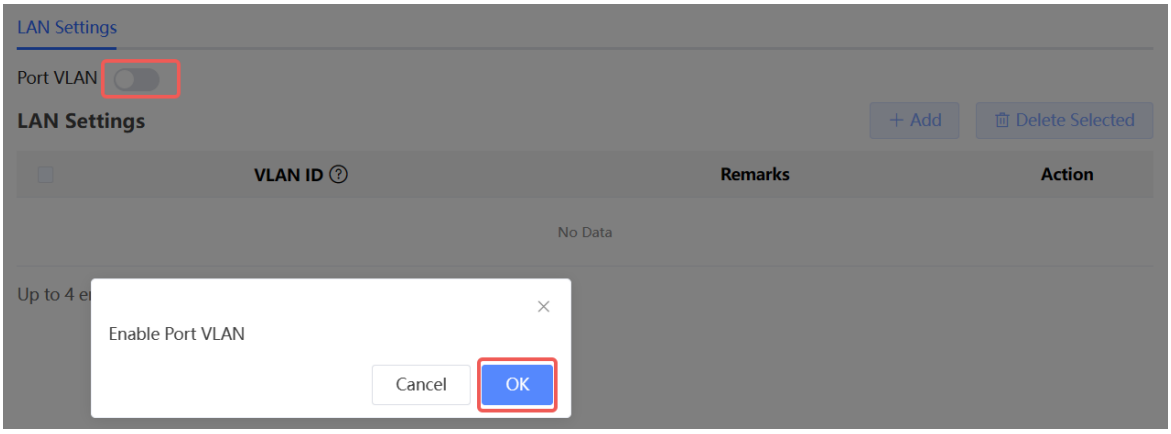
Caution

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

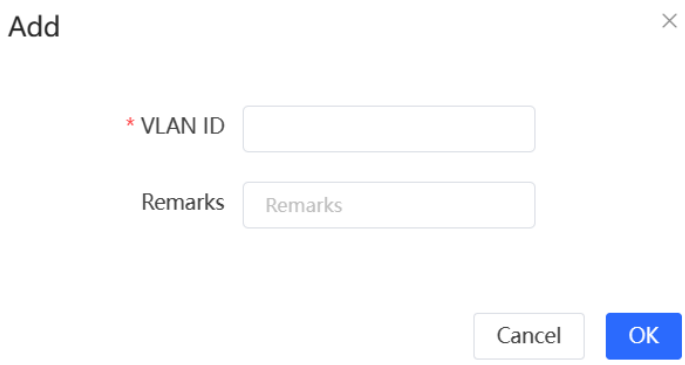
Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network > LAN > LAN Settings**.
- Method 2: Choose **Network-Wide > Workspace > Wired > LAN > LAN Settings**.

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

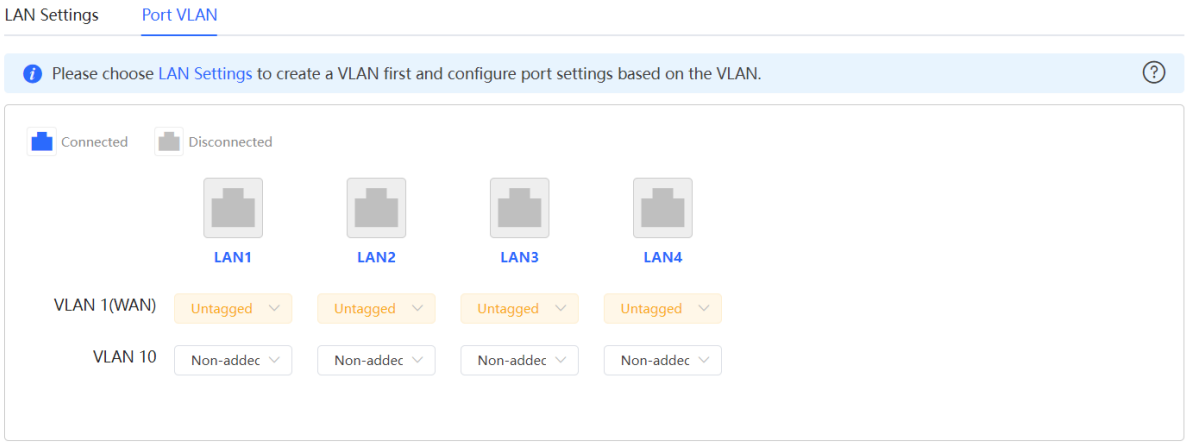


(2) Click **Add**. Enter the VLAN ID and description, and click **OK** to create a VLAN. The added VLAN is used to set the VLAN, to which a port belongs.



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

- **Untagged**: 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.
- **Tagged**: 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.
- **Non-added**: Configure the port not to allow packets from this VLAN to pass through. For example, if VLAN 10 and VLAN 20 are not added to port 2, port 2 will neither receive nor send packets from or to VLAN 10 and VLAN 20.



4.8 Changing MAC Address

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network > WAN > WAN**.
- Method 2: Choose **Network-Wide > Workspace > Wired > WAN > WAN**.

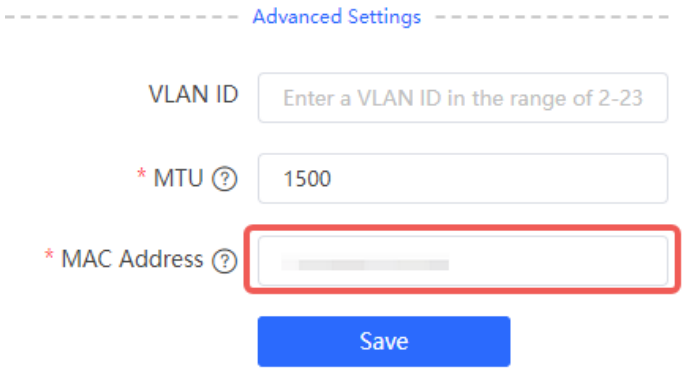
ISPs may restrict the access of devices with unknown MAC addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port.

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.

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

Caution

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

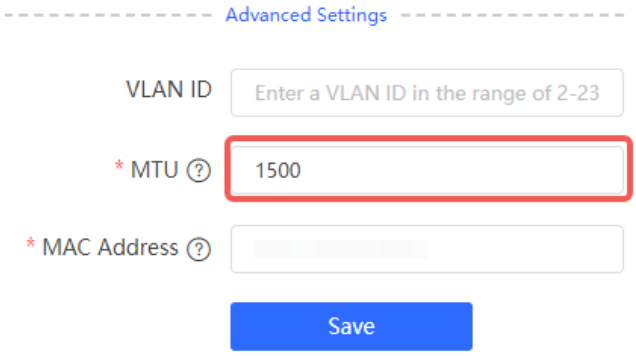


4.9 Changing MTU

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network > WAN > WAN**.
- Method 2: Choose **Network-Wide > Workspace > Wired > 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.



4.10 Configuring DHCP Server

Caution

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

4.10.1 DHCP Server

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

4.10.2 Configuring the DHCP Server Function

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network > LAN > LAN Settings**.
- Method 2: Choose **Network-Wide > Workspace > Wired > LAN > LAN Settings**.

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

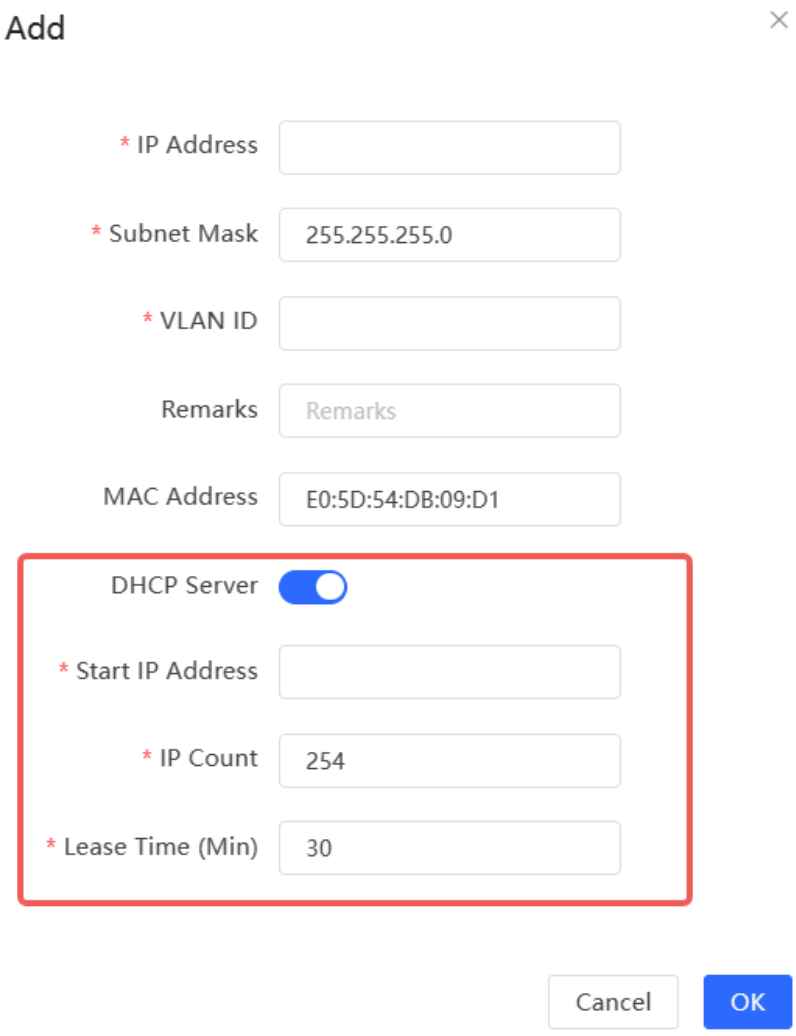
Caution

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

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

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

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

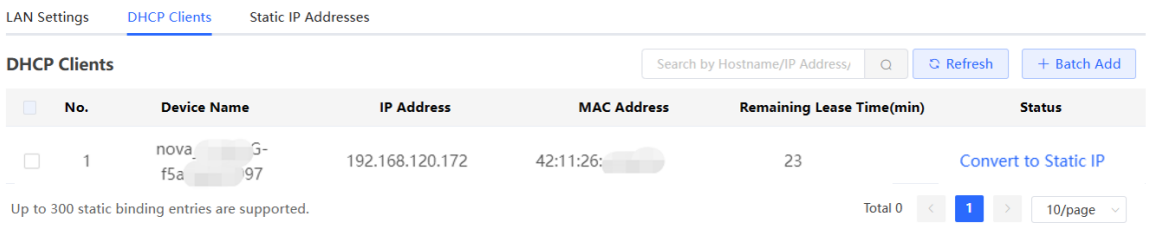


4.10.3 Displaying Online DHCP Clients

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network > LAN > DHCP Clients**.
- Method 2: Choose **Network-Wide > Workspace > Wired > LAN > DHCP Clients**.

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

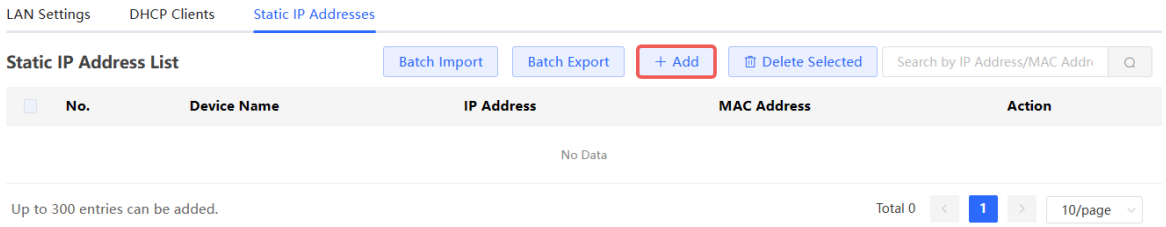


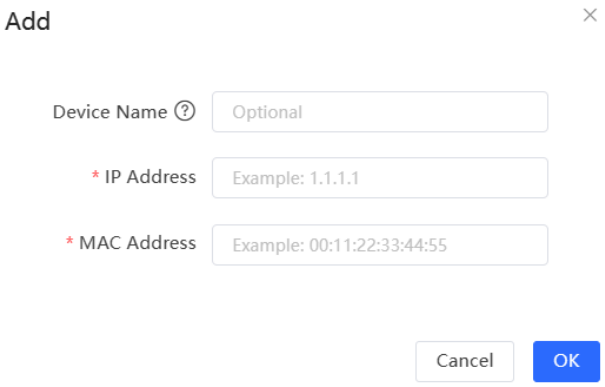
4.10.4 Displaying the DHCP Static IP Address List

Go to the configuration page:

- Method 1: Choose **One-Device** > **Config** > **Network > LAN > Static IP Addresses**.
- Method 2: Choose **Network-Wide > Workspace > Wired > LAN > Static IP Addresses**.

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

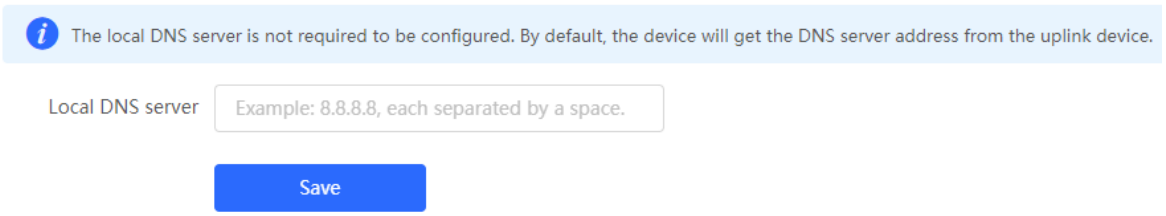




4.11 Configuring DNS

Choose **One-Device** > **Config** > **Advanced** > **Local DNS**.

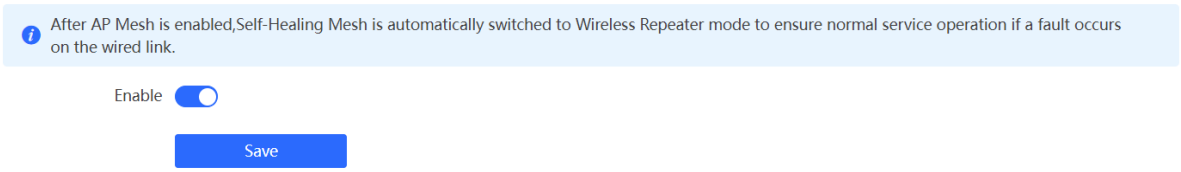
Enter the IP address of the DNS server and click **Save**. The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default. The default configuration is recommended. The available DNS service varies from region to region. You can consult the local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



4.12 Configuring Self-Healing Mesh

Choose **One-Device** > **Config** > **Advanced** > **Self-Healing Mesh**.

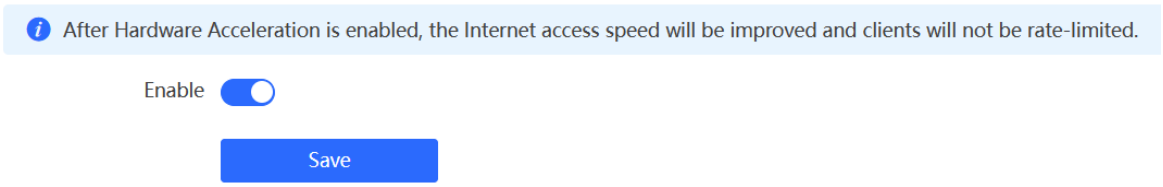
After AP Mesh is enabled, Self-Healing Mesh is automatically switched to Wireless Repeater mode to ensure normal service operation if a fault occurs on the wired link.



4.13 Hardware Acceleration

Choose **One-Device** > **Config** > **Advanced** > **Hardware Acceleration**.

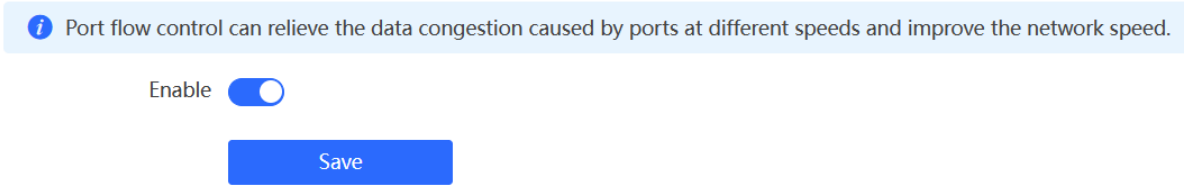
After Hardware acceleration is enabled, the Internet access speed will be improved.



4.14 Configuring Port Flow Control

Choose **One-Device** > **Config** > **Advanced** > **Port Settings**.

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



4.15 Configuring ARP Binding

Caution

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

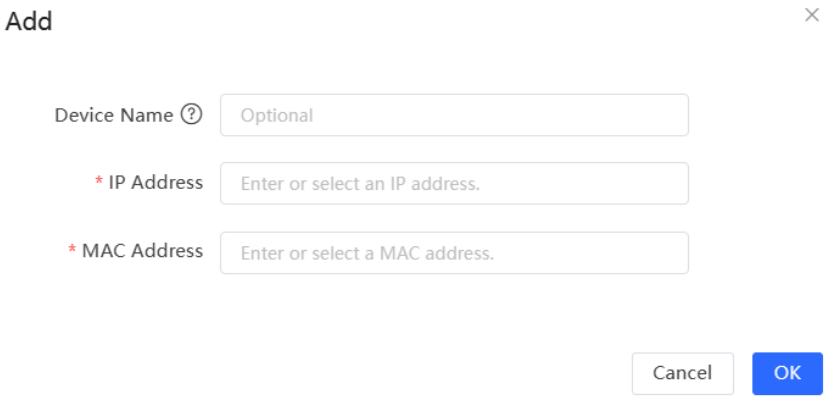
The device learns the IP and MAC addresses of network devices connected to ports of the device and generates ARP entries. You can bind ARP mappings to improve network security.

Choose **One-Device** > **Config** > **Security** > **ARP List**.

ARP mappings can be bound in two ways:

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

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



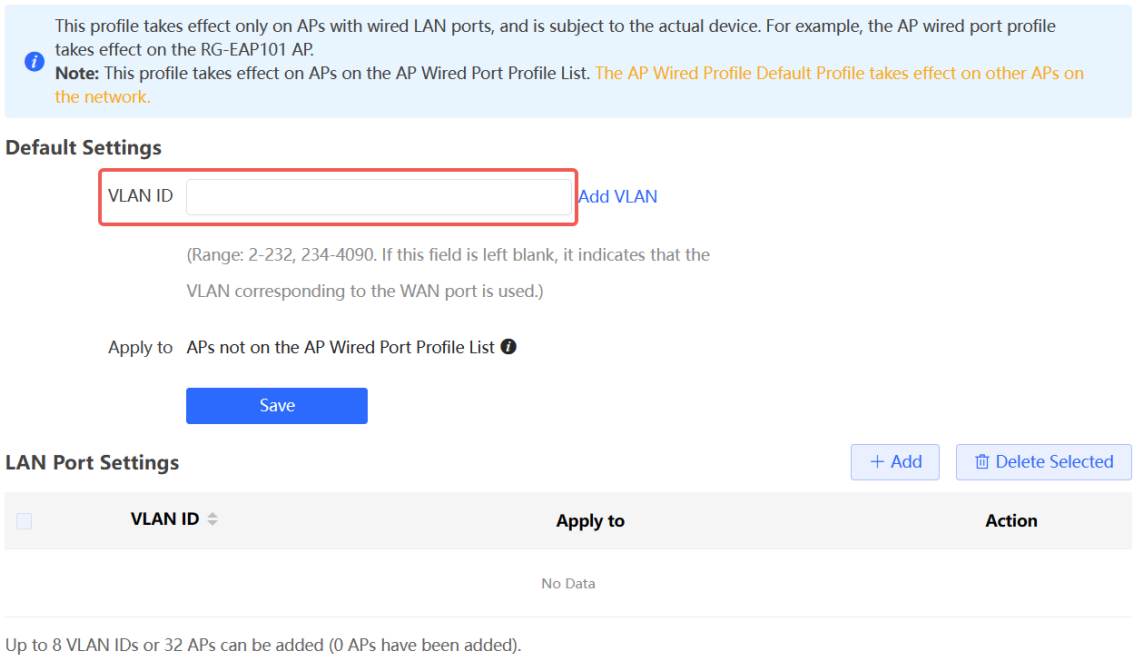
4.16 Configuring LAN Ports

Caution

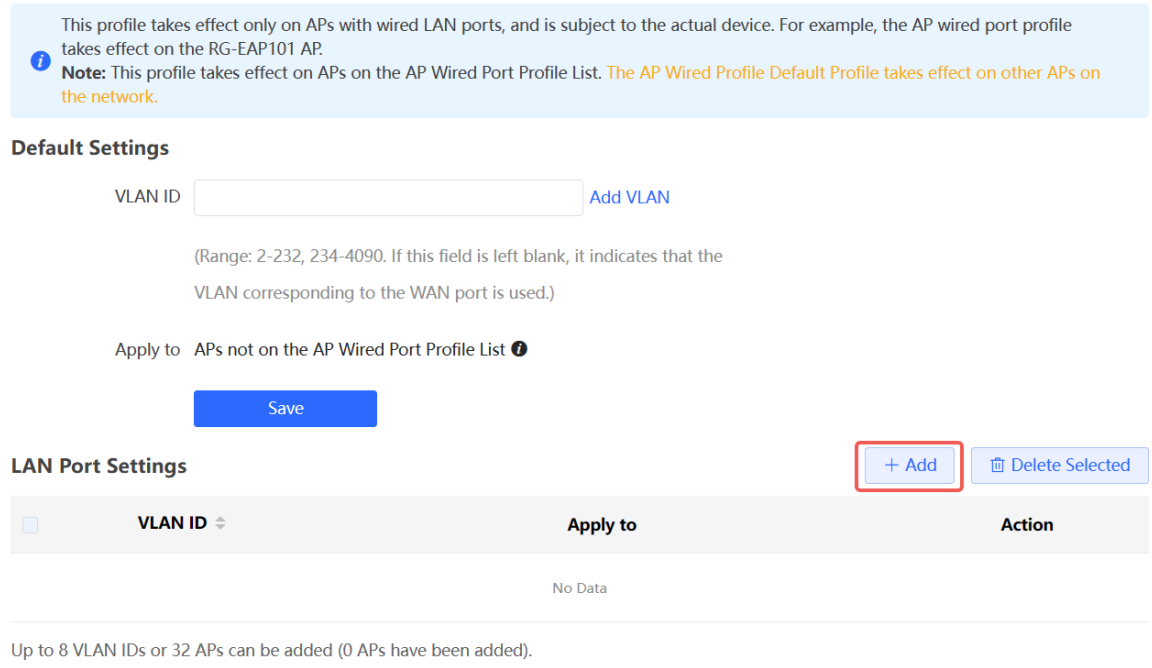
The configuration takes effect only on APs having wired LAN ports.

Choose **Network-Wide** > **Workspace** > **Wireless** > **LAN Ports**.

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



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



4.17 IPv6 Settings

Caution

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

4.17.1 Overview

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

4.17.2 IPv6 Basic

1. IPv6 Address Format

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

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

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

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

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

2. IPv6 Prefix

An IPv6 address consists of two parts:

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

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

3. Special IPv6 Address

There are also some special IPv6 addresses, for example:

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

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

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

4. N/AT66

IPv6-to-IPv6 Network Address Translation (N/AT66) is the process of converting the IPv6 address in an IPv6 packet header to another IPv6 address. N/AT66 prefix translation is an implementation of N/AT66. It replaces the IPv6 address prefix in the packet header with another IPv6 address prefix to achieve IPv6 address translation. N/AT66 can realize mutual access between an intranet and Internet.

4.17.3 IPv6 Address Assignment Methods

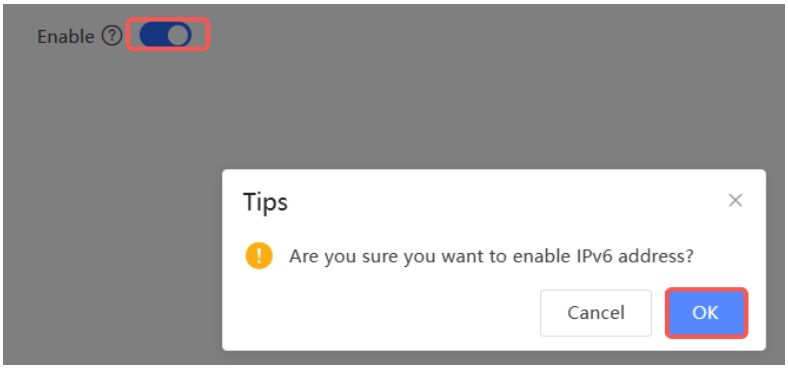
- Manual configuration: The IPv6 address/prefix and other network configuration parameters are manually configured.

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

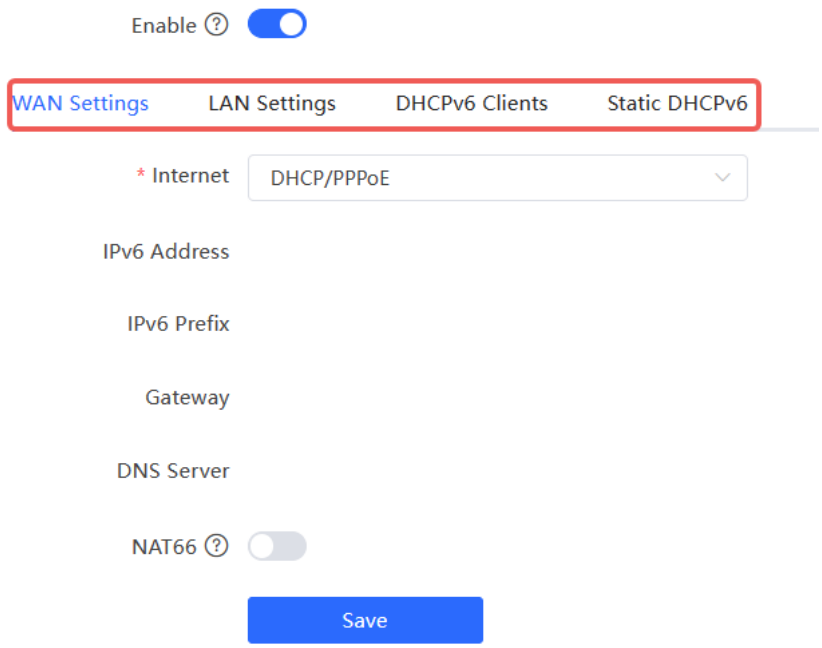
4.17.4 Enabling IPv6

Choose **One-Device** > **Config** > **Network** > **IPv6 Address**.

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



After IPv6 is enabled, you can configure the IPv6 addresses of WAN and LAN ports, view the DHCPv6 client, and configure a static DHCPv6 address for the client.



4.17.5 Configuring the IPv6 Address for the WAN Port

Choose **One-Device** > **Config** > **Network** > **IPv6 Address** > **WAN Settings**.

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

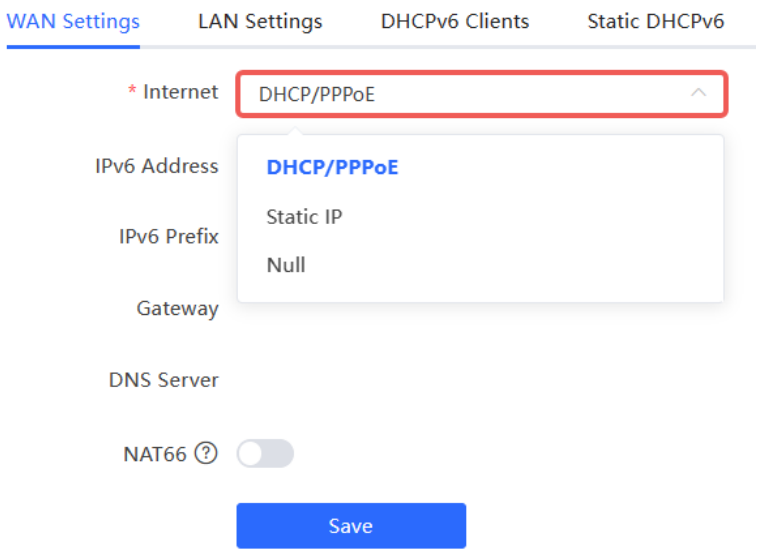


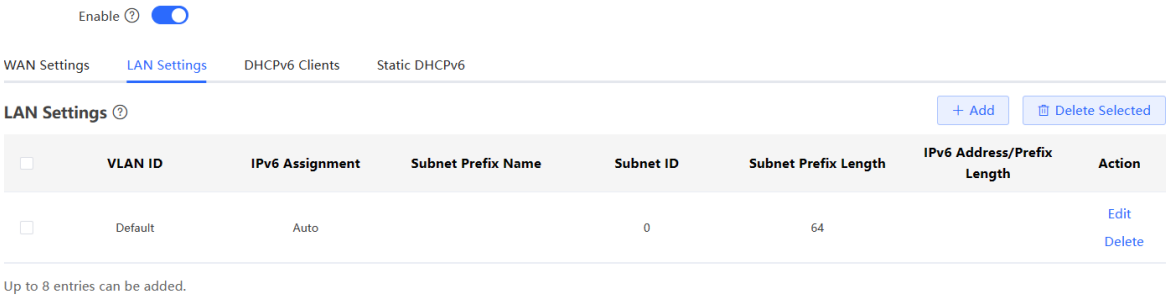
Table 4-3 WAN Port IPv6 Address Configuration Parameters

Parameter	Description
Internet	Specify the method for obtaining an IPv6 address for the WAN port. ● **DHCP/PPPoE**: The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device. ● **Static IP**: If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server. ● **Null**: The IPv6 function is disabled on the current WAN port.
IPv6 Address	If **Internet** is set to **DHCP/PPPoE**, the automatically obtained IPv6 address is displayed. If **Internet** is set to **Static IP**, you need to manually configure this parameter.
IPv6 Prefix	If **Internet** is set to **DHCP/PPPoE** and the current device obtains the IPv6 address prefix from the upstream device. The obtained IPv6 address prefix is displayed.
Gateway	If **Internet** is set to **DHCP/PPPoE**, the automatically obtained gateway address is displayed. If **Internet** is set to **Static IP**, you need to manually configure this parameter.
DNS Server	If **Internet** is set to **DHCP/PPPoE**, the automatically obtained DNS server address is displayed. If **Internet** is set to **Static IP**, you need to manually configure this parameter.
N/AT66	If the current device cannot access the Internet in DHCP mode or cannot obtain the IPv6 address prefix, you must enable N/AT66 to assign the IPv6 address to an intranet client.

4.17.6 Configuring the IPv6 Address for the LAN Port

Choose **One-Device** > **Config** > **Network** > **IPv6 Address** > **LAN Settings**.

When the device accesses the network in DHCP mode, the upstream device can assign an IPv6 address to the LAN port, and assign IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the upstream device cannot assign an IPv6 address prefix to the current device, you need to manually configure an IPv6 address prefix for the LAN port, and assign IPv6 addresses to the clients in the LAN by enabling the N/AT66 function (see 4.17.5 Configuring the IPv6 Address for the WAN Port).

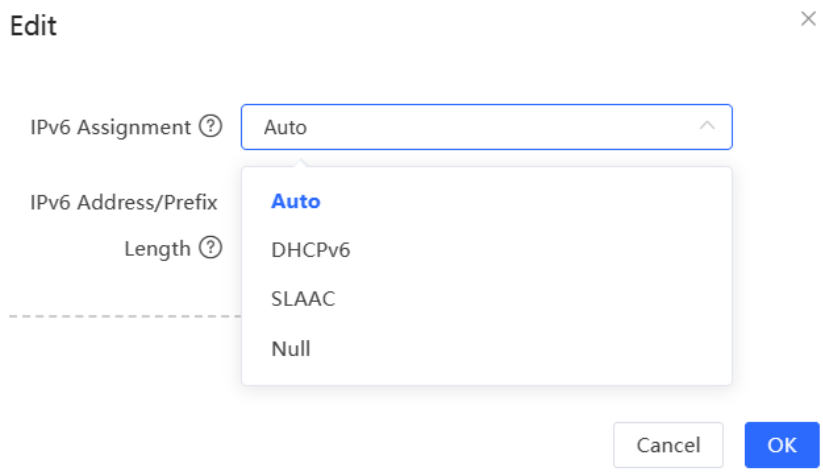


Click **Edit** corresponding to the default VLAN, and fill in a local address of no more than 64 bits in the **IPv6 Address/Prefix Length** column. This address will also be used as the IPv6 address prefix.

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

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

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



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

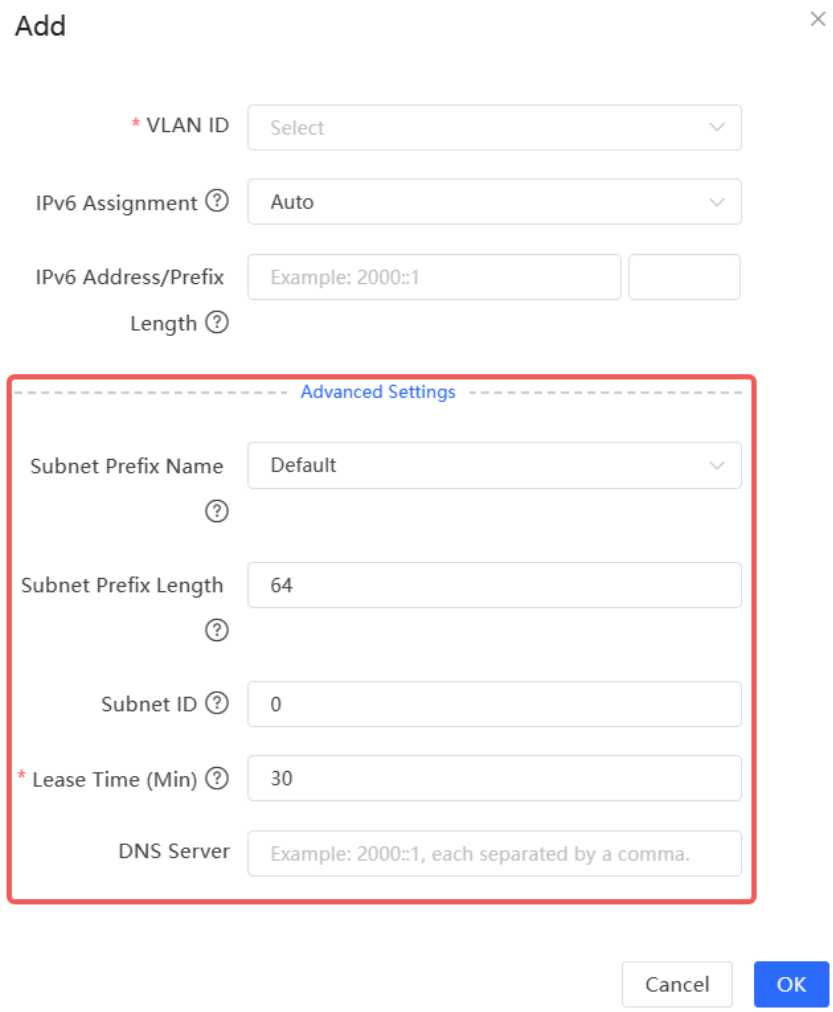


Table 4-4 LAN Port IPv6 Address Configuration Parameters

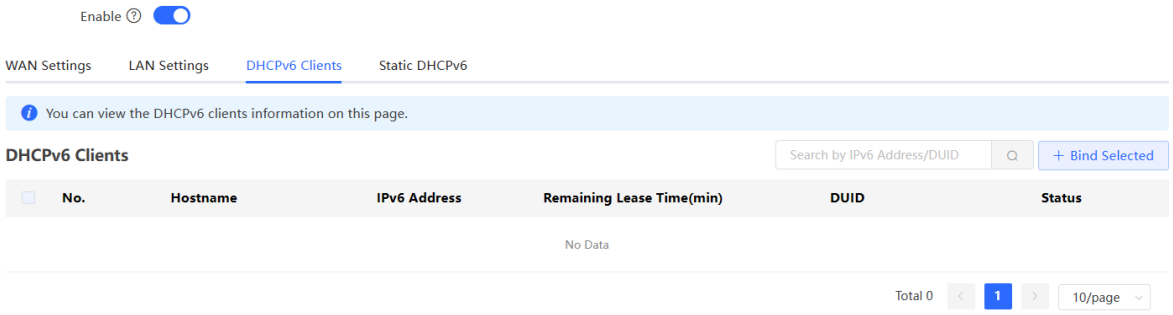
Parameter	Description
Subnet Prefix Name	Configure the interface from which the prefix is obtained, for example, **WAN_V6**. The default value is all interfaces.
Subnet Prefix Length	Configure the length of the subnet prefix. The value ranges from 48 to 64.
Subnet ID	Configure the subnet ID in hexadecimal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

4.17.7 Viewing DHCPv6 Clients

Choose **One-Device** > **Config** > **Network** > **IPv6 Address** > **DHCPv6 Clients**.

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

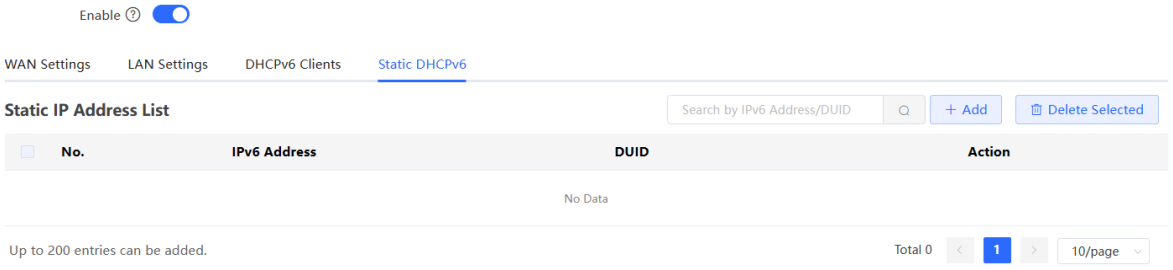
Enter an IPv6 address or DUID in the search bar, and click to quickly find the information of the specified DHCPv6 client.



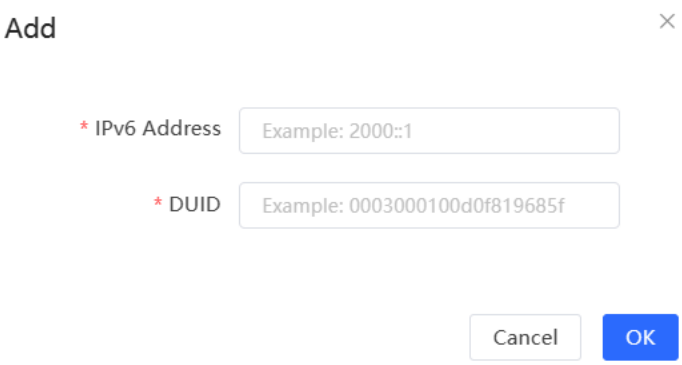
4.17.8 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client so that the client can obtain the specified address each time.

Choose **One-Device** > **Config** > **Network** > **IPv6 Address** > **Static DHCPv6**.



(1) Click **Add**.



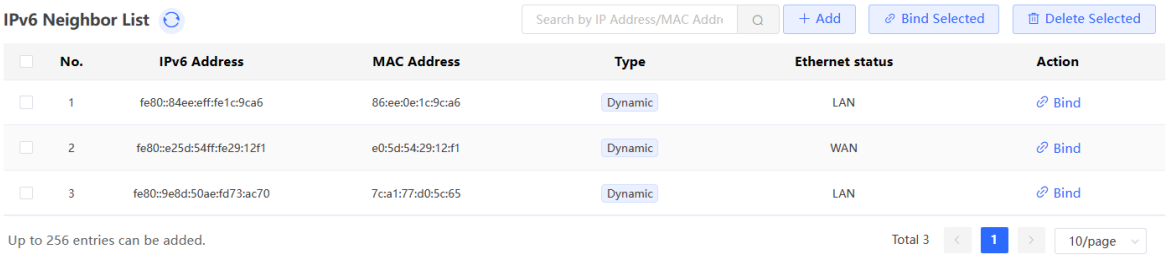
(2) Enter the IPv6 address and DUID of the client.

(3) Click **OK**.

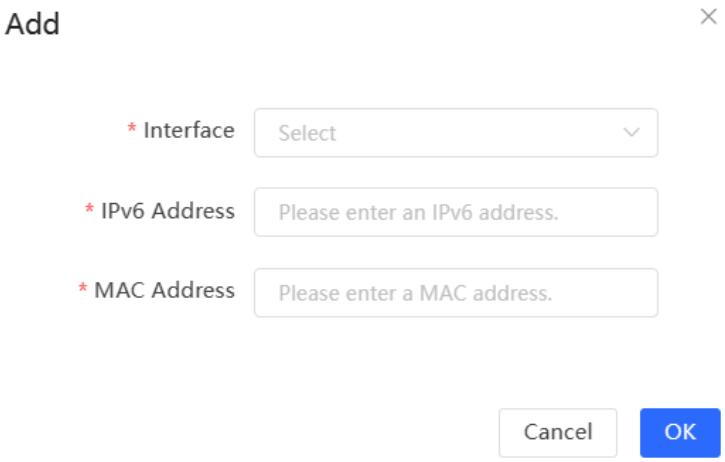
4.17.9 Configuring the IPv6 Neighbor List

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

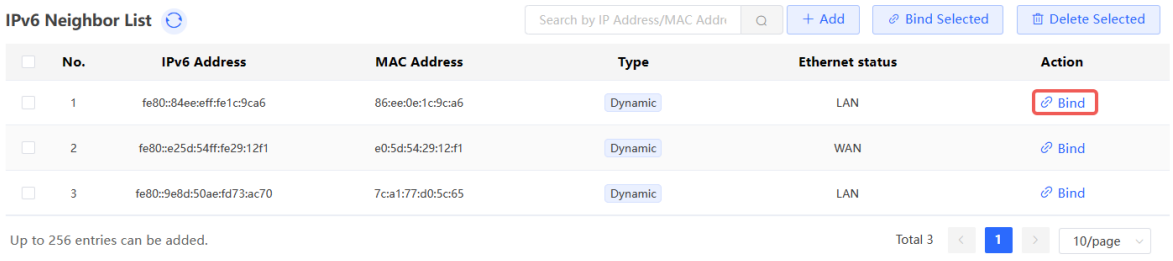
Choose **One-Device** > **Config** > **Security** > **IPv6 Neighbor List**.



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



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



5 Online Client Management

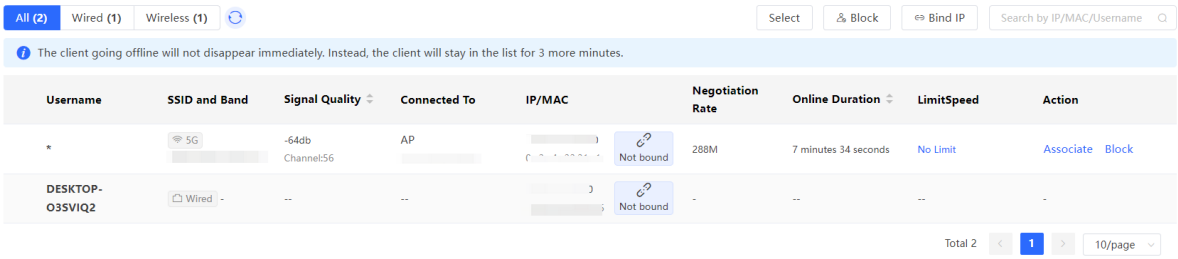
Caution

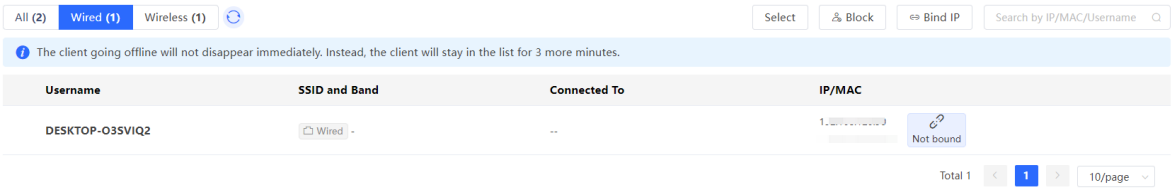
- When the AP is used as the primary device, clients on the network are only displayed when the AP works in router mode.
- When the AP is used as a secondary device, the functions presented in the web interface are based on the primary device on the network.

Go to the configuration page:

- Choose **Network-Wide** > **Clients**.
- AP as a secondary device: Choose **One-Device** > **Config** > **Clients**.

The client list displays wired and wireless on the current network, including the username, connection mode, associated device, IP/MAC address, IP address binding status, rate, and related operations.





- Click **Not Bound** in the **IP/MAC** column to bind the client to a static IP address.
- Click a button in the **Action** column to perform the corresponding operation on the online client. Wireless: Associate, and block can be configured.

Note

Client IP binding is only supported when the AP works in router mode.

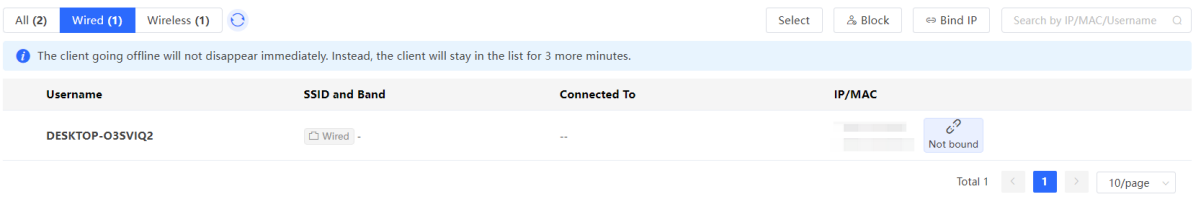
Table 5-1 Online Client Management Configuration Parameters

Parameter	Description
Username	Name of the connected client.

Parameter	Description
SSID and Band	Indicates the access mode of the client, which can be wireless or wired. The SSID and frequency band is displayed when a client is connected wirelessly.
Signal Quality	The Wi-Fi signal strength of the client and the associated channel. **Note** This information is displayed only in the wireless online client list.
Connected To	Indicates wired or wireless connection, the associated device and SN.
IP/MAC	Indicates the IP address and MAC address of the client.
Negotiated Rate	Negotiation rate between the client and the AP. **Note** This information is displayed only in the wireless online client list.
Online Duration	Client access duration. **Note** This information is displayed only in the wireless online client list.
LimitSpeed	Implement wireless speed limiting for clients to prevent certain clients from consuming large amounts of bandwidth resources. For details, see 5.4 Configuring Client Rate Limiting. **Note** This information is displayed only in the wireless online client list.
Action	You can click the corresponding button to perform association and block operations on online clients.

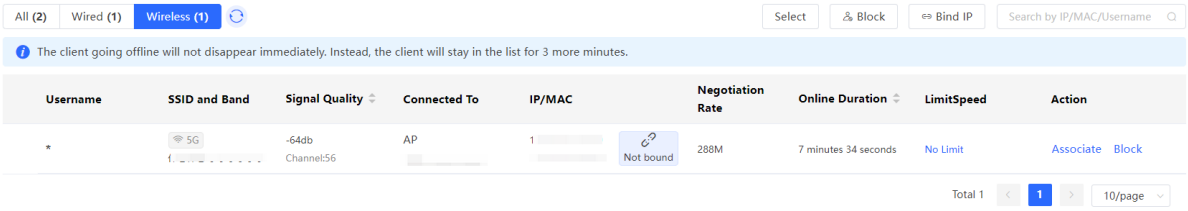
Wired Clients

Click the **Wired** tab to see details about wired clients.



Wireless Clients

Click the **Wireless** tab to see details about wireless clients.



5.1 Configuring Client IP Binding

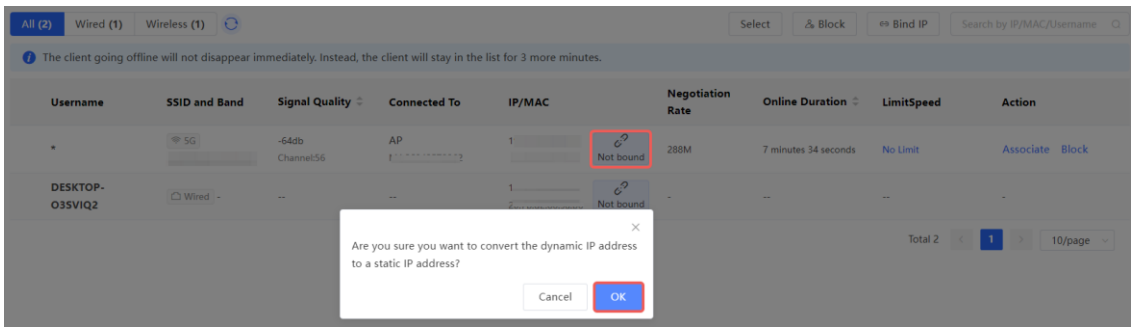
Caution

This function is supported only in router mode.

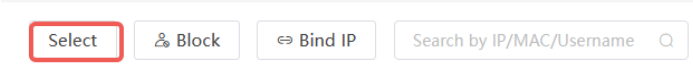
Choose **Network-Wide** > **Clients**.

IP address binding is a security and access control policy that associates a specific IP address with a specific device or user to achieve identity authentication, access control, monitoring, and accounting.

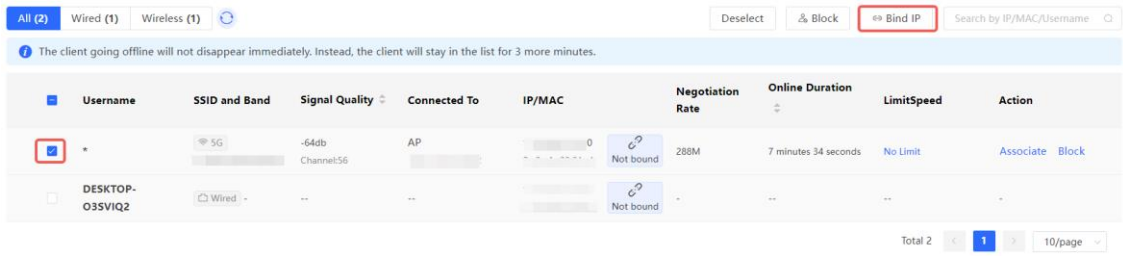
- Single client IP address binding
  Select the client to be bound with an IP address in the list, click **Not bound**, and click **OK** in the pop-up box to bind the client to a static IP address.



- Batch IP binding
  Click **Select**.

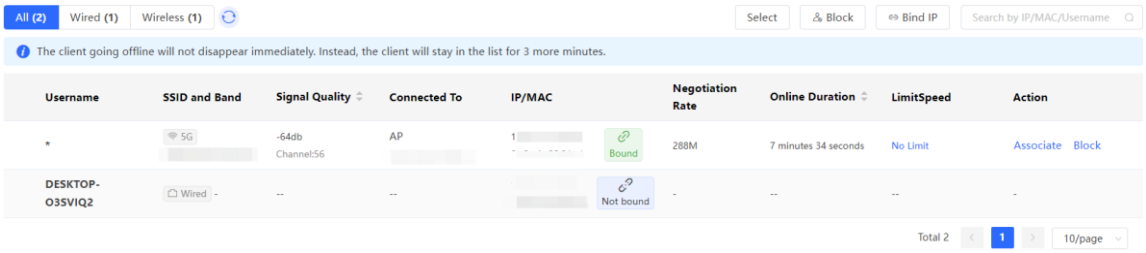


Select the clients to be bound, click **Bind IP**, and click **OK** in the pop-up box to bind the selected clients to a static IP address.



- Unbind an IP address

  Select the client to be unbound from the list, click **Bound**, and click **OK** in the pop-up box.



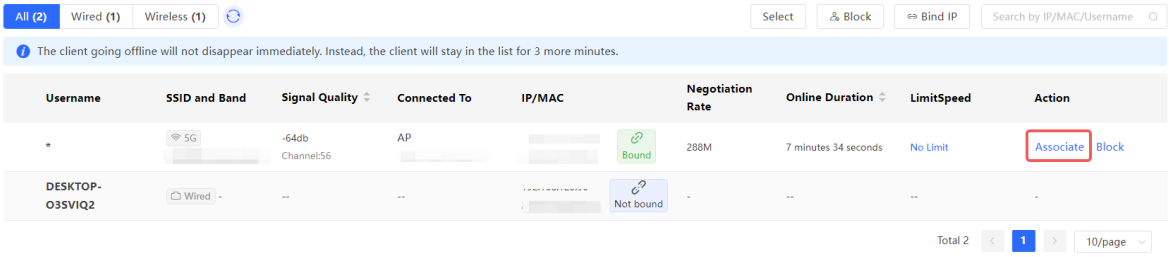
5.2 Configuring Client Association

Choose **Network-Wide** > **Clients**.

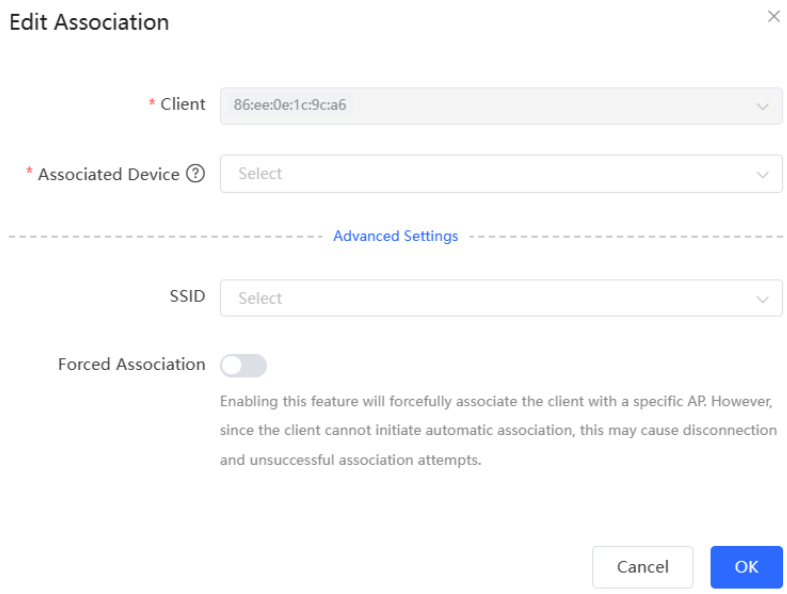
Caution

This function applies only to wireless clients.

Select a client in the list and click **Associate** in the **Action** column. You will be redirected to the **Edit Association** page.



The **Client** field is populated with the MAC address of the selected client and cannot be modified. The **Associated Device** field is populated with the associated device of the client by default. Set the SSID and the Forced Association feature as required, and click **OK**. For details, see 3.23 Client Association.



5.3 Blocking Clients

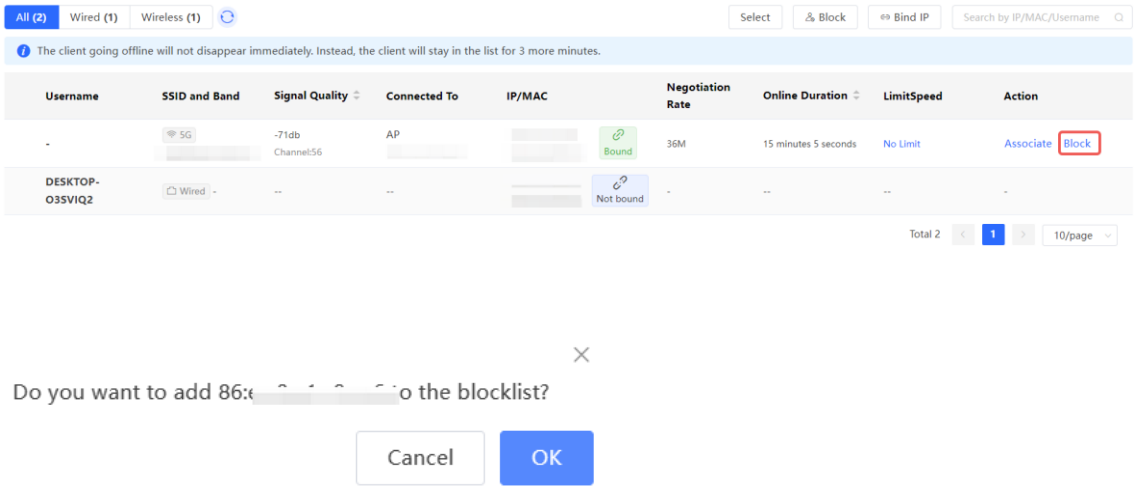
Choose **Network-Wide** > **Clients**.

An unauthorized client may occupy network bandwidth and pose security risks. You can block specified clients to solve the unauthorized access problem.

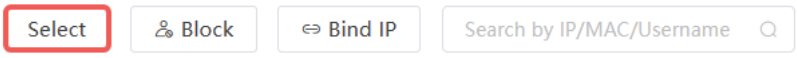
Caution

Client block is available only for wireless clients.

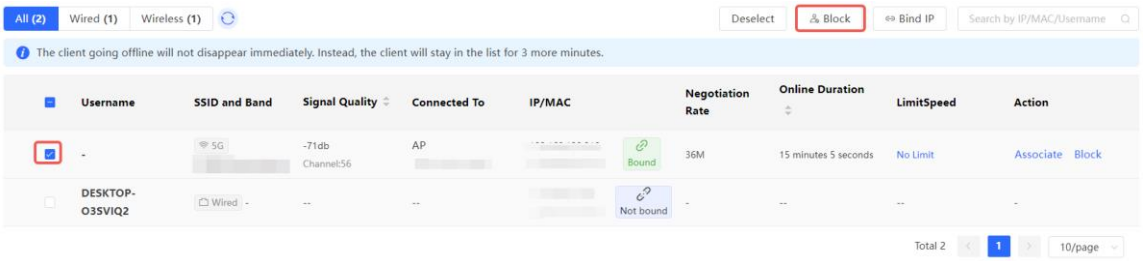
- Block a single client
  Select a client to block in the list, click **Block** in the **Action** column, and click **OK** in the pop-up box to block the selected client.



- Batch block clients
  a Click **Select**.

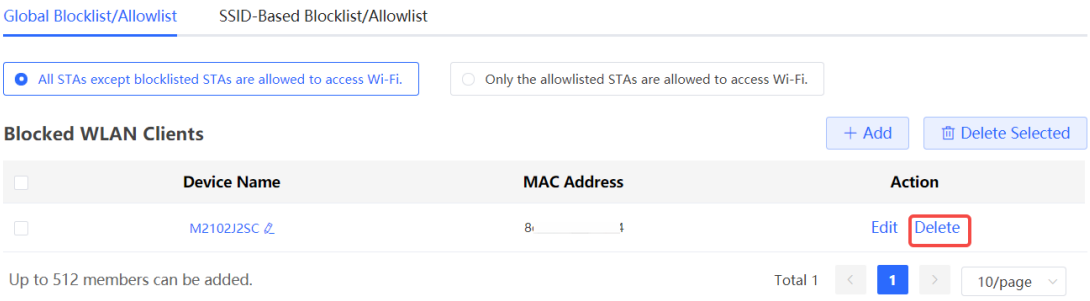


b Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.



- Cancel block
  Choose **Network-Wide** > **Workspace** > **Wireless** > **Blocklist/Allowlist** > **Global Blocklist/Allowlist.**

  Select the client to be removed from the blocklist in the wireless blocklist and click **Delete**.



5.4 Configuring Client Rate Limiting

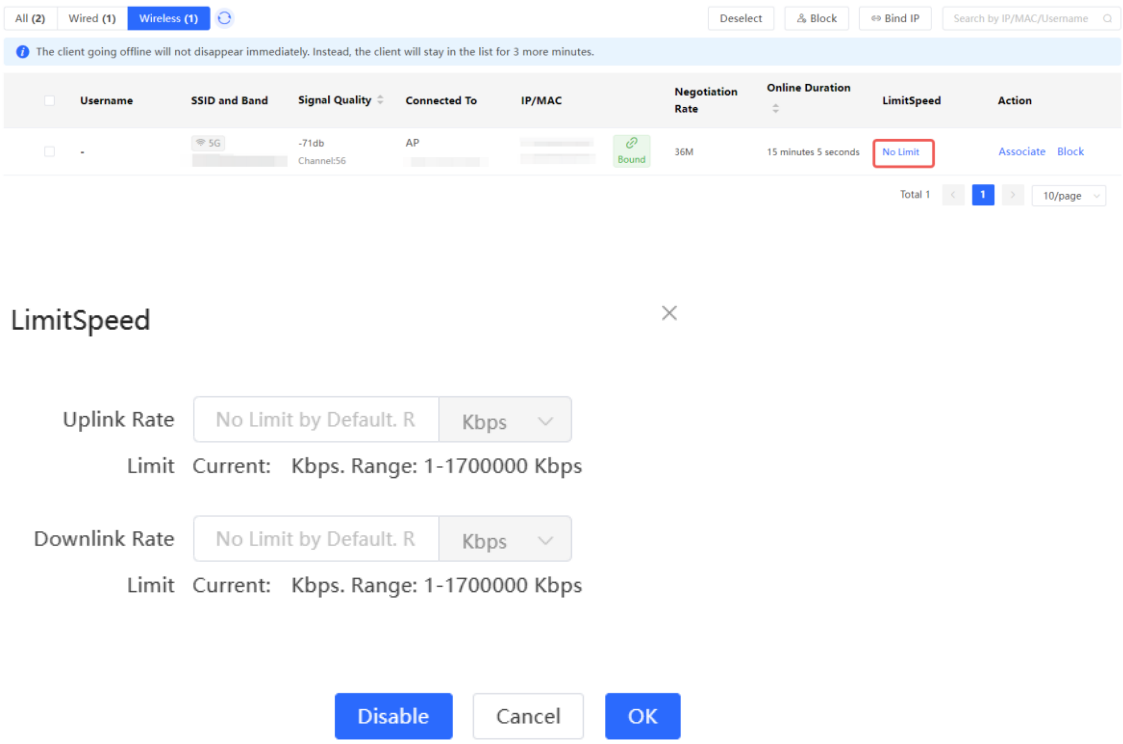
Choose **Network-Wide** > **Clients** > **Wireless**.

To ensure fair resource allocation, the network administrator can implement wireless rate limiting to prevent some users or devices from occupying a large amount of bandwidth and affecting the network experience of other users.

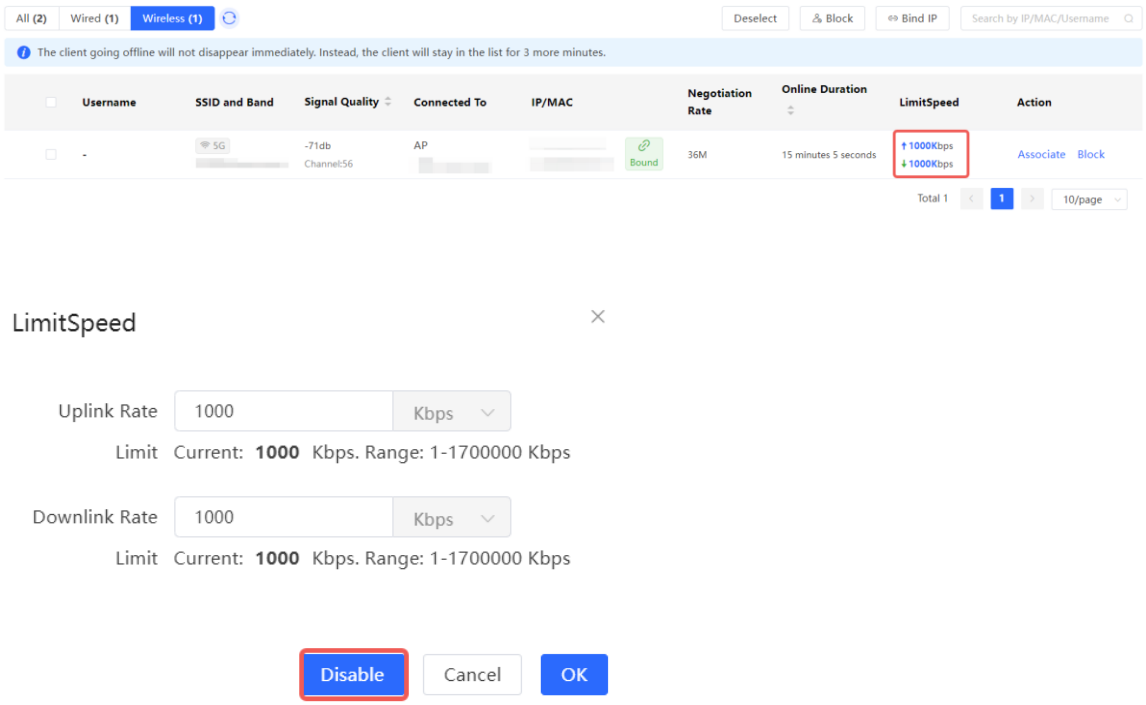
Caution

Rate limiting applies only to wireless clients.

- Configure rate limits for clients
  Click the **Wireless** tab, click the **LimitSpeed** column in the table, set the uplink rate limit and downlink rate limit, and click **OK**.



- Cancel rate limits
  Click the **Wireless** tab, click the **LimitSpeed** column in the table, and click **Disable**.

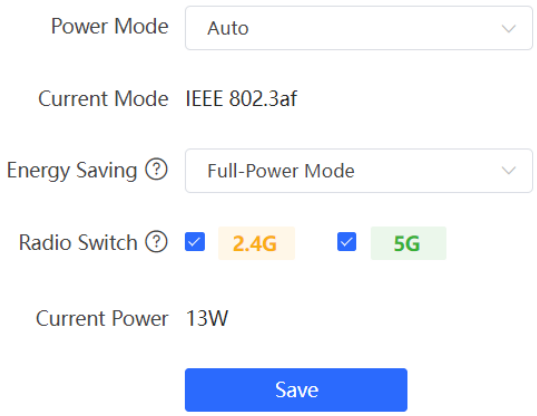


6 System Settings

6.1 PoE Settings

Choose **One-Device** > **Config** > **Advanced** > **PoE Settings.**

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



6.2 Setting the Login Password

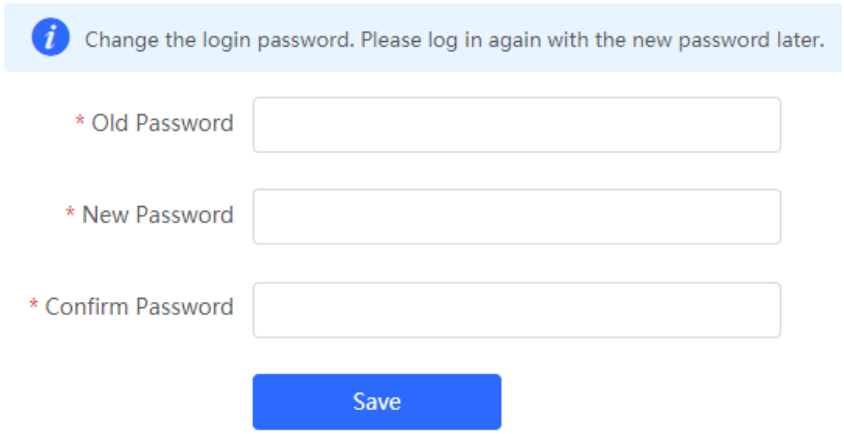
Go to the configuration page:

- In self-organizing network mode: Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Password**.
- In standalone mode: Choose **System** > **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.

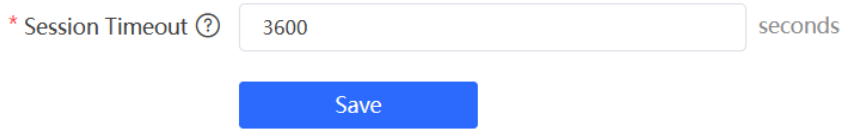


6.3 Setting the Session Timeout Duration

Go to the configuration page:

- In self-organizing network mode: Choose **One-Device > Config** > **System** > **Login**.
- In standalone mode: Choose **System** > **Login** > **Session Timeout**.

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



6.4 Setting and Displaying System Time

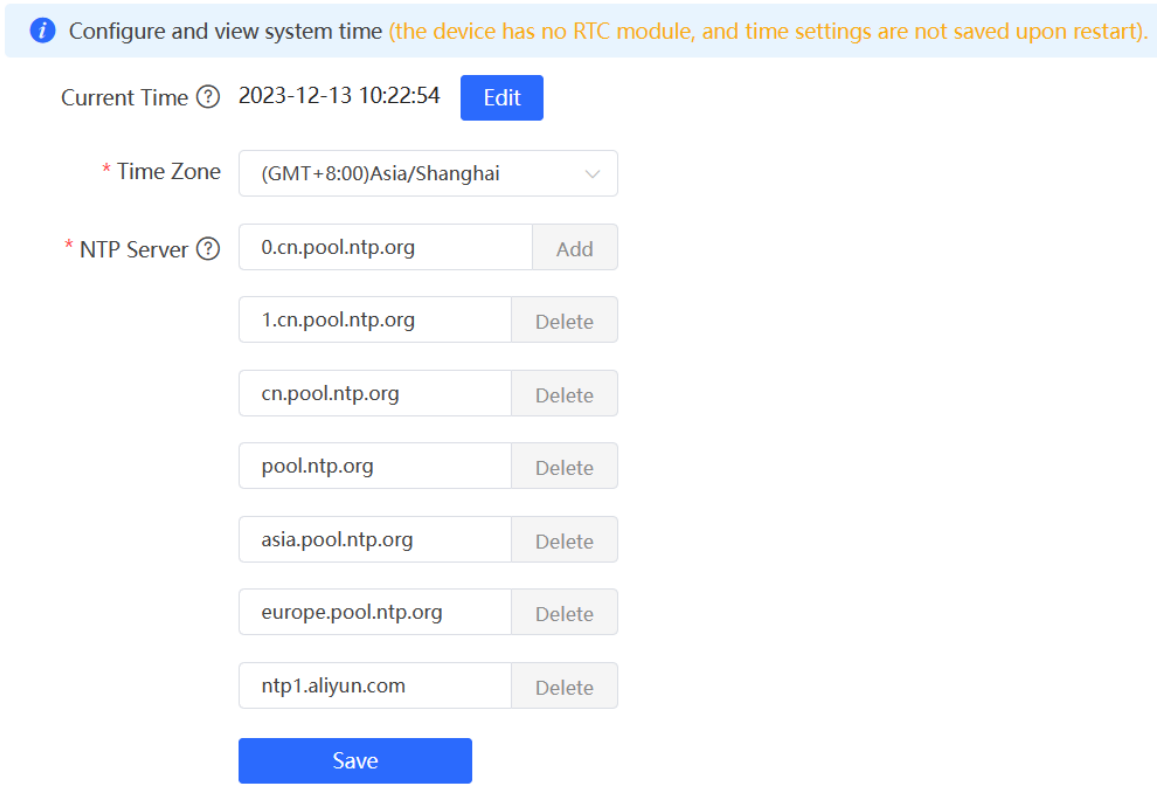
Go to the configuration page:

- In self-organizing network mode: Choose **Network-Wide** > **System** > **System Time**.
- In standalone mode: Choose **System** > **System Time**.

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the device supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server.

Caution

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



6.5 Configuring SNMP

6.5.1 Overview

The Simple Network Management Protocol (SNMP) is a protocol for managing network devices. Based on the client/server model, it can achieve remote monitoring and control of network devices.

SNMP uses a manager and agent architecture. The manager communicates with agents through the SNMP protocol to retrieve information such as device status, configuration details, and performance data. It can also be used to configure and manage devices.

SNMP can be used to manage various network devices, including routers, switches, servers, firewalls, etc. You can achieve user management through the SNMP configuration interface and monitor and control devices through the third-party software.

6.5.2 Global Configuration

1. Overview

The purpose of global configuration is to enable the SNMP service and make the SNMP protocol version (v1/v2c/v3) take effect, so as to achieve basic configuration of local port, device location, and contact information.

SNMP v1: As the earliest version of SNMP, SNMP v1 has poor security, and only supports simple community string authentication. SNMP v1 has certain flaws, such as plaintext transmission of community strings and vulnerability to attacks. Therefore, SNMP v1 is not recommended for modern networks.

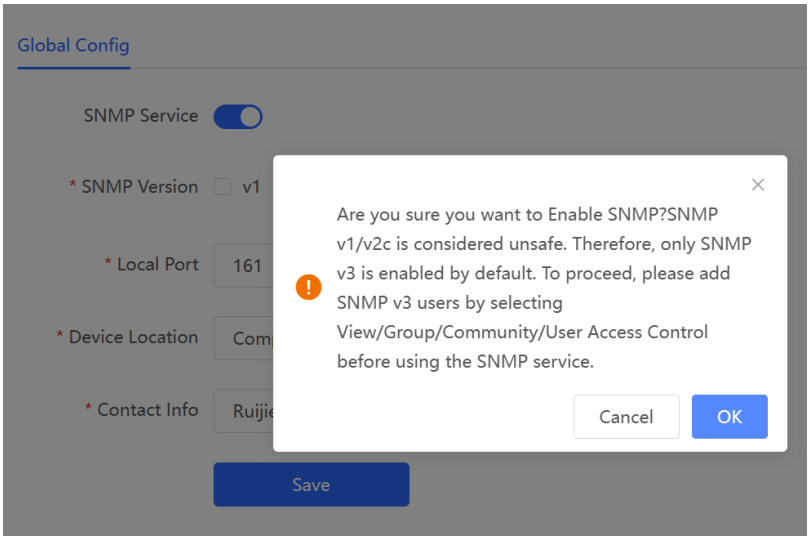
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

SNMP v3: As the newest version, SNMP v3 supports security mechanisms such as message authentication and encryption compared to SNMP v1 and SNMP v2c. SNMP v3 has achieved significant improvements in security and access control.

2. Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Global Config**.

(1) Enable the SNMP service.



When it is enabled for the first time, SNMP v3 is enabled by default. Click **OK**.

(2) Set SNMP service global configuration parameters.

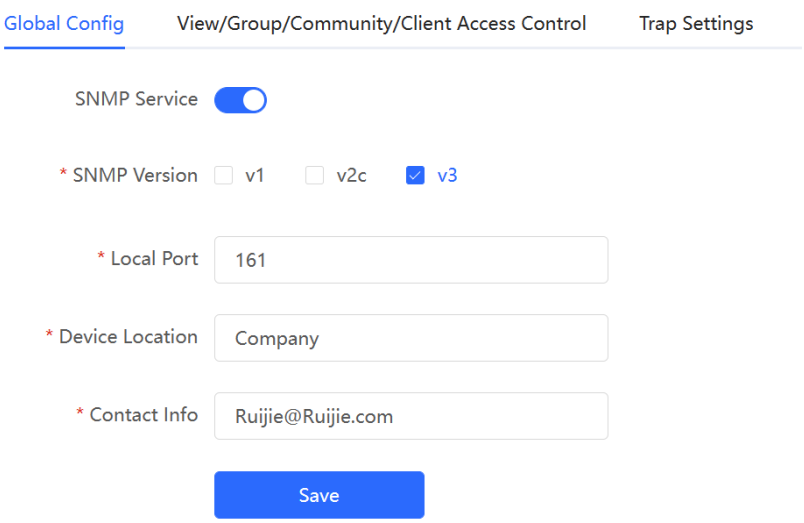


Table 6-1 Global Configuration Parameters

Parameter	Description
SNMP Service	Indicates whether SNMP service is enabled.
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.
Local Port	The port range is 1 to 65535.
Device Location	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Contact Info	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.

(3) Click **Save**.

After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

6.5.3 View/Group/Community/User Access Control

1. Configuring Views

- Overview

Management Information Base (MIB) can be regarded as a database storing the status information and performance data of network devices. It contains a large number of object identifiers (OIDs) to identify the status information and performance data of these network devices.

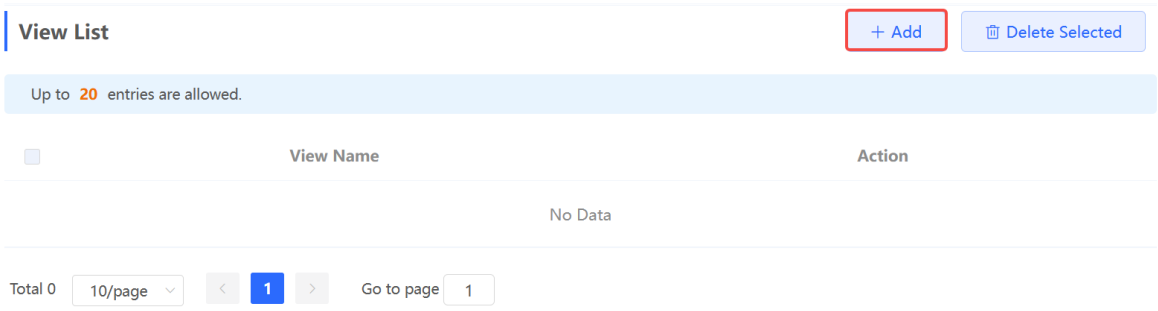
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

A view can have multiple subtrees. The management system can only access MIB nodes in these subtrees, and cannot access other unauthorized MIB nodes. This can prevent unauthorized system administrators from accessing sensitive MIB nodes, thereby protecting the security of network devices. Moreover, views can also improve the efficiency of network management and speed up the response from the management system.

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control** > **View List.**

(1) Click **Add** under the View List to add a view.



(2) Configure basic information of a view.

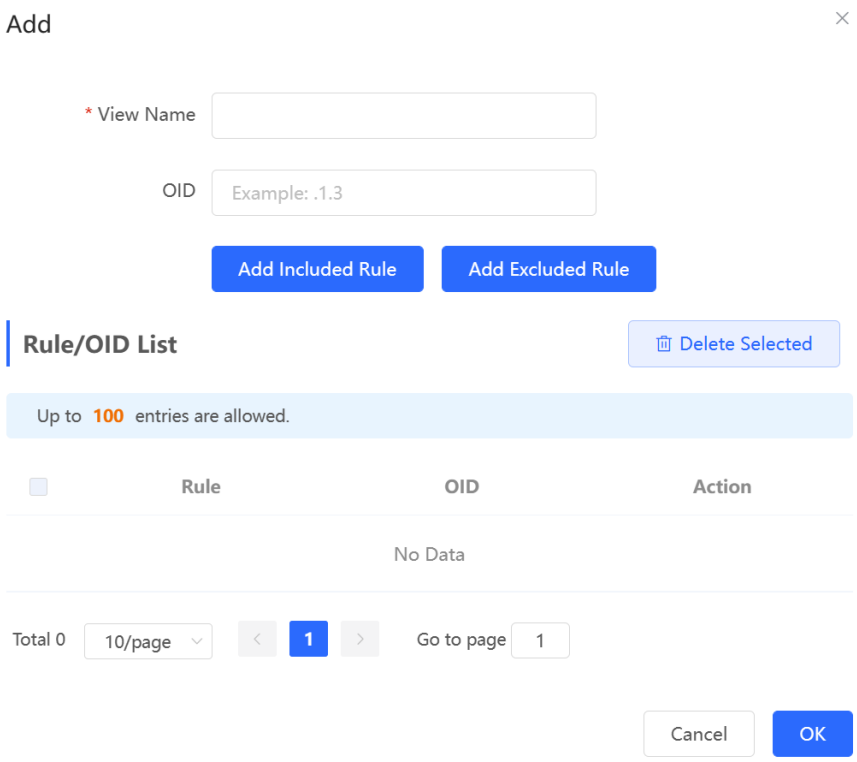


Table 6-2 View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.
Type	There are two types of rules: included and excluded rules. ● The included rule only allows access to OIDs within the OID range. Click **Add Included Rule** to set this type of view. ● Excluded rules allow access to all OIDs except those in the OID range. Click **Add Excluded Rule** to configure this type of view.

Note

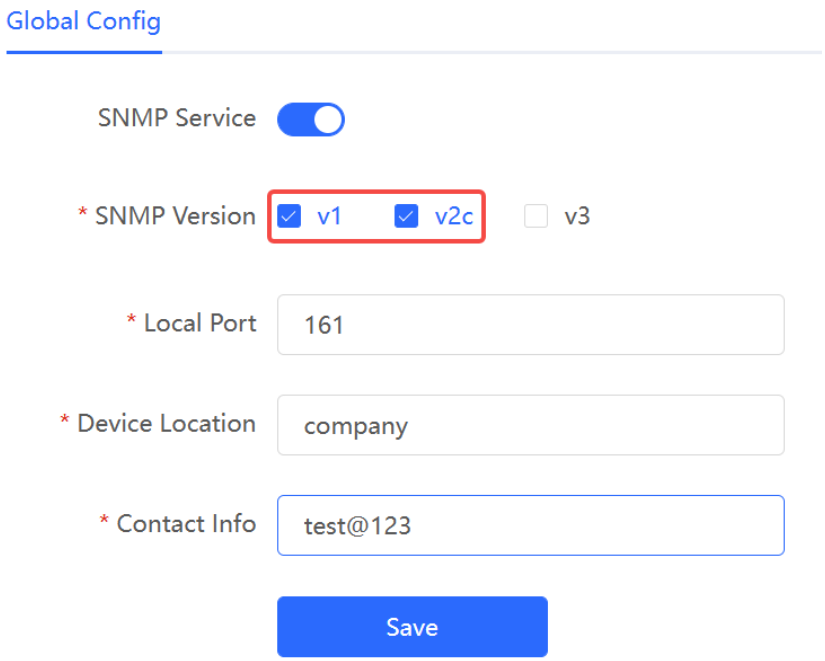
A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1/v2c Users

- Overview

When the SNMP version is set to v1/v2c, user configuration is required.



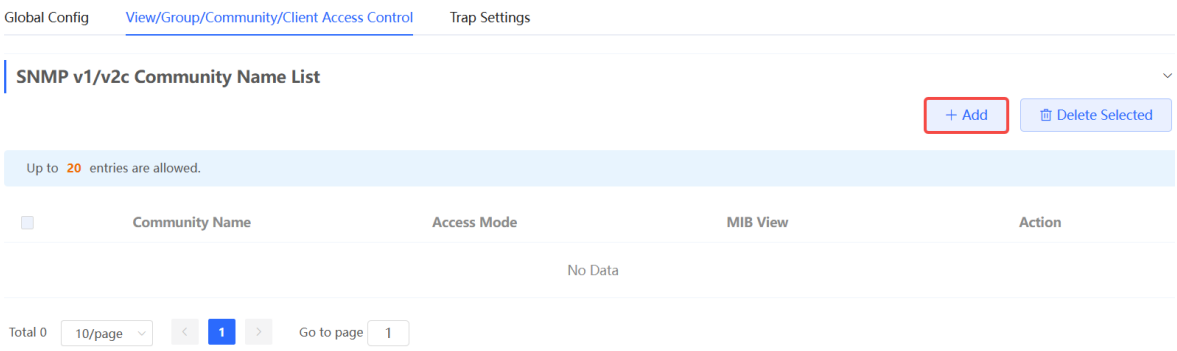
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control** > **SNMP v1/v2c Community Name List.**

(1) Click **Add** in the **SNMP v1/v2c Community Name List** pane.



(2) Add a v1/v2c user.

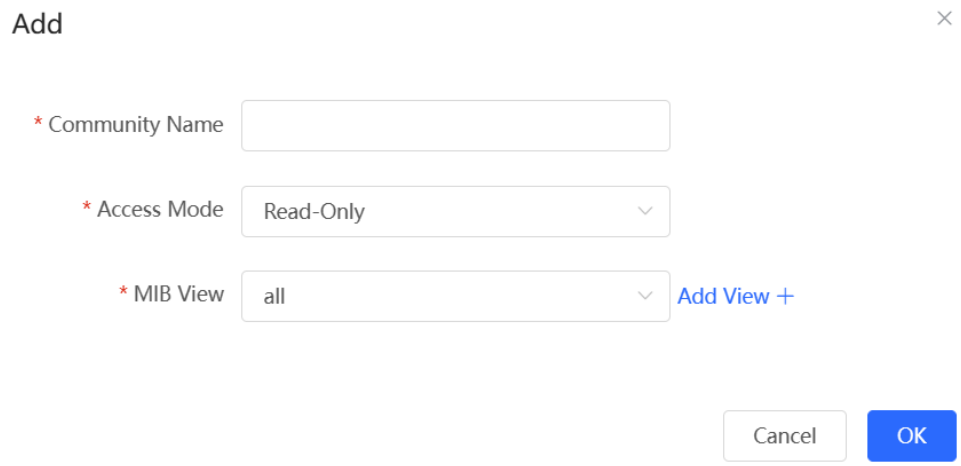


Table 6-3 v1/v2c User Configuration Parameters

Parameter	Description
Community Name	At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Access Mode	Indicates the access permission (read-only or read & write) for the community name.
MIB View	The options under the drop-down box are configured views (default: all, none).

Caution

- Community names cannot be the same among v1/v2c users.
- Click **Add View** to add a view.

(3) Click **OK**.

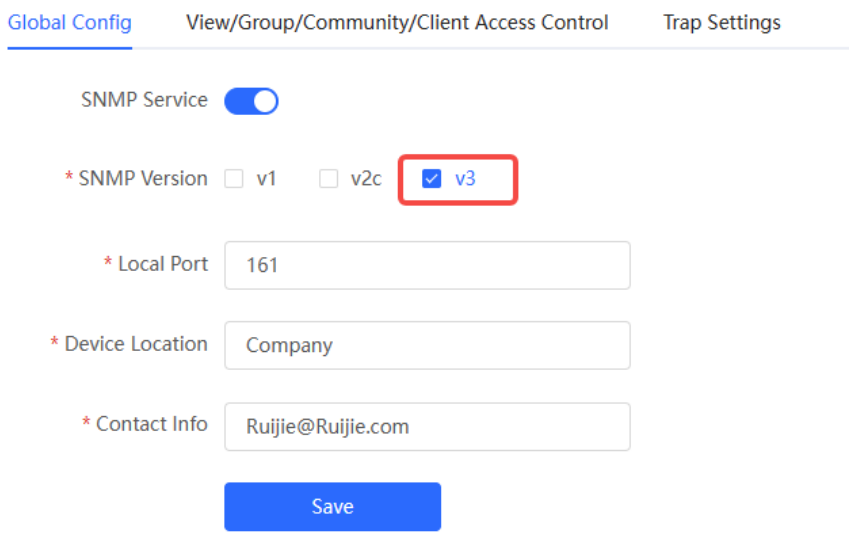
3. Configuring v3 Groups

- Overview

SNMP v3 introduces the concept of grouping to achieve better security and access control. A group is a group of SNMP users with the same security policies and access control settings. With SNMP v3, multiple groups can be configured, each with its own security policies and access control settings. Each group can have one or more users.

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.



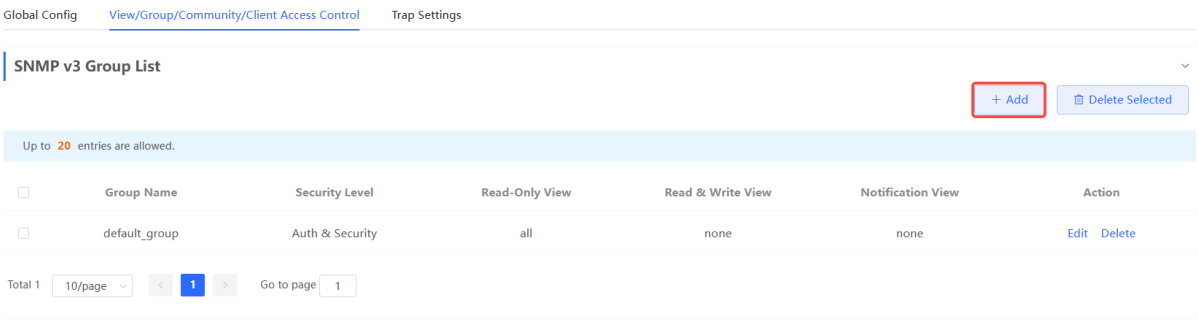
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control** > **SNMP v3 Group List.**

(1) Click **Add** in the **SNMP v3 Group List** pane to create a group.



(2) Configure v3 group parameters.

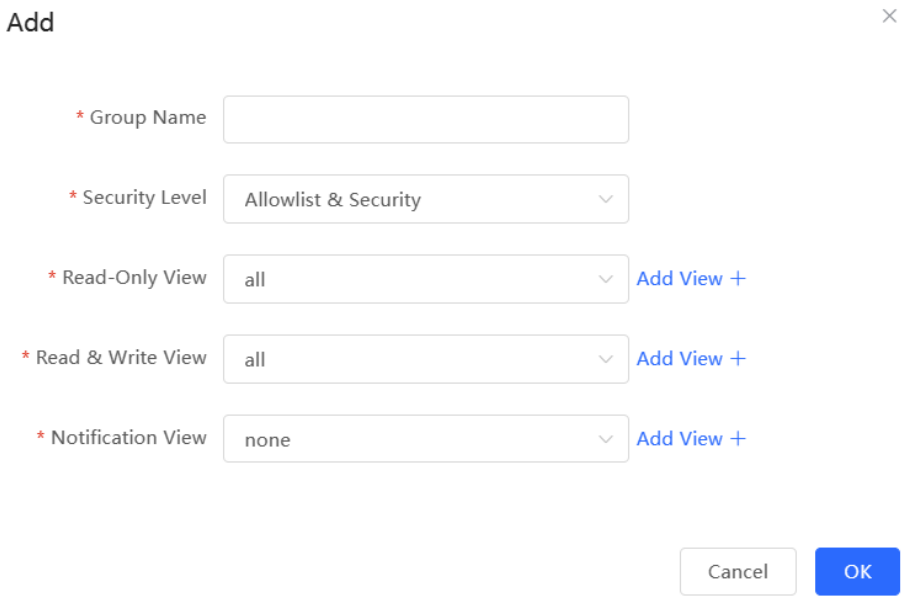


Table 6-4 v3 Group Configuration Parameters

Parameter	Description
Group Name	Indicates the name of the group. 1-32 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Security Level	Indicates the minimum security level (authentication and encryption, authentication but no encryption, no authentication and encryption) of the group.
Read-Only View	The options under the drop-down box are configured views (default: all, none).
Read & Write View	The options under the drop-down box are configured views (default: all, none).
Notification View	The options under the drop-down box are configured views (default: all, none).

Caution

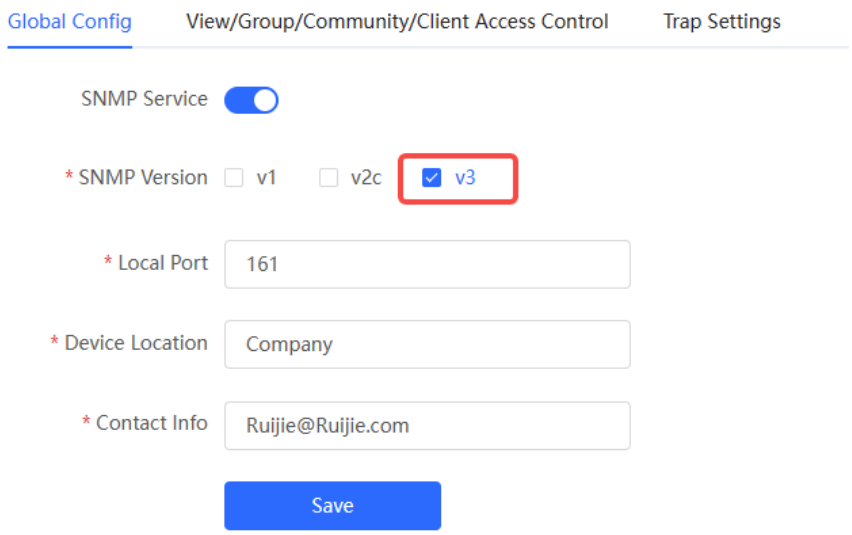
- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.



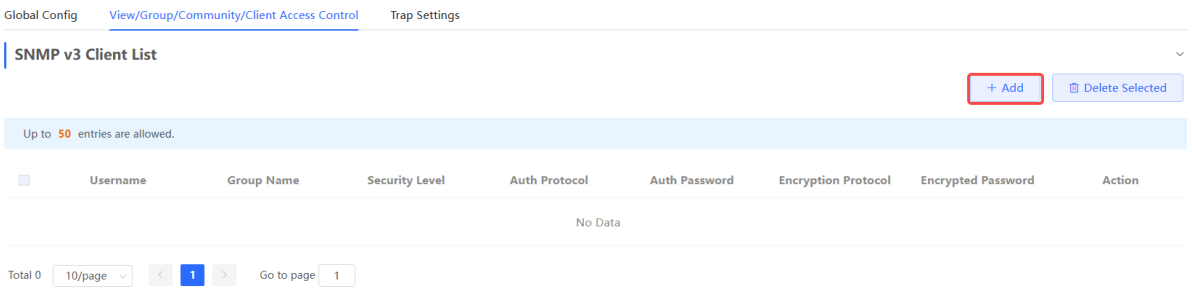
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control** > **SNMP v3 Client List.**

(1) Click **Add** in the **SNMP v3 Client List** pane to add a v3 user.



(2) Configure v3 user parameters.

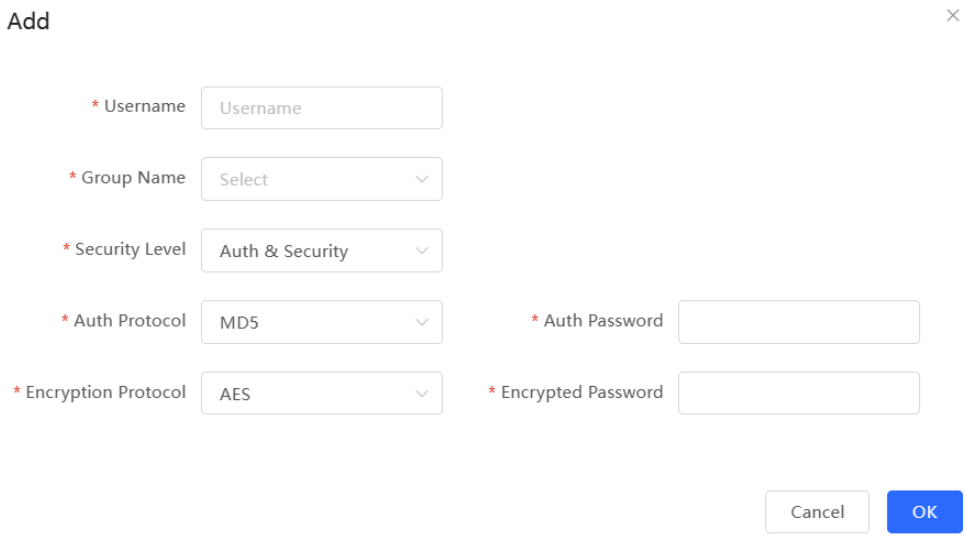


Table 6-5 v3 User Configuration Parameters

Parameter	Description
Username	Username At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Group Name	Indicates the group to which the user belongs.
Security Level	Indicates the security level (authentication and encryption, authentication but no encryption, and no authentication and encryption) of the user.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.

Parameter	Description
Encryption Protocol, Encrypted Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

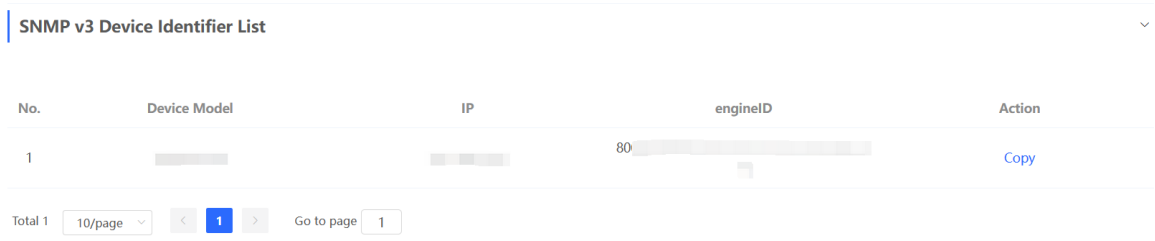
Caution

- The security level of v3 users must be greater than or equal to that of the group.
- There are three security levels, among which authentication and encryption requires the configuration of authentication protocol, authentication password, encryption protocol, and encryption password. Authentication but no encryption only requires the configuration of authentication protocol and encryption protocol, while no authentication and encryption does not require any configuration.

5. Viewing v3 Device Identifier

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control** > **SNMP v3 Device Identifier List.**

View the v3 device identifier in the **SNMP v3 Device Identifier List** pane.



6.5.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

- Application Scenario

You only need to monitor the device information, but do not need to set and deliver it. A third-party software can be used to monitor the data of nodes like 1.3.6.1.2.1.1 if v2c version is configured.

- Configuration Specification

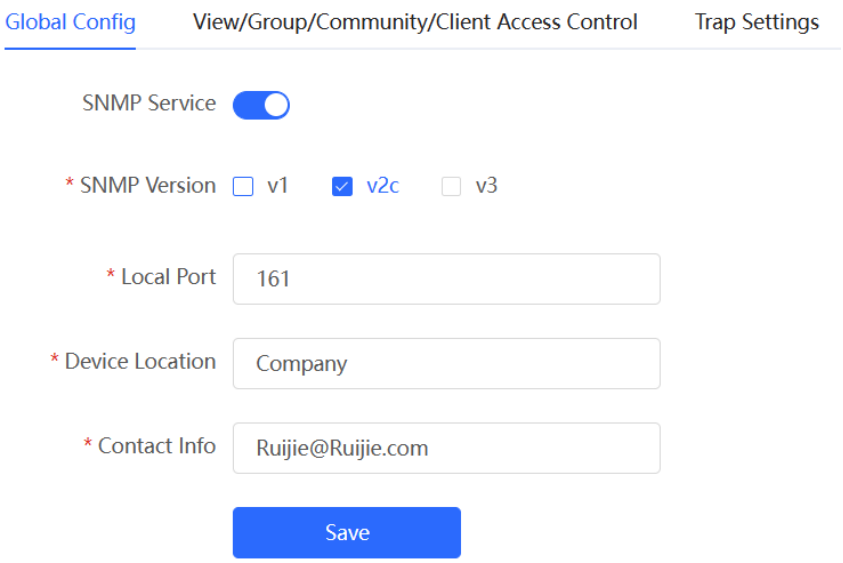
According to the user's application scenario, the requirements are shown in the following table:

Table 6-6 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "Ruijie_com", and the default port number is 161.
Read & write permission	Read-only permission.

- Configuration Steps

(1) In the global configuration interface, select v2c and set other settings as default. Then, click **Save**.

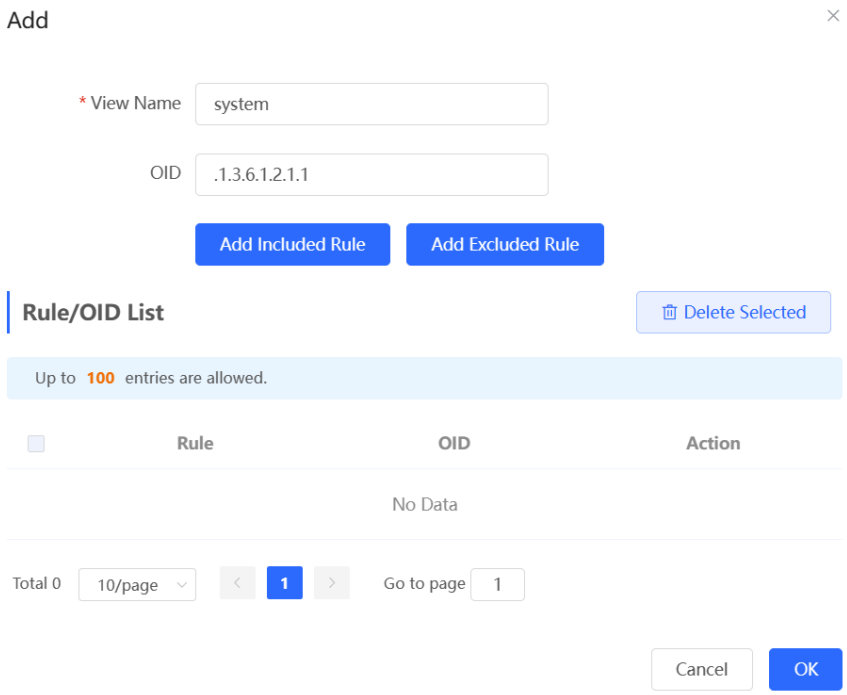


(2) Add a view on the **View/Group/Community/Client Access Control** interface.

a Click **Add** in the **View List** pane to add a view.

b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

c Click **OK**.

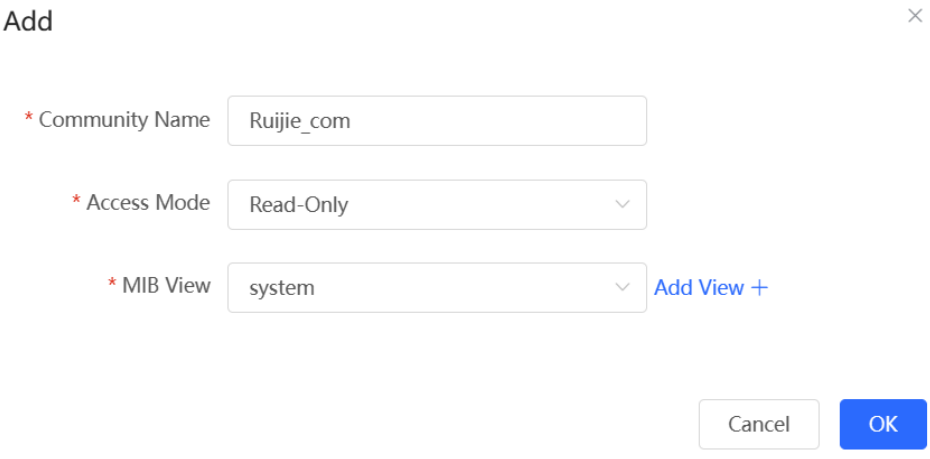


(3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.

a Click **Add** in the **SNMP v1/v2c Community Name List** pane.

b Enter the group name, access mode, and view in the pop-up window.

c Click **OK**.



2. Configuring SNMP v3

- Application Scenario

You need to monitor and control devices, and use the third-party software to monitor and deliver device information to public nodes (1.3.6.1.2.1). The security level of v3 is authentication and encryption.

- Configuration Specification

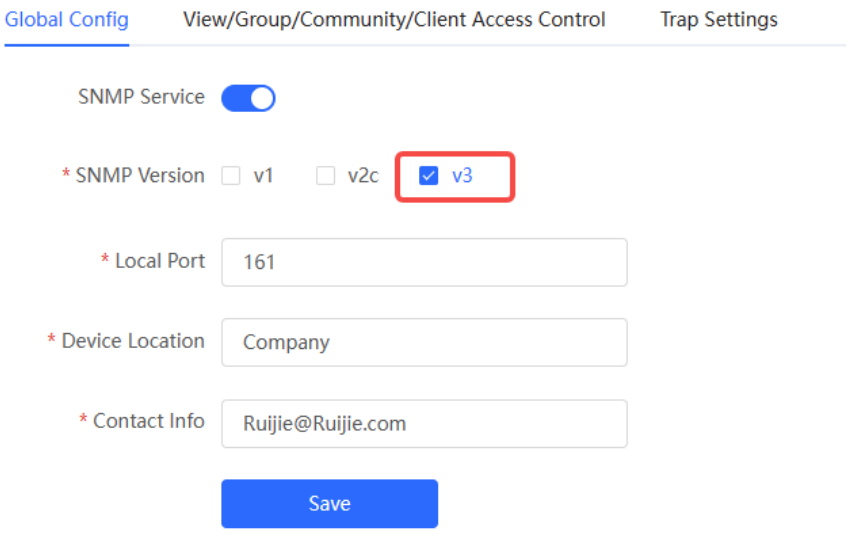
According to the user's application scenario, the requirements are shown in the following table:

Table 6-7 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.
Configuring v3 Users	User name: v3_user Group name: group Security level: authentication and encryption Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123
Version	For SNMP v3, the default port number is 161.

- Configuration Steps

(1) On the global configuration interface, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.

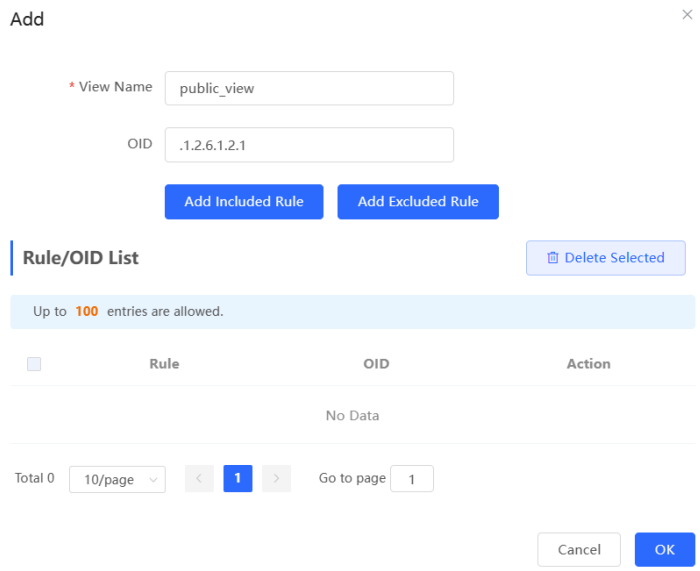


(2) Add a view on the **View/Group/Community/Client Access Control** interface.

a Click **Add** in the **View List** pane.

b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

c Click **OK**.

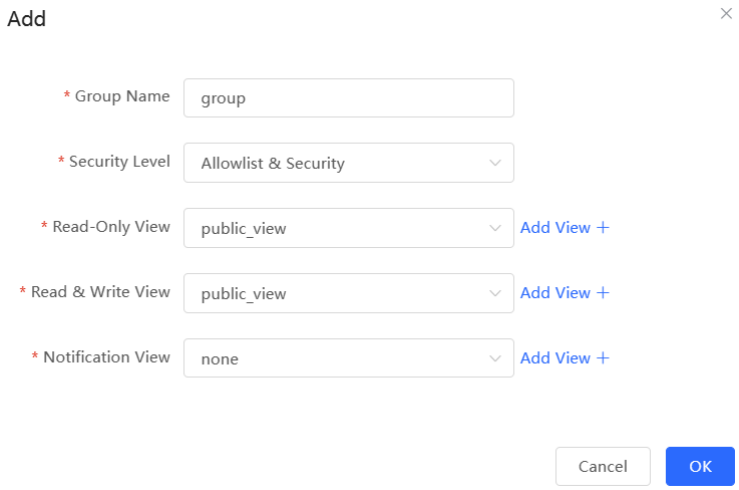


(3) On the **View/Group/Community/Client Access Control** interface, add an SNMP v3 group.

a Click **Add** in the **SNMP v3 Group List** pane.

b Enter the group name and security level on the pop-up window. As this user has read and write permissions, select public_view for read-only and read & write views, and select none for notify views.

c Click **OK**.

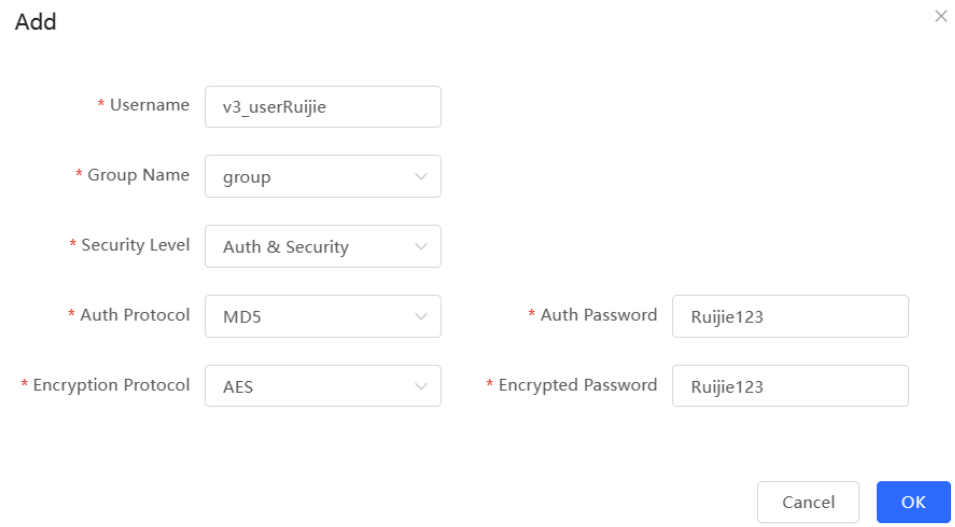


(4) On the **View/Group/Community/Client Access Control** interface, add an SNMP v3 user.

a Click **Add** in the **SNMP v3 Client List** pane.

b Enter the user name and group name in the pop-up window. As the user's security level is authentication and encryption, enter the authentication protocol, authentication password, encryption protocol, and encryption password.

c Click **OK**.



6.5.5 Configuring Trap Service

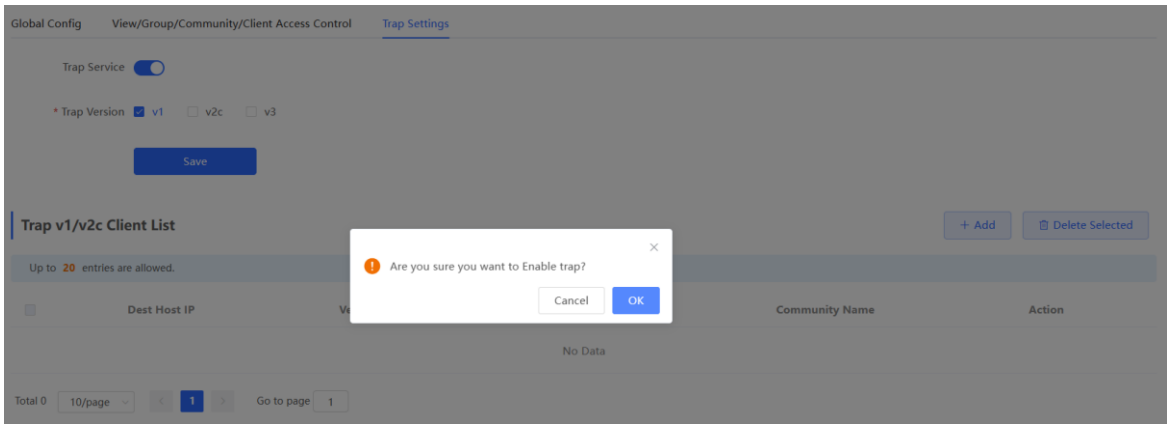
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring and fault diagnosis services, helping administrators discover and solve network problems in a timely manner.

1. Enabling Trap Service

Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Trap Settings.**

(1) Enable the trap service.



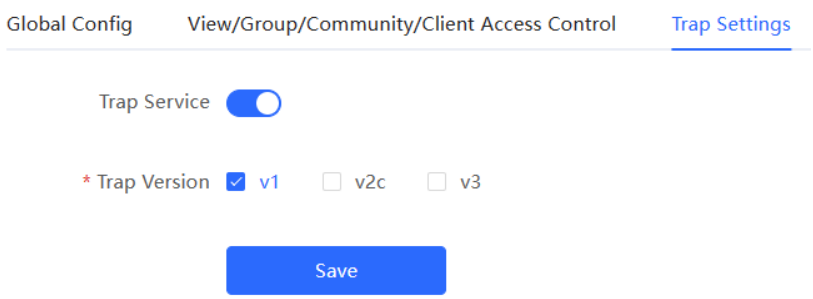
When the trap service is enabled for the first time, the system will pop up a prompt message. Click **OK**.

(2) Set the trap version.

The trap versions include v1, v2c, and v3.

(3) Click **Save**.

After the trap service is enabled, click **Save** for the configuration to take effect.



2. Configuring Trap v1/v2c Users

- Overview

Trap is a notification mechanism that is used to send alerts to administrators when important events or failures occur on devices or services. Trap v1/v2c are two versions in the SNMP protocol for network management and monitoring.

Trap v1 is the first version that supports basic alert notification functionality. Trap v2c is the second version, which supports more alert notification options and advanced security features.

By using trap v1/v2c, administrators can promptly understand problems on the network and take corresponding measures.

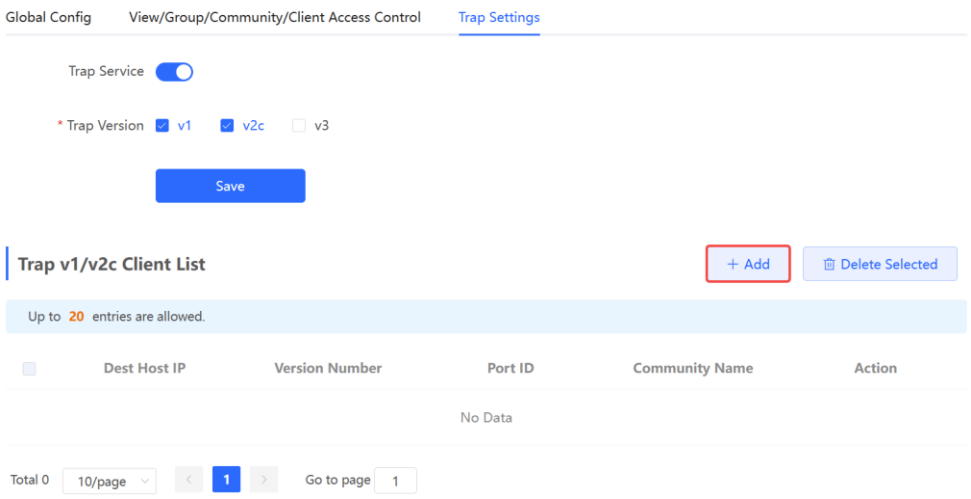
- Prerequisites

  Once trap v1 and v2c versions are selected, it is necessary to add trap v1v2c users.

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Trap Settings.**

(1) Click **Add** in the **Trap v1/v2c Client List** pane to add a trap v1/v2c user.



(2) Configure trap v1/v2c user parameters.

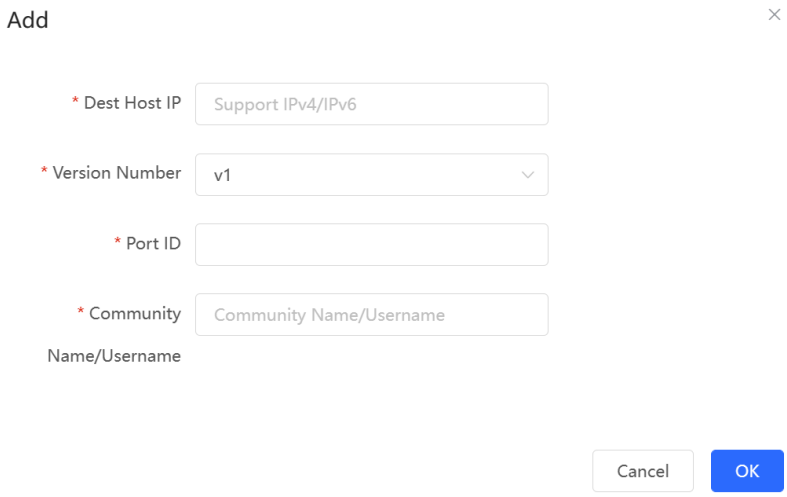


Table 6-8 Trap v1/v2c User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Version Number	Trap version, including v1 and v2c.
Port ID	The port range of the trap peer device is 1 to 65535.
Community Name/Username	Community name of the trap user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.

Caution

- The destination host IP address of trap v1/ v1/v2c users cannot be the same.
- Community names of trap v1/ v1/v2c users cannot be the same.

(3) Click **OK**.

3. Configuring Trap v3 Users

- Overview

Trap v3 is a network management mechanism based on the SNMP protocol. It is used to send alert notifications to administrators. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption features.

Trap v3 offers custom conditions and methods for sending alerts, as well as the recipients and notification methods for receiving alerts. This enables administrators to have a more accurate understanding of the status of network devices and to take timely measures to ensure the security and reliability of the network.

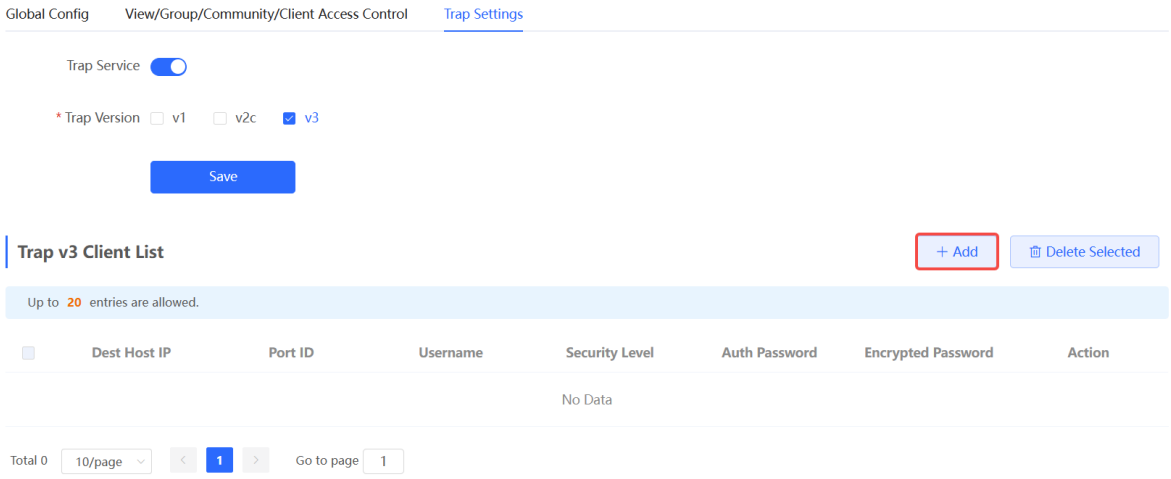
- Prerequisites

When the v3 version is selected for the trap service, it is necessary to add a trap v3 user.

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Trap Settings.**

(1) Click **Add** in the **Trap v3 Client List** pane to add a trap v3 user.



(2) Configure trap v3 user parameters.

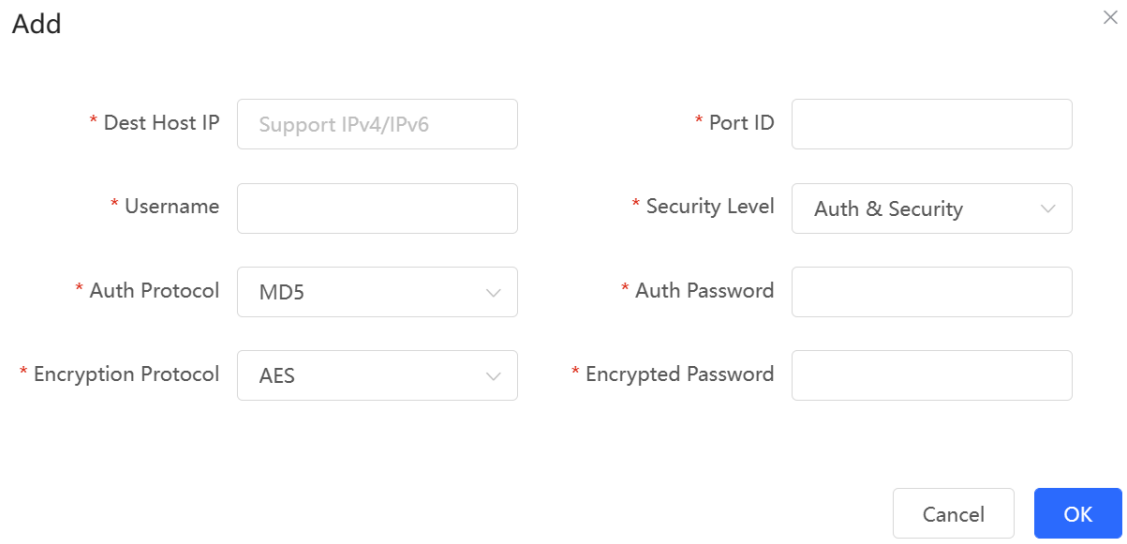


Table 6-9 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.

Parameter	Description
Username	Name of the trap v3 user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Security Level	There are three security levels for a trap user, which are "Auth & Security", "Auth & Open", and "Allowlist & Security".
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter must be set when the Security Level is Auth & Security or Auth & Open.
Encryption Protocol, Encrypted Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter must be set when the Security Level is Auth & Security.

Caution

The destination host IP address of trap v1/v2c/v3 users cannot be the same.

(3) Click **OK**.

6.5.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.85 and a port number of 166 to enable the device to send a v2c trap in case of an abnormality.

- Configuration Specification

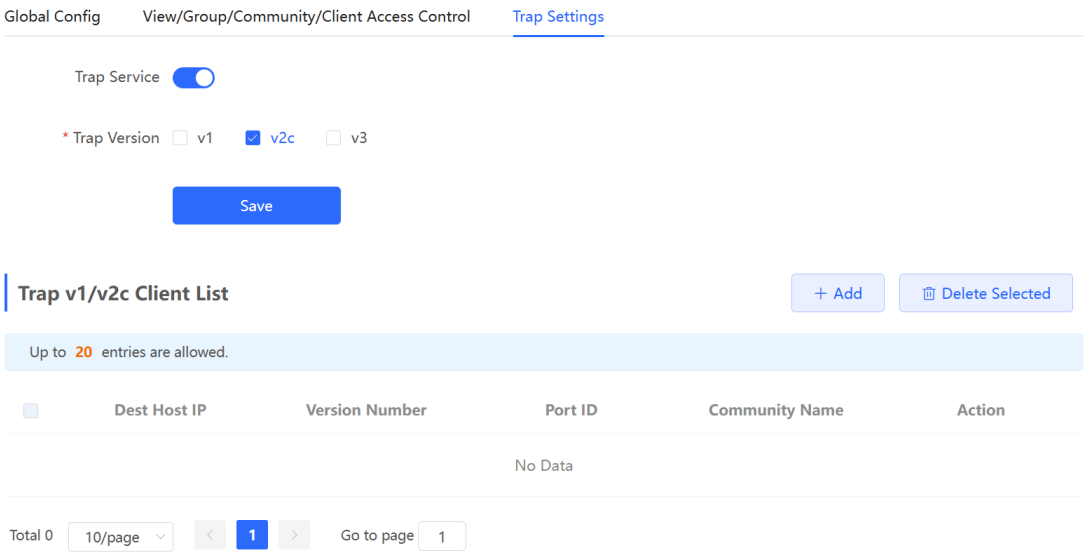
According to the user's application scenario, the requirements are shown in the following table:

Table 6-10 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port number is 166.
Version	Select the v2c version.
Community name/User name	Trap_ruijie

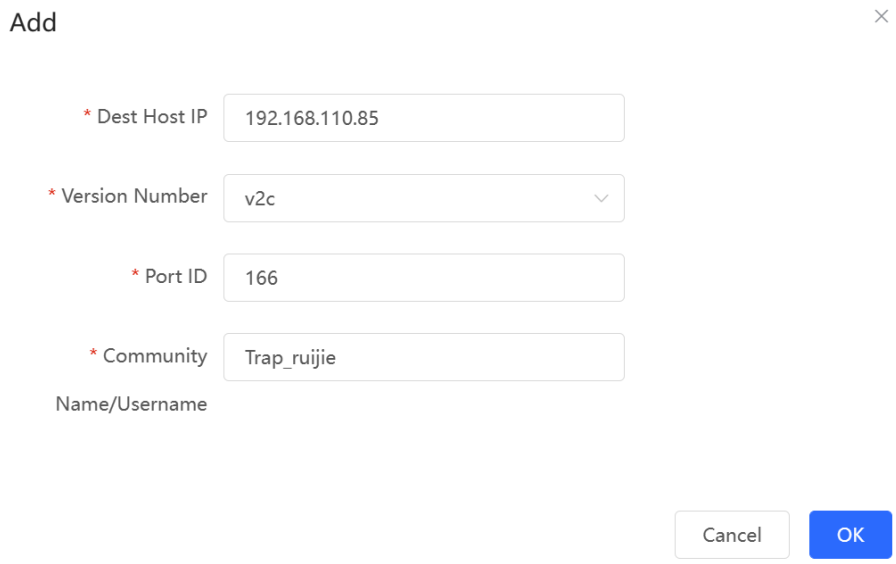
- Configuration Steps

(1) Select the v2c version in the **Trap Setting** interface and click **Save**.



(2) Click **Add** in the Trap v1/v2c Client List to add a trap v2c user.

(3) Enter the destination host IP address, version, port number, user name, and other information. Then, click **OK**.



2. Configuring Trap v3

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.87 and a port number of 167 to enable the device to send a v3 trap, which is a safer trap compared with v1/v2c traps.

- Configuration Specification

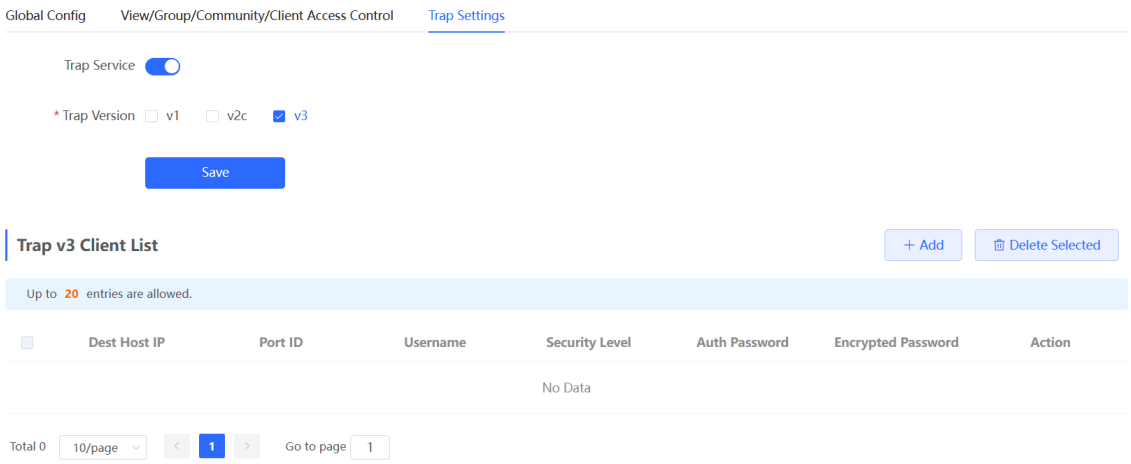
According to the user's application scenario, the requirements are shown in the following table:

Table 6-11 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.87, and the port number is 167.
Version and user name	Select the v3 version and trapv3_ ruijie for the user name.
Authentication protocol/authentication password Encryption protocol/encryption password	Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123

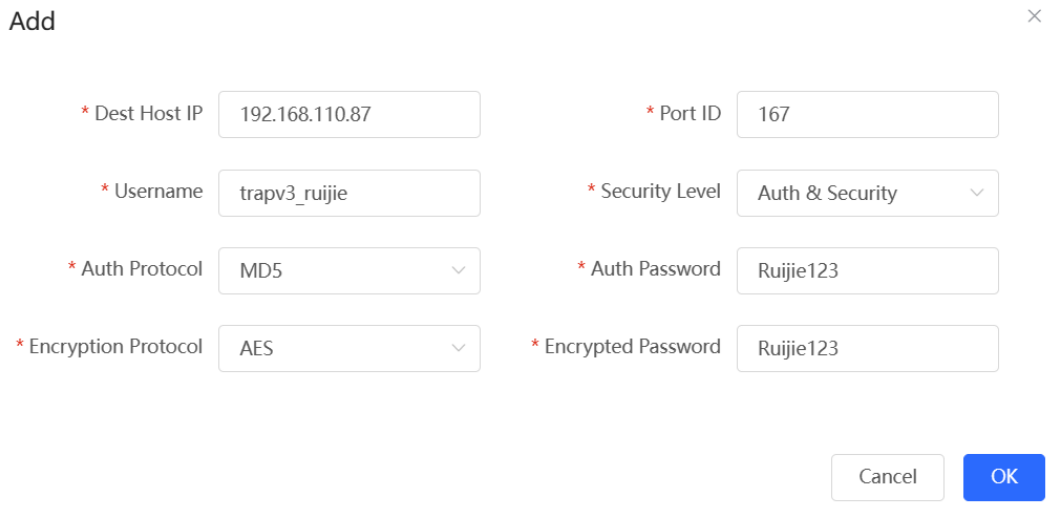
- Configuration Steps

(1) Select the v3 version in the **Trap Setting** interface and click **Save**.



(2) Click **Add** in the Trap v3 Client List to add a trap v3 user.

(3) Enter the destination host IP address, port number, user name, and other information. Then, click **OK**.



6.6 Configuring Reboot

Caution

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

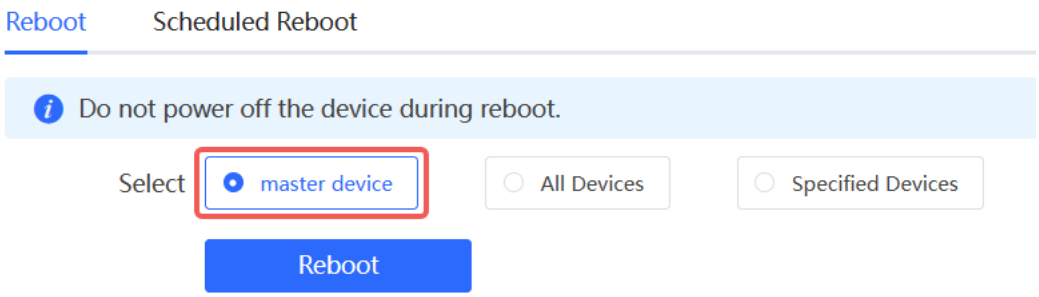
6.6.1 Rebooting the Master Device

In self-organizing network mode:

- Choose **Network-Wide** > **System** > **Reboot**. Click the **Reboot** tab and select **master device**.
- Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Reboot**. Click the **Reboot** tab and select **master**

device.

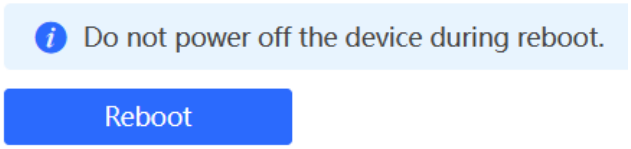
Click the **Reboot** button. The master device will restart.



6.6.2 Rebooting Local Device

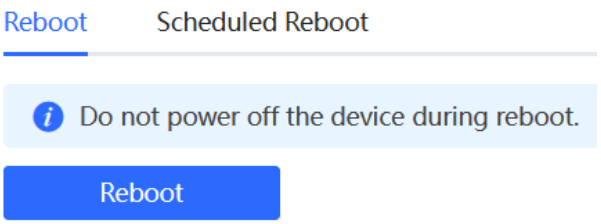
- In self-organizing network mode, choose **One-Device** > **Config** > **System** > **Reboot**.

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



- In standalone mode: choose **System** > **Reboot** > **Reboot**.

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



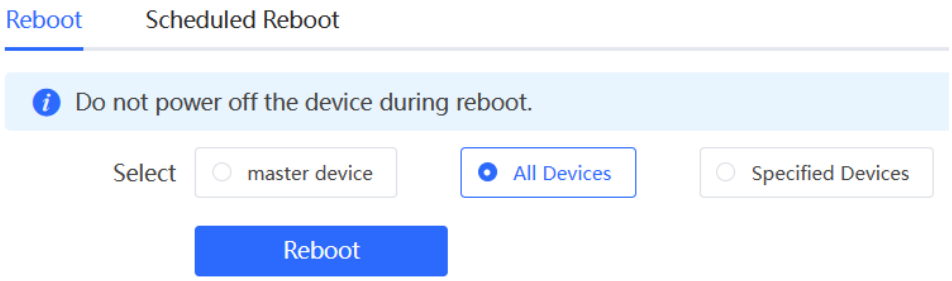
6.6.3 Rebooting All Devices on the Network

In self-organizing network mode, you can batch reboot all devices on the network.

Go to the configuration page:

- Choose **Network-Wide** > **System** > **Reboot**. Click the **Reboot** tab and select **All Devices**.
- Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Reboot**. Click the **Reboot** tab and select **All Devices**.

Click the **Reboot** button to batch reboot all devices on the network.



Caution

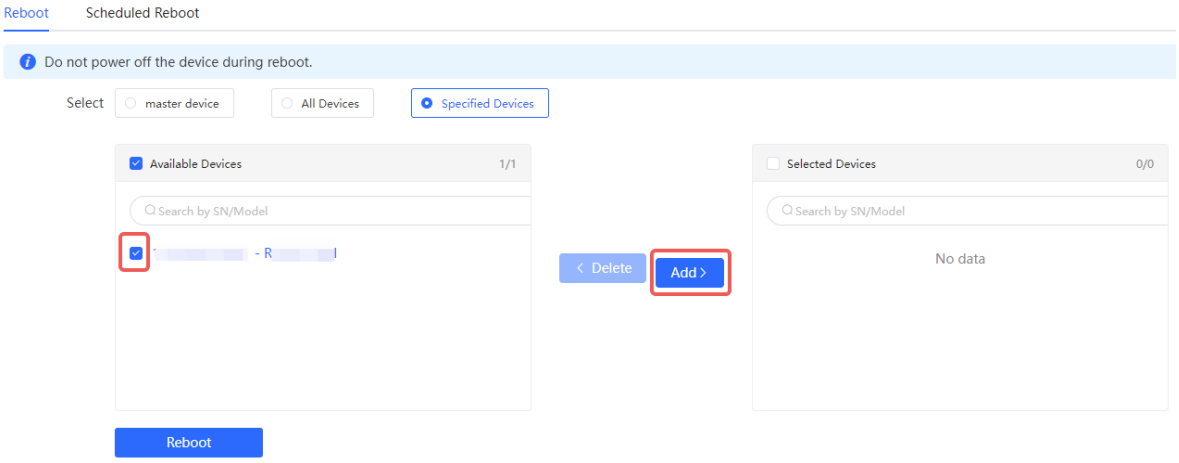
It takes time to reboot all devices in the current network. The action may affect the whole network. Please be cautious.

6.6.4 Rebooting the Specified Devices

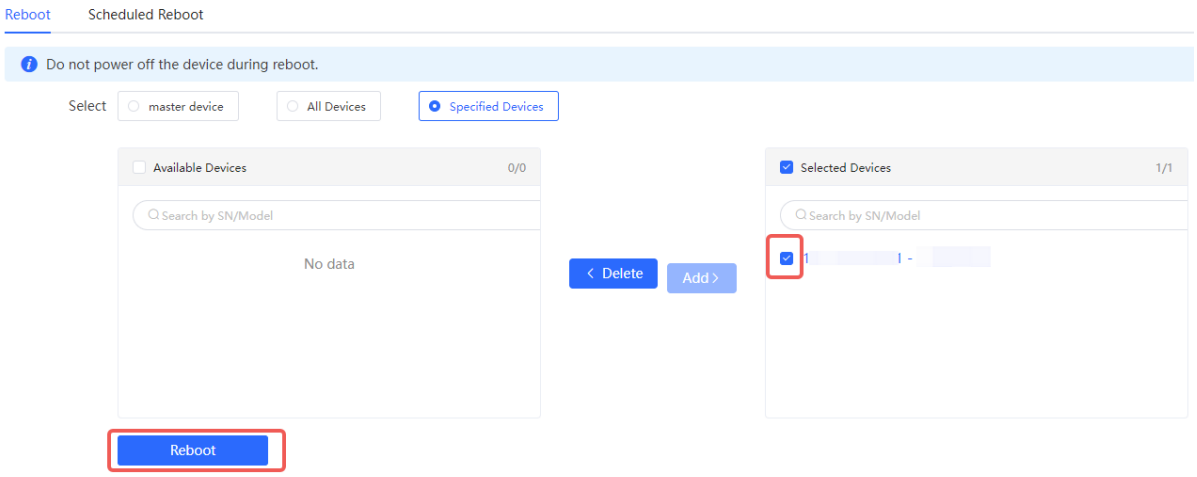
In self-organizing network mode, you can reboot specified devices in the network in batches. Go to the configuration page:

- Choose **Network-Wide** > **System** > **Reboot**. Click the **Reboot** tab and select **Specified Devices**.
- Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Reboot**. Click the **Reboot** tab and select **Specified Devices**.

Select required devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** on the right.



Click the **Reboot** button. Specified devices in the **Selected Devices** list will be rebooted.



6.7 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 6.4 Setting and Displaying System Time.

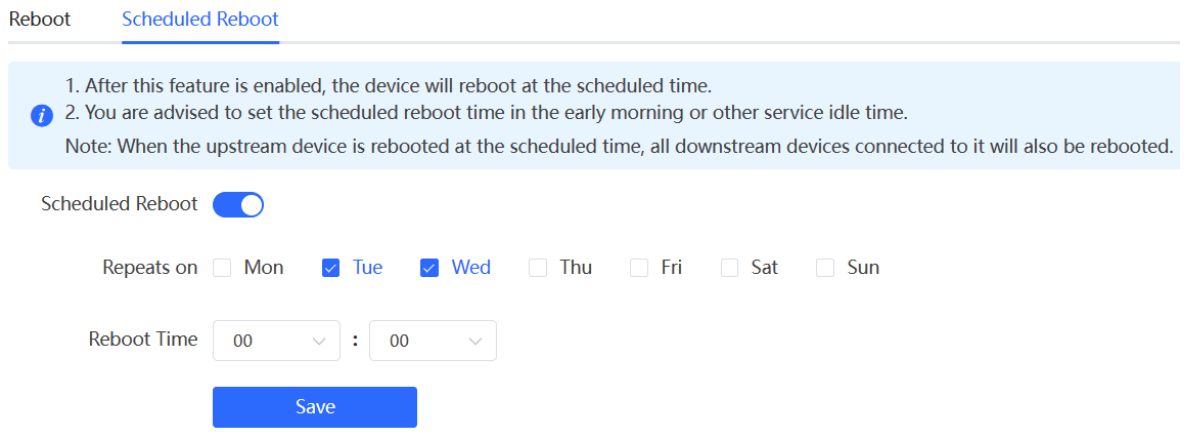
Go to the configuration page:

- Choose **Network-Wide** > **System** > **Reboot** > **Scheduled Reboot.**
- Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Reboot** > **Scheduled Reboot**.
- AP as master device: Choose **One-Device** > **Config** > **System** > **Reboot** > **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 **Scheduled Reboot**, 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.



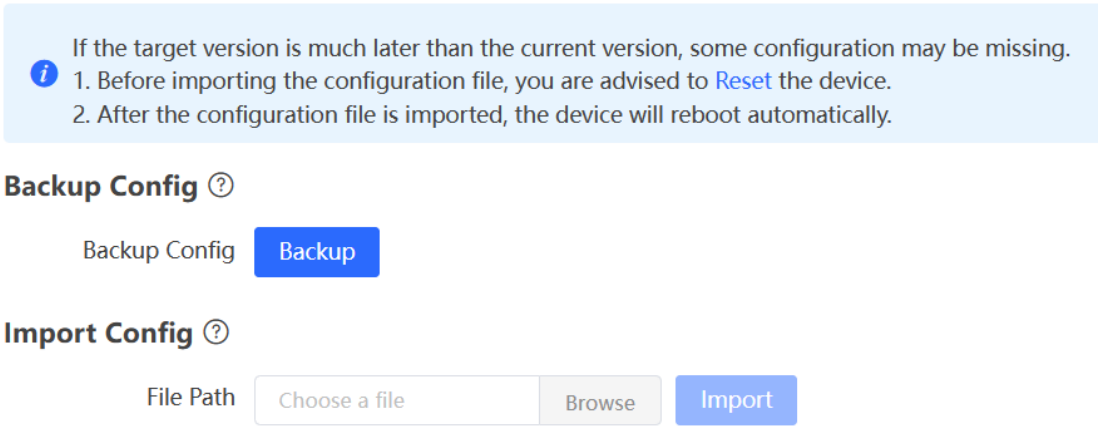
6.8 Configuring Backup and Import

Go to the configuration page:

- Choose **Network-Wide** > **System** > **Backup & Import**.
- Choose **One-Device** > **Config** > **System** > **Backup** > **Backup & Import**.

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

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

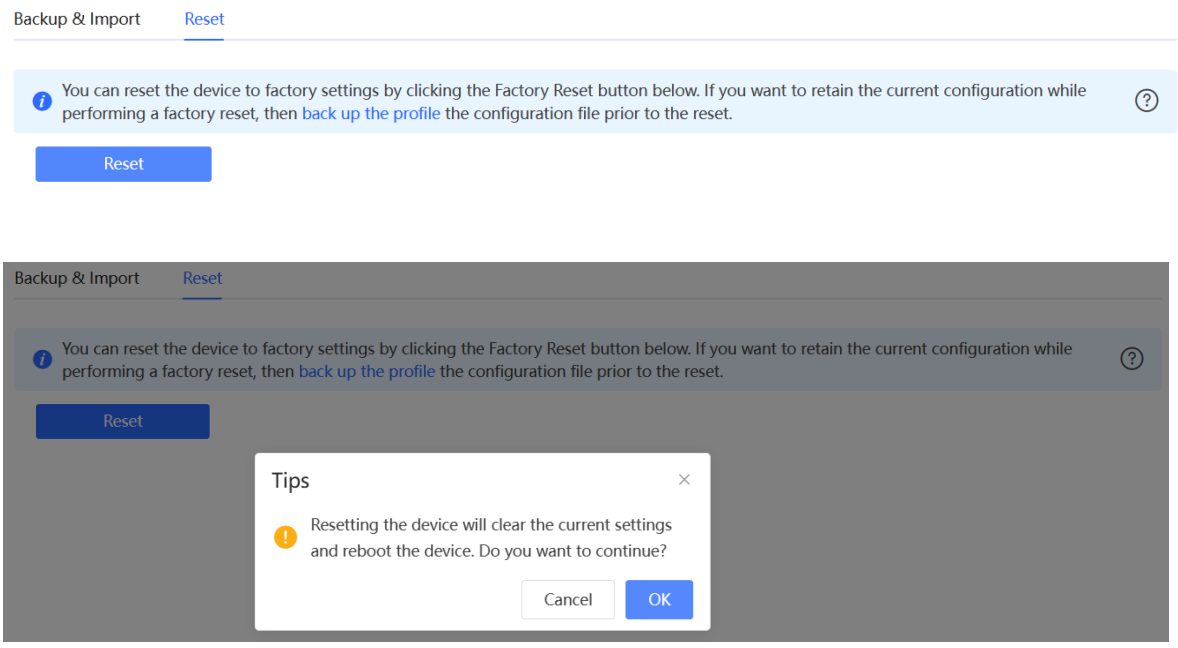


6.9 Restoring Factory Settings

6.9.1 Restoring the Current Device to Factory Settings

Choose **One-Device** > **Config** > **System** > **Backup** > **Reset**.

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



Caution

The operation will clear all configuration of the current device. If you want to retain the current configuration, back up the configuration first (See 6.8 Configuring Backup and Import). Therefore, exercise caution when performing this operation.

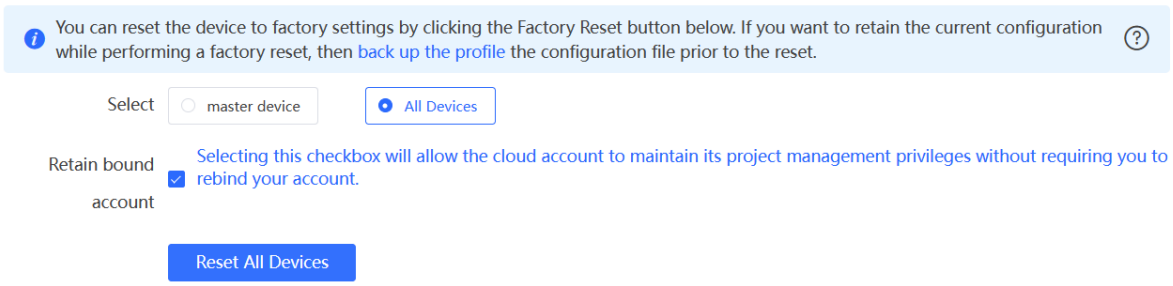
6.9.2 Restoring All Devices to Factory Settings

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

Go to the configuration page:

- Choose **Network-Wide** > **System** > **Reset.**
- Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Reset**.

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



Caution

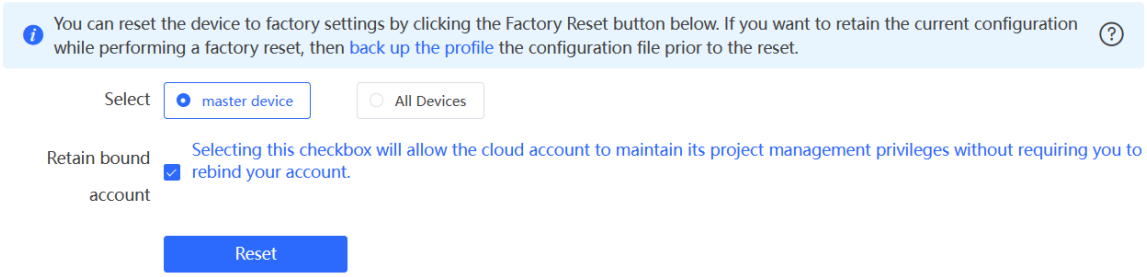
The operation will clear all configuration of all devices in the network. If you want to retain the current configuration, back up the configuration first (See 6.8 Configuring Backup and Import). Therefore, exercise caution when performing this operation.

6.9.3 Restoring Master Device to Factory Settings

Go to the configuration page:

- Choose **Network-Wide** > **System** > **Reset.**
- Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Reset**.

Select **master device**, and check or uncheck the box next to **Retain bound account**. Then, click **Reset**. The master device will be restored to factory settings.



Caution

This operation will clear the current settings of the master device on the network and reboot the device. If you want to retain the current configuration, back up the configuration first (See 6.8 Configuring Backup and Import). Therefore, exercise caution when performing this operation.

6.10 Performing Upgrade and Checking System Version

Caution

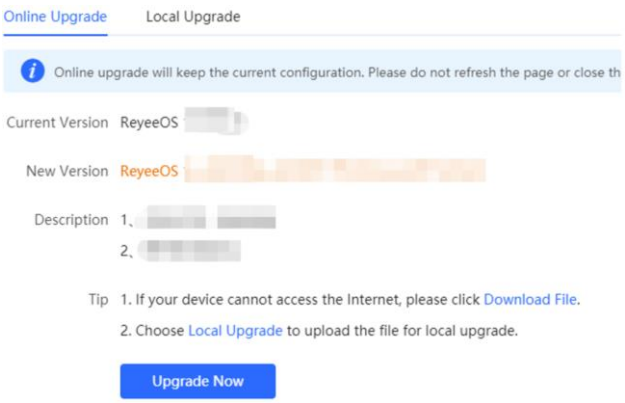
- You are advised to back up the configuration before upgrading the access point.
- After being upgraded, the access point will reboot. Therefore, exercise caution when performing this operation.

6.10.1 Online Upgrade

Go to the configuration page:

- Upgrade master device on the network: Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Upgrade** > **Online Upgrade**.
- Upgrade local device: Choose **One-Device** > **Config** > **System** > **Upgrade** > **Online Upgrade**.

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

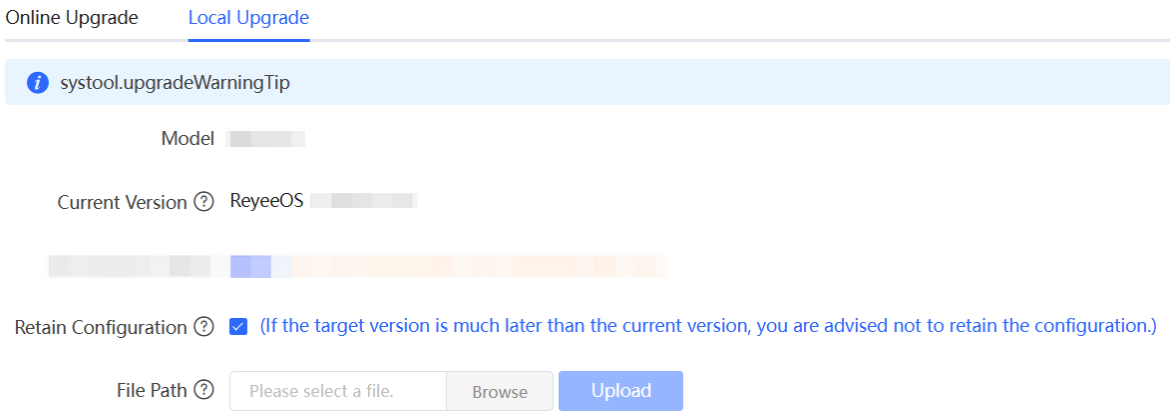


6.10.2 Local Upgrade

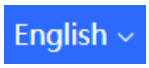
Go to the configuration page:

- Upgrade master device on the network: Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Upgrade** > **Local Upgrade**.
- Upgrade local device: Choose **One-Device** > **Config** > **System** > **Upgrade** > **Local Upgrade**.

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

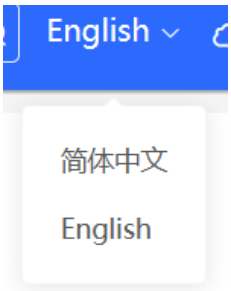


6.11 Switching System Language

Choose 

in the upper right corner of the Web page.

Click a required language to switch the system language.



6.12 Configuring LED Status Control

Caution

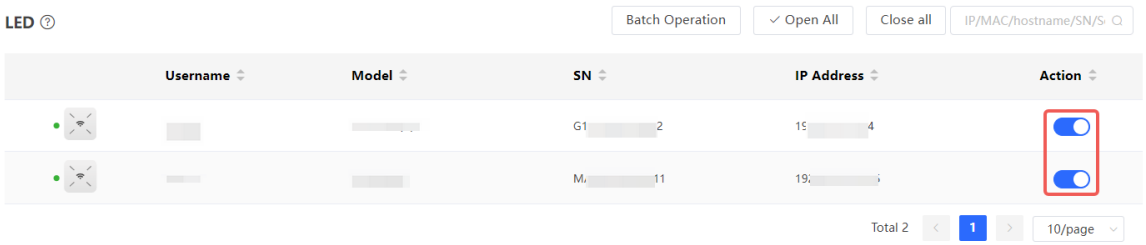
The LED Status Control function is not supported in the local device mode (self-organizing network is not enabled).

6.12.1 Configuring Standalone LED Status

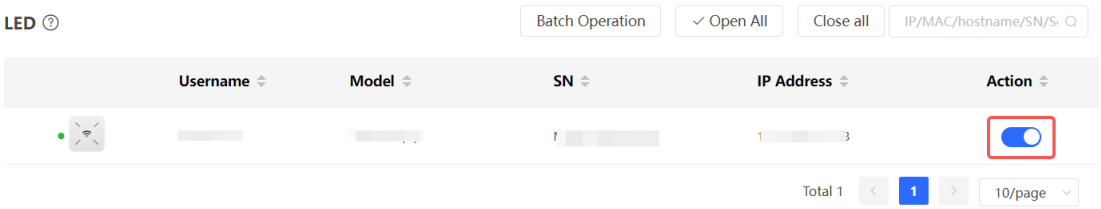
You can enable or disable the system LED status for individual wireless devices on the network.

Go to the configuration page:

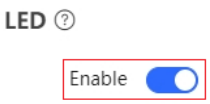
- Method 1: Choose **Network-Wide** > **Workspace** > **Wireless** > **LED**.



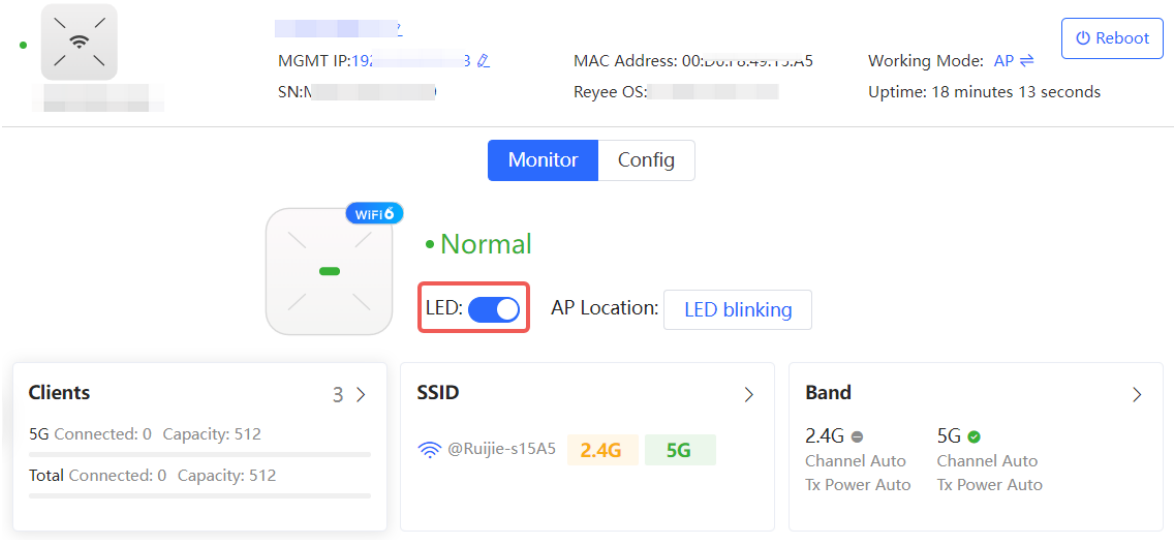
- Method 2: Choose **One-Device** > **Config** > **Network** > **LED**.
  - When the AP is the master device:



  - When the AP is a slave device.



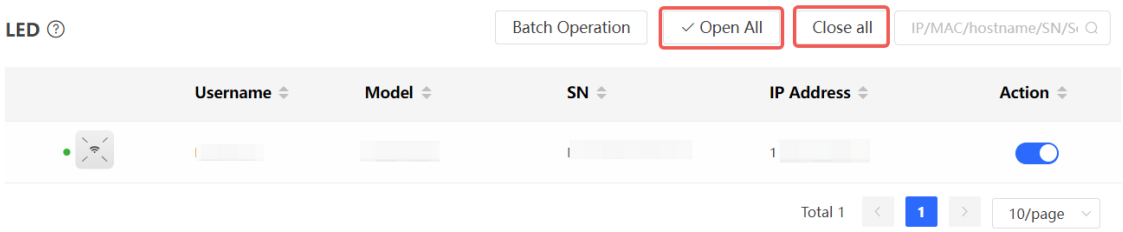
- Method 3: Choose **One-Device** > **Monitor** > **LED**.



6.12.2 Configuring Network-wide LED Status

Choose **Network-Wide** > **Workspace** > **Wireless** > **LED**.

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



6.13 Configuring Cloud Service

6.13.1 Overview

The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

By configuring Cloud Service, you can conveniently mange networks through Ruijie Cloud or the Ruijie Reyee app.

6.13.2 Configuration Steps

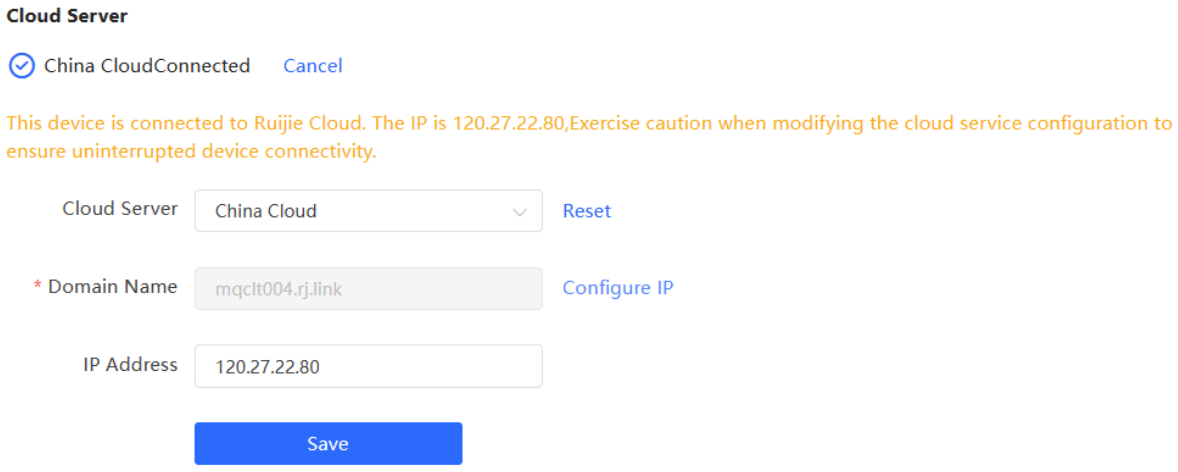
Choose **One-Device** > **Config** > **System** > **Cloud Service**.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Ruijie Reyee app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.

Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.



To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, enter the domain name and IP address, and click **Save**.

Note

If the server selected is not **Other Cloud**, the system automatically fills in the domain name and IP address of the cloud server. When **Other Cloud** is selected, you need to manually configure the domain name and IP address and upload the cloud server certificate.

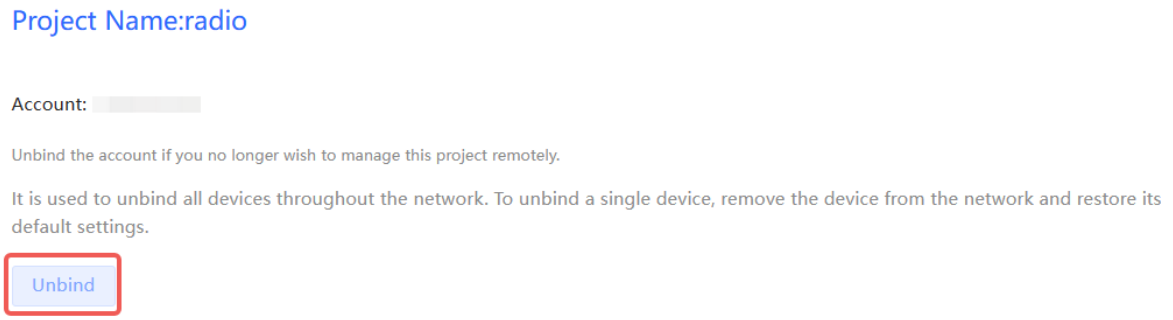
Table 6-12 Cloud Server Description

Parameter	Description
Cloud Server	Geographic location of the cloud server, including China Cloud, Asia Cloud, Europe Cloud, America Cloud, and Other.
Domain Name	Domain name of the cloud server.
IP Address	IP address of the cloud server.

6.13.3 Unbinding Cloud Service

Choose **One-Device** > **Config** > **System** > **Cloud Service**

You can click **Unbind** to unbind the account if you no longer wish to manage this project remotely.



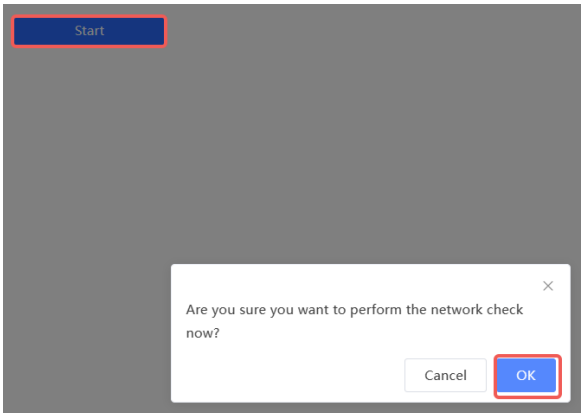
7 Network Diagnosis Tools

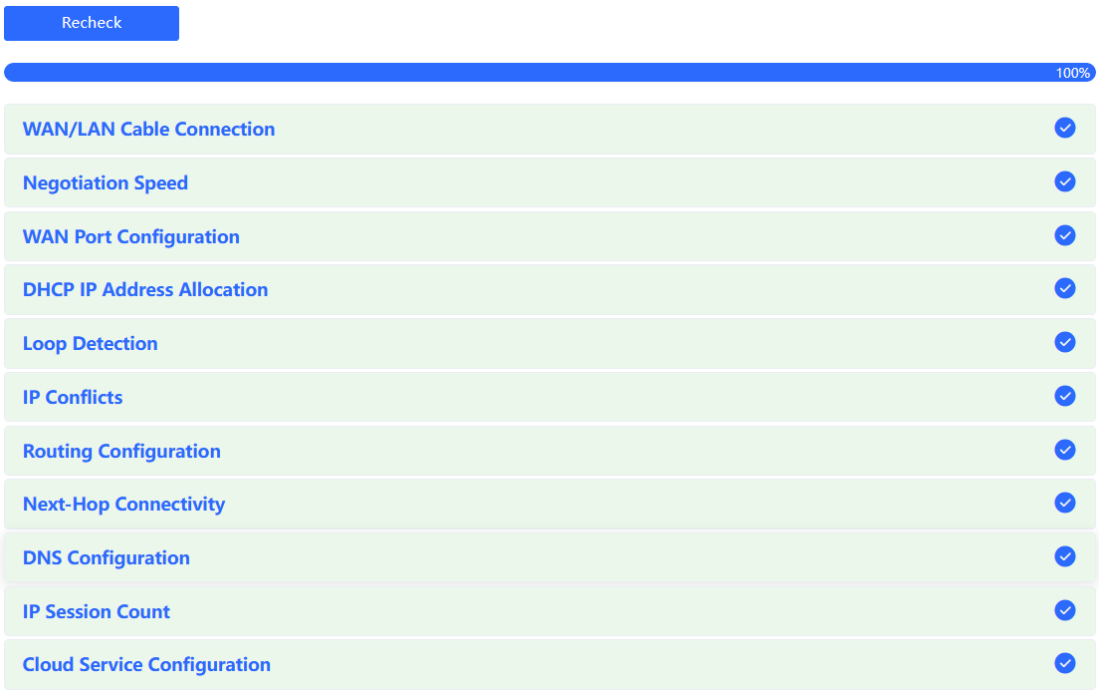
7.1 Network Check

When a network problem occurs on the device, perform a network check and configure the device based on the detection result.

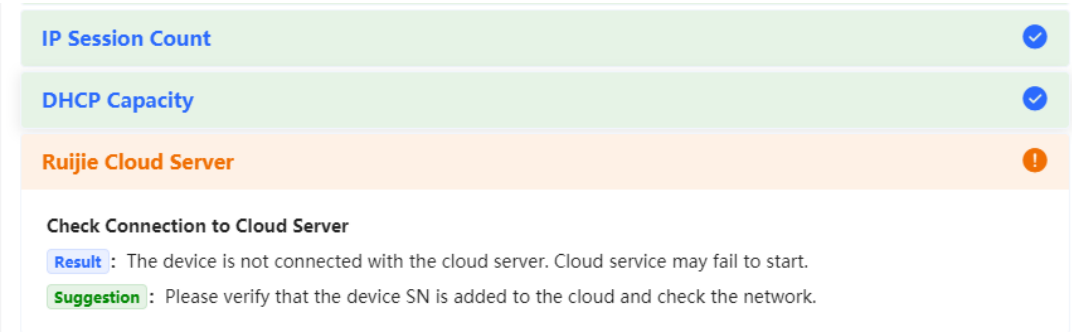
Go to the configuration page: Choose **One-Device** > **Config** > **Diagnostics** > **Diagnose**.

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





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

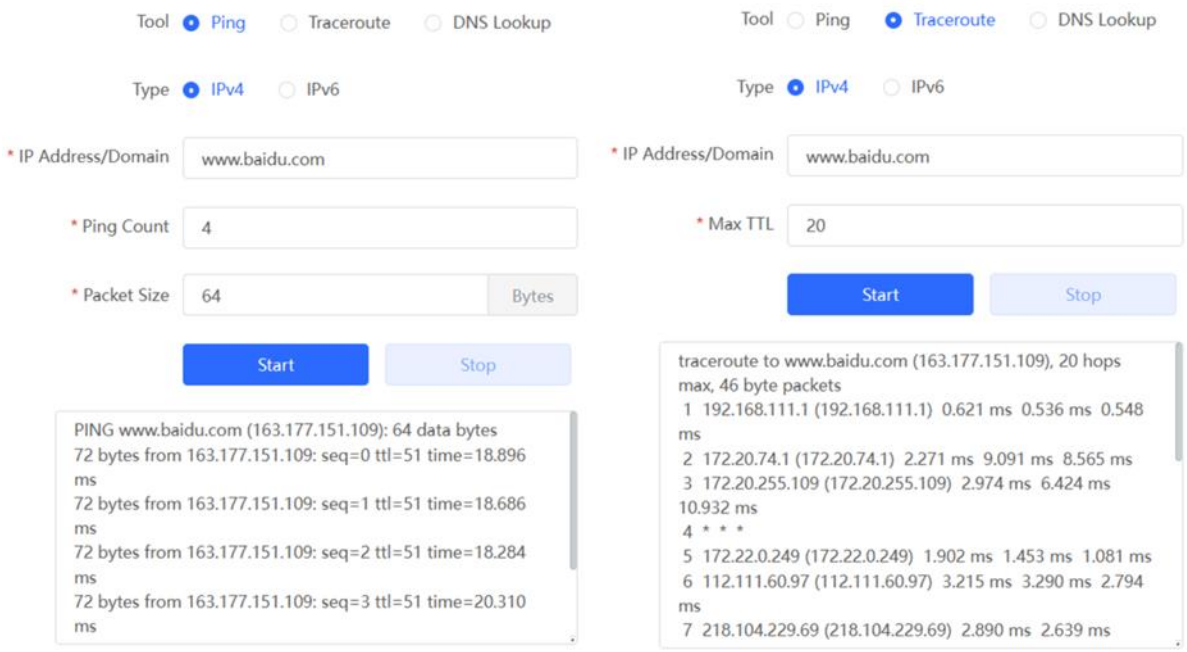


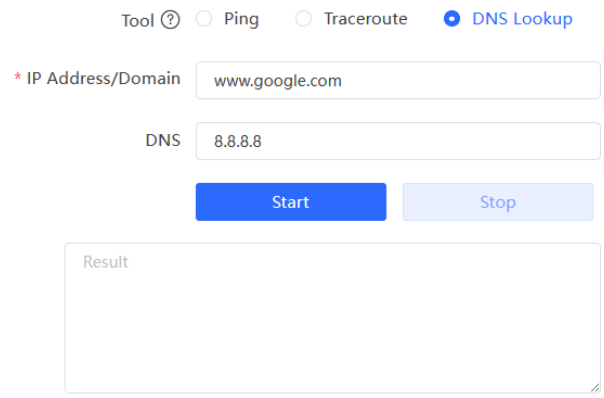
7.2 Network Tools

Choose **One-Device** > **Config** > **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.





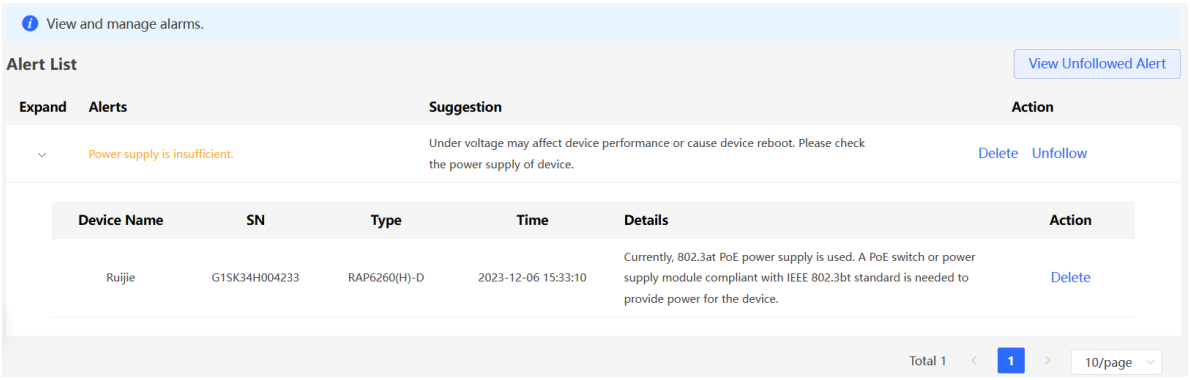
7.3 Alerts

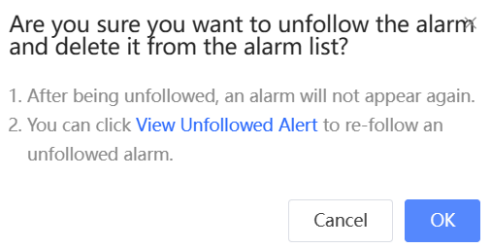
When a network exception occurs, the network overview page will display an alert and provide a suggestion. Click an alert in the **Alert Center** to view the faulty device, problem details, and description. You can troubleshoot the fault based on the suggestion.

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 this type of alarm.

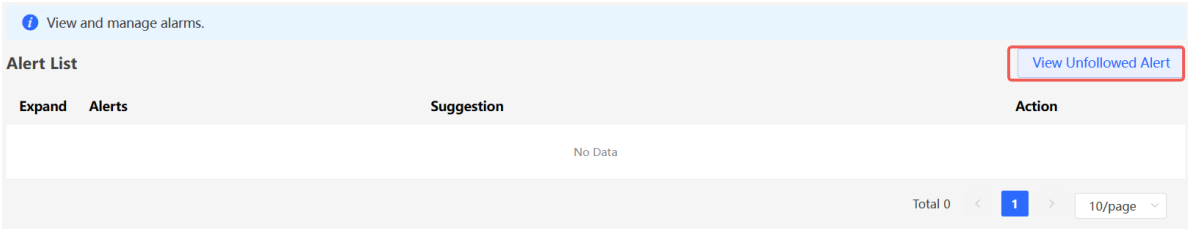
Caution

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





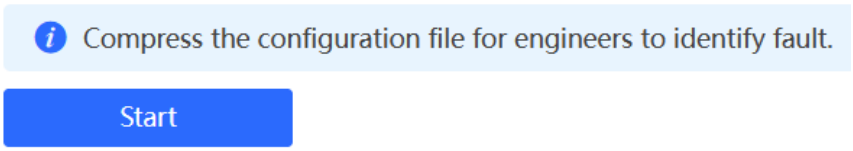
Click **View Unfollowed Alert** to view the unfollowed alert. You can follow the alert again in the pop-up window.



7.4 Fault Collection

Choose **One-Device** > **Config** > **Diagnostics** > **Fault Collection**.

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



7.5 Packet Capturing

Choose **One-Device** > **Config** > **Diagnostics** > **Packet Collection**.

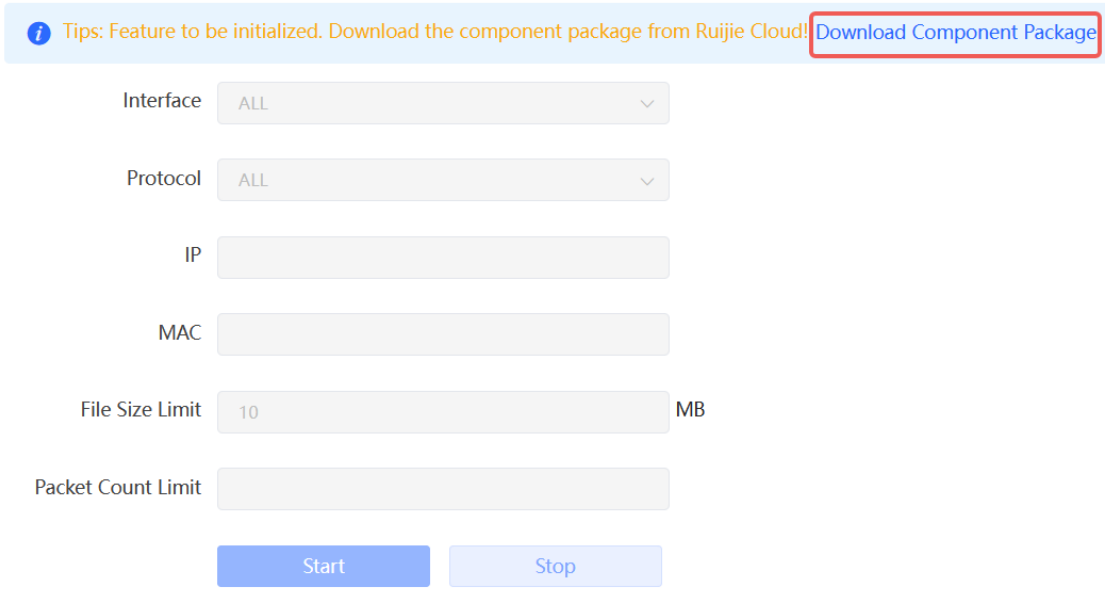
If the device fails and troubleshooting is required, the packet capture result can be analyzed to locate and rectify the fault.

Select an interface and a protocol and specify the host IP address to capture the content in data packets. Select the file size limit and packet count limit to determine the conditions for automatically stopping packet capture. (If the file size or number of packets reaches the specified threshold, packet capture stops and a diagnostic package download link is generated.)

Caution

The packet capture operation may occupy excessive system resources, causing network freezing. Therefore, exercise caution when performing this operation.

If you have not installed the packet capture component, you need to download it from the cloud by clicking **Download Component Package**.



The downloaded component package takes effect automatically. Click **Start** to execute the packet capture command.

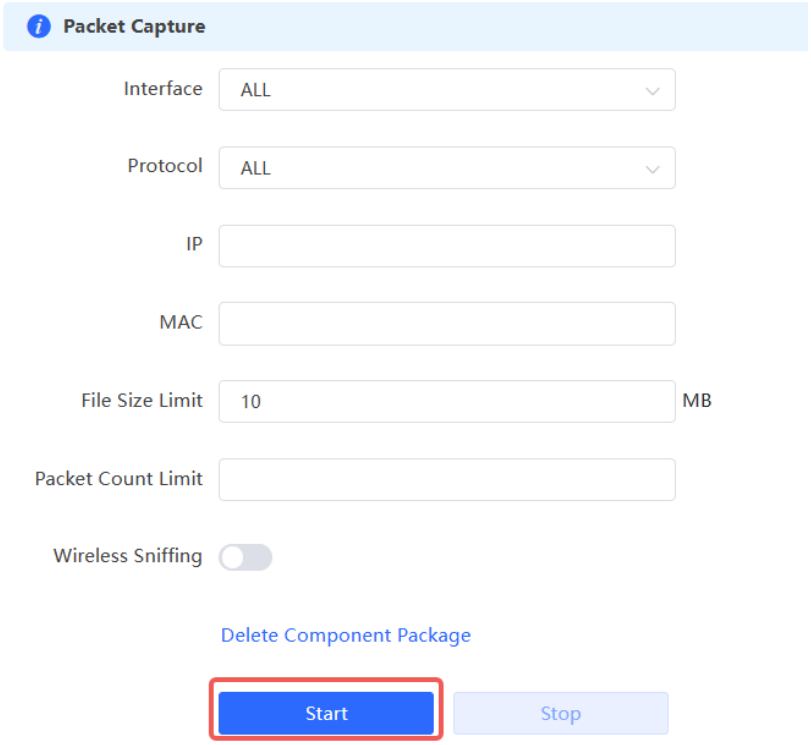
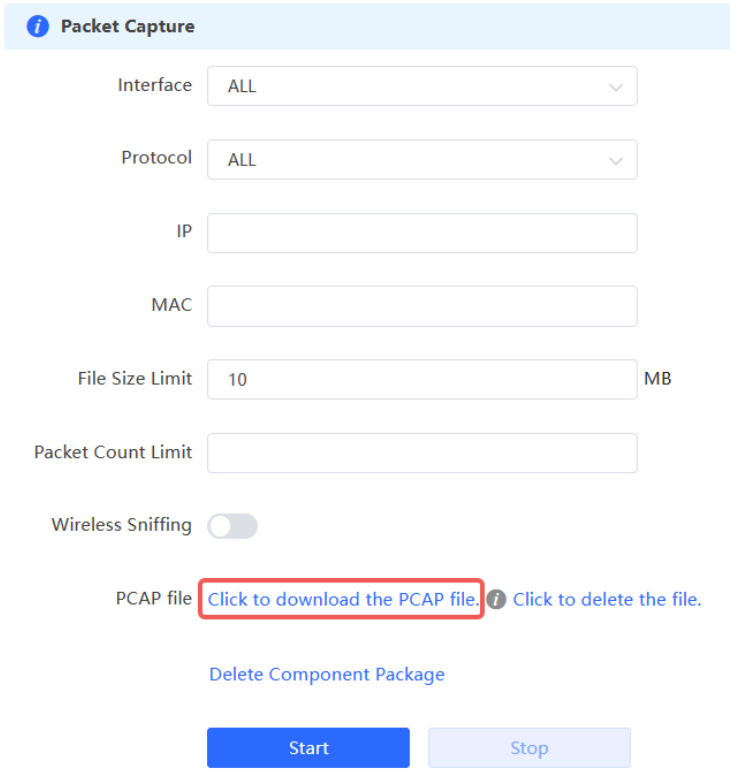


Table 7-1 Packet Collection Configuration Parameters

Parameter	Description
Interface	Physical or logical interface on the network
Protocol	Protocol used by the packet
IP	IP address of the device
MAC	MAC address of the device
File Size Limit	The maximum amount of data allowed to be stored within a certain time period. If this limit is reached during packet capture, new packet capture will be stopped, or excess packets will be discarded. The maximum limit is 10 MB.
Packet Count Limit	The number of packets stored and analyzed during packet capture. The maximum limit is 1500. **Caution** You can configure either the packet count limit or the file size limit, as they are mutually exclusive parameters.
Wireless Sniffing	You can select a wireless interface for packet capture only after enabling this function. After this function is enabled, the interface will be marked as Down, and the Wi-Fi network will be unavailable. To prevent users from forgetting to disable this function and causing the Wi-Fi network to be unusable, the system will automatically disable this function 10 minutes later after it is enabled.

Packet capture can be stopped at any time. After that, a download link is generated. Click this link to save the packet capture result in the PCAP format locally. Use analysis software such as Wireshark to view and analyze the result.



Caution

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.

8 FAQs

8.1 Login Failure

➢ **What can I do when I failed to log in to the web interface?**

Perform the following steps:

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

(1) 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.

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

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

8.2 Factory Setting Restoration

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

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

8.3 Password Loss

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

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